ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ЖОҒАРЫ ОҚУ ОРЫНДАРЫНЫҢ ҚАУЫМДАСТЫҒЫ

З. Б. ТУКУБАЕВ

ҚОЛДАНБАЛЫ АҚПАРАТТАР ТЕОРИЯСЫ

Оқулық

Алматы, 2012

УДК
ББК
Т

Қ.А. Ясауи атындағы ХҚТУ ОӘК нің ұйғарымымен баспаға ұсынылған (хаттама № 5, 2011 ж.).

Пікір жазғандар:
Физика-математика ғылымдарының докторы, профессор **Б. Турметов;**
Техника ғылымының докторы, профессор **О. З. Сембиев;**
Педагогика ғылымының докторы, профессор **Б. Д. Сыдықов.**

Тукубаев З. Б.
Т **Қолданбалы ақпараттар теориясы:** Оқулық. - Алматы, 2012. – 432 бет.

Оқулық ақпараттардың философиялық тұжырымдамасынан басталған; экосфераның техносферамен (инфосферамен) байланысы көрсетілген.

Ақпараттар теориясы Шеннонның және Хартлидің синтаксикалық теориясы негізінде қаралған; сигналдар мен оқиғалардың энтропиясын өлшеу, дискретті, үздіксіз сигналдардың ақпарат сыймдылығын арттыру әдістері және олардың сигнал мен кодтарды тиімділеуде қолданылуы көрсетілген. Мұрағаттауда қолданылатын Шеннон-Фано, Хаффмен кодтарын, берілгендер қорында және ішкі желілерде қолданылатын Хэмминг кодтарын, ауқымды желілерде қолданылатын циклдік кодтарды құру әдістері де қамтылған. Қателік түйіншегін табушы және түзетуші циклдік кодтар қатарында Боуз-Чоудхури-Хоквингем, Рид-Соломон, Рид-Маллер, Файр кодтары да қарастырылған.

Котельниковтің теориясының негізінде хабар көзі мен байланыс арнасын тиімділеу мәселелері қаралған. Өзара байланысты оқиғалар мен сигналдардың энтропиясы арқылы олар туралы толық ақпаратты есептеу және оларды болжауда Байес бағдаржолы (алгоритмі) берілген.

Ақпараттарды желіде қорғаудың осы кезде қолданылатын криптографиялық бағдаржолдары , электронды қолтаңба жасау бағдаржолдары да қарастырылған.

Оқулық жоғары оқу орындарындағы “Информатика”, “Ақпараттық жүйелер”, “Автоматтандыру және басқару”, “Есептеу техникасы және бағдарламамен қамтамасыз ету” мамандықтарының студенттеріне, ғылыми қызметшілер мен оқытушыларға арналған.

УДК
ББК

ISBN

Мазмұны

АЛҒЫ СӨЗ

Бұл кітаптың тарихы өткен ғасырдың алпысыншы жылдарынан басталған десек жаңылыс болмайды; студенттік жылдары автор ақпараттар теориясын алғаш рет оқып, сигналдар, кедергілер, ақпараттық арналар мен жүйелерді компьютерде үлгілеумен айналысты; диплом тақырыбы үштік негіздегі ақпаратты жеткізу жүйелерін компьютерде үлгілеу және оның нәтижелілігін зерттеу мәселесіне арналған еді. Сол кезде жаңа болған математикалық есептеу құрылғылары мен аспаптары мамандығын үздік дипломмен бітіріп, Кеңес Одағының Ғылымдар Академиясының Кибернетика Институтының күндізгі аспирантурасына жолдама алды. Сол Институттың Ақпараттар теориясы бөлімнің жетекшісі профессор Валиев Т. А. Қызылбайрақты байланыс Академиясын (Москва қ.) бітірген Ұлы Отан Соғысының Ардагері болатын.

Сол кезде Кеңес Одағында халық шаруашылығын басқарудың автоматтандырылған бірыңғай жүйесін құру үшін Одақтың Республикаларының жоспарлау орталықтарындағы компьютерлерді Москва қаласындағы Бас компьютермен байланыстыру және ауқымды желі құру мәселесі қойылды; бұған ұқсастық шет елдерде болған емес еді. Автор осы желінің бірнеше бағытын құруда қатысты. Сол кезде БЭСМ-6 сияқты өте күшті компьютерлер болғанымен санды компьютерлік желілер құрудың халықаралық протоколдары құрылмаған болатын; сондықтан желі құрушылар тек ғылыми білімдеріне сүйене отырып, сол ауқымды желілерді ғылыми тәжрибе ретінде құрды.

Автордың кандидаттық диссертациясының тақырыбы таржолақты (телефон) арналармен дискрет сигналдарды жіберуде жүйенің кедергіге шыдамдылығын және нәтижелілігін арттыруда сигналдарды тиімділеу мәселесіне арналған болатын. Бұл мәселені шешуде ақпараттар теориясының орны бөлек болды.

Диссертация қорғағаннан кейін автор қорғаныс саласындағы тақырыпқа көшті; мұнда ол алыстағы жылжымалы нысандарды басқару үшін арнайы автоматтандырылған радиожелілерін құру мәселесімен айналысты; мұнда қасақана қолдан жаратылған кедергілермен күресудің нәтижелі әдістерін іздестіру үшін арналарды, сигналдар мен күрделі түрдегі кедергілерді компьютерде үлгілеу және жүйенің нәтижелілігін зерттеу мәселесі негізгі болды.

Сол жылдары ғылыми-зерттеу жұмыстарын үздік орындағаны үшін авторға “Еңбек Ардагері” атағы да берілді.

Автор 180 нен астам ғылыми мақалалар мен әдістемелік құралдар, оқулықтар, 2 монография жазған. Жоғары оқу орындарында негізінен “Қолданбалы ақпараттар теориясы”, “Компьютер жүйелерінде ақпараттарды қорғау”, “Криптология”, “Есептеу желілері және телекоммуникациялар”, “Компьютер желілері”, “Басқару нысандарын үлгілеу және теңдестіру”, “Автоматика және телемеханика”, “Автоматтар теориясы және трансляторлар”, “Санақтық шешім қабылдау теориясы” және т.б. пәндерден сабақ берді.

КІРІСПЕ

Пән туралы қысқаша сипаттама: Қазіргі күнде Қазақстан "Электронды Үкімет" құрудың жаңа сатысына көшті; "Бір терезеден қызмет көрсету", азаматтар үшін "Біріздендірілген теңдестіру жүйесін" құру, кедендік жүйелерді, банк жүйелерін біріздендіру, оқу-білім, ғылым, медицина, өндіріс және т.б. салаларын заманға сай толық автоматтандыруда ақпараттық технология толық қолданылады. Алайда ескі ақпараттық технология аталған жұмыстарды толық орындауда заман талаптарына жауап бере алмайды; ақпараттың қауіпсіздігі, құжат айналамының жылдамдығы, ақпараттың әртүрлілігі және үлкен көлемі және т.б. Бұл жүйелер ақпараттар теориясы негізінде құрылған. Сондықтан да бұл теорияны үйретететін пән мамандықтардың арнайы пәндерінің қатарына кіреді.

"Ақпараттар теориясы" Шеннонның және Хартлидің синтактикалық теориясы негізінде құрылған болып, хабаларды арналармен ұзату кезінде, берілгендер негізінде сақтап қою уақытында хабарлардың кедегілер әсерінен бұзылуы, қасақана жаратылған кедергілерден сақтау және құпия ақпараттарды ұрлаудан қорғау сияқты мәселелерді шешуде бұл теория кең қолданылады; мұнда кедергілерден сақтау үшін кедергілерге шыдамды артықшылығы бар кодтар (қателіктерді анықтаушы және түзетуші кодтар) қолданылса, ал құпиялықты сақтау үшін криптографиялық кодтар (шифрлер) қолданылады; мұрағаттауда ақпараттарды сығымдап көлемін кішірейту үшін санақтық және арифметикалық кодтар кең қолданылады.

Қазіргі кезде "Электронды Үкімет" құрылу кезінде құжаттарды сенімді сақтау үшін электронды қолтаңба кең қолданыла бастады; мұнда электронды қолтаңба жарату әдістерінде де ақпараттар теориясы кең қолданылады.

Банк жүйесінде ақшалардың ағыны осы күнде толық автоматтандырылған болып, ақша айналымы құпия ақпарат айналымымен орын ауысқан. Бұл өте сенімді және ұтымды болып отыр.

Академик Харкевич А. А. және басқа ғалымдардың құндылықты (прагматикалық) теориясы зияткерлік немесе сарапшы (экспертті) жүйелер жаратуда кең қолданылады.

Бағдарламада Шеннонның “Ақпараттар теориясымен” бірге Котельниковтің потенциалды кедергіге шыдамдылық теориясы да берілген. Бұл теория ақпараттық сандық жүйелер құрылысында кең қолданылады.

Табиғи және қолдан қасақана жасалған кедергілермен күресуде, мұрағаттауда және ақпараттарды құпия сақтауда, құпия жіберуде, электрондық қолтаңба жаратуда да осы теориялар кең қолданылады.

Шеннонның “Ақпараттар теориясында” ақпараттың көлемдік өлшемі ретінде “энтропия” алынған болып, жай қарапайым оқиғалар энтропиясы, күрделі оқиғалар энтропиясы, шартты және орташа энтропия, олардың қасиеттері “информацияның” көлемін өлшеу үшін қолданылған. Осы теория негізінде қалыпты және тиімді ақпараттық жүйелер, нәтижелі кодтар құрылған.

Мұрағаттауда қолданылатын Хаффмен, Шеннон-Фано кодтары берілгендер негізінде, ішкі желілерде қолданылатын Хэмминг кодтары, ауқымды желілерде қолданылатын циклдік кодтар да бағдарламада қамтылған.

Қорғаныс техникасында қолданылатын ақпаратты алыстағы нысандарға сенімді жеткізу, өте нашар сигналдарды қабылдау үшін қолданылатын каскадты кодтау бағдаржолдары (Боуз-Чоудхури-Хоквигем, Рид-Маллер, Рид-Соломон кодтары) да бағдарламада берілген.

Пәннің мақсаты: Сандық ақпараттық (информациялық) технология өмірдің барлық салаларына күннен-күнге кең таралып, қолданылып келеді: медицина, оқу-ағарту, экономика, ғылыми жұмыстар, әлеуметтік қорғану, әскери және мемлекеттік қауіпсіздік, тұрмыстық және басқа көптеген жұмыстар сандық технология жәрдемісіз шешілмейді.

Өткен ғасырдың 70-жылдардың ақырында дербес компьютерлер өмірде кең қолданыла бастаған болса, ал 80-жылдарға келгенде жергілікті желілер құрылып, олар компьютер кластарында оншақты адамды нақты уақытта басқаруға мүмкіндік берді. Ал ол желілерді телефон арналармен бірнеше километрдегі басқа желіге қосу кең ауқымды сандық желілер құру және өте кең ауқымдағы техникалық жүйелерді нақты уақытта басқаруға мүмкіндік берді.

Оптикалық және сол сияқты жылдам арналардың пайда болуы ақпараттық сандық техниканың мүмкіншіліктерін шексіз арттырды.

Қазақстанда ақпараттық технологияны дамыту үшін техно-

парктер құрылған болып, сол технологияның техникалық және бағдарламалық жабдығын жаратуға толық мүмкіндік жаратылған.

Сондықтан қазіргі уақытта аталған мамандықтар бойынша теориялық білімі мықты ғылыми конструкторлық жұмыстарға мамандар өте қажет.

Пәнді оқып болғаннан соң студенттер ақпараттық технология жаратын технопарктерде істейтін және техника немесе бағдарлама жабдығын жасай алатын маман болып шығуы керек.

Пәннің міндеттері:

Компьютерлік желілер мен жүйелерде қолданылатын ақпаратты кодтау және декодтау әдістерін, олардың қай жерде және қай құрылымда орындалуын, желілерде қолданылатын кодтардың құрылысы мен істеу қағидаларын анық білуі керек.

Табиғи кедергілер көп болған жағдайларда ақпаратты табиғи кедергілерден пайда болатын қателіктерден қорғау әдістерінің теориялық негіздерін де білуі керек.

Ал көп жағдайда ақпарат ұрлануы немесе қасақана бұзылуы да мүмкін. Мұндай жағдайларда ақпаратты жасыру және қалпына келтірудің де теориялық негіздерін анық білу керек.

Ақпараттарды сақтауда немесе арнамен жіберуде ақпаратты сығымдау және қысқарту әдістері мен олардың теориялық негіздерін білуі керек.

Қысқасы, осы күнде қолданылып келе жатқан ақпараттық технологиядағы ақпараттарды өңдеу, сақтау және жіберу үдерісіндегі туындайтын аталған мәселелерді шешудің теориялық негіздерін толық меңгерген болуы керек.

Пререквизиттер: Пәнді үйренуге қажетті пәндер:

1. ықтималдар теориясы;
2. математикалық статистика;
3. стохастикалық үдерістер теориясы;
4. өрістер теориясы;
5. жиындар теориясы;
6. матрицалар теориясы;
7. дискретті математика және т.б. пәндерге сүйенеді.

Постреквизиттер: Оқытылатын пәннің білімі қолданылатын пәндер:

1. Техникалық, медициналық және т.б. диагностика және болжау.

2. Компьютер жүйелері мен желілерде ақпаратты қорғау.
3. Компьютер желілері.
4. Күрделі жүйелерді жобалауды автоматтандыру – САПР.
5. Күрделі жүйелерді басқаруды автоматтандыру – АУСС.

2. ЖҰМЫС ОҚУ ЖОСПАРЫНАН КӨШІРМЕ

№	Семестрлер	Аудиториялық сабақтар				Аудиториядан тыс сабақтар
		Дәріс	Тәжр	Семинар	Зертханалық	СОӨЖ
1	5	15	15	-	15	45
	Барлығы	15	15	-	15	45

3. ПӘН САҒАТЫНЫҢ БӨЛІНУІ

№	Тараулар атауы, реті	Аудиториядан тыс сабақтар			
		Дәр	Тәж	Зерт	СОӨЖ
11	**Ақпараттар теориясы; ақпараттың философиялық тұжырымдамасы, өлшемдері, түрлері.** Шеннонның ақпараттар теориясы; энтропия және оның қасиеттері. Тең ықтималды оқиғалар жүйесінде энтропия өлшемі. Информацияның аддитивтік немесе логарифмдік өлшемі. Хартли теңдеуі.	1	1	1	3
22	**Оқиғалар ансамблінің энтропиясы;** Әр түрлі ықтималды оқиғалар жүйесінде энтропияны өлшеу; Шеннон теңдеуі; шартсыз, шартты және өзара байланысты оқиғалар энтропиясы. Энтропияны қосу ережесі және информацияның көлемін өлшеу. Тәуелді және тәуелсіз оқиғалар энтропиясы.	1	1	1	3
33	**Тәуелді оқиғалардағы өзара алмасу ақпараты;** толық ықтималдық; Байес теңдеуімен тәуелді оқиғаларды болжамдау. Толық информацияның қасиеттері.	1	1	1	3

44	**Кездейсоқ шаманың эпсилон-энтропиясы;** Үздіксіз хабар көзінің дифференциалдық энтропиясы; қасиеттері. Кездейсоқ шаманың эпсилон-энтропиясы. **Ақпараттың мағыналық түрі;** мазмұндылық, маңыздылық, мақсатқа сайкес келетіндігі, тезаурус.	1	1	1	3
55	**Энтропия қасиеттерін ақпаратты сығымдауда қолдану;** нәтижелі (эффектив) кодтар; Нәтижелі кодтардың префикстік талабы; Шеннон-Фано кодтары. Қарапайым кодтар. Шеннон-Фано және Хаффмен кодтарын құру қағидалары.	1	1	1	3
66	**Сигналдар мен үдерістердің үлгілері.** Сигнал түсінігі, үлгілері. Детерминделген сигналдар; қуатының спектрлік тығыздығы; автокорреляциялық теңдеуі.	1	1	1	3
77	**Сигналдар мен үдерістердің үлгілері.** Стохастикалық үдеріс сигналдың үлгісі түрінде; Тұрақты және эргодикалық үдерістер; олардың спектрлік және жиіліктік сипаттамалары.	1	1	1	3
88	**Дискреттеу және кванттау**; олардың сандық жүйелерде қолданылуы; Кванттау шуылы; ақпаратты дискреттеу және қалпына келтіруде сапа шарттары. Бірқалапты дискреттеу. Котельников теоремасының амалдық маңызы.	1	1	1	3
99	**Дискреттеудің энтропиялық, экстраполяциялық әдістері.** Ең үлкен ауытқу бойынша дискреттеу; Тейлордың экстраполяциялық көпмүшелігі; бейімделуші дискреттеу. Үздіксіз хабарлардың энтропиясы және оның максимумын табу.	1	1	1	3
110	**Дискрет хабар көзінің ақпараттық сипаттамалары; үлгілері, өнімділігі, артықшылық;** сигналдар мен хабарлардың артықшылығын есептеу. Сигналдарды энтропия бойынша оңтайландыру. Қысқарту еселіктері. Үздіксіз хабарлардың энтропиясы және оның максимумын табу. Сигналдар мен хабарлардың артықшылығын есептеу. Сигналдарды энтропия бойынша оңтайландыру.	1	1	1	3

111	**Үздіксіз хабар көзінің ақпараттық сипаттары; үлгілері**, **жіберу жылдамдығы.** Үздіксіз байланыс арнасының өткізу қабілеттілігі; сигнал көлемі мен байланыс арнасының сиымдылығы. Хабар көзі мен байланыс арнасын, арналар мен хабарларды санақтық келістіру; кедергілі байланыс арнаның өткізу қабілеті. Хабар және арна көлемдері. Котельников теоремасының қолданылуы.	1	1	1	3
12	**Бөгеуілсіз дискрет байланыс арнасы бойынша хабар жіберу кезіндегі ақпараттарды кодттау.** Бөгеуілсіз арна үшін Шеннонның кодтау туралы негізгі теоремасы; Үздіксіз-санды түрлендірушіде Грей, Уолш, Радемахер кодтарын қолдану. Криптографиялық ақпаратты жабу қағидалары.	1	1	1	3
113	**Бөгеуілді дискрет байланыс арнасы бойынша хабар жіберу кезіндегі ақпараттарды кодттау.** Бөгеуілді байланыс арна үшін Шеннонның кодтау туралы негізгі теоремасы; бөгеуілді кодтау; жиынтықты (блокты) кодтау; топтық түзетуші кодтардың жалпы қағидалары; сапа көрсеткіштері; сызықты кодтар; топтық екілік код құру. Топтық кодтарды мажоритарлық декодтау.	1	1	1	3
14	**Түзетуші топтық кодтар**; **Циклдік кодтар.** Хэмминг кодтары. Топтық кодттарды кодтау және декодтау. Циклдік кодтар. Құраушы көпмүшеліктер, оларға қойылатын талаптар; құраушы көпмүшелікті таңдау; әртүрлі тәртіпті қателіктерді табу және түзету	1	1	1	3
15	**Циклдік кодтарды құру әдістері; матрицалық жазылуы; мажоритарлық декодтау.** Қателікті анықтаушы циклдік кодтардың сандық желіде қолданылуы. Қателік түйіншек табушы және түзетуші циклдік кодтар; Боуз-Чоудхури-Хоккенгем, Рид-Соломон, Рид-Маллер кодтары;	1	1	1	3
	Барлық сағат саны:	15	15	15	45

4. АРАЛЫҚ БАҚЫЛАУ (МОДУЛЬ) СҰРАҚТАРЫ

(модуль сұрақтары тараулар соңында берілген сұрақтармен толықтырылады)

Шеннонның ақпараттар теориясы; энтропия және оның қасиеттері. Тең ықтималды оқиғалар жүйесінде энтропия өлшемі.

1. Ақпараттар теориясы; ақпараттың (информацияның) жіктелуі.

2. Информацияның аддитивтік немесе логарифмдік өлшемі. Хартли теңдеуі.

3. Энтропия және оның қасиеттері.

4. Энтропияны қосу ережесі және ақпараттың көлемін өлшеу.

5. Оқиғалар ансамблінің энтропиясы; әр түрлі ықтималды оқиғалар жүйесінде энтропияны өлшеу; Шеннонның ақпараттар теориясы; Шеннон теңдеуі.

6. Тәуелді оқиғалардағы өзара алмасу ақпараты; толық ықтималдық.

7. Тәуелді және тәуелсіз оқиғалар энтропиясы. Байес теңдеуі.

8. Байес теңдеуімен тәуелді оқиғаларды болжамдау. Толық информацияның қасиеттері.

9. Кездейсоқ шаманың эпсилон-энтропиясы;

10. Үздіксіз хабар көзінің дифференциалдық энтропиясы; қасиеттері.

11. Ақпараттың мағыналық түрі; мазмұндылық, маңыздылық, мақсатқа сайкес келетіндігі, тезаурус.

12. Энтропия қасиеттерін ақпаратты сығымдауда қолдану; нәтижелі кодтар.

13. Нәтижелі кодтардың префикстік талабы; Шеннон-Фано кодтары.

14. Қарапайым кодтар. Шеннон-Фано кодын құру қағидасы.

15. Хаффмен кодын құру қағидасы.

16. Энтропия қасиеттерін ақпаратты сығымдауда қолдану.

17. Үздіксіз хабарлардың энтропиясы және оның максимумын табу.

18. Сигналдар мен хабарлардың артықшылығын есептеу.

19. Сигналдарды энтропия бойынша оңтайландыру.

20. Кодтардың артықшылығын есептеу.

21. Кодтарды энтропия бойынша оңтайландыру, нәтижелі кодтар.

22. Потенциалдық кедергіге шыдамдылық теориясы.

23. Котельников теоремасы, дискреттеу қадамы.

24. Дискреттеудегі жоғалған “информацияны” энтропиямен өлшеу.

25. Бөгеуілсіз дискрет байланыс арнасы бойынша хабар жіберу кезіндегі ақпараттарды кодттау.

26. Бөгеуілсіз арна үшін Шеннонның кодтау туралы негізгі теоремасы.

27. Үздіксіз-санды түрлендірушіде Грей, Уолш, Радемахер кодтарын қолдану.

28. Криптографиялық ақпаратты жабу қағидалары.

29. Бөгеуілді дискрет байланыс арнасы бойынша хабар жіберу кезіндегі ақпараттарды кодттау.

30. Бөгеуілді байланыс арна үшін Шеннонның кодтау туралы негізгі теоремасы.

31. Бөгеуілді кодтау; жиынтықты кодтау;

32. Топтық түзетуші кодтардың жалпы қағидалары; сапа көрсеткіштері.

33. Сызықты кодтар; топтық екілік код құру.

34. Топтық кодтарды мажоритарлық декодтау.

35. Энтропия қасиеттерін информацияны қорғауда қолдану.

36. Гаммалау қағидалары.

37. Абсолют криптотұрақтылықтың Шеннон анықтамасы.

38. Ақпараттар теориясының ақпараттарды қорғауда қолданылуы.

39. Код қашықтығы мен потенциалдық кедергіге шыдамдылық.

40. Ақпараттар теориясының кедергілер мен қателіктермен күресуде қолдану.

41. Топтық түзетуші кодтар.

42. Хэмминг кодтары.

43. Циклдік кодтар.

44. Циклдік кодтарда құраушы полиномға қойылатын талаптар.

45. Қателік түйіншегін табушы және түзетуші циклдік кодтар; Боуз-Чоудхури-Хоккенгем, Рид-Соломон, Рид-Маллер кодтары.

Ақпараттар технологиясының қоғам дамуындағы орны; ақпарат пен кибернетика ғылымдарының философиялық тұжырымдамалары

Осы бөлімде ақпарат және Информатика пәніне философиялық көзқарастар тарихына талдау жасау және кибернетика ғылымдарының нәтижелерін жалпылау негізінде қазіргі замандық философиялық тұжырымдама ұсынылған.

Президент Н. Назарбаевтің 2005 ж. “Жолдауында” атқарушы органдардың жұмыстарын жақсарту, халыққа және мекемелерге қызмет көрсетуді жақсарту мәселелері көрілген болса, солардың ішінде “бір терезеден қызмет көрсету” жүйелерін құру мәселесі де қойылған еді [1].

Президенттің 2006 ж. “Жолдауында” [2] аймақтық IT -орталық ретінде ақпараттық технология паркін құру және дамыту қажеттілігі айтылған.

Алматы қаласында финанстық орталық құру үшін керекті болған ақпараттық инфрақұрылым құру қажеттілігі де көрсетілген. Осы “Жолдауда” “Электрондық үкімет” құруды жеделдету мәселесі де қаралған еді.

“2030” Түбегейлі жоспарлық бағдарламасының ең негізгі бөлімінің бірі оқу-білім салаларын толық компьютерлендіру болып, ауыл мектептері 2003 жылдың өзінде-ақ толық компьютерлендірілген болатын.

Қазіргі күнде Алматы қаласында Қазақстанда жаратылған көптеген ақпараттық технологияның құралдарышығарылып жатыр.

Аталғандардың барлығы да Қазақстанда ақпараттық инфрақұрылым жаратылып, әлемдік инфосферадан тыс қалмауына және дамыған елдер қатарына қосылуына толық мүмкіншілік жасайды.

2006 ж. Президент Назарбаевтың “Жолдауында” күшті дамыған бәсекеге шыдамды 50 елдің қатарына қосылу мәселелерінің бірі етіп, жастарға жаңаша экологиялық тәрбие беру мәселесі де қойылған болатын; сондықтан жаңаша экологиялық философия жарату керек болып, сол философияның қалыптасуына үлес қосу мақсатында осы бөлімде кейбір негізгі мәліметтер келтірілді.

2012 ж. Президент Назарбаев “Жолдауында” Қазақстанда Электрондық Үкімет құруды толық амалға асыру мәселесін негізгі мәселе етіп қойды.

Дамыған елдердің алдынғы қатарындағы АҚШ-та мемлекеттік бюджеттің 60% астамы ақпараттық технологияларды жаратуға жұмсалады [13].

Өткен ғасырдың 20 жылдарында белгия ғалымы П. Отле “документация” атымен құжаттарды жинақтау, сақтау, қайта өңдеу, жіберумен байланысты үдерістерді жалпылау үшін осы пәнді ендіруді ұсынды [3,392]. Бұл пән Кеңес Үкіметінде 1952 жылы “Информатика” атымен Ғылыми информация Институтында, кейін ғылым академиясының ВИНИИТИ де құрылып, онда негізі ғылыми ақпаратты жинақтау, өңдеу және тарату мәселелері қойылды.

Өткен ғасырдың 60 жылдарында Францияда “Информатика” атты пән пайда болса да, ол ғылыми пән болып қала берді.

Кеңес мемлекеттерінде 1983 жылдан бастап “Информатика және

есептеу техникасы" жалпы пән ретінде қабылданып, мектептерде сабақ өтіле бастады.

Алғашқы компьютерлер 50 жылдары пайда болса да өте қымбат және үлкен болғандығы себепті бастапқы кезде олар тек қана ғылыми есептеу орталықтарында, қорғаныста және халық шаруашылығын басқару жүйелерінде ғана қолданылып, қарапайым халыққа жетіп келмеді; оларды қолдану жалғыз адамның қолынан келмей, бір машинаның өзі жүздеген адамдарды қажет етті.

Бастапқы кезеңде бұл пән (жалпы кибернетика пәнінің бір бөлімі ретінде қазіргі күндегіден бүтіндей басқа мағынада қаралды) ақпаратарды компьютерде автоматты түрде өңдеуді кеңінен қолдану мәселесімен ғана шұғылданып, байланыс жүйелерінде тек қана ғарыштық нысандарды басқаруда ғана қолданылды.

Микроэлектрониканың дамуы, микрокомпьютерлер пайда болуы натижесінде 1995 жылдардан кейін "MicroSoft" фирмасы "Internet Explorer" бағдарламасын жаратып, ғаламдық байланыс желілеріне жеке компьютерлер қосылу мүмкіншілігін берді; сөйтіп интегралданған ақпараттық жүйелер, яғни Ғаламтор жаратылды.

Мұнда байланыс түйіндеріндегі серверлер өте күшті болса да, көлемі өте кішкене еді (алдыңғы компьютерлермен салыстырғанда).

Бұл жүйе басқа да ақпараттық жүйелердің жылдам дамуына алып келді; жылжымалы телефондар, сандық фото және кино жабдықтар алынған бейне суреттерін жылдам түрде өте алысқа жіберу, қабылдап алу және уақытынша сақтап тұру мүмкіншілігі туылды.

Сандық бейнетелефон, телетайп пен телефакстың жаңа түрі-SMS пен Internet agent т.с. сияқты байланыстың жаңа түрлері пайда болып, бейнеконференциялар да өмірде қолданыла бастады.

Сайлау жүйесінде, Ұлтық бірыңғай тестілеуде, халыққа "Бір терезеден қызмет көрсетуде", авиабилеттерді және темір жол билеттерін алдынала бұйыруда, салық, банк, білім беру және т.б. көптеген салаларда Ғаламтор арқылы жұмыс істейтін интегралданған автоматты байланыс жүйелері кең қолданыла бастады.

Жаратылыстану ғылымдарының тұжырымдамасынан мәлім - адамзат қоғамының ғылым және білімдерінің дәрежесі оны қоршаған материалдық дүниенің қасиеттерін өлшеу, алынған өлшемдерді есептеу (қайта өңдеу) арқылы қоршаған материалдық дүниені анық тану дәрежесімен өлшенеді [6].

Алынған өлшемдерді математикалық жабдықтар жәрдемінде анық есептеулер сол материалдық дүниені анық тану немесе түсінуге мүмкіндік берді. Мысалы; әлемге әйгілі Альберт Эйнштейн 1905 ж. арнайы салыстырмалы теорияны, 1916 ж. жалпы салыстырмалы теорияны жаратып, атам заманнан келе жатқан: "масса, уақыт, арақашықтық өзгермейді, яғни абсолют" деген ұғымдар кейбір жағдайда (біз көріп тұрған макродүниеде) ғана дұрыс сияқты, ал микроәлемде және өте үлкен жылдамдықтарда мүлде дұрыс еместігін ешқандай тәжерибесіз математикалық есептеулермен дәлелдеді.

Сол уақытта ғылымда "материалистік"[*1] көзқарастар ұстын болғандығы себепті бұл теория көп уақыт қабылданбай келіп, 1950 жылдары синхрофазотрон, циклотрондар (микроэлементтерді жылдамдатқыштар) пайда болған соң ғана тәжрибетермен толық дәлелденіп, өмірде кең қолданыла бастады.

*1 – *сол кездегі материалистік көзқарас.*

1900 ж. квант теориясы пайда болып, кванттық механиканы Л.Бройл, Гейзенберг, Шредингер, Бор сияқты ғалымдар жаратқан болса, ал 1928 ж. Дирак релятивистік квант механикасын жаратты.

1897-1932 жылдары атом құрамы толық зерттеліп, электрон, протон, нейтрондар табылды. 1932-64 жылдары субатомдық элементар бөлшектер (нейтрино) табылды.

1964 ж. "Ұлы әсерлесу" теориясы жаратылып, адрондар, кварктар ашылды; электромагниттік, гравитациялық өрістердің құрылысы толық анықталып, әлемнің құрылысы айқындалғандай болды.

Бірақта бұлардың барлығы әлемнің сырлары толық ашылды деген сөз емес еді; оның сырлары шексіз көп болып қала берді.

Сонда қалай, ғасырлар бойы ғылымда қалыптасып кеткен ұғымдарды бекер етіп, құрылғы-аспаптар жәрдемінде анықтап болмайтын нәрселерді қалай дәлелдеу мүмкін деген сұрақ туады. Әрине, Эйнштейннің бұл теориялары оңайлықпен дүниеге келмеген. Дәл осындай жағдай кибернетиканың бастапқы кезеңдерінде де болып өтті.

XX ғасырдың 80-жылдарында американдық математик А.Д.Урсул да жаңа ғылымды түсіне қойған жоқ; ол былай деген:

"Кибернетика пәні – ғылыми білімдердің біртұтастығына жеткізетін әмбебаб негіз (база) бола алмайды; демек, философияны жарата (немесе өзгерте) алмайды" [6,317].

Атақты Галилео Галилей былай деген: “Менің ұғымымда, табиғаттың философиясы – ұлы кітапта жазылған. ... Бұл кітап математика тілінде жазылған; ал жазбасы – үшбұрыштар, дөңгелектер және т.б. денелер...”.

Ол денелерді **абсолютті ұғымдар** деп қараған болса, осы кезде де көптеген математиктер де математикалық формулаларды ***абсолютті*** деп қарайды!!!

Сөздің мәні қоршаған материалдық дүниені танудың жалғыз философиясы математикалық үлгілеу болды. Бұл түсінік осы заманға да жетіп келген болса, кибернетиканың дамуы оны біршама өзгертті.

Термодинамика теориясын жаратушы ғалымдар өткен ғасырда математикалық теңдеулер мен геометриялық денелердің де ***абсолютті еместігін*** анықтаған болса, бұл салыстырмалы теорияны одан біршама алдын орыс ғалымы Лобачевский Н. И. ашқан болатын.

Ол Евклидтің жаратқан геометриясын (натуралдық философия) керісін жаратып, **геометриялық денелер де абсолютті еместігін** дәлелдеген.

Бұл теорияны одан ары дамытқан Эйнштейн, Максвелл, Бор сияқты ғалымдар салыстырмалы теорияны геометриялық өлшемдерден уақыт, масса өлшемдеріне жалпылады.

Ғылымдардың дамуында - ғалымдар қоршаған ортадан алынған **ақпараттар** негізінде материалдық дүниедегі нысандар мен олардың қасиеттерінің үлгілерін немесе бейнелерін жарата отырып, қоршаған ортаны үйренді; білімдер базасы немесе ғылымдар жаратылды.

Ғылымның дамуына байланысты бұл білімдер, үлгілер толықтырылып, кей жағдайларда өзгертіліп отырылды.

Ең алғашқы үлгілер сандар мен математикалық теңдеулар, әр түрлі (сызықтық, интегралдық, дифференциалдық және т.б.) теңдеулер қолданылса, ал кейіншелік кездейсоқ сандар, үдерістер және тізбелерді зерттеу үшін таралу заңдары, корреляциялық және спектралдық қатыстар немесе матрицалар т.б. түрдегі үлгілер қолданылды.

Компьютер технологиясының дамуымен “ойындық мәселелерді” шешу үшін әртүрлі стохастикалық немесе еліктеушілік (имитациялық) үлгілер құрылды;

экспертті немесе зияткерлік жүйелер жаратылды. Мысалы үшін, автор еңбектерінде Марковті және Марковті болмаған,

тұрақты болмаған үдерістердің еліктеушілік үлгілерін құрып, олардың анықтық дәрежесін (адекваттық) қателіктің қуатымен емес, жоғалтқан сигнал **энтропиясымен** өлшеуді ұсынды [70].

Ақпарат туралы түсінік әр заманда әртүрлі болып келді; Массачусетс технология институтының физигі Сет ЛЛоид бүтін жұлдыздық әлемді гигант компьютермен салыстырып, ал элементар бөлшектердің бір кванттық жағдайдан басқа жағдайға өтуін компьютердегі жадтың 1 ден 0 ге өтуімен салыстырып көрсетеді [6,314].

Сонда компьютердегі ақпарат ағынын элементар бөлшектер әрекетімен салыстыра отырып, компьютер жылдамдығын немесе қуатын сол физикалық жүйенің жалпы энергиясына теңестіреді. Мұндағы философиялық көзқарас - ақпарат тек қана адамзат, жанжануар, өсімдіктерге ғана тән емес, жалпы материалдық дүниеге тән қасиет деп қаралады; мұнда ол биологиялық **тірі дүниенің ерекшеліктерін (өзгешеліктерін) аңғармайды.**

Осы сияқты "қиялшылық" көзқараста бұдан бірнеше мың жыл бұрын грек философы атақты математик Пифагор келесідей көзқараста болды [26,55-64]; "...әлемді сандар билейді..." деген сөздердің мағынасы табиғаттағы барлық құбылыстар мен нысандарды сандармен өрнектесе болады деген ұғымды білдірсе, екінші жағынан, "…тәңірі алдын сандарды және геометриялық денелерді жаратып, кейін солардың көмегімен материалдық дүниені жаратқан…" деген ұғымда болды; бұған негізгі себеп дөңгелектің ұзындығы мен диаметрінің арасындағы қатнас қалдықсыз еместігінде болды. Ал π деген санды кез келген санға көбейтсек те бүтін саннан соң бөлшекті қалдықтар қала беретіні мәлім. Ғалымның түсінігі бойынша атомнан да кішірек нәрсе – бұл сандар ғана болады. Осыдан шығатын қорытынды ұғым – сандар жәрдемінде шексіз кіші "материалдық болмаған" нәрселерді де есептесе, өлшесе немесе "көрсе болады" деген. Ол кездегі ұғым бойынша атомнан кіші **материалдық нәрсе жоқ** болатын, яғни материяның шегі атоммен аяқталатын. Бұл әрине дұрыс емес пікір екенін төменде көреміз.

Дәл сондай-ақ өте алыстағы галлактикадан тыс жатқан кеңістіктер мен өшіп қалған жұлдыздарды да есептеп тапса болатындығын түсіндірген. Иррационал сандарға да сол мағынада қараған.

Ол уақытта ақпараттар тек қана сандар мен әріптер арқылы өрнектелген болатын. Бұл үшін барлық түрдегі ақпарат сөздерге,

кейін әріптерге айналдырылған және қағаз немесе пергаментке жазылған.

Әртүрлі көлемдік нысандар мүсін немесе сурет түрінде көрсетілген.

Ән-күйлік дыбыстарды ешқандай сөздермен немесе әріптермен көрсету мүмкін болмады. Сондықтан **Пифагор ән-күйлік дыбыстарды анық жеткізіп беру үшін** октавалар жәрдемінде барлық есітілетін дыбыстық ауқымды сегізге бөліп, (олардың арасы 7 аралық) **нотаны ендірді.**

Нота жәрдемінде кез келген ән-күйлік дыбыстарды өте анық бұзбастан өрнектесе болады. Жеті пернемен 128 түрлі дыбыстар шығарса болатындығы есептеп табылған. Сонда әрбір көршілес адам есітетін дыбыстардың айырмашылығы шамамен 30 герцтен аспайды, ал адам құлағы мұндай жиілікті сезе қоймайды [автор].

Пифагордың "октавасы" мен **7 өлшемдік сандары** қазіргі замандық ақпараттық технологияда **ақпараттың негізгі өлшемдері ретінде қабылданған;** октава - **байттық өлшем** ретінде алынған болса, ал 7 – сол байттағы **информативтік таңбалар** саны.

Замандық ақпараттық технологиядағы ақпараттардың барлық түрінде (мәтіндік, аудио және бейне) екілік сандар хабардың ең негізгі түрі екендігі мәлім.

XVIII - ғасырда орыс ғалымы Н.И. Лобачевский былай деген: "Тәңір берген сөздер бізді өзгелердің ойымен байытса, ал математикалық таңбалар тілі – және де анығырақ, дамыған тіл...".

Атақты грек философы Аристотель "Силлогизм" ғылымын жарата отырып, жай және күрделі сөйлемдер арасында ойлаужүйесі (логикалық) амалдарды орындағанда жаңа мәнді және мағыналы сөйлем келіп шығатындығын көрсетті.

Мұнда логикалық амалдарды орындау – ойлау үдерісіне эквивалент болды. Бұл жерде негізгі аргумент болып сөйлемдер қатнасса, олар анық мағыналы "информацияны" немесе ақпаратты білдіреді.

Демек, тек "информация" негізінде ой құралады. "Информацияны" өңдеу нәтижесінде жаңа ой туады. Бұл жасанды парасаттың (интеллекттің) негізгі қағидасы еді.

Математикалық ойлау жүйесінің негізін қалаған неміс математигі Лейбниц математикалық ойлау жүйесі екілік санау жүйесінен басталатынын, сол жүйеде ойлаушы және есептеуші машиналар жасау мүмкіндігін айтты.

Лейбництің бұл ұғымы неден пайда болды екен? Есептеу үшін ондық жүйе де жеткілікті емес пе еді? Бірақ ол есептеуден гөрі ойлаужүйесі амалдарын “дұрыс-жалған” немесе “бар-жоқ” деген амалдар орындаумен шешуді ойлаған еді.

Ирландия ғалымы Д. Буль ойлаужүйесі алгебрасын, яғни ойлау алгебрасын жаратып, оның негізгі элементі ретінде екілік санау жүйесін алды.

Ақпараттар немесе информация тұжырымдамасы да тарихта көптеген рет өзгерістерге ұшырады; ал табиғат құбылыстарын үйренуші үлгілер де көптеп өзгеріп отырды; математикалық үлгілеу мүмкін болмаған пәндер қоғамдық деп, ал мүмкін болған пәндер жаратылыстану пәндері болып келген болса, ендігіде (кибернетика дәуірінде) бұл тұжырымдама да өзгерістерге ұшрай бастады.

Кибернетика пәні бұл екі пәндер тобын да өз ішіне алып, адам ойлайтын (немесе қоғамдық) мәселелерді техника немесе машина жәрдемінде шешетін болды; яғни математикадан да тыс мәселелер шешілетін болды;

Сөйтіп, ендігі заманда “кибернетика” ғылымдар “патшасы” бола бастады.

Әрине бастапқы кезеңде ғалымдардың өзі де бұған көніге қоймады. Бірақта көп ұзамай адамдар барлық ақыл жұмыстарын компьютерге жүктеп, “апатты” естен шығара бастады.

Ақпараттық технологияға назар тастасақ, 19 ғасырда бірінші баспа станоктары пайда болса, 20 ғасырдың басында телеграф, радио, телефондар, ал орта кезінде - компьютер, телекөрсеткіштер жаратылды.

20 ғасыр ақырында интегралданған ақпараттық жүйелер – Ғаламтор және т.б. жүйелер құрылды. Бұл жүйелер Жердің кез келген жерінде информацияны қабылдап, өңдеп, алысқа жеткізіп беріп, сақтап тұра алады және күндіз-түні тоқтамай істейді. Ғаламтор жер шарын қоршаған “тірі мүше”ге ұқсас екендігін көреміз; оның өлі материядан айырмашылығы – ондағы үдерістер жоғарғы зияткерлік үдерістер болып, жеке адамның парасатынен анағұрлым жоғары дәрежеде болды және “ғаламдық парасаттың” үлгісін жаратты.

Информация сөзінің тырнақшасыз жазылуының себебі төменде көрсетіледі.

Ақпараттық үлгілер ұғымы да мүлдем өзгеріп кетті; енді ол мәтін және теңдеулер түрінде ғана емес, суреттер немесе қимылдағы ны-

сандар түрінде болып, электронды түрде ақпараттар негізінде немесе Ғаламторда үздіксіз әрекетте болатын болды; иіс пен дәмнің де үлгілері құрылды; бұл тарихта болмаған жағдай.

XX ғасырда ***ақпарат*** әлеуметтік өмірдің негізгі атрибутына айналды; кибернетиканың, байланыстар теориясының және басқару теориясының дамуы ақпараттық қоғам құрылысына алып келді.

Кибернетика ғылымының және Информатика пәнінің дамуы арқасында қоғамдық және жаратылыстану ғылымдары интеграцияланып кете барды; қоғамдық пәндердің көпшілігі кибернетикада одан ары дами бастады.

Өткен ғасырдың 80-жылдары кеңес одағының ғалымы академик В.М. Глушков былай деген: "...келесі ғасыр – қағазсыз ақпараттық технологиялар заманы болады..." [33].

Кибернетиканың негізін қалаған ғалым Норберт Винер былай деген: "...қай жерде ақпараттық немесе ғылымдық жағдай сол уақыттағы қажеттілікке толық жауап беретін болса, сыртқы мұхитты үздіксіз бақылап, оған белсенді әсер етуде ақпарат өте маңызды екендігін толық түсінген мемлекетте ғана ең сенімді қауіпсіздік болады...". Бұл пікірді толығымен дұрыс деп болмайды; себебі материя шексіз және үздіксіздігін зерттеген орта ғасыр ғалымдары Омар Хайям, Ибн Сина ж.т.б. Материя мен Жаратушыны бірдей деп түсінген болатын және Оны толық зерттеп болмайтынын түсінген.

Мұндай пікірді Эйнштейн, Максвел, Планктер де қолдаған.

Сондықтан адамзатты негізгі тұлға етіп қарап, "*сыртқы мұхиттқа белсенді әсер ете беру"* табиғатқа және экологияға үлкен зиян келтіруі және үлкен қауіп-қатерге алып келуі мүмкіндігі осы кезде зерттеліп келеді.

Өткен заманда көптеген ғылыми бағыттардың синтезінен кибернетика пәні келіп шықты; біріншіден, тірі мүшелер, есептеуіш машиналары мен автоматтардың әрекеттерін анализ етуге жалпы көзқарас ретінде.

Екіншіден, ақпараттарды ұзату (арнамен жіберу) теориясы мен санақтық физика теорияларының синтезінен келіп шықты.

Бұл жерде "ақпарат" түсінігі зияткерлік өмірде ақпараттық қарым-қатынастардағы негізгі атрибут болады. Ал ақпараттық қарым-қатынастар барша тірі және жасанды жүйелердің керекті атрибуты болды.

Инфосфера көлеміндегі барша дүниеқұрылымның негізгі қасиеттерінің бірі – ақпараттық қарым-қатынастар. "Инфосфера"

деп ақпарат айналым ететін шын дүниенің бір бөлігіне айтамыз; бұл жүйенің құрамдас бөліктері – адамдар қоғамы, ақпаратты ұзатушы, қабылдаушы, қайта өңдеуші, сондай-ақ тауарды автоматты түрде істеп шығаратын жүйелер; бұлардың барлығында да тірі адамдар қатысады.

Қазіргі заманда ақпарат немесе "информация" түсінігі қай категорияға жатады?

Қазіргі уақытта кибернетикалық әдістер және компьютер қолданылмайтын бірден-бір пән қалған жоқ. Себебі, барлық пәндер ақпаратарды жинақтап, оларды өңдеу нәтижесіне негізделген; сондықтан ақпараттарсыз ешқандай пән болуы мүмкін емес.

Пәндердің жаңа түрлері – зияткерлік эксперт жүйелері пайда болып, мамандық бойынша әрқандай сұрақтарға жылдам және дұрыс жауап бере алатын болды; мұндай жүйелер нақты уақытта басқару жүйелерінде және өмірдің көптеген салаларында қолданылып келеді.

Сол жаңа пәндердің бірі компьютерлік диагностика жәрдемінде ауыру-сырқаттарды немесе техникадағы бұзылуларды, ауа райын және сол сияқтыларды алдын ала болжау мүмкіндігі туылды.

Компьютерлік үлгілер және зияткерлік жүйелер жәрдемінде күрделі роботтар жаратылып, басқа да ешқандай әдістермен шешуге болмайтын мәселелер шешіле бастады.

Ақырғы уақытта жапон ғалымдары иісті анық өлшей алатын және қайтадан дәл сондай иісті шығара алатын компьютерлік құрылымдар жаратты. Осы кезде иісті жылжымалы телефонмен жіберу де сынақтан өтті. Алайда мұндай телефонды қолдануға рұқсат берілмеді.

Сол ғалымдар көп өтпей "сезім мүшелерін" жаратып, жасанды парасатты компьютерлер құрып шығарды. Қысқасы, математика құралының күші жетпеген өте күрделі мәселелер кибернетика ғылымында өз шешімін тапты. Сонымен бірге, адамның дүниеге көзқарасы мүлде өзгерді.

Жаңа заманда өте күрделі жүйелер пайда болып, олардың іс әрекеттерін анық түрде математикалық әдістермен зерттеу, жарату да мүмкін болмады.

Бұған мысал, осы заманда кең қолданылып келе жатқан анық емес ойлау жүйесі эксперт жүйелерінде шешім қабылдау бағдаржолдарын анық түрде математикалық үлгілермен көрсету мүмкін емес.

Сондай-ақ әртүрлі ойын бағдарламалары да ешқандай матема-

тиканы қажет етпейді. Мұндай бағдарламалар негізінде жаратылған тренажерлар білім беру салаларында: ұшқыштар, шоферлер, ғарышкерлер, әскерлер, спортсмендер, әртүрлі мамандар дайындауда кең қолданылып келеді.

Түбегейлі жоспарлы ойын бағдарламалары әскерді немесе бөлімшесін соғыс кезінде басқаруға үйретсе, күрделі медициналық және т.б. амалдарды орындаудағы қызметін айтпаса да болады.

Кеше математикалық жолдармен шешілмейтінге шығарылған көптеген мәселелер бүгінгі күнде кибернетикада шешіліп, амалда қолданылып келеді.

Кибернетика және оның бөлімдері болған информатика, биоинформатика, телепатия, телекинез т.с.с. ғылымдар қоршаған ортаға жаңаша көзқараспен қарауды тудырып, ***жаңа философияны жаратты***; теориялық жағынан информация және автоматтар теориясы, бейнетану және санақтық шешімдер қабылдау теориясы, бағдаржолдар, тілдер мен бағдарламалау теориясы және т.с.с. теориялар пайда болды.

Бұл туралы атақты Билл Гейтц мына пікірде болды: ...егерде барлық адамдарды компьютермен жабдықтап, олар Ғаламтормен жұмыс істесе, онда дүниеде ешқандай да мәселелер қалмайтындығын айтқан еді.

Әрине кибернетика пәні тірі әлемді толық қамтыған ғылым болғандығы себепті кибернетика заманында жаңа мәселелер пайда болды:

тірі адамдар вирустармен кеселденсе, кибернетикалық жүйелер де вирустарға шалдыға бастады; тірі адамдарда заң бұзушылар болса, кибернетикалық дүниеде хакерлер пайда болды; адамзат өмірінде ұрылар болса, компьютер дүниесінде пираттар пайда болды т.с.с.

Дәл осы күні Урсулдің философиясын ешкімде қолдай қоймайды.

Информатика және соған байланысты кейбір жаңа пәндер (парапсихология, телекинез, телепатия, нейрофизиология, т.с.с.) дами келе адамдарда жаңаша көзқарас (философия) пайда болып, ол да уақыт өткен сайын өзгеріп бара берді.

Философия не және қалай жаратылады? Ғасырлар бойы жаратылыстану ғылымдарымен шұғылданған ғалымдар ғана философ деген атаққа ие болды; өздерінің қоршаған материалистік дүниені зертей отырып, философиялық тұжырымдар жасады. Кей кезде діни және философиялық көзқарастар арасында қайшылықтар

да болып тұрды; бұған себеп, философияда екі түрлі бағыт болып, материалистік көзқараста ғылыми табыстар тәжрибелермен дәлелденсе, ал қиялшылық бағыт абстрактты математика немесе діни ережелерге сүйенді.

Сол кездегі материялистер атомнан кіші материя жоқ деген қате пікірде болған.

Осы көзқарас өткен ғасырда өзгерді; мысалы, ... ***масса ешқашан өзгермейді*** немесе ***абсолют*** деп санаған болсақ, А. Эйнштейн масса, уақыт, кеңістіктегі арақашықтық та санақ нүктесіне байланысты түрде өлшенетіндігін, олардың үшеуі де өзгеруі мүмкіндігін, яғни ***абсолютті еместігін дәлелдеді***.

Бұл теория қиялшылық (идеалистік) және материалистік ***көзқарастар арасындағы қарама-қарсылықтарды жойып, шекараны алып тастады.***

Өткен ғасырдың басында термодинамикалық теорияны жаратқан А. Эйнштейн және т.б. ғалымдар әлемнің қалай пайда болғандығын, оның құрылысын толық түсіндіре білді; барлық біз көріп тұрған әлем бір уақытта бір ғана қара нүктеден “Бүкіл әлемдік қопарылыстан ” жаратылған деген болжамды ұсынды.

Бұл болжамның діни көзқарастардан айырмашылығы болмады; қазіргі күнде де бұл болжамға ешкім қарсы бола қойған жоқ.

Әрқандай философиялық көзқарастар жергілікті аралықтарда ғана дұрыс болып, басқа аралықта басқаша заңдылықтар табыла берді. Олар көбінесе алдыңғысына сәйкес келе бермеді.

Ал философия тек қана жаратылыстану ғылымдарымен шектеліп қала береді ме?

Адамның ақпаратық құрылымы өте күрделі екендігі және әлемдік ғарыштық ақпаратық дүниемен байланысты екендігін қазіргі заман ғылымы толық дәлелдеп отыр. Ғасырлар бойы өте “нәзік” энергоинформациялық дүние тек қана **діни кітаптарда** ғана айтылып, ғылымның кей салаларында ғана зерттеліп келді; мысалы парапсихология, экстрасенсорика, медиатация және сол сияқты.

Ал Информатика пәні техникалық пәндер қатарына қосылып, ***“информация” ұғымы тірі әлемнен тыс қаралып*** келді. Бұл түсінік мүлде дұрыс емес екендігін түсінуге әрекет етейік.

Қазіргі заманда озық философиялық тұжырымдамаларда тірі әлемнің барлығы да ***энергоинформациялық дүниелерден құралған***

және бұл дүние әлемдік ғарыштық дүниенің бір кішкене ажыралмас бөлігі деп қаралады.

Адамның физикалық денесі дөрекі "материалдық" дүниеге жататын болса, ал оның "жаны мен рухы" материяның өте нәзік (көрінбейтін) бөлігіне жатады. Ал *парасатқа* келетін болсақ, ол жинақталған "ақпараттарды" қорыту негізінде пайда болады.

Ашировтың түсінігі бойынша адамның *ақыл – парасаты (санасы)* оның парасаты + адам жаны+ рухының жиынынан құралады; ал *парасат* онда жинақталған "ақпараттар" қорытындысы деп түсіндіріледі.

Бұл түсініктер қазіргі замандық көптеген ғылымдарда дәлелденіп отыр.

Осы сияқты пікірді осыдан мың жыл бұрын атақты ғалым Ибн Сина да айтқан болатын; ол: "... ақыл жан иесі..." деп, жан мен ақылды - күшке, яғни энергияға теңейді. Атақты Ибн Синаның пікірінің дұрыстығын осы кездегі ғалымдар толық дәлелдеп отыр.

Алайда атақты Н. Винер "информация" материяға да, энергияға да жатпайды деген ойда болды. Әрине, бұл дұрыс пікір емес.

Енді "*информация*" және *энергетикалық дүниенің бірлігіне* тоқталайық.

Өткен ғасырда адамзат өмірі үшін ең керекті нәрсе энергия болып және соған сәйкес көптеген ғылыми теориялар жаратылған еді; мысалы үшін, А. Эйнштейн, Д. Больцман және т.б. **термодинамика теориясын** жаратып, бірнеше Нобельдік силықтарға ие болды.

Больцманның газдар үшін жаратқан термодинамика теориясына келсек, газдардың энергия сыймдылығын өлшеу үшін "Энтропия" ұғымын ендірді; оны мына теңдеумен өрнектеді: $H(X)=\sum_{i=1}^{N} P_i \log P_i$. Мұнда P_i - газ молекуласының әрбір энергетикалық жағдайының ықтималдығы десек, ал $N-$ сол көлемдегі газ молекулаларының саны болса, онда екілік жүйеде газдың энергия сиымдылық мөлшері ондағы бит өлшеміндегі информация сиымдылығына тең болып отыр.

Дәл осы теңдеуді Шеннон информацияның **көлемін (тек көлемін)** өлшеу үшін қолданды. Оның құрылымын бұл теңдеумен мағынасын өлшеп болмайды.

Басқа мысал, компьютер жадына 1 килобит хабар жаздық делік.

Сонда хабарлар компьютер жадындағы 1 мың триггерге “жазылуы” керек; “жазылу” дегеніміз триггер өзінің алдынғы жағдайын өзгертеді дегенмен тең.

Триггердің 2 ғана жағдайы болып, 1 бит информация сақтай алады. Оның энергия сиымдылығы да шартты түрде 1 битке тең; яғни информация және энергия сиымдылықтары бір түрлі болып, екеуі де бір түрлі мағынада қаралады.

Бірақта барлық триггерлер өз жағдайын өзгерте қоймайды.

Мысал үшін, 700-і өз жағдайын өзгертті делік. Сонда бұл триггерлердің потенциалдық энергиясы өзгерді.

Компьютер жады алған энергия шартты түрде екілік өлшемде 700 битке тең болады. Ал алынған “информация” мөлшері де дәл соған тең.

Мысалда “информацияның” (0,7 кбит) хабардан (1 кбит) кем екендігін көреміз. Осы мысалдан энергия мен “информация” арасындағы байланысты анық түсінсе болады. Сонда, хабар сырттан келген әсер етуші энергия болса, ал “информация” тірі мүшенің қабылдап алған энергиясын көрсетеді.

Бұл жерде “тірі мүшенің” деген сөз информацияның пайда болу шарты екенін айта кету керек; яғни осы үдеріс компьютерде өткен болса, қабылданған энергия хабар күйінде қала береді.

Адам миында 10^{12} ден көп нейрондар болып, әр нейронның жағдайы екеу емес, мың да емес, онан да анағұрлым көп; яғни үздіксіз функция түрінде болғандықтан шексіз көп деп түсіну керек.

Әрқандай “информация” алынғанда мидың ішкі энергиясы да дәл сол мөлшерде өзгереді. Бірақта миға “информация” жеке нейрондарға емес, көлемді голограмма түрінде жазылатындығы себепті мидың сиымдылығы шексіз екен деуіміз орынсыз; адамның миын өте көп шегарадан тыс істете беру оның шаршап, адамның әртүрлі психикалық кеселдерге алып келуі мәлім.

Жалпылап айтқанда **“информация”** – тірі мүшедегі биоэнергетикалық үдерістерге байланысты болып, биологиялық **энергияның жоғары ұйымдасқан (математика тілімен айтқанда векторлық) түрі** десек болады; бұл мәселемен осы кезде әлемде бірнеше ғылым симбиозы (нанотехнология, нейробиокибернетика, информатика, когнита технология және т.б.) бірге шұғылданып келеді.

1923 жылы А. Г. Гурвич ***тірі жасушалардың энергетикалық***

биоөрісі барлығын анықтап, ол өрісте тірі мүше (организм) туралы толық генетикалық "информация" барлығын айтты [7,17].

Осы жасушалар тірі мүше туралы "информацияны" ***ультракүлгін ауқымда*** кодталған электромагнит сигналдарын таратады.

Жасуша өлгенде оның биоөрісі жоғалып кетеді; яғни жасушаның ***жаны*** оның ***биоөрісімен*** анықталады; бұдан ***жан - материяның бір көрінісі*** екенін түсінеміз.

Жасушалық өрістер мен мүшенің тарататын сыртқы торсиондық өрістері бір түрлі екендігі анықталған; сол өрістер адам құрылысын, өмірінің келешегін де толық көрсете алатын болды.

Биоөрістер энергияның бір түрі екендігі, ал энергия материяның ең негізгі түрі екендігі бәрімізге мәлім. Сонымен "...Жаратушы нұрмен жан бітірді..." деген сөздердің ешқандай қатесіз екенін көріп отырмыз.

Ал егерде жан энергияның бір түрі болса, онда оның (энергияның) ізсіз жоғалып кетпейтіні де анық емес пе. Сонымен ...жан...энергия... информация...деген түсініктер өзара тығыз байланысты екендігі осыдан көрініп тұр.

Тірі жасушаға сыртқы әсер болғанда, ондағы биоөріс уақытынша өзгеріп, биоинформациялық серпіндер (импульстер) - сигналдар пайда болады; олар орталық жүйке жүйесіне - мыйға барып жетеді және ондағы нейрондардың жағдайын өзгертеді, яғни жазылады; көз рецепторлары жарықтық сигналдарын биотоққа айналдырса, мұрын рецепторлары - иіс, ауыз рецепторлары- дәм, құлақ рецепторлары – дыбыс, терідегі рецепторлар - температура, басымды биотоқ сигналдарына айландырады. Бұл құбылыстар - энергоинформациялық құбылыстар.

Бірақта сол үдерістердің барлығында да **тірі жасушалар** қатысып, биоток немесе биоөрістер тірі жасушалардағы үдерістердің бір көрінісі ғана болып, ***"тірі"*** деген мағынаны білдіреді.

Бұл жерде **жасуша** әрі биосигнал шығаратын биогенератор, әрі мидан немесе жүйке жүйесінен келген биосигналдық командаларды орындайтын биомотор қызметін атқарады.

Сондықтан **"Информация"** ұғымын **"тірі жан"** ұғымынан **бөлектеп** қарауға болмайды және "информация" ұғымына берілген *нақтылы анықтамаларға* қазіргі заманда басқаша түрде қарау керек болады; автордың түсінуінше "информация" бұл сыртқы ортаның тірі мүшеге әсер етуі арқасында оның ішінде болатын тітіркенуі

немесе ішкі қалдықты энергоинформациялық өзгерістері; ол өзгерістер тірі мүшелердің өзін сыртқы ортаның әсеріне бейімдеуі (адаптация) және өзін "аман сақтап қалуы" үшін қолданатын негізгі құралы екенін айту керек. Демек, үдерістер әсерден кейін өзгерген түрде жалғаса береді. Мұндай бейімделу өлі дүниедегі ақпараттық жүйелерде болмайды.

Ішкі энергоинформациялық өзгерістер тірі жасушалардың қатысуымен болып, ***"тірі жан"*** деген сөздің өзі сол **"*энергоинформациялық үдерістер бар*"** дегенмен немесе мүшедегі "***информация***" дегенмен тең болып отыр.

Сондықтан, биоток немесе биоөрісті қандай түсінсек, ***"информацияны"*** да сондай, яғни энергияның биологиялық бір түрі деп түсінуіміз керек; яғни ол тірі мүшенің ішіндегі **тірі үдеріс** болып, **"жан"** деген ұғымның бір көрінісі.

Демек, жансыз нәрседе "информация" түсінігі мағынасыз болады.

Ал хабар, ақпарат т.с.с. "информацияның" үлгілері ғана болып, олар сигналдармен таратылады және "информацияның" **мүшеде пайда болуына** себепші болады.

Ақпараттар теориясында да "**информация"** және **хабар ұғымдары бөлектеп қаралады;** теорияның негізінде, мысал үшін, кем хабармен көбірек "информацияны" мұрағатта сақтап қою мүмкіншілігі, көбірек хабармен "информацияны" арнамен анық сенімді жіберу мүмкіншілігі немесе өте көп хабармен "информацияны" көрсетпей құпия түрде арнамен жіберу мүмкіншілігі сияқты мәселелер қаралады.

Бірақ, көбінесе түркі тілдерде ақпарат, хабар деген сөздермен "информация" ұғымы эквивалент деп қаралып, "информация" сөзі мүлде қолданылмайды. Айта кететініміз, ақпарат, хабар – сыртқы үдерістер болса, ал **"информация"** тірі мүшенің ішіндегі **тірі үдеріс** болып, тек сол мүшенің **тітіркенуімен** немесе **"жанымен"** өлшенеді.

Мысалы, орыс тілінде ақпарат, хабар деген сөздер орнына вести, сообщения сөздері қолданылып, ал "информация" деген сөз бөлек мағынада айтылады; мысалы, информационные сообщения немесе информационные вести сөздері.

Информацияны былайша оңай түрде түсіндірсе болады; "информация" хабардың біз түсініп, өзімізге қабылдаған бір бөлігі ғана болады. Сондықтан да, "информация" көлемі хабардан көбінесе кем болады.

Ақпараттар теориясының негізін қалаған К.Э. Шеннон жоғарыдағы теңдеумен екілік “информацияның” **көлемін ғана** өлшеді. Мұнда ол мүшені қабылдаушы деп абстракт түрде қарайды да оның тітіркенуінің көлемін ғана өлшейді. Бірақ қабылдаушының ***тірі екені*** туралы сөз болмайды.

“Информацияның” ең кіші көлемдік өлшем бірлігі – екілік бірлік болып, bit (Binary digit), біздің тілде “екілік санақ ” деген мағынаны білдіреді.

Демек, “информацияны” энтропиямен өлшенуі және энергияны өлшеу теңдеуінің қолданылуы кездейсоқ емес; олардың табиғаты бір түрлі екендігін көрсетеді.

Бірақта микродүниеде “информация” ұғымы энергия ұғымымен біртүрлі болса, ал макродүниеде “информация” ұғымы энергиядан айырмашылығы бар; бұған ұқсастық келтіру қиын болса да келесідей мысалды қарайық; егер энергияны локомотив десек, пойыздың өзін - сигналдар деуге, жүктің барлығын - хабар, ақпарат десек, ал “информацияны” сол пойызда тасып келе жатқан жүктердің біз қабылдайтын керекті бөлімі десе болады.

Және бір мысал, “А” деген әріптің “информация” сиымдылығы ағылшын тіліне қарағанда орыс тілінде көбірек болса, қазақ тілінде онан да көп болады (“информация” сиымдылығын энтропиямен өлшегенде).

Әріпті хабардың бір бөлімі деп түсіну керек. Сол әріпті ASCII, МТК-5, КОИ-8 кодтарында кодтау үшін 8 екілік таңба керек болса, ал Хэмминг кодында – 12 таңба, циклдік кодта – 11 таңба, мажоритарлық кодта – кемінде 24 таңба, Хаффмен, Шеннон-Фано кодтарында - 3-4 таңба кетеді.

Сигналдың энергиясы таңбалар санына пропорционал өзгереді. Сондықтан ақырғы кодттар хабарды мұрағаттауда, ал мажоритарлық кодтар хабарды өте алысқа жіберуде қолданылады.

Әр таңбалы жіберу үшін әр түрлі сигналдар қолдану мүмкін болса, бір түрлі сигналдың өзінің де энергиясы әр түрлі болуы мүмкін. Сондықтан “информация” теориясы сигналдар теориясынан басталып, олардың энергетикалық және ақпараттық мүмкіншіліктерін үйретеді.

XX ғасырдың ортасы, соңы және XXI ғасырдың басы “Информатика” және ақпараттық технологиялар ғасыры болды; ғалымдардың басым көпшілігі ақпараттық технологиялар мен жүйелер жарату-

мен айналысып, дамыған елдердің негізгі капиталы – ақпараттық жүйелер жаратуға бағытталған болды; мысалы үшін, "Microsoft" корпорациясы бүгінгі күнде байлығы бойынша бірінші орында тұрады.

Ақпараттардың адамзат қоғамындағы орны туралы аталған корпорацияның бастығы Билл Гейтц өзінің "Ақыл жылдамдығындағы бизнес" деген кітабында былай деген: "Келешекте бизнестің негізгі түрі – ақпарат немесе ақпараттық жүйелер болады".

Бұдан оншақты жыл бұрын Индияда "Информатика" министрлігі әлемде бірінші болып құрылды және қоғамда тірішіліктің негізгі саласына айналды.

Өткен ғасырда ғылымның ең алдынғы шебінде **кибернетика ғылымы** болса, сол ғылымның ең негізгі бөлігі – **Информатика** болып, оның теориясы **ақпараттар теориясы** болды.

Ал кибернетика ғылымының жаратылуы – санақтық термодинамика ғылымымен тікелей байланысты болып, ақырғысы - энергия құбылыстарын зерттеді. Л. Больцман, Дж. К. Максвелл, А. Эйнштейндер сол ғылымның негізін қалаған ғалымдар, яғни бірінші кибернетиктер десе болады.

Мұнда Больцман **газдардың энергиясын энтропия немесе айып теңдеуімен** өлшеген болса, сол өлшемдермен К.Э.Шеннон **"информация" мөлшерін** өлшеп, **сол теңдеуларды өзгертпей** қолданды.

Энтропия "информацияның" синтаксикалық өлшемін көрсетсе, ал айып теңдеуі оның құндылықты өлшемін береді. Мұның себебі – **энергия және "информация" түсініктері бір-біріне өте жақын болып, біріншісі өлі дүниенің негізгі құраушысы болса, ал екіншісі – тірі дүниенің негізгі құраушысы болады.**

Алайда бізге көрінетін макродүниеде олар әртүрлі болып көрінеді. Сол өзгешеліктерді атап өтейік:

1. "Информация" қолданушыға қатысты субъектив әсер, ықпал болып, қолданушыға байланысты болады. Бір қолданушы "информацияны" қабылдап болған соң, сол қолданушыға "информация" қалмайды. Дәл сол "информация" басқа қолданушыға "информация" бере алады. Қысқасы, бір хабарды көбейтіп, көпшілікке тарату мүмкін. Мұнда "информация" көбейеді деген сөз емес. Бірақта, оның әсері көбейеді.

2. "Информация" уақытқа байланысты өзгеретін әсер, ықпал,

“информацияның” құны уақытқа байланысты болады. Бірақта жаратылыстану ғылымдарындағы кейбір заңдылықтар уақытқа байланыссыз болып, көптеген ғасырлар бойы өз құндылығын жоғалтпайды.

3. “Информацияның” құндылығы субъектив әсер, ықпал болып, қолданушыға байланысты; қолданушының зияткерлік дәрежесі қанша жоғары болса, соншалықты “информация” құндырақ болуы мүмкін.

Қазақстанда инфосфера немесе инфроқұрылым құрылып келе жатыр; адамдардың психологиясы, философиясы да соған бейімделіп, өзгеріп келеді; мысал үшін, 10 - 20 жыл бұрын дербес компьютер (ДК) оншалықты қажет болмаса, қазіргі күнде онсыз ешкім тіршілік ете алмайтын болды.

Жоғарыда атап өтілгендей, Үкіметтің қабылдаған үкімдерінде 2030, 2015 ж.ж. Түбегейлі жоспарлық бағдарламаларында, 2004 ж. кеден, әлеуметтік қамсыздандыру, салық министрлігінде, білімді, ғылымды, медицина ж.т.б. салаларды ақпараттандыру туралы үкімдер қабылдаған болса, одан бері Президент Н. Назарбаевтың әр жылғы “Жолдауларында” бұл мәселелер негізгі мәселелердің бірі болып отыр.

Президент Н. Назарбаевтің 2005 ж., 2006 ж., 2007 ж., 2012 ж. “Жолдауларында” халықтың әлеуметтік жағдайын жақсарту, орындаушы аспаптың жұмыстарын жеделдету мақсатында “Бір терезеден қызмет көрсету ” жүйелерін іске қосу, “Электрондық Үкіметт” құруды жеделдету, “Электрондық құжат және электрондық қолтаңба” туралы заң қабылданып (2003 ж.), жалпы теңестірулік нөмірлерін де іске қосу мәселелері қойылған болатын.

Мұның барлығы Қазақстанда инфрақұрылым жаратып, әлемдік инфосфераға қосылуына мүмкіндік жаратып отыр.

Қоғамды ақпараттандыру қоғамның жалпы түрде білімділігін арттыра отырып, адамдардың белсенді жұмысшы қабаттарының артуына, олардың әлеуметтік-саяси және экономикалық жағдайының жоғарылауына алып келеді.

XXI ғасыр “информациялық қоғам” ғасыры болып, алдын инфосфера, кейін ноосфера құрылады; инфосферада барлық адамдар “информациямен” толық қамсыздандырылып, әлеуметтік-экономикалық, мәдени, білім және ғылым медицина дәрежесі өте жоғары дамыған жағдайда болады.

Кейінгі кезеңде ноосфера құрылады; Вернадскийдің “ноосфера-

сында” табиғаттың және қоғамның дамуы адамзаттың санасы, ақыл-есімен таңбаланады; ол Жердің дамуы үшін жалғыз дәлел бар – ол адамдар санасының күшейуі деген пікірді айтады.

Ашировтың “ноосферасының” айырмашылығы - Вернадский Жерде білімді қоғам жаратылып, ол қоғам қоршаған ортаны, яғни экологияны сақтайды деген ұғымдары адамдар экологияны өздері үшін сақтайды деген мағынада айтылған еді; мұнда адамзатты негізгі тұлға етіп көрсеткен; “ғарыштық сананы” немесе осы кезде Материяны анық түрде көрсетпейді.

Көптеген философиялық көзқарастарды толық талдай отырып, кітапта үшінші мыңжылдықта философиялық көзқарас қандай болуы керектігіне тоқталады; бұл көзқараста адамзат табиғатпен толық бірлесіп, биосфераның жаңа жағдайына көшеді деген ұғымды ноосфера жаратады деп толықтырады; мұндағы ноосфера жалғыз ғана адамзат санасынан құралып қалмай “ғарыштық санадан” да құралғандығы айтылады.

Мұнда адамдар тек қана әлеуметтік-экономикалық жағдайды дұрыстап қана қоймай, Жер планетасының “тірі мүше” екендігін дұрыс түсіне отырып, экологиялық таза орта жаратады.

Көптеген философиялық көзқарастарда да адамзат дүниесі, қоғамдағы заңдылықтарды бір бөлек (қоғамдық пәндерде), қоршаған орта немесе табиғаттағы заңдылықтарын басқа бір бөлек (жаратылыстану пәндерінде) деп қаралса, осы заман тұжырымдамасында барлық ***әлемдегі құбылыстар бір бүтін*** деп қаралады.

Ал “информация” - өткен заманда энергияның бір түрі деп қаралса, қазіргі күнде энергиядан анағұрлым бай түсінік болып, сол ***тірі әлемнің ең негізгі құраушы бөлімі*** екендігі ***заманымыз философиясының да негізі*** болып отыр.

Қазіргі күнде Қазақстандағы саясат та жаңа ***“жасампаздық философия”*** негізінде құрылған.

Президент Н. Назарбаевтың “Жасампаз көшбасшылық” философиясының нәтижелері өмірдің барлық салаларында көрініп отыр;

-“күшті дамыған” елдер діндер арасындағы қарама-қарсылықты өршітіп отырғанда, біздің елде әртүрлі діни конфессиялар достасып, діни тәрбие қайта жолға қойылды;

-жастарға жаңа философияны үйрету, өзінтану, экология, замандық жаратылыстану тұжырымдамасы т.с.с. жаңа пәндер өтіліп, жастар жаңаша философиялық көзқарас негізінде тәрбиелеу жолға қойылды.

Осы оқулықта “Информацияның” философиялық тұжырымдамасын берудегі негізгі мақсат – “информацияның” тірі жан ұғымымен байланысты екенін түсіндіру; ал жан ұғымы биология, физиологиясы және сол сияқты ғылымдарда үйренілгенмен оның табиғаты қандай және оның өлшем бірліктері бола ма деген сұраққа ешқандай жауап тауып болмайды!

Ақпараттар теориясы ақпараттың көлемдік өлшемдерін, олармен әртүрі амалдар жасауды үйреткенмен оның (бұл жерде ***информацияның***) ***тірі жанмен байланысты*** екенін анық көрсетпейді!

Ең қиыны - информацияның жан деген ұғыммен, ал жан дегеніміз биологиялық дүниедегі энергияның түрі екені, ал энергия материяның ең негізгі құраушы бөлігі екенін түсіну ғалымдардың өзіне де қиындау болады. Сондықтан, осы кітапта автор өте көптеген осы және өткен заман ғалымдарының, философтардың еңбектеріне негізделіп, рух-жан-информация-энергия-материя ұғымдарына анықтама беріп, олардың ажыралмас бірлігіне келіп тоқталады.

Осы күні Елбасымыздың нұсқауымен **“*...пәнаралық зерттеулер тәжірибесін кеңейту...*”** мәселесі қойылды; осы бағытта мемлекеттің тәуелсіздігін нығайту жолындағы ***өзекті тақырыптың бірі, өнегелі құндылықтың негізгісі – адамдардың өмірге, дінге және замандық ғылымға (философияға) деген дұрыс көзқарасын қалыптастыру болды*** **[3,4]**.

I ТАРАУ.
АҚПАРАТТЫҢ ЗАМАНАУИ ФИЛОСОФИЯЛЫҚ ТҰЖЫРЫМДАМАСЫ; ҚОҒАМ ДАМУЫНДАҒЫ ИНФОСФЕРАНЫҢ ОРНЫ.

1.1 Ақпараттың философиялық тұжырымдамасы; инфосфераның қоғам дамуындағы орны.

Президент Назарбаевтің “Вашингтон таймс” газетінде “Жас өскін демократиялардың әлеуеті” мақаласы басылып шықты [3]. Мұнда Президент әлемге жаңа “Жасампаз көшбасшылық” философиясын ұсынды.

“Жасампаз көшбасшылық” философиясы осы кезде **ең озықты философия болып, “...басқаларға көрсете алатын маңызды өнеге**…” ретінде көрсетілген.

Қазақстанда Президент Назарбаевтың бастауымен Ұлттар Ассамблеясы және діни конфессиялардың одақтастығы құрылған болып, діндер мен ұлтардың еркін дамуына мүмкіншілік жасалды.

Пәнді академик Ашировтың “...Наука должна быть нравственно-религиозной, а религия – научной...”, - деген сөздерімен бастағымыз келеді [7].

Тірі әлемді зерттеу, адамзаттың жан дүниесін, ақыл-есін, парасатын, қала берсе, көңіл-күйі мен сана-сезімін зерттеу ерте замандық философтардың ғылыми еңбектерінің негізі болған; миды және ойлау үдерісін көп зерттеген Аристотель болып, өзінің “Логика” атты кітабында адамның ойлау үдерісін түсіндіре алды. “Sillogizm” теориясында ойлау үдерісінде адам сөйлемдермен ойлайтынын зерттеген; екі сөйлемді біріне бірі қатысты түрде логикалық өңдегенде (талқылағанда), үшінші сөйлем шығатындығын дәлелдеген; сонымен қазіргі замандағы кибернетиканың бөлімі болған жасанды парасаттың негізін қалаған [26,73,74]. Алайда орта ғасырда ғылым ежелгі Грекиядан Шығысқа ауысып, Орталық Азияда да көптеген ғалымдар жаратылыстану ғылымы мен философияны одан ары дамытты; Пифагор ән-күйлік нотаны ойлап тапқан болса, ал Әл Фараби еңбектерінде ән-күйлік дыбыстардың үстінде арифметикалық амалдарды орындай отырып, жаңа ән-күйлік дыбыстар жарату мүмкіндігін тапқан және жасанды интелекттің жаңа түрін ашқан.

Ал Омар Хайям 0 санын есептеуге ендіре отырып, физикалық

вакуумде де материя бар екенін және оның үздіксіздігін дәлелдеген. Осы күндері Омар Хайямның лирикалық жанрда жазылған рубаилары философиялық ойдың тереңдігімен әлемнің төрт тарапына барлық елге кең тараған болса да, оның ғылыми философиялық еңбектері толық үйренілген емес; мысалы, наурыз мерекесін, осы күндегі күнтізбелікті анық есептеп тапқанын көпшілік біле бермейді.

Шығыс философиясының ерте Грек философиясынан айырмашылығы - жанды тірі дүниені зерттеуде тек қана тәжірибелер, теңдеулер және қара сөздермен шектелмей ғылыми нәтижелерді поэзия және лирика жәрдемінде баяндап, адамзат тарихына бағасыз мұра ретінде қалдырған.

Адамзаттың сана-сезімін зерттеуде замандық ғылым - жасанды парасаттың жаңа салаларын (парапсихология, экстрасенсорика, нейрофизиология, нейрожелілер және т.б.) атауға болады.

Әлемге даңқы тараған Абу Али ибн Сина тірі дүниенің физиологиялық құрылысын тәжрибелермен толық зерттеген болып, адамның "нәзік дүниесін" лирика немесе поэзия жәрдемінде түсіндіре білді.

Бұл ғалым әрі математик, әрі физик, әрі астроном, әрі лирик, әрі ақын-жазушы, атақты философ, сол заманда теңі жоқ дәігер-тәуіп болған; ол әлемге 400 ден аса ғылыми еңбектер мен трактаттар қалдырды.

"Білім кітабы","Нұсқаулар мен өсиеттер" кітаптары философияда ерекше орын алса, ал "Емші ілімінің каноны" (яғни, "Әл-Канун фи-т-таиб") және 43 трактаты медицинада шығыс және батыс елдерінің негізгі кітабына айналды.

Оның трактаттары XII ÷ XYII ғасырлар арасында Европа ғылымында негізгі құрал болып, 30 рет қайта басылған [3].

"Жаратушының тілі ұлы", "Құстар" кітаптарының философияда орны бөлек болса, олардың ықпалы көп уақыт батыс жазушыларына әсері мол болды; Данте, Роджер Бэкон, Ұлы Альберт, Фома Аквинский, Дунс Скот, Вильям Оккам және т.б. еңбектерінде кездеседі. Сондай-ақ Шекспирдің, Гетенің, Браунингтің шығармаларында Ибн Синаның еңбектерінің әсері көрінеді.

"Әділеттілік кітабында" автор 28 мың мәселені көтеріп, Батыс пен Шығыс философтарының жұмыстарына дұрыс баға берген; мұнда Аристотельдің еңбектеріне дұрыс баға беріп, оның ізбасарларын сынға алған.

“Данышпан нәменің“ “Метафизика“ тарауындағы негізгі ұғымдарды талдады. “Жан” туралы кітапта Аристотельден гөрі Платондық тұжырымдамаға жақын болып, мұнда Дене мен Жан мәселесі негізігі болды.

Ибн Сина философиясында **Болмыстың** (материяның) **бір-тұтастығын** көрсетіп, философияны үшке бөлді: **физика, ойлау жүйесі (логика) және метафизика.**

Ойлау жүйесін – табиғат пен адамды танып, білу туралы ғылым десе, ал метафизиканы - тұтас болмысты танып білу туралы ғылым деді.

Ол **табиғатты** санадан тыс **шын** деп, **ойлаужүйесі дәрежелері шын** дүние **заңдылықтар**ына **сәйкес** келеді деді.

Метафизикасындағы негізгі ұғым - **эманация (**эволюция) **теориясы** болды; жансыз және жанды дүниенің жаратылуын ол табиғи эманация жолымен жаралған деп, мұнда эманацияны жүргізіп отыратын “ойлы ақыл” заңдылықтары бар дейді де, **шын идеализмді** (Платон, Пифагор, кейнгі кезде Гегель т.б.) қолдайды.

Пифагор:... дүниені басқарушы дербес күш-сандар! - десе, ал Платон:...жалпы ұғымдар мен көзқарастар!- деді.

Ал Ибн Сина: ...егер жаратушы мәңгі болса, дүние де мәңгі...- дейді; мұны: “... дүниенің көзі материя, ал материя - мәңгі,” - деп түсіндіреді де диалектикалық материализмге келеді; себеп пен салдар өзара байланысты болатынын көрсетеді. Мұнда ол: “...**философия шын заңдылықтар**ға, дәлелдерге **негізделсе**, ал **теология** тек қана **сенімге негізделеді**”,-деді.

Адамның ақылы мен жаны туралы кітапта “....ақыл иесі **жан** болып, ол екіге – **әрекет күші** мен **қиал күшіне** бөлінеді,”- деді;

“**әрекет күші** - адам денесінің **қимыл-әрекетін басқаратын жаны**,”- деп, оны қос мәнді, біріншісі - хайуандық құмар күші, елес пен сезім күшімен байланысты болса, ал екіншісі - қияли ақылмен байланысты”, - деді.

Ибн Сина антик заманның қарапайым материализміне (Гераклит, Демокрит және т.б.) арқа сүйеп, оны дамыта отырып, метафизикалық материализмге (Бэкон Ф., Гобс Т., Ламперти Ж., Дидро Д. т.б.) жеткізген болса, онда да тоқтап қалған жоқ. Ол философияның **шын заңдылықтарға** негізделетінін анық білгені үшін оның дәлелі ретінде **тәжрибелерді** алды.

Ал материяның шексіздігін білген ол ғылымның дамуына байланысты **философиялық көзқарастың да шексіз дамитынын** анық білді.

Сонымен бірге ол діни көзқарастарды анық түсіне білді; басқа философтардан ерекшелігі ол ***діни ережелер мен философиялық пікірлерді ұштастыра*** білді.

Ибн Сина философиясы осы кезде де ең озық философия болған **ғылыми материализмге** қосылады.

Сондықтан да оны дүние ғалымдары ғасырлар бойы қолданып, медицина ғылымына сол адамның атын қойған.

Шын идеализм жаратылыстану ғылымдарының дамуына байланысты өзгере отырып, **ғылыми** немесе **диалектикалық материализмге** жалғасады.

Бұған мысал, 19 ғасырдың ақырында неміс ғалымдары ***Н.Бор, Резерфорд*** т.б. электрон, протон, нейтронды тапты; "…электронның массасы "абсолют"және 9×10^{-28}граммға тең, олардан кіші материя жоқ",- деген пікірмен олар **шын идеализмге** жүгінді [28].

Алайда сол кездегі диалектикалық материализмді жақтаушылары (Ресей философтары) электроның массасының "абсолют екендігі" бүгінгі ғылым горизонты болса, ол горизонт ертең ғылым дамуымен ары қарай жылжып, электроның массасының **абсолют болмайтындығын** айтқан [6,28].

Солар айтқандай-ақ 1905 жылы ***А.Эйнштейн*** арнайы салыстырмалы теориясында микроэлементтердің (электрон да соның ішінде) энергиясы немесе массасы, көлемдік және уақыт өлшемдері олардың инерциал координат системасындағы салыстырмалы жылдамдығына байланысты түрде өзгеріп, **абсолют еместігін** дәлелдеді.

Ал **геометриялық денелердің да абсолютті еместігін** ***Н.И.Лобачевский*** дәлелдеп, Евклид геометриясының керілемесін жаратқан.

Бұл теориялар материализм мен идеализм арасындағы **шекараны алып тастады**; микроәлемде әрқандай геометриялық денелер, сандар немесе ұғымлар, заттардың түрі-түсі, т.б. ***ұғымдардың барлығы да материалдық*** екендігі дәлелденді.

"Жанның" материалдық барлық екенін және жойылып кетпейтінін тек діни кітаптарда ғана жазылған десек жаңылыс болар еді.

Ерте грек ғалымы ***Сократ*** жан жойылмайды, ол мәңгі...деген пікірді айтқан болса, ал орта ғасыр философы ***Ибн Синаның*** пікірі

одан да анығырақ болып, ақылды да (яғни информацияны да) жанға немесе күшке (энергияға) байланысты етіп көрсетеді; ол сондай-ақ тірі дүниедегі **жан** да, **"информация"** да немесе **адамның ойы** да **материалдық** деген пікірді айтқан [5,6,7]; яғни сол кездің өзінде ақ материализм, идеализм және діни пікірлер арасындағы "қайшылықтар" жоқтығын айтқан.

"Информацияның" материалдық барлық екенін біздің жастарымыз анық түсінеді; себебі жылжымалы телефонға единицаларды сатып алу үшін ақша жұмсау керек қой.

Энергияның да қымбаттап бара жатқаны, соның үшін соғыстар болып жатқаны бәрімізге аян.

Өткен ғасырда академик ***Глушков В.М., Колмогоров В., Эшбилер Р***. ақпаратты тірі жанды жәндіктер ойлауы нәтижесінде пайда болады деп, оның тірі ***жанды дүниеге байланысты*** екендігін айтқан; яғни "информацияны" жанды дүниенің айырылмас бөлімі ретінде қараған.

Алайда ***Винер*** термодинамика теориясын да, салыстырмалы теорияны да түсінбеген сияқты; кейбір ғалымдар сияқты ***материяны бір, энергияны басқа, ал информацияны және басқа*** деп түсінген сияқты.

Энергияның өзі де материяның ең негізгі құраушы бөлігі екенін, оның салыстырмалы түрде өлшенетінін және көрінбейтіндігін кейбір ғалымдар осы кезде де түсіне қоймайды.

Өткен ғасырда Макс Планк: ... барлық материялдық дүние жалғыз вибрациялық (жоғары жиілікті тербеліс) энергиядан құралған... деген пікірге келіп, материя көзге көрінбейтін өрістен тұратынын дәлелдеген; бұдан материяның үздіксіздігі мен шексіздігіне көз жеткізген және дінге деген пікірін өзгерткен.

Алайда бұл түсінікті орта ғасырдағы шығыс философтары да айтып кеткен емес пе еді?

Диалектикалық материализм жолындағы ұлы ғалымдардың көпшілігі дінге қарсы болған емес; себебі олар материяның шексіздігін және үздіксіздігін білген және Материяның (діни ұғымда – Жаратушының) құдретті күшінің шексіздігіне көз жеткізген.

"Материалистік" және "идеалистік" көзқарастарды діни кітаптарға немесе өзара қарсы қою ***білімнің шектелгендігінен*** ғана болады.

Ғылым дами келе әлемнің көптеген сырларын аша береді және кешегі ұғымдардан (философиядан) "қателіктер" таба береді.

Бұл үдеріс шексіз өтеді; себебі "шындықтың" өзі де салыстырмалы екендігін жоғарыда атап кеттік. Тек бір ғана ақиқат бар; ол Жаратушының құдретінің шексіздігі! Мұны материалистер "Энергияның сақталу заңымен" түсіндірсе, ал қиялшылар дәл осы заңдылықтарды "жаратылыстың... жалпы ұғымдары ..."деп түсіндіреді.

Түсініктер әртүрлі болғанымен, ақиқат біреу: материяның шексіздігі мен үздіксіздігінде.

Мұны дәлелдеген орта ғасыр ғалымдары – Омар Хайям, Ибн Сина және т.б. болды; мысалы, ұлы математик және астроном Омар Хайям физикалық вакуумде материя бар деп, оны 0 санымен таңбалап, санақ жүйесіне ендірген.

Жаратылыстану ғылымындағы **атақты ғалымдарымыздың** "Ұлы Кітаптың" ақиқаттығына ғылыми жолмен көз жеткізуі диалектикалық материализм философиясының осы кезде де шындық екенін көрсетеді [5-8].

Осы кезде экология, медицина және кибернетика салаларында көптеген ғылыми еңбектер жарық көрді. ***Алайда жаратылыстану пәндері мен қоғамдық пәндер арасындағы алшақтық ғалымдарымыздың философиялық білімдерінің нашарлығына*** әкелді.

Осы күні Елбасымыздың нұсқауымен ***"...пәнаралық зерттеулер тәжірибесін кеңейту..."*** мәселесі қойылды; осы бағытта мемлекеттің тәуелсіздігін нығайту жолындағы ***өзекті тақырыптың бірі, өнегелі құндылықтың негізгісі – адамдардың өмірге, дінге және замандық ғылымға (философияға) деген дұрыс көзқарасын қалыптастыру ...*** **[3,4]** болды.

Жоғарыда аталған еңбектерде биосфераның адамзат саулығына, қала берсе, рухани өміріне де әсері мол екені зерттелген.

Ибн Сина "жан" ұғымын толық зерттеген болса да, осы кезде көптеген ғылыми еңбектерде "**информация"** мен "**жан"** туралы анық пікірлер жоқ болып, "**информация"** ұғымы мен **хабар, ақпарат** ұғымдары арасында **айырмашылық** аңғарылмайды.

Пәннің ақтуалдығы - Осы кезде Еліміз әлемдік кеңістікте танылып отырғанда, қоғамдық білімдер мен жаратылыстану білімдері бірігіп, философиялық білімдер негізгі орын алғанда әрбір пән де философиядан анық орын алуы керек болады.

Сондықтан ақпараттар теориясының басында осы пәнге философиялық көзқарастардың тарихы және осы кездегі заманауй көзқарастарға тоқталдық.

Осы кезде кейбір ғалымдарымыз да хабар мен "информацияның", тірі және өлі материяның айырмашылығын толық ажырата алмады. Бұған мысал өткен ғасырда атақты Винер Н. былай деген: "Информация – бұл материяға да, энергияға да жатпайды...-". Онда неге жатады? деген сұрақ әрине философияның негізгі сұрақтарының бірі болады.

Одан кейінгі замандағы ғалымдар да "информацияны" толық түсіндіре алмаған. Мысалы үшін атақты ғалымдар В.Колмогоров, В.М. Глушков, У.Эшбилер былай деген: ***"Ақпарат – бұл нысанның қасиеті ме немесе сол нысан басқа ақылды барлық тарапынан ұйрену нәтижесінде пайда болады ма?- деген сұраққа дәл анық жауап беру қиын"***... дейді.

Ақпарат қабылдаушының жеке өзінің қабілетіне байланысты ма, жоқ па? - деп анықсыз қалдырады.

Осы пәннің мақсаты осы **философиялық сұраққа** жауап беру.

Медицина саласындағы ғалымдар "**информация"** ұғымын әлдеқайда **анығырақ** түсініп, оны медицина саласында қолданып та келеді [29-31]. Мұндағы ...мағынаны "информацияның" энергиясы... деген түсінік басқа саладағы ғалымдарды ойлантырады; сондай ақ "информация", "жан"...түсініктері өте күрделі философиялық түсініктері болғандықтан, кейбір ғалымдардың анық емес түсініктері байқалады; мысалы: "... информация – это универсальное свойство предметов, явлений, процессов..."деп түсінтірсе, ал кейбір жерде: "... кто или что генерирует информацию в человеческом организме?"[32] деген немесе "информация" және сана немесе энергия және материя түсініктерінің араларында қандай байланыстар бар?" деген немесе ..."информацияны", оның мағынасын өлшеп бола ма? - деген сияқты көптеген сұрақтар туындайды.

Ғылымдардың жаңа салалары болған парапсихология, экстрасенсорика, телекинез және т.б. бағыттары аталған құбылыстарды зерттеп, медицина және басқа салаларда қолданып та келеді.

Сондай ақ "жоғары немесе нәзік материяға" немесе "ғарыштық санаға" арқа сүйейтін, жаңа ғылыми салалар пайда болды [7].

Ғылыми зерттеулерде [29-32] адамдардың пікірі, ойы суға, қоршаған ортаға әсер ететіндігі, сол ортаның өзгертетіндігі және олардың кері әсері анықталған.

Өсімдіктерге радиотолқындармен немесе психологиялық әсер етумен көп өнім алу осы күнде тәжрибетермен толық дәлелденген; дәл осы жолмен академик Аширов бидайдан мол өнім алғандығы шындық.

Аталған сұрақтарға жауап іздеу осы бөлімнің **негізгі мақсаты** болды.

Осы сияқты сауалдар экологтар, биологтар, кибернетиктерді де қызықтырады. Бұл сұрақтарға жауап беруден алдын акад. Ашировтің "Экология сознания" атты кітабына [7] және автордың мақалаларына [73,74] тоқталып, ***"информацияның"*** тірі мүшенің ***жанымен байланысты*** екенін көреміз.

"Жан" ұғымын, қысқа түрде, мүшеде үздіксіз жүріп отыратын көптеген биоэнергетикалық үдерістердің жалпы түрі десе болады.

Ал хабар, ақпарат және т.б. тірі мүшеге сырттан әсер ететін энергия түрлері екенін көреміз. Сонда әсерді тірі дене 5 мүшелерімен (көз, құлақ, ауыз, мұрын және басқа тері мүшелерімен) қабылдайды. Ал алтыншы мүше көбінесе айтылмайды; бұл дененің барлық мүшелерімен, жүйке жүйелерімен қабылданатын толқындар.

Мүше - бұл өте күрделі **кибернетикалық жүйе** болып, әрбір жасуша сол жүйенің элементі болады [25,29]. Ол сыртқы әсерді қабылдап, электро- серпіндерді генерациялайды да, бүтін денеге таратады; әрі сол сияқты сигналдарды жүйке жүйесінен қабылдап, механикалық жұмыстарды да орындайды. Жоғары жүйке жүйесі (ми, жұлын, т.б.) бұл сигналдарды қабылдап, көп жағдайларда "сақтап қояды" және тітіркену жауабын береді.

Сонда әрбір жасушаның өзі де көп функциялық кибернетикалық жүйе болады [7,25,29]. Жасушалар **әртүрлі** болады; **көру мүшелеріндегі** жасушалар **жарық нұр**ларына **тітіркену** ететін болса, ал тері және басқа топтағылар **жылу** және **механикалық әсерлерге** тітіркену береді.

Құлақ мүшелеріндегі жасушалар **төмен жиілікті әсерлер**ге (дыбыстық жиілікке) тітіркену етеді. **Мұрын, ауыз** жасушалары **иіс** пен **дәм** әсерлеріне тітіркену етеді.

Сонымен бірге мүшеде бірнеше үдерістер (зат алмасу, энер-

гоинформациялық үдерістер, жасушалардың үздіксіз өсу, көбею, өлу және с.с.) үздіксіз түрде өтіп жатады.

Сырттан болған әсерлер мүшеде сақталып қалып, ішкі үдерістерді де біршама өзгертеді; мұнда сыртқы үдерістер әсерінің энтропиясын H_0, ал ішкі үдерістер энтропиясын H_1 десек, сонда әсерден кейінгі ішкі энтропия ΔH қа кемейіп, $H_2 = H_1 - \Delta H$ \, яғни $H_2 \langle H_1$ болады. Әсерден алдын: $\Delta H_1 = H_1 - H_0$ болса, әсерден кейін $\Delta H_2 = H_2 - H_0$, $\Delta H_1 \rangle \Delta H_2$ болады; яғни тірі мүшедегі үдерістердің энтропиясы сыртқы әсер энтропиясына "жақындап" барады. Егер осы әсер **ұзақ уақытта тұрақты** болса, онда $\Delta H_2 \to 0, H_2 \to H_0$ болады да, мүше энтропиясы сыртқы ортаның энтропиясына жуықтап барады; яғни: $H_2 \approx H_0$. Бұл үдеріс **бейімделу (**өзін өзі қайта ұйымдастыру- самоорганизация) үдерісі деп аталады да, мұнда ішкі энтропияның кемейуі ΔH сырттан алынған энергия мөлшеріне тең болып, **қалдықты энергияны** немесе "**информацияның көлемін"** береді.

Айта кететін жайт, информация тек энергия көлемімен, яғни энтропиямен өлшеніп қана қоймай, оның бейнесі немесе келбеті немесе құрамы (структурасы) да негізгі қызмет атқарады; бұлар информацияның мағынасын (семантикасын) береді.

Ал ақпараттың көлемдік (синтаксикалық) өлшемінен оның мағыналық өлшемдері қымбаттырақ болады.

Сыртқы әсерді ΔH түрінде сақтап қалып, соған бейімделуі жоғары дәрежеде ұйымдасқан жүйелерде (жануарлар мен адамда) жүйке жүйелерінде "саналы түрде" өте жылдам орындалса, ал төменгі дәрежеде ұйымдасқан жүйелерде (өсімдіктер) жасуша орнында өте баяу орындалады.

Өлі әлемнен **айырмашылығы** – сыртқы әсерден кейін ішкі үдерістер біршама өзгерген түрде өте береді де, сол өзгеру де бірден орындалмайды; яғни әсер тоқтағанда да сол әсер **"естен шықпастан"**, бейімделу одан ары жүре береді. Мұнда атап кететін негізгі нәрсе – тірі мүше жоғары ұйымдасқан түрдегі **инерциялды** жүйе болуы.

Сондықтан, CD-R, CD-RW...де жазылған сигналдар хабар түрінде өзгерместен қала берсе, ал мида немесе басқа тірі жасушада жазылған сигналдар сол мүшеде өтіп жатқан үдерістерге әсер етіп, ондағы бейімделу үдерісін "басқарады"; яғни сигналдар тірі түрдегі энергияға - информацияға айналуы үздіксіз көрінеді.

Қысқасы, **информация –** сыртқы энергетикалық әсерден **тірі мүшенің ішінде** пайда болатын **қалдықты энергетикалық өзгерістер** болып, ол энергияның өлі энергиядан өзгешелігі оның келбеті немесе құрылымына қарай мағынасы да әртүрлі болады және соған байланысты түрде сондағы **бейімделу** үдерісін басқарады; мұнда ішкі үдерістер мағынаға байланысты **өзгерген түрде** жалғаса береді.

Осыдан, "информация" сөзінің "**ин**..." бөлімі **сыртқы әсерден** деген мағынаны білдірсе, ал "**форомация**..." деген бөлімі **өзгерістер** деген мағынаны білдіреді. Бұл энергетикалық өзгерістер биологиялық "жанды" макромолекулаларда (аминоқышқылдар, рибонуклейн немесе дезоксирибонуклейн қышқылдары, және т.б.) өтетін үздіксіз "жанды" биоэнергетикалық үдерістердің көрінісі болады.

Демек, **информация** ұғымы тек қана **тірі жанды биологиялық мүшелерге ғана тән ең негізгі** қасиет болып, мүшеден тыс информацияның ұқсасы – **хабар, ақпарат** қана болады. Информация мүшенің ішінде болғанымен оның сыртына да **өріс** түрінде тарай алады [7]. Сондай екен жанды әлем қай уақытта және қалай басталған деген сұрақ туындайды.

Тірі әлемге саяхат жасау үшін оның келіп шыққан тегі - өлі дүниені қарастырайық; Пифагор заманында атомнан кіші материя жоқ деген болсақ, қазіргі күні материя 0 ден $+\infty$ ке дейін оң материя, ал 0 деп $-\infty$ ке дейін антиматерия барлығы дәлелденген. Мұнда 0 – **физикалық вакуум** болып, **материяның "тыныштық" жағдайын** көрсетсе, ал кері энергиялы позитрон, антикварк сияқты элементтер, галлактиканың ортасынан табылған кері материялы екі "қара тесік" антиматерияның барлығын көрсетеді.

Адамзат санасы ұқсастыққа негізделген болып, мұнда: "...әрбір "заттың" массасы болуы керек...", – дейміз. Алайда әзіргі күнде материяның өлшемі - жалғыз ғана **энергия** екені дәлелденген. Макс Планктің еңбектерінің нәтижесінен мұны көреміз.

Академик Аширов [7] **макроәлем**ді 4-ке: қатты, сұйық, газ және плазма (макроәлемде **бостықта материя жоқ** деп есептеледі) деп бөлсе, ал **микроәлем**ді жаратылыстану тұжырымдамасы 3-ке [6]: **элементар бөлшектер**, **электромагнит өрісі** мен **басқа өрістер** және **физикалық вакуум** деп бөледі. Сондай-ақ [7] **торсиондық өрістер**дің толық зерттелмегені айтылды.

Өткен ғасыр ғылыми жаңалықтарға толы болды [6,25,28,33,35].

Өткен ғасырдың 20 жылдары (1927 ж.) ағылшын ғалымы Поль Дирак электронды зерттей келе, **антиэлектронды** тапты; оның энергиясы жай электрондыкіне **кері** болып шықты. Демек, біз білетін дүниеден басқа кері – **антидүние** бар.

Іле-шала электромагнит өрісі де кванталатындығы анықталды.

Бұл "эфир" туралы ұғымды да өзгертіп жіберді.

Сонда "эфир - бос" болып шықты. Алайда сол кезде жасалған Гейзенбергтің "анықсыздығында" энергияның сақталу заңы қысқа мерзімде бұзылған сияқты болып көрінді; мұнда микробөлшектер вакуумда энергияны өте кіші уақытта эфирден "қарызға" алып, сол бөлшектер өмірінің соңында "қарызды" эфирге қайтарып береді де жойылып кетеді.

Вакуумның орташа энергиясы 0 болып, ол жерде материя "орташа тыныштық" жағдайда "**бар**" болып шықты.

Дирак, Паули, Гейзенберг, кейінгі кезде Фейнман, Швингер, Томонаги және т.б. еңбектерінде қоршаған **материяның "біртұтастығын", яғни физикалық вакуумде** де **материя "үзілмейтіндігін"** дәлелдеді.

Әрқандай элементар бөлшектер адрондардан құралған болса, олар бариондар мен мезондарға; бариондар протон және нейтрондарға, ал олар кварктер мен лептондарға ажыралады.

Мезондар антикварктерге ажыралады [6]; ал өрістер де әртүрлі калибрлі кванттарға бөлінеді. Мұнда өріс кванттары: гравитон, фотон деп бөлінеді.

Нашар әсер етуші кванттар 3 түрлі бозондар құрады.

Ядродағы протон және нейтрондар 3 кварктен құрылған болып, ал кварктер мен лептондар энергетикалық дәрежесіне қарай бөлінеді.

Бозондар нейтрон мен протондарға әсер етуінен, олардағы кварктер дәрежесі өзгеріп тұрады, яғни $d \leftrightarrow u$.

Бұл протондардың нейтрондарға айналуы және керісінше, нейтрондардың протондарға айналуына себеп болады.

Сонымен, микробөлшектер, әртүрлі өрістер мен физикалық вакуум **материяның** әртүрлі **энергетикалық жағдайлары**н көрсетіп, **энергияның өзгеруі материяның түрінің өзгеруіне** әкеледі**.** Мұнда **энергияның сақталу заңы бұзылмайды**.

Өлі дүниенің құрылысы туралы мәліметтен соң жоғарыда аталған жанды әлем қай уақытта және қалай басталған? – деген сұраққа жауап

беру үшін ӨМІР деген ұғымға анықтама берейік! Академик Волкенштейн [6] өмір туралы былай деген: "... **Өмір** бұл **макроскопиялық, гетерогендік, ашық, өте орнықсыз жүйелердің жасау түрі** болып, **өзін қайта құру** және **өзінен көбейу қасиетіне ие** болады…". Мұнда **макроскопиялық** дегені – тірі мүше (бактериялардан бастап) немесе оның ішкі жүйелері (подсистема) көптеген атомдардан немесе молекулалардан құрылған болуы керек; **гетерогендік** – мүше әртүрлі заттардан тұруы керек; **ашықтық** - сыртқы ортамен үздіксіз зат алмасып тұруы керек; **өте орнықсыз жүйе** ғана өзін қайта құра алады.

Өмірдің негізгі таңбасының бірі – **химиялық құрылыстары ұқсас** болып, барлығында ды **оттегі, сутегі, көміртегі, азот, фосфор, күкірт** болады. Барлық **тірі жүйелер шектелген уақытта жасайтын** болып, бұл қасиет олардың **өзінен көбейуін** талап етеді. Осы қасиет олардың түрлерінің өзгеруіне және ортаға сәйкес **бейімделуіне** әкеледі.

Тітіркену – сыртқы энергетикалық немесе информациялық әсерлерге қарсы әсер етеді. **Дискреттік** – өзара байланысты дискрет элементтерден тұрады. **Бүтіндік** – барлық элементтер тек күрделі жүйе бірбүтін болғанда ғана жасайды және істейді. Бұл **анықтаманы** талдай келе **тірі мүше - күрделі кибернетикалық жүйе** екені анық көрінеді [6,7,25, 29].

Қазіргі кезде биологияның 3 концептуалдық дәрежеде көрсе болады: дәстүрлі, физика-химиялық және даму. Бүгінгі күнде теориялық биология қалыптасып, оның негізгі мәселесі – **өмірдің бірыңғай теориясын** жарату болды. Волкенштейн математиканы "жәрдемге шақырған" болса, биологиялық нысаның күрделі кибернетикалық жүйе екенін аңғарған жоқ.

Өткенде к**ибернетиканың бөлімдері** болған жасанды интеллект жүйелері математикалық ойлау жүйесі негізінде құрылған болып, екілік санақ жүйесінде істеген. Ендігіде ол жүйелер анықсыз ойлау жүйесі немесе гибридті нейрожелілер, генетикалық бағдаржолдар негізінде құрылған болып, олардың жұмыс істеу қағидасы адамның миының ойлау қағидасымен бірдей болды [35].

Генетикалық бағдаржолдарды орындауда осы күнгі компьютерлер нәтижелі болмады. Сондықтан да нанотехнология жәрдемінде адам миындағы нейрондарға ұқсас гетероқұрылымды кристалдар құрылып, аталған бағдаржолдарды орындайтын нейрокомпьютердің элементтері жаратылды.

Нейрокомпьютерлер жаратуда көптеген мемлекеттер істеп келе жатыр; осы салада Ресей ғалымы академик Альферов гетероқұрылымды кристалдар жаратып, екі рет Нобель силығына ие болды.

Кибернетиканың негізгі мақсаты - күрделі биологиялық жүйелерді зерттеу және сол сияқты машиналар жарату болды [25,33].

Тірі жүйелердің кибернетикалық жүйе екендігін дәлелдеу үшін олардың **ұйымдастыру құрылымын талдау керек;** бұдан **өмірдің құрылыс дәрежелерінің иерархиясы** анықталып, олар **нақты түрде тәртіптелген** болып шықты.

Тірі құрылымдардың элементі ретінде **жасушалардың** ашылуы осы құрылымдардың **жүйелі** және **бірбүтін** екендігі тірі дүниенің **иерархиялылығын** одан ары дамытуға мүмкіндік берді.

Кибернетикалық жүйелердегідей [6] тірі әлемді бейнелеуде де **құрылымдық дәрежелер тұжырымдамасы** қолданылады; мұнда: төменгі дәреже жоғарғы дәрежеге **бағынышты** түрде болып, бұл дәрежелердің барлығы **бірбүтін жүйені** құрайды. Мұнда құрылымдық дәрежелер өздерінің **күрделілігімен** және **атқаратын жұмысымен** ерекшеленеді.

Тірі материяның ең төменгі дәрежесі – **молекула-генетикалық** дәреже болып, мұнда **өлі** дүниенің **атомдық-молекулалық** дәрежесінен **тірінің макромолекуласына** өтеміз.

Тірі әлем белоктардан тұрса, олар көптеген құрылымдары ұқсас және қайталанушы мономерлер – аминоқышқылдардан құрылған болады. Олардың әрқандай түрде тізбектеліп қосылуынан белок полимерінің нұсқалары пайда болады. Белок құрамында 20 түрлі аминоқышқылдар мономері болуы мүмкін.

Тірімолекулалардың**өзгешелігі**-**молекулалықасимметриялық** (**хиралдық).** Белоктар тірі әлемге жатқанымен оларда **өзінен көбею** немесе **ұрық қуалау** сияқты (***информациялық) қасиеттер*** табылмайды. Ал **бұл қасиеттер** тірі жасушаның ядросындағы ***нуклеин қышқылдарынан*** табылды. Бұл қышқылдар 2 ге: ***рибонуклеин қышқылы*** **- РНК** және ***дезоксирибонуклейн қышқылы*** **– ДНК** деп бөлінеді. ДНК ширатылған екі мономерлік молекулалар тізбегінен тұрады.

ДНК бөлек бөлімдерден тұрып, олар **хромосома** деп аталады; оларда **ген**дер орналасқан. Адам мүшесіндегі жасушада 46 хромосома анықталған [29,30].

Жасушалардың көбею үдерісі – **митоза** зертелгенде ядродағы хромосомалар әрқайсысы тең екіге бөлінеді; сондықтан олардың генетикалық құрамы өзгермейді.

Жасушалар – тірі система болып, мүшенің құрылысын, өмір сүру келбетін және көбеюін қамтамасыз етеді.

Барлық мүшелердің жасушаларының құрылысы, заттық құрамы **ұқсас** келеді. Жасушаларда өтетін көпбағанды күрделі үдерістерді басқаратын құрылым (структура) – ядрода орналасқан **нуклейн қышқылының молекулалары**нан құралған **ұзын тізбектер**.

Даму (эволюция) үдерісінде алғашқы жасушаларда ядро болмаған; бұған бір жасушалы амеба, бактериялар жатады. Алғашқы дәуірде жасушалар екіге: ядросыз – **прокариоттар** және ядролы-**эукариоттарға** бөлінді.

Жердің геологиялық өмірінің басталуына 4 млрд жыл болса, сол дәуірде мүшелердің ең қарапайым түрі – **прокариоттар** пайда болды. Олар ауадан көмір қышқыл газын алып, күн нұрын жұтады. Фотосинтез тітіркенуінен өзіне көміртекті, ал атмосфераға оттегін шығарды.

Оттегі көбейген соң 2,6 млрд жыл бұрын **эукариоттар** пайда болды. Бұл топқа **өсімдіктер, омыртқалы** және **омыртқысыздар** жатады. **Жәндіктер**дің пайда болуына ~ 1800 млн жыл болды. Өмірі шектелгендіктен эукариоттар даму жолмен өте **күрделі органикалық үлгі** құрып, біржасушалы жәндіктерден **көпжасушалы биосистемалар** келіп шықты; бұл өмірдің бифуркациясына (бірден өзгеру түрі) әкелді.

Көпжасушалы өмір басталуымен Жерде өмірдің **әртүрлі үлгілері** жылдам көбейіп кетті де, олардың күрделілігі де асып, көп узамай "**ойлаушы саналы" жүйелер** пайда болды.

Өлі дүние мен тірі дүние аралығында **вирустар** орналасқан. Олар бактериялардан 50 есе кіші (20 дан 300 нанометр).

Жасушадан жоғары дәреже – тоқымалар. **Тоқыма** жасушалардың біртүрлі дәрежеде ұйымдасуынан құрылады. Осы тоқымалардан тірі мүшенің әртүрлі **мүшелері** құрылады.

Мүше дәрежесіне бірге жұмыс атқаратын бірбүтін органдар жүйесі - мүше жатады.

Мүше дәрежесінің алдынғы дәрежеден айырмашылығы – мұнда тірі жүйелердің әртүрлі көптеген жүйелері бар.

Қауымдалу (популяция) – бір түрдегі мүшелер жиыны болып, жалғыз бір **генофонд** жаратады.

Түр бірнеше қ**ауымдалу**дан тұрады. Осы дәрежеде биологиялық даму үдеріс амалға асады.

Биоценоз орынында қауымдалулар қоғамы тарихи тұрақтанған болып, бұл **қауымдалу**лар өзара және қоршаған ортамен зат алмасады.

Биосфералық дәрежеде биоценоздар жиынынан Жердің **биосфера**сы құрылады. Аталған дәрежелердің әрқайсысы бөлек бір ғылымда зерттеледі; мысалы, молекула дәрежесі – **молекулалық биологияда, генетикада**;

жасуша дәрежесі – **цитологияда, микробиологияда**;

тоқымалар, мүшелер дәрежелері – **анатомия, физиологияда;**

мүшелер, популяциялар, түрлер – **зоология, ботаникада**;

биоценоз, биосфера дәрежесі – **экология** ғылымы шұғылданады.

Тірі әлемді экологиялық зерттеуде **экосфераны** күрделі **кибернетикалық жүйе** деп есептеп, оны зерттеуде **системология** немесе **жүйелі әдістер**ді қолдану орынды болады [25,33]; мұнда **макроәдістерді** қолдана отырып, биосфераны зерттеуде ол **страттарға** ажратылады; ең жоғары страт-экосфера болып, мұнда зерттеулермен экология пәндері шұғылданады. Одан төменгі стратта зоология мен ботаника пәндері қ**ауымдалу** мен түрлерді зерттейді; анатомия мен физиология стратында тоқыма мен мүшелер зерттелсе, цитология мен микробиология стратында жасушалар зерттеледі. Молекулалық биология мен генетика стратында тірі әлем молекулалық дәрежеде зерттеледі. Әрбір ғылымда **жүйелік (системалық)** қолданылып, сол ғылым **декомпозиция** әдісімен бөлімдерге бөлінеді және сол бөлімдер бөлек түрде зерттеледі.

Тәжрибелік зерттеу жұмыстарында биология саласында көп жағдайда өлшемдер көлемі кемдігінен нақтылы әдістерді қолдану қолайсыз болады. Өлшемдер саны жеткіліксіз болғандықтан кейбір жағдайда жалғыз ғана бір өлшеммен шешім қабылдауға тура келеді; мұндай жағдайларда **экспертті (сараптау) жүйелер (ЭЖ)** теориясы қолданылады.

Соңғы жылдары жасанды интеллект жүйелері саласында анықсыз ойлау жүйесі немесе гибридті ЭЖ дамып келеді [33,35].

Кибернетиканың негізін қалаған Н. Винер жануарлар мен

машина арасындағы байланысты зерттеп, жануарлардың жүйке жүйесін өте күрделі кері байланысты кибернетикалық жүйе ретінде қарады; мұнда атап кететін негізгі жайт - ***сигналдарды жарататын да, оны қабылдайтын да, жеткізіп беретін де тірі жасушалар*** болды.

Мұндай сигналдармен істейтін жасанды құрылымдар жаратылған болып, олар хабарларды сигналдар арқылы бейнелейді. Ал хабарлар немесе сигналдар тірі мүшенің ішінде оның **тітіркенуіне** байланысты түрде "**информацияға"** айналады; яғни тек **тірі мүше ішінде** ғана "**информация"** пайда болады.

Адам миына ұқсас машина жарату мүмкін бе? Ол тірі мидың қатыстарын толық орындай алады ма?...

Адам миында $\approx 10^{11} \div 10^{12}$ нейрондар болып, әр нейронда 20 дан 10000 $\approx 10^{15} \div 10^{16}$ға дейін дендриттер мен синапстар болады. Ал адам денесіндегі жасушалары ға жетеді [6,29,35]. Мұнда әрбір жасуша үздіксіз өзгеруші күрделі жүйе болып, олардың арасындағы байланыстар да өте күрделі.

Осы күнде гетероқұрылымды элементтерден анықсыз ойлау жүйелі нейрожүйелер және нейрожелілер құрылып, олардың негізінде нейрокомпьютерлер жаратылуда; олардың құрылысы мен істеу қағидасы тірі мүшедегі мидың құрылысы мен жүйке істеу қағидасына өте ұқсас болады.

Күшті дамыған елдерде (АҚШ, Ресей, Китай, Жапония ж.т.б.) өте күшті суперкөмпьютерлер жаратылған болып, миды зерттеу нақты уақытта жүргізіліп отыр.

Осы кезде Қазақстан Президенті Н. Назарбаев Қытаймен келісім шарт түзіп, осы кезде Астанада суперкомпьютерлік орталық ашу үстінде жұмыстар жүргізіліп отыр.

Техникалық информациялық жүйелердің тірі әлемге ұқсас жерлері көп; ең негізгі ұқсас жері – техникалық жүйелерде **иерархиялы** (көп бағанды) **бағынышты байланысты** дәрежелер (страттар) түрінде құрылған болып, жоғарыда айтылғандай информацияның айналымдық сатылары тірі мүшелердегі сияқты. Мысалы, Ғаламтордың OSI протоколындағы 7 дәрежелі құрылысы экосфераның көпбағанды құрылысына ұқсас түрде құрылғандығын анық көрсе болады [34].

Бақылау және емтихан сұрақтары.

1) Қазақстанда осы кездегі жаңа философиялық бағыт қандай?

2) Президент Назарбаевтың “Жасампаз көшбасшылық философиясының” маңызы неде?

3) Ақпарат (“Информация”) және кибернетика ғылымдарының тарихы.

4) “Информация” туралы атақты ғалымдардың философиялық көзқарастары қандай болған?

5) “Информация”-ның өлі дүниедегі энергиядан қандай айырмашылығы бар?

6)“Информация”-ның биологиялық дүниедегі материалдық энергетикалық көріністері.

7) Инфосфераның және ноосфераның қоғам дамуындағы қызметі.

8) Информатика пәні қандай пән қатарына жатады?

9) Кибернетика ғылымдарының табиғатқа байланысы; техносфера мен экосфераның, ноосфераның араларындағы байланыс қандай?

Өзіндік жұмыстар тақырыптары:

1) Президент Н. Назарбаевтың “Жасампаз көшбасшылық философиясы” және оның осы кездегі дүниежүзілік үдерістерге әсері.

2) Өткен замандардағы ақпарат (Информация) туралы философиялық көзқарастар және осы кездегі философиялық көзқарастарды талдау.

3) Ақпараттар теориясының ақпараттық технологияның дамуындағы орны.

4) Ақпараттық технологияның инфосфера және ноосфера құрылысындағы орны.

5) Инфосфера, ноосфера, техносфера және “ғарыштық сана” тісініктерінің арасындағы байланысты талдау.

1.2 Ақпарат түрлері; өлшемдері.

Ақпараттар теориясының негізгі мәселелерінің бірі – ақпараттың көлемі мен сипатын анықтау болады. Ақпараттар теориясында ақпараттың өлшемдерін анықтайтын үш бағыт бар; құрылымдық, санақтық және мағыналық.

Құрылымдық теория ақпараттар массивінің дискретті құрылымын қарастырылады; бұл олардың ақпараттық элементтерін санау немесе ақпараттар массивін қарапайым кодттаумен орындалады. Ақпарттық жүйелердің (байланыс арналарының, жады құрылымдарының және т.б.) мүмкіншілігін анықтау үшін қолданылады.

Санақтық теорияда энтропия түсінігі қолданылады; ол анықсыздық өлшемі ретінде қолданылып, оқиғалар мен хабарлардың ықтималдығын немесе хабарлардың ақпарат сиымдылығын көрсетеді. Ақпараттық жүйелердің қолданылуында олардың санақтық сипаттарын анықтау үшін қолданылады.

Мағыналық теория ақпараттың мақсатқа сай екенін, құндылығын, пайдалылығын көрсетеді. Көбінесе жасанды интеллект жүйелерінде ойлаужүйесі бағадаржолдардың нәтижелілігін анықтауда қолданылады.

Алайда осы күнде ақпарат көзі, арна және ақпарат қабылдаушылардың қасиеттерін де есепке ала отырып, ақпаратты бағалаудың жалпыланған түрлері де пайда болды.

Ақпарат көздері және олар құрған хабарлар да дискретті және үздіксіз деп бөлінеді. Дискретті хабарлар санақты элементтер жиынынан тұрып, олар хабар көзінде уақыт аралығында тізбектелген түрде пайда болады.

Сонда элементтер жиыны хабар көзінің әліпбиі деп аталады; ал элементтері - әріптер деп аталады. Алайда бұл жерде әріп түсінігі жазбадағы әріп түсінігінен анағұрлым кең - әріптер түсінігіне цифрлар және басқада таңбалар кіреді. Әліпбидегі әріптер саны оның көлемі деп аталады.

Дискретті ақпарат көзі шекті уақытта хабарлардың шекті көлемін жаратады. Дискрет хабарлардың типтік көрінісіне кейбр әліпбиде жазылған мәтін, таңбалар тізбегімен берілген сандар жатады.

Үздіксіз хабар берілген уақыт аралығында өзгеруші физикалық шама түрінде болады.

Мұндайда шекті уақыт аралығында хабардың шекті жиынын шығарып алу үшін сигналды дискреттеумен (уақыт аралығында) немесе кванттаумен (деңгей бойынша) амалға асырылады.

1.2.1 Ақпараттың құрылымдық, геометриялық, комбинаторлық, аддитивтік (Хартли), санақтық (Шеннон) түрлері

Ақпараттық құрылымдық өлшемінде ақпараттық кешеннің тек дискрет құрылымы ғана қаралады; ондағы ақпараттық элементтің саны, олардың арасындағы байланыс және олардың қисындастыруы қаралады.

Ақпараттық элемент деп оның ажыралмайтын бөлігі қаралады - яғни кванттар қаралады. Кванттар деп нақты ақпараттық кешендердің дискрет үлгісіндегі ақпарат түсініледі.

Құрылымдық теория ақпараттың геометриялық, комбинаторлық, аддитивтік өлшемдеріне қарай бөлінеді.

Осылардың ішінде ең кең тарағаны – екілік аддитивтік өлшем болған Хартли өлшемі болып, ол ақпараттың көлемін екілік өлшемде – битпен өлшейді.

Геометриялық өлшем.

Геометриялық өлшем түрінде ақпараттың көлемін өлшеу сызықтың ұзындығын өлшеуге немесес осы ақпараттық кешеннің геометриялық үлгісінің ауданы мен көлемін дискрет бірліктер болған кванттарда өлшеуге келтіріледі. Геометриялық өлшемде берілген құрылымдық габаритте ақпараттың потенциалдық, яғни максимал мүмкін болған саны өлшенеді.

Мұны зерттелетін ақпараттық жүйенің ақпараттық сиымдылығы деп атаймыз. Ақпараттық сиымдылық барлық өлшемдер бойынша дискрет мәндердің жиыны түрінде есептеледі. Ақпараттық сиымдылық толық ақпарат массивінде қанша квант барлығын көрсететін сан түрінде көрінеді.

Геометриялық өлшемді тек ақпарат көлемін бағалауға ғана емес, сонымен бірге бөлек хабардағы ақпарат көлемін өлшеу ішін де қолданса болады.

Мысал үшін ақпарат XTN толық кешенімен берілген болсын. Дискретті санақтар әрбір X,T,N оқтары бойынша $\Delta_X, \Delta_T, \Delta_N$ аралықтарында өткізілсін делік. Сонда үздіксіз ақпарат көптеген кванттарға ажыралып, олардың саны әрбір оқ бойынша: $m_X = \frac{X}{\Delta_X}, m_Y = \frac{T}{\Delta_T}, m_N = \frac{N}{\Delta_N}$ болады. Сонда XTN толық кешенінде ақпарат көлемі кванттарда геометриялық әдіспен өлшегенде келесідей болады: $M = m_X m_T m_N$.

Дискреттеу оқтар бойынша біркелкі болмауы да мүмкін; сондай ақ уақыт бойынша да тұрақты болмауы да мүмкін. Онда ақпарат көлемі де күрделі теңдеумен өрнектеледі.

Комбинаторлық өлшем.

Комбинаторлық өлшем ақпаратты ақпарат элементтерінің әртүрлі қисындастыруымен өрнектегенде қолайлы болады; мы-

салы, ақпаратты ұзату арнасымен жібергенде әрбір хабар әрібін әртүрлі комбинациямен таңбаласа болады. Элементтерден әртүрлі қисындастыруын құру хабарды кодтау болып табылады. Мұнда ақпарат саны немесе көлемі элементтер қисындастыруы санымен өлшенеді.

Сонымен ақпараттық кешеннің құрылымдық көлемінің потенциалдық мүмкіншіліктерінің комбинаторлық қасиеттері бағаланады.

Мұнда кешендер әртүрлі элементтерімен болуы мүмкін; сондай ақ олардың арасындағы байланыс немесе позициясы әртүрлі болуы мүмкін.

Егер элементтердің қандай да бір таңбасы басқасынан ерекше болса, онда олар біртүрлі болмайды; мысалы, келбеті, көлемі, түсі ж.т.б.

Барлық таңбалары біртүрлі элементтердің позициясы немесе күйі әртүрлі болғанда, олар әртүрлі болады. Осындайда элементтердің орны бүтін қисындастыруына әсер етеді; мысалы, позициялы санақ жүйесі, бейнелердің жаратылуы және т.б.

Мысалы, бір немесе нөлдің орыны ауысқанда бүтін қисындастыруы өзгереді: 1110 және 0111 немесе 0001 және 1000.

Бірінші жағадйда 0 орын ауыстырып отыр; ал екіншісінде – 1. Бірінші мысалда 14 саны 7 ге, ал екіншісінде - 1 саны 8 ге айналды.

Одан да анық түсінікті мысал болып нүктенің кеңістікте орын ауыстыруымен сурет немесе денелер жасауын айтсақ болады.

Комбинаторикада элементтердің әртүрлі байланыс түрлері қарастырылады.

Әртүрлі **құрамдас жиындар** (**сочетания**) жалпы саны h болып, әрбір жиында l элементтен болғанда, ол жиындар элементер құрамымен ерекшеленеді. Ол жиындардың мүмкін болған саны:

$$Q = \left(\frac{l}{h}\right) = \frac{h!}{l!(h-l)} = \frac{h(h-l)...(h-l+1)}{1\times 2\times 3\times ...\times l}.$$

Әртүрлі құрамдас жиындар элементтері қайталануы да мүмкін; мұнда элемент l рет қайталануы мүмкін. Мұндайда әртүрлі жиындар саны келесідей болады: $Q = \left(\frac{l}{h}\right)_{повтор} = \frac{(h+l-1)!}{l!(h-l)!} = \left(\frac{l}{h+l-1}\right)$.

h элементтерінің **орын ауыстыруы** (**перестановка**). h элементтерінің орын ауыстыруының мүмкін болған саны келесідей: $Q = 1\times 2\times ...\times h = h!$

Егер элементтері қайталанатын болып, мысалы, бір элемент α рет, екінші элемент β рет, үшінші элемент γ рет қайталанатын болса, онда жиындар саны келесідей болады: $Q = \frac{(\alpha + \beta + ... + \gamma)!}{\alpha!\beta!...\gamma!}$.

h элементтерінің әрбір *l* элементтен **қайта орналастыруда (размещения)** әрбір жиын құрамымен және элементерінің тәртібімен ерекшеленеді. Мұнда мүмкін болған жиындар саны келесідей болады: $Q = \left(\frac{l}{h}\right)_{повтор} = h^l$.

Мысалдар қарастырайық. Әртүрлі **құрамдас жиындар** үшін, мысалы, 10 элементтен 0,1,2,3,4,5,6,7,8,9 келесідей жиындар/ құрылымдар/ құраса болады:

$$Q = \frac{10!}{0!(10-0)!} + \frac{10!}{1!(10-1)!} + ... + \frac{10!}{10!(10-10)!} = 1 + 10 + 45 + 120 + 210 + 252 + 210 + 120 + 45 +$$

+10+1=1024 құрылымдар құрса болады.

Осы *h=10* элементтерінің **орын ауыстыруы** (**перестановка**) мынаны береді: құрылымдар болады.

Осы *h=10* элементтен қ**айта орналастыруда (размещения)** потенциалдық ақпарат көлемі: $Q = h! = 1 \times 2 \times ... \times 10 = 3628800$ құрылым болады.

Хартлидің аддитивтік өлшемі.

Ақпараттар теориясында сандар мен кодтар комбинаторикасы маңызды қызмет атқарады. Сандардың тереңдігі *h nен* ұзындығы *l* деген түсініктер ендіреміз. Сандардың тереңдігі *h* деп қабылданған әліпбидегі әртүрлі элементтер (таңбалар) санына айтамыз.

Санның тереңдігі санақ жүйесінің немесе кодтаудың негізіне сәйкес келеді. Бір толық әліпби бір сандық ұяшықты толтырып, оның тереңдігі *h* қа тең болады. Әрбір уақыт мезгілінде *h* мүмкін болған таңбаларден тек біреуі ғана істетіледі. Геометриялық үлгі интерпретациясында таңба орындалуы деп оның ұяшықтан сыртқа қарай шығуын және сыртта көрінуін айтамыз.

Мұнда барлық таңбалар запасы (қоры) ұяшықта болады. Техникада бұл тиісті таңбалы алдына немесе артқа жылжытумен амалға асады.

Санның ұзындығы деп ұяшықтар санына айтамыз; яғни әліпбидің

қайталау санына айтып, ол керекті санды өрнектеуге жетерлі болуы керек.

Санның ұзындығы санақ жүйесенің немесе кодтау жүйесенің орындығына тең болады. Әліпбидердің *l* ұяшықтарынан құрылған бір жиын бір сандық қатарды құрап, бір толық *l* ұзындыққа ие болған санды көрсетуі немесе сақтауы мүмкін. Кейбір N санымен өлшенетін сандарды **сандық өріс** деп атайды.

Сандық қатар түрінде көрсетілетін тереңдігі *h* және ұзындығы *l* болатын сандарды мына теңдеумен көрсетсе болады: $Q = h^l$, яғни қатар сиымдылығы санның ұзындығына экспоненцалды байланысты болады.

Санды қатардың геометриялық үлгісін әртүрлі санақ жүйесінде көрсетсе болады: *h*=1-бірлік, *h*=2 екілік, *h*=10 ондық және шексіз *h*= ∞ санақ жүйесінде көрсету мүмкін.

Код негізі *h* өзгергенде ұяшықтың сыймдылығы өте жылдам экспоненциалды заңмен өседі; мысалы, *h*=1 болғанда әрбір сан қатарында мына сандар болады: 0,1,2,3,...,8,9. Ал *h*=2 болғанда әрбір сан қатарында мына сандар болады: 00,01,02,...,98,99.

Ал *h*=3 болғанда әрбір сан қатарында мына сандар болады*:* 000,001,002,...,998,999.

Осындай ақпараттың жүйенің мүмкін болған істетілу салаларына тоқтайық;

а) Роликті санағыш (счетчик) *l* ролик болып, әрбірінде *h* цифралар болады.

б) Қисындастыруылы коммутатор *l* қосқышы болып, әрбірі *h* тізбекті қосады.

в) компьютер жадысында *l* ұяшығы болып, әрбірі *h* тізбегін қоса алады.

г) *l* дискрет элементтен құралған сурет болып, суреттің әрбір элементі *h* тондық немесе түстік градацияға ие болады.

д) әдеби баспа мәтіннің парағы болып, әр парақта l_1 қатар және әр қатарда l_2 әріп болсын (орта есеппен). Сонда барлығы $l = l_1 \times l_2$ сандық немесе әріптік ұяшықтары болып, әрбірінің тереңдігі *h* болады.

Аталған жағдайдың барлығында жалпы жағдайлар жиыны экспонента бойынша табылады. Бұл жүйелер ақпарат сиымдылығын өлшеуге өте қолайсыз болады. Сондықтан Хартли екілік логарифмдік аддитивті өлшем ендірді; ол ақпараттың

екілік өлшемі болып қысқаша bit – “бит” деп оқылады. Мұнда Q санының өзі емес, оның екілік логарифмі алынады: $I = \log_2 Q = \log_2 h^l = l \log_2 h \ \ bit,$

Мұнда *I* **Хартли бойынша ақпарат өлшемі.**

Егерде санда разядтар саны 1 ге (сан ұзындығы *l*) тең болып, екілік жүйе қабылданған (сан тереңдігі *h* екіге тең) болса және екілік логарифм қабылданған болса, ақпараттың потенциалдық көлемі бір битке тең болады:

$\log_2 2 = 1$ бит.

Бұл қабылданған бағалау жүйесіндегі ақпараттың өлшем бірлігі болады.

Бұл бір элементар оқиғаның болуы немесе болмауын көрсетеді.

Аддитивті өлшемнің қолайлылығы қосындылау мүмкіндігін береді және ақпарат көлемі сан ұзындығы *l*-ге, яғни сандық ұяшықтар санына пропорционал болады..

Ендірілген ақпарат өлшемі екілік таңбалар (0 және 1) санына эквивалентті болады. Мұнда 1 битке бір екілік таңба (0 және 1) сәйкес келеді.

Айталық ондық санақ жүйесінде 1000 саны берілген болсын; мұнда h=10 болады. Дәрежелер саны l=4 болуы керек еді. Алайда берілге жүйеде барлық орында таңбалар ең кіші мәнімен берілген (0 және1). Орындағы таңбаларды максимал түрде алсақ келесідей санға өтеміз: Q=1000 ≈ 999. Сондықтан l=3 деп аламыз. Сонда потенциалды ақпарат саны келесідей табылады:

$I = \log_2 Q = \log_2 h^l = \log_2 10^3 = 3\log_2 10 \approx 10$.

h=2 *деп, l* ді табамыз. $Q = 2^l; \log_2 Q = l \times \log_2 2 = l$.

Осындай болғанда: $l = \log_2 1024 = 10 \approx I$. Бұл дегеніміз екілік санақ жүйесінде осы сан он екілік бірлікпен көрсетіледі, яғни: $Q = 1024 \approx 1023 = 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 1111111111$.

Жуықтап өрнектегенде егер сан бүтін болса сол санды алу керек; ал егер сан бөлшек болса, ең жақын бүтінге жуықтау керек болады.

Егер ақпарат көзі бірнешеу болса, онда ақпараттың жалпы көлемі сол ақпараттарды қосумен табылады, яғни келесідей:

$I(Q_1, Q_2, ..., Q_R) = I(Q_1) + I(Q_2) + ... + I(Q_R)$.

1 Зертханалық жұмыс

Мәселе 1: 1 байтқа неше әріп (таңба) жазса болады және оның информация көлемі қандай болады?

Шешімі: 1 байт 8 бит ке тең. Әріптер саны $Q = 2^8 = 256$ әріп болады. Информация көлемі $l = \log_2 256 = 8bit$ болады.

Мәселе 2: Үздіксіз хабарды дискреттегенде оның әрбір дискреті 1 байтқа жазылады; өлшемдердің анықтығын 2 есе арттыру үшін неше дәреже қосу керек? Шешімі: Өлшемдердің анықтығын 2 есе арттыру үшін 1 бит қосу керек, яғни 9 бит болуы керек.

Мәселе 3: Үздіксіз хабарды дискреттегенде оның әрбір дискреті 2 байтқа жазылады; өлшемдерді 1 байтқа жазғандағыға қарағанда неше есе анықтық артады? Шешімі: $Q_2 = 2^{16} = 65536bit$, $Q_1 = 2^8 = 256bit$; $Q_2 / Q_1 = 65536/256 = 256$ есе артады. Демек ақпарат көлемі 2 есе артқанда, анықтық 256 есе артады.

Мәселе 4: 2048 саны неше бит көлемді ақпаратты береді?

4096 саны ше? 8192 саны ше? 16384 саны ше? 32768 саны ше? 65536 саны ше?

Мәселе 5: 2048 саны мен 16384 сандарын екілік жүйеде жадының қанша көлеміне жазса болады?

Мәселе 6: 32768 саны 16384 санына қарағанда қанша есе көбірек жадыны иеленеді?

Мәселе 7: 32768 саны 65536 санына қарағанда неше есе кем жады иеленеді?

Мәселе 8: Q1=1024,Q2=2048, Q3= 4096 болса, онда осы үш ақпарат көзін қосқанда біріккен ақпарат көзінің ақпарат көлемі қанша болады?

Мәселе 9: Дәрежелер саны *l*=4 *болғанда екілік санақ жүйесінен h*=2 *ондық санақ жүйесіне өткенде h*=10 *ақпарат көлемі неше есеге артады?*

Мәселе 10: Роликті санағышта (счетчик) *l*=9 ролик, әрбірінде *h*=9 цифралар болса, онда осы санағыш нешеге дейін санайды?

Ал егер сол счетчикте *h*=2 цифралар болса ше?

Мәселе 11: Қисындастырулы коммутатор *l*=10 қосқышы болса, әрбірі *h*=2 тібекті қосса, онда коммутатор жалпы неше тізбекті қоса алады?

Мәселе 12: әдеби баспа мәтіннің әр парақында l_1 28 қатар және әр қатарда l_2=70 әріп болсын (орта есеппен). Сонда барлығы $l = l_1 \times l_2$ сандық немесе әріптік ұяшықтары болса, әрбірінің тереңдігі *h*=128 болса, онда жалпы жағдайлар жиыны қанша болады?

1.2.2 Тең ықтималды оқиғалар жүйесінде энтропия өлшемі. Информацияның аддитивтік немесе логарифмдік өлшемі. Хартли теңдеуі.

Көп жағдайда информацияны өлшегенде сызықтық өлшем істетіледі; мысалы, жадының көлемін өлшегенде немесе регистрдің информация сыймдылығын өлшегенде т.с.с. Мұндай жағдайда информацияны өлшеу үшін Хартли мынаны ұсынды; төменде көрсетілгендей куб алайық (кубтың үшінші өлшемі көрсетілмеген);

8-орын	7-орын	6-орын	5-орын	4-орын	3-орын	2-орын	1-орын

Әрбір дәрежеге бір цифра жазылады; мұнда цифраның санақ негізі әртүрлі болуы мүмкін; айталық оны *h* деп таңбалайық. Онда дәрежелер саны *h* болады.

Сонда бір қатарға сиятын информацияның мөлшері *Q* келесідей табылады*:* $Q = h^l$. Мысалы, егер *h*=2 болып, ал дәрежелер саны бір байт болса, барлық таңбалар саны $Q = 2^8 = 256$ таңба болады.

Алайда бұл түрдегі өлшем қолайсыз болды. Сондықтан оның логарифмі алынды. Сонда өлшемдер саны дәрежелер санына тең болып шықты.

Екілік жүйеде дәрежелер саны бит (bit) өлшеміне тең болды; бит-екілік өлшем деген мағынаны білдіреді.

Мысалы, 1000 санын ондық жүйеде былай өрнектесе болады*;* $l = \log_2 Q = \log_2 h^l = \log_2 10^3 = 3\log_2 10 \approx 10$. Ал екілік жүйеде $l = \log_2 1024 = 10 \approx I$ ..

Информацияны өлшеуде сызықтық өлшем өте қолайлы болады; мысалы, бірнеше информация көздеріндегі информацияны қосу үшін; $I(Q_1, Q_2, ..., Q_r) = I(Q_1) + I(Q_2) + ... + I(Q_r)$.

Суреттерді кодтап ұзақ уақытқа сақтау үшін суреттің тік және горизонталь өлшемдерін біле отырып, оның ауданын табамыз; $L_1 L_2$;

оларды дискреттеу қадамдары $\lambda_1 \lambda_2$ берілген болса, онда суреттегі информация мөлшері келесідей болады: $I = \frac{L_1 L_2}{\lambda_1 \lambda_2} \log_2 h$.

Дискрет оқиғалар энтропиясы. $X = \{x_1, x_2, ..., x_m\}$ байланыссыз оқиғалары беріліп, олардың әрбірінің ықтималдықтары вектор түрінде берілсін; яғни $P = \{p_1, p_2, ..., p_m\}$ болсын. Оқиғалар ***байланыссыз*** болғанда энтропия келесідей есептеледі: $H(X) = -\sum_{i=1}^{M} P_i \log P_i$ болады.

Ақпараттар теориясында біріне бірі **байланыссыз немесе қайталанушы** оқиғалардағы ақпараттарды есептеу өте көп жағдайда қолданылады.

Бұған мысалдар көп; мысалы, ұшақ немесе зымыран (ракета) ұшып келеді; оған атылған оқ немесе снарядтың тию ықтималдығы анық және өзгермейтін болсын. Оны құлату үшін неше рет ату керек? Немесе, машинадағы деталдің сенімділігі анық; оның қанша уақыт сенімді істеп тұруын есептеу керек. Осы сияқты көп мысал келтіру мүмкін.

Мұндай жағдайларда **Бернуллидің теңдеуі** ықтималдықтарды есептеуге қолданылады. Ол келесідей: $P_{n,m} = C_n^m P^m q^{n-m}$ болып,

мұнда $C_n^m = \frac{n!}{m!(n-m)!}$.

Мұнда $P_{n,m} = C_n^m P^m q^{n-m}$ ықтималдығы былай оқылады: *n* тәжірибеден *m* рет бір оқиғаның орындалу ықтималдығы. Мысалы, *n* рет оқ атылса, содан *m* рет оқ тию ықтималдығы қандай болады?

Мысал. Монета үш рет тасталады. Сонда гербтің түсу ықтималдығын табу керек болсын.

Гербтің түсу ықтималдығын табу үшін оның бір рет, екі рет, үш рет түсу ықтималдығын табамыз; яғни $C_3^1 = ? C_3^2 = ? C_3^3 = ?$ Жоғарыдағы теңдеуді пайдаланып, $P_3^1 = ? P_3^2 = ? P_3^3 = ?$ тауып, олардың қосындысын аламыз.

Алайда бірге орындалатын оқиғалар теоремасын қолдансақ, онда P=1-q, q=1-p теңдеуға қойсақ, мынаны табамыз; $P_{000} = 1 - q^3$ =1-$\left(\frac{1}{2}\right)^3 = 1 - \frac{1}{8} = \frac{7}{8} = 0{,}875$.

Алайда **Бернулли теңдеуін қолдану** *n* нің **оншалықты үлкен**

болмаған, ***p*-нің оншалықты кіші болмаған** мәндерінде орынды болады.

Ал ***n*-нің өте үлкен**, ***p*-нің өте кіші мәндерінде** Бернулли теңдеуін қолдану **тиімді болмайды**; себебі *n* нің өте үлкен мәндерінде $C_n^m = \frac{n!}{m!(n-m)!}$ теңдеуіндағы әсер, ықпалиалдарды есептеу мүмкін болмайды.

Сондықтан **мұндай жағдайларда Пуассон теңдеуін қолданған жөн** болады. Оқиғалардың ықтималдықтарын тауып болған соң энтропия Шенноның немесе Хартлидің теңдеулерімен есептеледі.

Пуассон теңдеуі: $P_{n,k} = \frac{\lambda^k \bullet e^{-\lambda}}{k!}$, мұнда $\lambda = np$.

1.2.1 Зертханалық жұмыс

Құрылғы 1000 элементтен құралған. Т уақытта элементтің істен шығу ықтималдығы 0,002 тең. Т уақытта 3 элементтің істен шығу ықтималдығын табыңыз?

Шешімі: *n өте үлкен, ал p-нің мәні өте кіші; сондықтан* Пуассон *теңдеуін қолданамыз:*

$$\lambda = 1000 \bullet 0{,}002 = 2;\ P_{n,k} = \frac{\lambda^k \bullet e^{-\lambda}}{k!} = \frac{2^3 \bullet e^{-2}}{3!} = \frac{8 \bullet e^{-2}}{6} = 0{,}180.$$

1.2.2 Зертханалық жұмыс

200 детальдің ішінде 4 жарамсыз болу ықтималдығын табу керек. 1 элементтің жарамсыз болу ықтималдығы 0,01 тең. $P_n(k) = ?$ $P_{200}(4) = ?$

Шешімі: *n өте үлкен, ал p нің мәні өте кіші; сондықтан* Пуассон *теңдеуін қолданамыз:*

$$\lambda = 200 \bullet 0{,}01 = 2;\ P_{n,m} = \frac{\lambda^k \bullet e^{-\lambda}}{k!} = \frac{2^4 \bullet e^{-2}}{4!} = \frac{16 \bullet e^{-2}}{24} = 0{,}09$$

1.2.3 Зертханалық жұмыс

Құрылғы 2000 элементтен құралған. Т уақытта элементтің істен шығу ықтималдығы 0,001 тең. Т уақытта 4 элементтің істен шығу ықтималдығын табыңыз.

Шешімі: *n өте үлкен, ал p- нің мәні өте кіші; сондықтан* Пуассон *теңдеуін қолданамыз:*

$$\lambda = 200 \bullet 0{,}01 = 2;\ \ P_{n,m} = \frac{\lambda^k \bullet e^{-\lambda}}{k!} = \frac{2^4 \bullet e^{-2}}{4!} = \frac{16 \bullet e^{-2}}{24} = 0{,}09$$

1.2.4 Зертханалық жұмыс

300 детальдің ішінде 3 жарамсыз болу ықтималдығын табу керек?

1 элементтің жарамсыз болу ықтималдығы 0,02 тең. $P_n(k) = ?$

$P_{300}(3) = ?$

Шешімі: *n өте үлкен, ал p нің мәні өте кіші; сондықтан* Пуассон *теңдеуін қолданамыз:*

$$\lambda = 300 \bullet 0{,}02 = 6;\ P_{n,k} = \frac{\lambda^k \bullet e^{-\lambda}}{k!} = \frac{6^3 \bullet e^{-6}}{3!} = \frac{216 \bullet e^{-6}}{6} = 0{,}089235$$

1.2.3 Ақпараттың санақтық түрлері. Шеннон теңдеуі.

Ақпараттың санақтық өлшемінде ақпарат кездейсоқ оқиға, мән, кездейсоқ функцияның орнылалуы туралы ақпарат деп қаралып, ал ақпараттың көлемі осы оқиғалардың, мәндердің, қатыстардың априорлық ықтималдықтарына байланысты түрде қаралады.

Сондықтан өте жиі орындалатын оқиғаларда ықтималдық бірге жақын болып, олар туралы ақпаратттың информативтігі кем болады.

Дәл осындай осыған кері оқиғалар, яғни ықтималдығы өте кем оқиғалар туралы ақпараттың да информативтігі кем болады.

Оқиға және антиоқиға екілік оқиғалар тобын құрайды; оқиғаның орнылалу ықтималдығын p=1 деп таңбаласақ, ал орындалмауын p=0 деп таңбалаймыз.

Антиоқиғаны q деп таңбаласақ, оқиға мен антиоқиғаның арасындағы қарама-қарсы қатынас былай таңбаланады: p=1-q, яғни әрқашанда $p+q$=1 болады.

Осы қарама-қарсы оқиғалардың әрқайсысының ықтималдығы 0,5 болғандағы яғни $p=q$=0,5, оқиғаның орындалуының анықсыздығы максимал дәрежеде болып, мұндай жағдайда алынған ақпараттың информативтігі де максимал дәрежеде көп болады. Бір тәжрибенің бірнеше нәтижесі болуы мүмкін болса,

осы нәтижелер жиынын **оқиғалар ансамблі** немесе **оқиғалардың толық тобы** деп атаймыз. Мұнда оқиғалар ансамблінің немесе оқиғалардың толық тобы ықтималдықтарының қосындысы әрқашанда 1 ге тең болады, яғни: $p_1 + p_2 + ... + p_k = 1$.

Үздіксіз кездейсоқ Х шамасын өлшегенде оның әрбір мәні **элементар оқиға** деп қаралады. Жалпы алғанда $x_1, x_2, ..., x_k$ оқиғалар жиынын қандайда бір физикалық жүйенің *к* мүмкін болған дискрет жағдайы деп, немесе өлшенетін шаманың *к*- мәні деп, немесе ретеуіш органның *к* - жағдайы деп, өндірістік құрылғының элементтерінің *к* - жағдайы деп ж.с.с.ларды түсіну керек болады.

Төменде кестеде ансамбльдің сұлбасы келтірілген.

Тәжрибе нәтижелері	A_1	A_2	.....	A_k
Өлшенетін шаманың мәндері	x_1	x_2	....	x_k
Мәндердің ықтималдығы	p_1	p_2	....	p_k

Әдетте бұл оқиғалар бір уақытта орындалмайды, яғни сол оқиғалардың бір мезетте жалғызы ғана орындалады. Олар толық (генералды) топты құрап, мұнда мына шарт орындалады:

$$\sum_{i=1}^{k} p(x_i) = p(x_1) + p(x_2) + ... + p(x_k) = 1.$$

Жалпы жағдайда ықтималдықтар тұрақты болмайды. Олар уақыт аралығында шарттарға және жағдайларға байланысты өзгеруі де мүмкін.

Сонда олардың санақтық сипаттамалары (дисперсия, орташа мәні) да өзгеруші шамалар болады. Осылармен анықталатын үдерістер де тұрақты болмайды.

Әртүрлі ықтималды оқиғалар жүйесінде энтропияны өлшеу. Ақпараттың санақтық өлшемі. Шеннон теңдеуі.

Логарифмнің негізі 2 болғандықтан, анықсыздықтың өлшем бірлігі келесідей болады:

$H_1 = \log_2 2 = 1$ bit. Информация өлшемі мен энтропия өлшемдері біртүрлі болады. Жоғарыдағылардан $H(\alpha) = \log_2 K$.

Тәжрибе нәтижесі	A_1	A_2	A_3	...	A_k	$\sum$
ықтималдықтары	$\frac{1}{k}$	$\frac{1}{k}$	$\frac{1}{k}$	...	$\frac{1}{k}$	1

Әрбір тәжрибенің энтропиясы: $H(\alpha)=\frac{1}{k}\log_2 k=-\frac{1}{k}\log_2\frac{1}{k}$.

Оқиғалар байланыссыз болғанда энтропия келесідей есептеледі:

$H(X)=-\sum_{i=1}^{M}P_i\log P_i$ болады.

Егер ықтималдықтар өзара тең болса, онда олардың қосындысы

$$H(X)=-\sum_{i=1}^{M}P_i\log P_i=\log M$$

Яғни мұндай жағдайда энтропия максимал болады және Хартлидің теңдеуі шығады.

Осы теңдеуден мынаны тапса болады: $H(X)=M\left[-\log P\,(X)\right]$, яғни оқиғалар ықтималдығының математикалық күтіліміне тең болады.

Үш шекті сұлба ,

$$\left\|\begin{matrix}X\\P\end{matrix}\right\|=\left\|\begin{matrix}x_1,x_2\\p_1,p_2\end{matrix}\right\|,\ \left\|\begin{matrix}Y\\Q\end{matrix}\right\|=\left\|\begin{matrix}y_1,y_2,y_3\\ \\ \frac{q_1}{p_k}\frac{q_2}{p_k}\cdots\frac{q_n}{p_k}\end{matrix}\right\|,\ \left\|\begin{matrix}Z\\S\end{matrix}\right\|=\left\|\begin{matrix}x_1,x_2,...,x_{k-1},y_1,y_2,...,y_n\\p_1,p_2,...,p_{k-1},q_1,q_2,...,q_n\end{matrix}\right\|$$

берілген болса, олардың энтропиялары аддитивті болуы үшін олардың энтропиялары үшін келесідей теңдік орындалуы керек: $H(Z)=H(x)+p_kH(y)$.

Мұнда $p_k=\sum_{j=1}^{n}q_j$, ал элемент $x_k\equiv Y$ дискретті ақпарат көзі деп қаралады.

Сонда $\left\|\begin{matrix} Y \\ Q \end{matrix}\right\| = \left\|\begin{matrix} y_1, y_2, y_3 \\ q_1, q_2, ..., q_n \end{matrix}\right\|$ болғандықтан, шекті сұлба алу үшін әрбір q_i -ді p_k -ға бөлеміз; сонда $\sum_{j=1}^{n} \frac{q_i}{p_k} = 1$ болады, яғни шекті сұлба алынады; сондықтан $H(y) = -\sum_{j=1}^{n} \frac{q_j}{p_k} \log \frac{q_j}{p_k}$ болады.

1.3 Зертханалық жұмыс

Мәселе 1: Дискретті ақпарат көзі М элементті шекті әліпбиден тұрады; оның элементтері $x_1, x_2, ..., x_m$ болып, олардың ықтималдықтары $P(x_1), P(x_2), ..., P(x_m)$.

Бұларды матрица түрінде көрсетсе болады: $\left\|\begin{matrix} X \\ P \end{matrix}\right\| = \left\|\begin{matrix} x_1, x_2, ..., x_M \\ P_1, P_2, ..., P_M \end{matrix}\right\|$;

бұл кейде шекті сұлба (схема) деп аталады.

Осы ақпарат көзінің информация сыймдылығы қалай табылады?

Мәселе 2: Екі ақпарат көзі берілген**:** $\left\|\begin{matrix} X \\ P \end{matrix}\right\| = \left\|\begin{matrix} x_1, x_2 \\ P_1, P_2 \end{matrix}\right\|$, $\left\|\begin{matrix} Y \\ Q \end{matrix}\right\| = \left\|\begin{matrix} y_1, y_2, y_3 \\ q_1, q_2, q_3 \end{matrix}\right\|$, келесідей жағдайда : $P_1 = P_2$ және $q_1 = q_2 = q_3$ болғанда қайсы көздің информация сиымдылығы артық болады?

Мәселе 3: Дискретті ақпарат көзі матрицамен берілген:

$\left\|\begin{matrix} X \\ P \end{matrix}\right\| = \left\|\begin{matrix} x_1, ...x_2, ...x_3 \\ 1/5, 4/15, 8/15 \end{matrix}\right\|$ оның орташа энтропиясын есептеңдер және төмендегі шекті сұлбалардың энтропиларымен салыстырыңдар; мұнда энтропиялардың аддитивтілігіне көз жеткізіңіздер.

$$\left\|\begin{matrix} x_1, ...x_2 + x_3 \\ 1/5, ...4/5 \end{matrix}\right\|; \left\|\begin{matrix} \frac{x_2}{x_2 + x_3}, \frac{x_3}{x_2 + x_3} \\ q_1 ..... q_2 \end{matrix}\right\|;$$

Бірінші матрицаның екінші және үшінші элементтерінің қосындысы екінші матрицаның екінші элементіне тең.

Мәселе 4: $\left\|\begin{matrix} x_1,.....x_2 \\ 1/5,....4/5 \end{matrix}\right\|$ берілген болса, оның оң жақтағы элементін екіге бөліп жазайық $\left\|\begin{matrix} X \\ P \end{matrix}\right\| = \left\|\begin{matrix} .x_2,.....x_3 \\ 4/15,8/15 \end{matrix}\right\| \to \left\|\begin{matrix} Y \\ P \end{matrix}\right\| = \left\|\begin{matrix} .y_1,.....y_2 \\ 4/15,8/15 \end{matrix}\right\|$. Алайда бұл матрица шекті сұлба емес, себебі ықтималдар қосындысы 1 ге тең емес. Оны бірге теңестіру үшін әрбір элементті 4/5 ке бөлу керек; сонда келесідей шекті сұлба аламыз: $\left\|\begin{matrix} Y \\ P \end{matrix}\right\| = \left\|\begin{matrix} .y_1,.....y_2 \\ 1/3,2/3 \end{matrix}\right\|$. Олардың жиындысы ретінде мына матрицаны алса болады. $\left\|\begin{matrix} Z \\ S \end{matrix}\right\| = \left\|\begin{matrix} x_1,.....y_1,.....y_2 \\ 1/5,4/15,8/15 \end{matrix}\right\|$.

Сонда энтропияның адитивтік шарты орындалады, яғни ақырғы сұлба үшін мына шарт орындалады: $H(Z) = H(x) + p_k H(y)$.

Мәселе 5: Мына үш шекті сұлбалардың энтропияларын есептеңдер: $\left\|\begin{matrix} Y \\ P \end{matrix}\right\| = \left\|\begin{matrix} .y_1,.....y_2 \\ 4/15,8/15 \end{matrix}\right\|$

$\left\|1/256..255/256\right\|; \left\|1/2...1/2\right\|; \left\|7/16...9/16\right\|$. Осында энтропиялардың үздіксіздігін көрсетіңдер.

Мәселе 6: Екі ақпарат көзі берілген. Олардың әрбірі ұзындығы 15 элементке тең келесідей хабар шығарады: 021202120212021 және 012101201101201. Мұнда әр элементтің орташа саны өзгермейді. Қай көздің элементі орта есеппен көбірек ақпарат береді?

Мәселе 7: Келесідей ақпарат көзі берілген болып, ондағы энтропияның аддитивтік қасиетін тексеру керек?

$\left\|\begin{matrix} X \\ P \end{matrix}\right\| = \left\|\begin{matrix} x_1.....x_2.....x_3.....x_4 \\ 1/2.\ 1/4.\ 1/8.\ 1/8 \end{matrix}\right\|$. Осы матрицаның үшінші және төртінші элементтерін қосып, мынаны аламыз: $\left\|\begin{matrix} X \\ P \end{matrix}\right\| = \left\|\begin{matrix} x_1.....x_2.....x_3 + x_4 \\ 1/2...1/4.....1/4 \end{matrix}\right\|$.

Ал бұл матрицаның ақырғы элементтерін қосып, мынаны алса болады: $\left\|\begin{matrix} X \\ P \end{matrix}\right\| = \left\|\begin{matrix} x_1.....x_2 + x_3 + x_4 \\ 1/2.....1/2 \end{matrix}\right\|$.

Мәселе 8: X және Y әліпбилерінің элементтері санақтық бай-

ланысты. H(x)=8 bit, H(y)=12 bit. H(x/y) максимал мүмкін болған шегараларда өзгергенде H(y/x) шартты энтропиясы қай шегарада өзгереді?

1.2.4 Энтропия түсінігі; қасиеттері

Әрбір ситуацияны сипаттайтын сипаттама **энтропия** деп аталады.

Энтропия түсінігі грек тілінен **эн-тропе - айналым** деген мағынаны білдіріп, көптеген бірқатар білім салаларына таралды.

Термодинамикада энтропия заттың жылулық күйінің ықтималдығын көрсетеді, ал математикада - ситуацияның немесе мәселенің анықсыздық жағдайын көрсетеді. Ал Информатикада - ол ақпарат көзінің информативтігін немесе информация шығарып беру қасиетін көрсетеді.

Бұл аталған түсініктердің барлығы да біріне-бірі жақын болып, жалпы айтқанда жағдайлардың күтілмегендік дәрежесін көсетеді.

Больцманның екінші термодинамика заңы бойынша тұйықталған кеңістіктің энтропиясы келесідей болады: $H = -\frac{1}{N}\sum_{i=1}^{k} n_i \ln \frac{n_i}{N}$, мұнда N- осы кеңістіктегі молекулалар саны, n_i - мына жылдамдықтардағы $v_i + \Delta v$ молекулалар саны.

Алайда $\frac{n_i}{N} = p_i$ болғандықтан келесідей жазса болады:

$$H = -\sum_{i=1}^{k} p_i \ln p_i .$$

Натуралды логарифмнен екілік логарифмге өту үшін мына теңдікті қолданса болады: $\log_2 M = 1{,}44$. Сондықтан:

$$H = -1{,}44 \sum_{i=1}^{k} p_i \log_2 p_i .$$

Сонымен, логарифмдердің негізі әртүрлі болғанда тек қосынды таңбасының алдындағы еселік қана өзгереді. Осы жерде айта кететін нәрсе әрқашанда теориялық деңгейде шексіз анық (идеал) сипаттамалар бола бермейді; бастапқы шарттар мен параметрлердің өзгерместігі немесе тұрақтығы.

Амалда әрқашанда бірер нәрсе өзгереді; егер жағдай параметрі өзгермесе, уақыт пен орынның өзгеруі жаңа ақпарат әкеледі. Ал егерде ақпарат көзінде барлығы өзгермеген жағдайда ақпарат

қабылдаушы субьекттің өзі өзеруі мүмкін болады. Сондықтан амалда барлық әсер, ықпалдарды (факторларды) есепке алу керек болады; не, қашан, кім, кімге, не үшін, қалай, т.с.с.лардың барлығын есепке алу керек болады. Сондай-ақ ақпараттың түрін, уақытын, жіберушіні, қабылдаушыны, қолдану шарттарын және т.б. барлық өзгерістерді есепке алу керек.

1.2.5 Оқиғалар ансамблінің энтропиясы; шартсыз, шартты, өзара байланысты оқиғалар энтропиясы.

Оқиғалардың толық группасы **ансамбль** деп аталады; басқаша айтқанда олар бірге орындалатын оқиғалар өрісін құрап, олардың ықтималдықтарының таралу заңы анық болады және ықтималдықтарының **қосындысы бірге тең** болады.

Осы жерде оқиғалардың шекті жиыны назарда тұтылады; сондай ақ күйлердің, мәндердің, жағдайлардың ж.т.б.дың шекті жиыны назарда тұтылады.

Ансамблдің энтропиясы оның анықсыздылығының сандық өлшемі болып, оның информативтігін көрсетеді. К.Э.Шеннон санақтық ақпараттар теориясын немесе байланыстар теориясын 1947-48 жылдары ұсынды; мұнда энтропия сандық жағынан көптеген оқиғалардың тәжрибелерінің ықтималдықтарына байланысты функцияның орташасы деп түсініледі.

Айталық тәжрибенің барлық мүмкін болған нәтижелері N болсын; соның ішінде *к*- сы әртүрлі болсын. Соның ішінде *i* тәжрибесі n_i рет қайталансын және оның қосқан информациясының көлемі I_i деп бағалансын. Онда бір тәжрибеден алынған информация көлемі келесідей болады: $I_{ср} = \dfrac{n_1 I_1 + n_2 I_2 + ... + n_k I_k}{N}$.

Сонда әрбір оқиғадан кейінгі алынған информация оның ықтималдығына p_i байланысты болады және оның екілік логарифмімен өлшенеді: $I_i = \log_2 \dfrac{1}{p_i} = -\log_2 p_i$ болады.

Онда орташа ақпарат былай өлшенеді:

$$I_{ср} = \frac{n_1(-\log_2 p_i) + n_2(-\log_2 p_i) + ... + n_k(-\log_2 p_i)}{N}.$$

Осы өрнекті келесідей таңбалаймыз:

$$\frac{n_i}{N} = p_i,\ I_{cp} = \frac{n_1(-\log_2 p_i) + n_2(-\log_2 p_i) + ... + n_k(-\log_2 p_i)}{N}.$$

$$I_{cp} = p_i(-\log_2 p_i) + p_2(-\log_2 p_i) + ... + p_k(-\log_2 p_k) = -\sum_{i=1}^{k} p_i \log_2 p_i.$$

Ақырғы өрнек энтропия деп аталып, *H* әрпімен таңбаланады және екілік санақ жүйесінде битпен өлшенеді; яғни $H = -\sum_{i=1} p_i \log_2 p_i.$

Осында логарифмнің негізі **энтропияны** немесе **информацияның** өлшеу бірлігін көрсетеді. Егер логарифмнің негізі екіге тең болса, онда энтропия өлшемі бит болады. Көбінесе екілік бағдаржол қолданылады; себебі ол ақпаратты битпен өлшейді; екілік ойлау жүйесімен жақсы келіседі, екілік кодтаумен және екілік релелік техникамен де жақсы үйлеседі.

Энтропия бір хабарға тура келетін немесе өлшенетін *X* шамасының ақпарат көлемі *I* дің математикалық күтілімі деп анықталуы мүмкін:

$$H(X) = M[I(X)] = -\sum_{i=1}^{k} p_i \log_2 p_i.$$

Мұндағы *H(p)* теңдеуі $\boldsymbol{p}=(p_1, p_2, ..., p_k)$- нәтижелер ықтималдығының векторы, мына төмендегі шарттарға жауап береді:

1) ***H(p)*** $0 \le p_i \le 1$ аралығында үздіксіз болады, яғни ***p-*** ның азғана өзгеруінде Н шамасы аз өзгереді.

2) ***H(p)*** ***p*** ға салыстырғанда симметриялы болады, яғни p_i аргументтерін қалағанша орын ауыстырғанда өзгермейді.

3) $H(p_1, p_2, ..., p_{k-1}, q_1, q_2) = H(p_1, p_2, ..., p_k) + p_k \times H(q_1 / p_k, q_2 / p_k),$

4) яғни x_k оқиғасы екі $x_k^{'}, x_k^{''}$ оқиғаларынан құралған болса және олардың ықтималдықтары $q_1, q_2, q_1 + q_2 = p_k$ болса, онда жалпы энтропия екі энтропияның қосындысына тең болып, біріншісі - ажыралмаған жүйенің энтропиясына, ал екіншісі - ажыралған бөлімінің шартты q_1 / p_k, q_2 / p_k ықтималдықтарының p_k салмағымен алынған шартты энтропиясына тең болады.

Мұны ***энтропияның аддитивтік қасиеті*** деп атайды.

5) Егер $n<m$ болса, онда $F(n) < F(m)$ болады, мұнда $F(n)=H(1/n, 1/n, \ldots, 1/n)$, $F(m)=H(1/m, 1/m, \ldots, 1/m)$; яғни $F(n)$ теңдеуі қатаң түрде өседі.

Шеннон өлшемін Хартли өлшемінің тең емес ықтималдықты

оқиғалар үшін құрылған жалпыламасы деп қараса болады.

Ол ақпарат көзінің санақтық сипаттамасын есепке алуына мүмкіндік береді.

Осы қасиеттерден келесідей леммаларды дәлелдеусіз келтіреміз;

Лемма 1. $H(1,0)=0$.

Лемма 2. $H(P_1,P_2,...,P_n,0)=H(P_1,...,P_n)$.

Лемма 3.

$$H(P_1,...,P_{n-1},q_1,...,q_n)=H(P_1,...,P_n)+P_n*H\left(\frac{q_1}{P_n},...,\frac{q_m}{P_n}\right);P_n=q_1+...+q_m>0.$$

Лемма 4.

$$H(q_{11},q_{12},...,q_{1m};q_{21},...,q_{2m};...;q_{n1},...,q_{nm})=H(P_1,...,P_n)+\sum_{i=1}^{n}P_i*$$

$$*H\left(\frac{q_{i1}}{P_i},...,\frac{q_{im}}{P_i}\right);P_i=q_{i1}+q_{i2}+...+q_{im},i=1,2,...,n.$$

Лемма 5. $F(m\times n)=F(m)+F(n)$.

Сондай ақ:

$$H\left(\frac{1}{mn_i},...,\frac{1}{mn_i}\right)=H\left(\frac{1}{n},...,\frac{1}{n}\right)+H\left(\frac{1}{m},...,\frac{1}{m}\right).$$

Лемма 6. $F(n^m)=m*F(n)$.

Лемма 7. $F(n)=\log_b n$, *в* – кез келген константа.

Энтропияның кейбір қасиеттері:

1. Энтропия нақты және кері емес шама болады*; себебі кезкелген* p_i $(0\le p_i\le N)$ *үшін* 0 *мен* 1 *аралығында өзгереді;*

ал $\log p_i$ *кері болғандықтан, -* $p_i \log_2 p_i$ *оң болады.*

2. ***Энтропия - шегараланған шама.*** *-* $p_i \log_2 p_i$ *қосылғышы үшін* $0\le p_i\le 1$ *ауқымында шегаралануы анық көрініп тұр.* $p_i \log_2 p_i$ *ның шегі* $p_i \to 0$ *да Лопитал заңы бойынша* 0 *ге тең болады.*

3. ***Энтропия нөлге тең болады, егер күйлер ықтималдықтарының бірі 1- ге тең болса.***

4. ***Энтропия максимал болады, егер ақпарат көзінің барлық күйлерінің ықтималдықтары тең болса;*** *бұл Лагранждың анықсыз көбейткіштер әдісімен дәлелденеді.*

5. *и* ***ақпарат көзі*** u_1, u_2 ***күйлерімен берілген болса, оның энтропиясы*** *0* ***және*** 1 ***аралығында өзгеріп, ол күйлердің ықтималдықтары өзара тең болғанда өзінің максимал дәрежесіне жетеді:*** $p(u_1) = p(u_2) = 0{,}5$.

6. ***Бірнеше өзара санақтық байланыста болмаған ақпарат көздерінің біріккендегі энтропиясы сол ақпарат көздерінің энтропияларының қосындысына тең болады.***

7. ***Энтропия деп ансамблден бірер күйді таңдап алудағы анықсыздыққа айтамыз.***

Энтропия тек қана дискрет ақпарат көзін ғана емес, сондай ақ үздіксіз ақпарат көздерін де сипаттай алады; мұндай ақпарат көзі үшін энтропияны **дифференциалды** деп атайды.

$$H(U) = \int_{-\infty}^{\infty} p(u)\log p(u)du - \lim_{\Delta u \to 0} \log \Delta u \,.$$ Оң жақтағы шама Δu кванттау қадамы болып, ол шама $\Delta u \to 0$ ұмтылғанда шексіздікке ұмтылады; бұл дегені таңдау ықтималдығы немесе *H(U)* да шексіз көп болады дегенді білдіреді.

Ал оң жақтағы бірінші мүше шекті мәнге ие болып, тек *U* дың таралу заңдылығына байланысты болады.

Өлшеулер теориясында **эпсилон-энтропия** түсінігі кең қолданылады; ол өлшеу үдерісіндегі қателіктің есебінен хабар энтропиясының кемейуін көрсетеді. Айталық *Y (өлшеу нәтижесі)* нысанның шын шамасының мәні X туралы алынған ақпарат шамасы болсын. Сонда өлшем қателігі мына шарттқа жауап беруі керек:

$\left(\overline{Y - X}\right)^2 \le \xi^2$ Мұнда минимум $p_x(x/y)$ тің барлық таралу заңдары бойынша ізделуі керек. Сонымен, анықтама бойынша:

$$H_\xi(x) = \min_{p_x(x/y)} \left[H(x)\right] - H(x/y) \,.$$

Осы теңдеуді толық жазғанда келесідей болады: $H_\xi(x) = \min_{p_x(x/y)} \iint p_X(x,y)\log \frac{p_X(x,y)}{p_X(x)p_Y(y)}dxdy$. Қалыпты сандар үшін оңай есептеледі.

1.4 Зертханалық жұмыс

Мәселе 1.

$\left\|\begin{matrix} X \\ P \end{matrix}\right\| = \left\|\begin{matrix} x_1, x_2, ..., x_M \\ P_1, P_2, ..., P_M \end{matrix}\right\|$ ансамблінде $P_2 = 1$ болса, осы жүйенің эн тропиясы неге тең болады?

3-қасиетке байланысты, егер күйлер дің бірінің ықтималдығы 1 ге тең болса, онда жүйенің энтропиясы нөлге тең болады. Мұны есептеп дәлеледесе болады.

Мәселе 2.

$\left\|\begin{matrix} X \\ P \end{matrix}\right\| = \left\|\begin{matrix} x_1, x_2, ..., x_M \\ P_1, P_2, ..., P_M \end{matrix}\right\|$ жүйеде $P_1 = P_2 = ... = P_M$ болса, энтропиясы 4- және 5- қасиеттерге байланысты максимал болады.

Мұны дәлелдеу үшін, $P_1 = P_2 = 0{,}5$ деп алып, энтропияны есептейік.

Кейін $P_1 = 0{,}1$ $P_2 = 0{,}9$ деп энтропияны есептейік. Және ықтималдықтарды өзара тең болмаған түрлі жағдайлардыа энтропияны есептейік. Сонда байқайтынымыз, оқиғалардың ықтималдықтары өзара жақындаған сайын жүйенің энтропиясы арта береді және олар өзара тең болған жағдайда энтропия максимал шамаға жетеді. Керісінше, ықтималдықтары бірінен бірі қаншалықты алшақтау болса, соншалықты энтропия кем болады.

Мәселе 3.

Өзара байланысты болмаған ақпарат көздері берілген; олардың біріншісінің энтропиясы $H_1 = 9bit$, ал екіншісінікі $H_2 = 12bit$ . . Сол ақпарат көздерінің біріккендегі энтропиясы қандай болады?

Шешімі: 6-қасиетке байланысты сол ақпарат көздерінің энтропияларының қосындысына тең болады; яғни $H = H_1 + H_2 = 9 + 12 = 21bit$ болады.

Мәселе 4.

Екі ақпарат көзі берілген болып, олардың ықтималдықтары келесідей болсын: $P_1 = 0{,}1$ $P_2 = 0{,}9$. Оқиға орындалғанда бірінші оқиға орындалды. Сонда алынған информация қандай болады?

Шешімі: 7- қасиет бойынша оқиға орындалған соң энтропия апостериорлы деп аталады. Ал оқиға орындалмағандағы энтропия априорлы деп аталады. Сонда алынған информация априорлы энтропиядан апостериорлы энтропияның айырмасына тең болады.; яғни $I = H_{aprior} - H_{apocter} = -0{,}1\log 0{,}1 - 0{,}9\log 0{,}9 - 0{,}1\log 0{,}1 = -0{,}9\log 0{,}9.$

Ал егер екінші оқиға орындалса, алынған информация мыныдай болады:

$$I = H_{aprior} - H_{apocter} = -0{,}1\log 0{,}1 - 0{,}9\log 0{,}9 - 0{,}9\log 0{,}9 = -0{,}1\log 0{,}1.$$

Осыны талдай отырып, келесідей қорытынды жасаса болады: ықтималдығы кем оқиға орындалғанда ықтималдығы көп оқиға орындалғанға қарағанда көбірек информация алынады.

Мәселе 5.

$H(x) = -\sum_{i=1}^{M} p_i \log p_i$ теңдеуі $p_1, p_2, ..., p_M$ мәндеріне қарағанда симметриялы және үздіксіз екенін көрсетіңдер. Графигін сызыңдар.

Мәселе 6: Энтропияның үздіксіз және симметриялы екенін тексеру үшін мына $H(X) = P_i \log P_i$ функцияның графигін сызыңдар; мұнда ықтималдық 0 ден 1 ге дейін 0,05 қадаммен өзгерсін.

Мәселе 7: Келесідей жүйе берілсін: $\begin{Vmatrix} X \\ P_i \end{Vmatrix} = \begin{Vmatrix} x_1 ... x_2 ... x_3 \\ 1 .... 0 .... 0 \end{Vmatrix}$; яғни оның бір жағдайы анық берілген болсын. Сонда энтропияны есептеңдер.

Мәселе 8: Жүйе өзінің төрт жағдайымен берілген болсын; бірақ ол жағдайлар әртүрлі таралу заңымен берілген. Сонда қайсы таралу заңында энтропия максимал болады?

Жүйенің нөмірі	1-жағдайын. ықтималд.	2-жағдайын. ықтималдығы	3-жағдайын. ықтималдығы	4-жағдайын. ықтималдығы
1-жүйе	0,5	0,2	0,25	0,05
2-жүйе	0,25	0,25	0,25	0,25
3-жүйе	0,2	0,3	0,25	0,22

1.2.6 Энтропияны қосу ережесі, информацияның көлемін өлшеу; Тәуелді және тәуелсіз оқиғалар энтропиясы.

Энтропия - анықсыздық дәрежесі деп түсіну керек.

Анықсыздық дәрежесін функция ретінде қарап, оны анықтайық. Жоғарыда қаралған мысалға қайтайық. Дискрет оқиғалар энтропиясы. $X = \{x_1, x_2, ..., x_m\}$ байланыссыз оқиғалар жүйесі түрінде

беріліп, олардың әрбірінің ықтималдықтары вектор түрінде берілсін; $P = \{p_1, p_2, ..., p_m\}$ болсын.

1. Егер m=1 болғанда, анықсыздық жоқ болады; яғни оқиға алдынан мәлім болады. m нің мәні артқан сайын, энтропия да арта түседі.

2. Энтропияны $f(m)$ деп таңбалап, екі өзара байланыссыз оқиғалар α және β ны қарастырайық; олардың орындалу сандары k және l болсын.

Осы екі оқиға бөлек орындалса, онда олардың жеке алғандағы энтропиялары сол оқиғалардың бірге $\alpha\ \beta$ орындалғандағы энтропиясынан кем болады.

Мұнда сол оқиғалардың бірге өткізілгендегі энтропиясы олардың жеке өткізілгендегі энтропияларының қосындысына тең болады; $f(\alpha\ \beta)=f(\alpha)+f(\beta)$; $f(kl)=f(k)+f(l)$; бұл энтропияны қосу ережесі.

3. Егер $k>l$ болса, онда $f(k)>f(l)$ болады. Ақырғы екі ереже логарифмдердің қасиетінен шығады; яғни көбейтіндінің логарифмі олардың логарифмдерінің қосындысына тең болса, үлкен санның логарифмі де үлкен болады деген ережелерден.

Логарифмнің негізі 2 болғандықтан, анықсыздықты өлшем бірлігі келесідей болады:

$H_1 = \log_2 2 = 1$ bit. Информация өлшемі мен энтропия өлшемдері біртүрлі болады. Жоғарыдағылардан $H(\alpha) = \log_2 K$.

4.

Тәжрибе нәтижесі	A_1	A_2	A_3	...	A_k	$\sum$
ықтималдықтары	$\frac{1}{k}$	$\frac{1}{k}$	$\frac{1}{k}$	...	$\frac{1}{k}$	1

Әрбір тәжрибенің энтропиясы: $H(\alpha) = \frac{1}{k}\log_2 k = -\frac{1}{k}\log_2 \frac{1}{k}$.

Оқиғалар байланыссыз болғанда энтропия келесідей есептеледі:

$H(X) = -\sum_{i=1}^{M} P_i \log P_i$ болады.

Егер ықтималдықтар өзара тең болса, онда олардың қосындысы

$$H(X) = -\sum_{i=1}^{M} P_i \log P_i = \log M \cdot \qquad (1.1)$$

Яғни мұндай жағдайда **энтропия максимал** болады.

Осы теңдеуден мынаны тапса болады:

$H(X) = M\left[-\log P\,(X)\right]$, яғни оқиғалар ықтималдығының математикалық күтіліміне тең болады.

Біріккен жүйенің энтропиясы.

Айталық екі ансамбль берілсін: $X = \{x_1, x_2, ..., x_n\}, i = \overline{1,n}$ және $Y = \{y_1, y_2, ..., y_m\}, j = \overline{1,m}$. Онда біріккен ХУ ансамблінің матрицалық көрінісі келесідей болады: $\begin{Vmatrix} x_1y_1, x_1y_2, ..., x_1y_m \\ x_2y_1, x_2y_2, ..., x_2y_m \\ ..... \\ x_ny_1, x_ny_2, ..., x_ny_m \end{Vmatrix}$; бұл жүйенің жағдайлар саны *m*n* болады.

Әрбір ХУ жүйесінің жағдайының өзінің ықтималдығы болады; сонда осыған сай дәл осындай ықтималдықтар матрицасын көрсетсе болады.

Ал оған сәйкес ықтималдықтар матрицасын келесідей көрсетсе болады:

$$p(x_i, y_j) = \begin{vmatrix} p(x_1, y_1).\ p(x_1, y_2)....p(x_1, y_m) \\ p(x_2, y_1).\ p(x_2, y_2)...p(x_2, y_m) \\ ..... \\ p(x_n, y_1)p(x_n, y_2)....p(x_n, y_m) \end{vmatrix}.$$

Мұнда

$$P_{n,m} = P\left[(X \approx x_n), (Y \approx y_m)\right].$$

Онда біріккен ХУ ансамблінің біріккен энтропиясын табу үшін мына теңдеу істетіледі: $H[X,Y] = H[X] + H[Y/X] = H[Y] + H[X/Y]$. (1.1)

Біріккен жүйенің энтропиясы былай есептеледі:

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P_{ij} \log P_{ij}\,. \qquad (1.2)$$

Яғни $H(X,Y)=\sum_{i=1}^{n}\sum_{j=1}^{m}\eta(P_{ij})$. (1.2')

Математикалық күтілім түрінде былай жазылады:

$$H[X,Y]=M[-\log P[X,Y]].$$

Х және У жүйелері байланыссыз болғандағ мынаны жазса болады;

$$H[X,Y]=H[X]+H[Y]. \quad (1.3)$$

Жалпы жағдайда $H[x_1,x_2,...,x_k]=\sum_{i=1}^{k}H(x_i)$.

Ақырғы екі теңдеу байланыссыз құрамды элементті жүйелер үшін **қосу теңдеулері** деп аталады.

Мұнда жеке ансамблдердің (Х,У) энтропияларын табу үшін мыналар орындалады:

- жоғарыдағы ықтималдықтар матрицасының элементтерін қатарлар бойынша қосумен Х элементтерінің ықтималдықтары табылса, ал сол матрицаның элементтерін бағандар бойынша қосумен У элементтерінің ықтималдықтары табылады;
- Шеннонның энтропияны есептеу теңдеуімен әрбір ансамблдің энтропиясы табылады.

Сонда қатарлар бойынша қосындылап, келесідей қосындыларды матрицаның оң жағындағы бағанда аламыз:

$$\begin{vmatrix}\sum_j p(x_1,y_j)\\ \sum_j p(x_2,y_j)\\ .....\\ \sum_j p(x_n,y_j)\end{vmatrix}.$$

Бұлардан энтропия табамыз:

$$H(X)=-\sum_i\sum_j p(x_i y_j)\log\sum_j p(x_i y_j). \quad (1.4)$$

Дәл осындай жолмен төменгі қатарда бағандар бойынша қосындылап, мыналарды аламыз:

$$\sum_i p(x_i, y_1); \sum_i p(x_i, y_2); \ldots \sum_i p(x_i, y_m).$$

Бұлардан энтропияны табамыз:

$$H(Y) = -\sum_i \sum_j p(x_i, y_j) \log \sum_i p(x_i, y_j). \quad (1.5)$$

Жоғарыдағы қосынды матрицадан шартты ықтималдықтар келесідей табылады:

$$p(x_i / y_j) = \frac{p(x_i, y_j)}{\sum_i p(x_i, y_j)} = \frac{p(x_i, y_j)}{p(y_j)}; \; p(y_j / x_i) = \frac{p(x_i y_j)}{\sum_j p(x_i, y_j)} = \frac{p(x_i, y_j)}{p(x_i)} \quad (1.5\text{-}1)$$

Орташа немесе толық шартты ықтималдықтардың энтропиясын жоғарыдағы (1.1) теңдеуден тапса да болады:

$$H[X,Y] = H[X] + H[Y/X] = H[Y] + H[X/Y];$$
$$H[Y/X] = H[X,Y] - H[X].$$
Немесе: $$H[X/Y] = H(X,Y) - H(Y). \quad (1.6)$$

Шартты энтропиялар.

X,Y жүйелері беріліп, олар біріне бірі байланысты болсын.

Сонда $P(y_j / x_i)$ - $X \approx x_i$ оқиғасы амалға асқанда, $Y \approx y_i$ болуының ықтималдығы болсын. Осындайда ***жеке шартты энтропия*** былай анықталады:

$$H[Y / x_i] = -\sum_{j=1}^{m} P(y_j / x_i) \log P(y_j / x_i).$$

Бұл Y жүйесінің $X \approx x_i$ болғандағы шартты энтропиясы болады; мұнда энтропия матрицаның қатары бойынша есептеледі.

Ал енді мына шартты энтропияны есептеу матрицаның бағаны бойынша жүргізіледі: $H[X / y_j] = -\sum_{i=1}^{n} P(x_i / y_j) \log P(x_i / y_j)$ (1.7)

Осы жүйенің ***орташа немесе толық шартты энтропиясы*** келесідей анықталады:

$$H[Y / X] = -\sum_{i=1}^{n} P_i H(Y / x_i) = -\sum_{i=1}^{n} P_i \sum_{j=1}^{m} P(y_j / x_i) \log P(y_j / x_i). \quad (1.8)$$

Яғни оны мына түрде жазса болады:

$$H[Y / X] = \sum_{i=1}^{n} \sum_{j=1}^{m} P_i \eta[P(y_j / x_i)]. \quad (1.9)$$

Алайда бұл (1.8), (1.9) теңдеулар өте күрделі болып, олардан гөрі (1.6) теңдеуді қолданған абзал.

X,Y жүйелері өзара байланысты болғандағы энтропия.

$$H[X,Y]=H[X]+H[Y/X] \qquad (1.10)$$

Жалпы жағдайда

$$H[x_1,x_2,...,x_s]=H[x_1]+H[x_2/x_1]+H[x_3/x_1x_2]+...+H[x_s/x_1x_2...x_{s-1}]. \qquad (1.11)$$

Өзара байланысты жүйелерде: $H[X,Y]\le H[X]+H[Y]$ болады.

1.5 *Зертханалық жұмыс*

А және В жүйелерінің бірікен жүйесінің элементтерінің ықтималдықтар матрицасы берілген:

$$P(A,B)=\begin{vmatrix}0,3 & .... & 0 & ..... & 0\\ 0,2 & .. & 0,3 & ... & 0,1\\ 0 & .... & 0,1 & ..... & 0\end{vmatrix} \qquad \begin{matrix}P(a_i)\\ 0,3\\ 0,6\\ 0,1\end{matrix}$$

$$P(b_j).....\quad .0,5\ ...\ 0,4\ ....\ 0,1$$

1. Оң жақтағы баған бойынша есептеп, $H(A)$ тапсақ, төменгі қатар бойынша есептеп, $H(B)$ ны табамыз;

$$H(A)=-\sum_{i=1}^{n}p(a_i)\log_2 p(a_i)=-(0,3*\log_2 0,3+0,6*\log_2 0,6+0,1*\log_2 0,1)=1,294bit,sost$$

$$H(B)=-\sum_{j=1}^{m}p(b_{ij}\log_2 p(b_{ji}=-(0,5*\log_2 0,5+0,4*\log_2 0,4+0,1*\log_2 0,1)=1,36bit,sost$$

2. Жеке шартты энтропияларды табу үшін (1.5-1) теңдеуларды пайдаланамыз:

$$p(a_1/b_1)=\frac{p(a_1,b_1)}{p(b_1)}=\frac{0,3}{0,5}=0,6;..p(a_2/b_2)=\frac{p(a_2,b_2)}{p(b_2)}=\frac{0,3}{0,4}=0,75;$$

$$p(a_3/b_2)=\frac{p(a_3,b_2)}{p(b_2)}=\frac{0,1}{0,4}=0,25;..p(a_2/b_3)=\frac{p(a_2,b_3)}{p(b_3)}=\frac{0,1}{0,1}=1;$$

$$p(a_3/b_1)=p(a_1/b_2)=p(a_1/b_3)=p(a_3/b_3)=0;$$

Осылардан келесідей матрицаны аламыз:

$$p(a_i / b_j) = \begin{vmatrix} 0,6.....0.....0 \\ 0,4....0.75....1 \\ ...0....0,25....0 \end{vmatrix}$$

3. Осы екі матрица және төмендегі теңдеулармен толық шартты энтропияларды табамыз:

$$H(A/B) = -\sum_i \sum_j p(b_j) p(a_i / b_j) \log_2 p(a_i / b_j) = -\begin{bmatrix} 0,5 * (0,6 \log_2 0,6 + 0,4 \log_2 0,4) + \\ 0,4 * (0,75 \log_2 0,75 + 0,25 \log_2 0,25) + \\ 0,1 * (1 \log_2 1) \end{bmatrix} \approx$$

$$\approx 0,485 + 0,324 = 0,809 bit / sost.$$

4. Немесе осыны мына теңдеумен де тапса болады:

$$H(A/B) = \sum_i \sum_j p(a_i, b_j) \log_2 p(a_i / b_j) = -\begin{pmatrix} 0,3 \log_2 0,6 + 0,2 \log_2 0,4 + 0,3 \log_2 0,75 + \\ 0,1 \log_2 0,25 \end{pmatrix} =$$

$$== 0,3 * 0,736 + 0,2 * 1,321 + 0,3 * 0,415 + 0,1 * 2 \approx 0,809 bit / sost$$

$H(B / A)$ ны табу үшін жоғарыдағыларды қайталаймыз; яғни шартты ықтималдықтар матрицасын құрамыз:

$$p(b_j / a_i) = \begin{vmatrix} ....1.....0.....0 \\ 0,333...0.5...0,167 \\ ....0.....1.....0 \end{vmatrix}$$

$H(A/B) = -\sum_i \sum_j p(a_i) * p(b_j / a_i) \log_2 p(b_j / a_i) \approx 0,875 bit / sost$, немесе екінші жолмен келесідей табамыз:

$$H(A/B) = -\sum_i \sum_j p(a_i, b_j) \log_2 p(b_j / a_i) \approx 0,875 bit / sost.$$

5. Өзара байланысты ансамблдердің толық энтропиясын келесідей табамыз:

$$H(A,B) = -\sum_i \sum_j p(a_i, b_j) \log_2 p(a_i, b_j) = 2,17 \, bit / sost$$

Жоғарыдағыларды келесідей тексерсе болады:

$$H(B / A) = H(A,B) - H(A) = 2,17 - 1,294 \approx 0,876$$

$$H(A/B) = H(A,B) - H(B) = 2{,}17 - 1{,}36 \approx 0{,}81$$

Зертханалық жұмыс

X,Y оқиғалар ансамлінің шартты және толық ықтималдықтары төмендегі кестеде келтірілген. Ансамблдердің шартты, жеке және толық энтропияларын табу керек.

	x_1	x_2	x_3	$P(y_j)$
y_1	0,1	0,2	0,3	0,6
y_2	0,25	0	0,15	0,4
$P(x_i)$	0,35	0,2	0,45	1

5 теңдеуден:

$$H(X) = -\sum_{i=1}^{3} P(x_i)\log P(x_i) = -0{,}35\log 0{,}35 - ... = 1{,}5129;$$

$$H(Y) = -\sum_{i=1}^{2} P(y_j)\log P(y_j) = -0{,}6\log 0{,}6 - ... = 0{,}971;$$

$$H(XY) = -\sum_{j=1}^{2}\sum_{i=1}^{3} P(x_i y_j)\log P(x_i y_j) = -0{,}1\log 0{,}1 - ... = 2{,}2282$$

$$H[X,Y] - H[X] = H[Y/X] = 2{,}2282 - 1{,}5129 = 0{,}7158;$$
$$H[X,Y] - H[Y] = H[X/Y] = 2{,}2282 - 0{,}971 = 1{,}2572.$$

1.7 Зертханалық жұмыс

Берілген 1010101 кодының информация сиымдылығын табыңдар! 1 және 0 таңбаларының ықтималдықтары келесідей берілсін:

P_1	0,1	0,5	0,9
P_0	0,9	0,5	0,1

1.8 Зертханалық жұмыс

Ақ-қара түсті экранда $N = 5 \times 10^5$ элемент бар; олар байланыссыз және тең ықтималды болса, экранның информация сиымдылығы қандай? $H(X) = \log(2^N) = N \log(2) = 5 \times 10^5$ бит болады.

1.9 Зертханалық жұмыс

Кадрде пикселдер саны $N = 625 \times 600$.

Әр пиксельде $u = 0 \div 8 \vee, \Delta u = 1 \vee$ болса, кадрдың информация сиымдылығы қандай?

$I(X) = H(X) = \log N = \log(625 \times 600 \times 8)$ бит болады.

1.10 Зертханалық жұмыс

X,Y екі әліпбиі берілген болып, *Z=X+Y* болсын. Мына жағдайларда: *X,Y*-өзара байланыссыз; *X,Y* өзара байланысты; *X,Y* өзара тең, яғни $X \equiv Y$ болғанда *H(Z/Y)* шартты энтропиясы неге тең болады?

1.11 ***Зертханалық жұмыс***

x_i, y_j - өзара байланысты және байланыссыз болғанда мына энтропиялар арасындағы қатысты анықтаңдар; $H(x), H(y), H(x/y), H(y/x), H(x,y), H(x/y_j), H(y/x_i)$.

1.12 ***Зертханалық жұмыс***

H(x),H(y),H(y/x)=1 bit болса, онда *H(x/y)=?* қандай болылады?

Шешімі: H(x/y)=H(x)+H(y)-H(xy); H(xy)=H(y)-1 bit; H(x/y)=H(x)+1 bit.

1.13 Зертханалық жұмыс

Мына матрица берілген: $P(X,Y) = \begin{Vmatrix} 1/8. & 1/8. & 1/8 \\ 1/8 & .... & 0 .... 1/8 \\ 1/8. & 1/8. & 1/8 \end{Vmatrix}$;

Мына энтропияларды анықтау керек: *H(x),H(y),H(x/y),H(y/x),* $H(x/y_1), H(y/x_1), H(x,y)$?

1.14 Зертханалық жұмыс

$H(x,y) \le H(x) + H(y)$ екендігін түсіндіріңіз.

1.15 ***Зертханалық жұмыс***

Екілік, ондық және натуралдық ақпараттың өлшем бірліктерінің өзара қатысы қандай болады?

1.3 Өзара алмасу ақпараты; толық ықтималдық; Байесс теңдеуімен болжау бағдаржолы.

X жүйесіндегі элементтерді зерттегенде, зерттелген элементтердің энтропиялары нолге айналып, ал зертелмегендері қала береді анықсыз болып. Сонда зерттелгендерінің қосындысы алынған "информацияинформацияға" тең болады. Зерттелгендерін *Y* жиыны деп, алынған "информацияны" сол энтропиялар айырмасы түрінде жазса болады;

Сонда, $I(YX) = H(X) - H(X/Y)$, $I(YX) = H(Y) - H(Y/X)$ – өзара алынған "информациялар" болады.

Ал толық "информация" былай табылады:

$I(YX) = H(Y) + H(X) - H(XY)$.

Мұнда $H(YX) = H(Y) + H(X/Y) = H(X) + H(Y/X)$.

$I(YX) = H(Y) + H(X) - H(XY)$ - толық "информация" екі ансамбльдегі "информациялардың" толық жиыны болады.

Бұл екі энтропияның қосындысы мен олардың біргелік энтропиясының айырмасына тең болады.

Толық энтропияның қасиеттері.

1. Толық энтропия симметриялы функция *X* пен *Y-ке* қарағанда. $I(YX) \le H(X)$.

2. *X* туралы *Y*- тен алынған информация *X* тің энтропиясынан артпайды.

$I(YX) \le H(X)$. Бұл информация максимумына жетеді, егер *H(X/Y)*=0 болса. Мұндай жағдайда $H(X/Y)=0$ болып, максимал дәрежеге жетеді.

3. Егер *Y* тәжірибелер *X* ансамблін өзгертпесе, яғни *X* және *Y* өзара байланыссыз болса, онда $I(YX) = 0$ болады;

мұндай жағдайда $H(X/Y) = H(X)$ болып, $I(YX) = H(X) - H(X) = 0$ болады. Бұларды көрсету үшін Венн диаграммасын қолданса болады.

4. $I(YX) \ge 0$ болады; ақиқаттан да $I(YX) = H(Y) + H(X) - H(XY) \ge 0$.:

Логарифмдер түрінде келесідей болады:

$$I(YX) = \sum_{i=1}^{n}\sum_{j=1}^{m} P(x_i, y_j)\log\frac{P(x_i, y_j)}{P(x_i)P(y_j)}.$$

Ал математикалық күтілім түрінде былай жазылады:

$$I(YX)=\sum_{i=1}^{n}\sum_{j=1}^{m}P(x_i,y_j)\log\frac{P(x_i,y_j)}{P(x_i)P(y_j)}.$$.

X жүйесі туралы толық информация $I(X)=H(X)=\sum_{i=1}^{n}P_i(-\log P_i)$ болып, мұнда $-\log P_i$, x_i тәжрибесінің жеке информациясын білдіреді.

Байес теңдеуімен тәуелді оқиғаларды болжау әдісі. Толық ықтималдық теңдеуі.

$P(A)=\sum_{i=1}^{n}P(H_i)P(A/H_i)$, мұнда

: $P(H_i)$- H_i болжамының априорлы ықтималдығы; $P(A/H_i)$ - H_i болжамының орындалғандағы A оқиғасының шартты ықтималдығы; $P(A)$- A оқиғасының толық ықтималдығы.

Болжамдар теоремасы немесе Байесс теңдеуі.

$P(H_i/A)=\frac{P(H_i)P(A/H_i)}{\sum_{i=1}^{n}P(H_i)P(A/H_i)}$, мұнда $P(A/H_i)$ - мысалы, ұшақтың әртүрлі оқ тигендегі жығылу ықтималдығы; $P(H_i)$- неше рет оқ тиюнің априор ықтималдығы. Сонда алдын ала ұшақты құлату үшін неше оқ тигізу керек болатындығын болжау теңдеуі.

Сондықтан бұл бағдаржолды басқада көптеген әсер, ықпалды және оқиғалы әртүрлі мәселелерді шешуге қолданса болады. Мысалы, медициналық диагностикада әртүрлі кеселдерді анықтау үшін, геологияда қазба байлықтың түрін анықтау үшін, метеорологияда ауа райын анықтау және т.б. көптеген мәселелерді шешу үшін қолданса болады.

Төменде анықсыз ойлау жүйесіда құрылған ауа райын анықтаушы бағдаржол қарастырылған.

***Зертханалық жұмыс* 1.3.1**

Берілгендер ретінде F_1,F_2,F_3 әсер, ықпалдары және оларға сай олардың болжамдары H_1,H_2, 1- кестеде берілген.

Осы статистикадан оқиғалардың априорлық және шартты ықтималдықтары есептеледі. Мұнда әрбір әсер, ықпал үш дәрежеге бөлінген; мысалы, самал-нашар (слабый), орташа (умеренний), қою (пасмурно).

Осы әсер, ықпаллармен F_1,F_2,F_3 санақтық ықтималдықтардың

анықсыз жиындары құрылған. Мысалы, әсер, ықпал F_1- (Самал) анықсыз жиын $\{0{,}3584, F_1', 0{,}5094, F_1'', 0{,}1321, F_1'''\}$ құраса, мұнда әсер, ықпал F_1 - нашар, F_1'' - орташа самал, F_1''' - күшті самалды көрсетеді, ал олардың алдында сенімділік еселіктері көрсетілген. Әсер, ықпал F_2 (ылғалдық) анықсыз жиынды $\{0{,}6603, F_2', 0{,}2264, F_2'', 0{,}0943, F_2'''\}$ құрайды, мұнда әсер, ықпал ретінде ылғалдық алынған; F_2 - жоғары ылғалдық, F_2'' - орташа ылғалдық, F_2''' - төмен ылғалдық; Әсер, ықпал F_3- (Бұлт) анықсыз жиынды $\{0.094, F_3', 0.1509, F_3'', 07547, F_3'''\}$ құрап, мұнда F_3 - ашық, F_3'' - бұлтты, F_3''' - қою бұлтты білдіреді.

Кесте 1.

Бақылау күніндегі ауа райы		Келесі күнгі жағдайлар саны 173 күн.	
		Жауынды күндер (H_1) 53 күн; 0,3	Ашық күндер (H_2) 120 күн; 0,7
Самал (F_1)	Нашар (Слаб)	19; 0,358527;	52; 0,4333
	Орташа (Умер)	27; 0,50943	44; 0,3667
	Күшті (Сил)	7 ; 0,1321	24; 0,2
Ылғал (F_2)	Жоғары (Выс)	35; 0,6604;	18; 0,15
	Орташа (Сред)	12; 0,22646;	42; 0,35
	Төмен (Низк)	6; 0,1132	60; 0,5
Бұлт (F_3)	Ашық (Ясн)	5; 0,0943	83; 0,69167;
	Бұлт (Обл)	8; 0,1509	27; 0,225
	Қою бұлт (Пасм)	40; 0,7547	13; 0,08333

3 параметр (әсер, ықпаллар) өлшенеді: Самал, ылғалдық, бұлт. Олар 1- кестеде көрсетілген. 2 болжам болжанады: $H_1 -$ жауын, $H_2 -$ ашық күн.

1) **Максимал шындық болжамы.**

Әсер, ықпалдардың шартты ықтималдықтары:

$$P(F/H_i) = P(F_1, F_2, F_3/H_i) = P(F_1/H_i) \bullet P(F_2/H_i) \bullet P(F_3/H_i); i = 1,2$$

екі оқиғаға H_1, H_2.

$$P(F/H_i) = P(F_1, F_2, F_3/H_i) = P(F_1/H_i) \bullet P(F_2/H_i) \bullet P(F_3/H_i);$$

оқиғаға H_1.

$Q(F/H_i) = Q(F_1, F_2, F_3/H_i) = Q(F_1/H_i) \bullet Q(F_2/H_i) \bullet Q(F_3/H_i)$;

оқиғаға H_2.

Кейін, екі шартты ықтималдықтардан үлкені таңдалады және сонымен шешім қабылданады;

$P(F/H_1) = 0{,}0132$, $Q(F/H_2) = 0{,}00675$. Келесідей болғандығы себепті $P(F/H_1) > Q(F/H_2)$, **жауын жауады** деген шешім қабылданады.

2) **Апостериор ықтималдықтар әдісі.**

Жауынның ықтималдығы Байестің теңдеуімен есептеледі:

Кейінгі күнде жауын болуының апостериор ықтималдығы мына теңдеумен есептеледі:

$$P(H_1/F) = \frac{P(F/H_1) \bullet P(H_1)}{P(F/H_1)P(H_1) + Q(F/H_2)Q(H_2)} = 0{,}463.$$

Кейін, жауынның априорлық ықтималдығы есептеледі - $P(H_1)$=0,30 және апостериор ықтималмен салыстырылады $P(H_1/F)$.

Апостер ықтималдық (0,463) априор ықтималдықтан көп (0,30) болғандықтан, келесі күні **жауын болады** деп күтіледі.

3) **Апостериор ықтималдықтың максимумы әдісі**.

Басқа оқиғаның апостериор ықтималдығы Байес теңдеуімен

есептеледі, яғни $Q(H_2/F)$.

$$Q(H_2/F) = \frac{Q(F/H_2) \bullet Q(H_2)}{P(F/H_1)P(H_1) + Q(F/H_2)Q(H_2)} = 0{,}537.$$

$$P(H_1/F) = \ 0{,}463.$$

Олар салыстырылып, үлкені анықталады; $P(H_1/F) < Q(H_2/F)$, яғни **ашық күн** болады деген шешім қабылданады.

Зерттеулер нәтижелерін қорытып, келесідей шешімге келсе болады:

1) Көп жағдайларда әсер, ықпаллар және оқиғалар саны көп болғанда шындыққа ұқсастық теңдеуін құру мүмкін болмайды және нақтылы әдістерді қолдану да мүмкін болмайды. Сондықтан, мұндай жағдайларда анықсыз жиындар мен анықсыз Ойлау жүйесін (логика) қолданған қолайлы болады. Мұнда әрбір әсер, ықпал мен оқиғаға анықсыз жиындар құрылады.

2) Әсер, ықпаллар мен оқиғалардың шекаралық мәндері

істетілмейді; мұнда әсер, ықпалдың айқын мәнінің орнына анықсыз жиынның элементі істетіледі. Сондықтан шекараны табу, функцияны дифференциалдау сияқты амалдар орындалмайды.

3) Шешімнің сенімділігін артттыру үшін әсер, ықпаллар санын немесе олардың бөлшектенуін (градациясын) көбейту керек болады. Алайда мұны тек өлшемдер саны жетерлі дәрежеде көп болғанда қолданса болады.

4) Апостериор ықтималдықтың төмен мәндерінде ≈(0,35-0.45) немесе олардың айырмашылығы кем болғанда ≈0,1-0,3, Болжамдардың максималдығы шартын қолдану қолайлы болады.

Ал апостериор ықтималдықтың жоғары мәндерінде 0,8 – 0,9 немесе олардың айырмашылығы үлкен болғанда ≈0,3-0,6 тек Байес шартымен шектелсе болады.

Төменде осы бағдаржолдың бағдарламасы Турбо Пролог тілінде жазылған.

Программаның мәтінді

```
predicates
nondeterm vivod
nondeterm apost(real,real,real,real)
nondeterm vivMPG(real,real,string)
nondeterm vichis(string,string,string,real,real)
nondeterm veter(string,real,real)
nondeterm vlaj(string,real,real)
nondeterm oblach(string,real,real)
goal
vivod.
clauses
vivod:-clearwindow,write("Veter: "),readln(VT),
write("Vlajnost: "),readln(VL),
write("Oblachnost: "),readln(OB),vichis(VT,VL,OB,P,Q).
vichis(Vtr,Vlj,Obl,P,Q):-veter(Vetr,VT1,QT1),
vlaj(Vlajn,VL1,QL1),oblach(Obla,OB1,QB1),Vetr=Vtr,Vlajn=Vlj,
Obla=Obl,P=VT1*VL1*OB1,
Q=QT1*QL1*QB1,apost(P,Q,A,B).
apost(P,Q,A,B):-A=(P*0.3)/(P*0.3+Q*0.7),B=(Q*0.7)/
(P*0.3+Q*0.7),
vivMPG(A,B,R),write("MaxApostVer: ",R).
vivMPG(A,B,R 1 1):-A>B,R1="Budet dojd".
```

vivMPG(A,B,R1):-A<=B,R1=”Budet yasno”.
veter(“Slab”,0.358,0.43).
veter(“Umer”,0.51,0.37).
veter(“Siln”,0.132,0.2).
vlaj(“Visok”,0.66,0.15).
vlaj(“Sredn”,0.226,0.35).
vlaj(“Nizkiy”,0.113,0.5).
oblach(“Yasno”,0.094,0.692).
oblach(“Oblachno”,0.151,0.225).
oblach(“Pasmurno”,0.755,0.083).

1.4 Кездейсоқ шаманың эпсилон-энтропиясы;

Үздіксіз хабар көзінің дифференциалдық энтропиясы; қасиеттері.

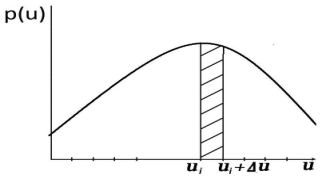
Энтропия тек қана дискрет ақпарат көзін ғана емес, сондай ақ үздіксіз ақпарат көздерін де сипаттай алады; мұндай ақпарат көзі үшін энтропияны **дифференциалды** деп атайды.

$$H(U) = \int_{-\infty}^{\infty} p(u)\log\ p(u)du\ - \lim_{\Delta u \to 0} \log\ \Delta u\ .$$

Оң жақтағы екінші мүшеде Δu кванттау қадамы болып, ол шама $\Delta u \to 0$ ұмтылғанда шексіздікке ұмтылады; бұл дегені таңдау ықтималдығы немесе H(U) да шексіз көп болады дегенді білдіреді.

Ал оң жақтағы бірінші мүше шекті мәнге ие болып, тек U дың таралу заңдылығына байланысты болады.

Өлшеулер теориясында **эпсилон-энтропия** түсінігі кең қолданылады; ол өлшеу



1.1-сурет үдерісіндегі қателіктің есебінен

хабар энтропиясының кемейуін көрсетеді. Айталық Y (өлшеу нәтижесі) нысанның шын шамасының мәні X туралы алынған

ақпарат шамасы болсын. Сонда өлшем қателігі мына шартқа жауап беруі керек:

$\overline{(Y-X)^2} \le \xi^2$ Мұнда минимум $p_x(x/y)$ тің барлық таралу заңдары бойынша ізделуі керек. Сонымен, анықтама бойынша:

$$H_\xi(x) = \min_{p_x(x/y)} [H(x) - H(x/y)].$$

Осы теңдеуді толық жазғанда келесідей болады:

$$H_\xi(x) = \min_{p_x(x/y)} \int\int p_{XY}(x,y) \log \frac{p_{XY}(x,y)}{p_X(x) p_Y(y)} dxdy .$$

Қалыпты сандар үшін оңай есептеледі.

1.4.1 Үздіксіз хабар көзінің дифференциалдық энтропиясы; қасиеттері.

Амалда хабар көздерінің кейбірінде олардың мүмкін болған күйлер саны континуум болады; ондай хабар көздерін үздіксіз хабар көздері деп атайды. Көп жағдайда кванттау және дискреттеу құрылымдарымен олар дискреттік түрге өткізіледі. Алайда ақпарат үздіксіз түрде де жіберілетін құрылымдар көп ұшырайды.

Мұндай хабар көзінде таңдау анықсыздығының бағасы немесе энтропиясының өзіне сай қасиеті болады. Біріншіден, хабар көзі шығаратын мәндер математикалық тұрғыда үздіксіз функция болады. Екіншіден, кездейсоқ шаманың кез келген уақыт мезгіліндегі ықтималдығы нөлге тең болғандығы үшін оның энтропиясын тауып болмайды.

Үздіксіз кездейсоқ шама U және оның нығыздық теңдеуі $p(u)$ болса, оны n кіші аралықтарға бөлеміз; ол аралықтардың үлкендігі Δu (1.1-сурет) болсын.

Осындайда u дың $(u_i, u_i + \Delta u)$ аралығының ішіндегі кез келген орындалуында U дискрет кездейсоқ шамасының u_i мәні орындалуы етті деп қабылдаймыз. Δu мәні кішкетай болғандықтан u мәнінің мына $u_i, u_i + \Delta u$ аралықтағы ықтималдығы $p(u_i \le u \le u_i + \Delta u)$:

$$P(u_i \le u \le u_i + \Delta u) = \int_{u_i}^{u_i + \Delta u} p(u) du \approx p(u_i) \Delta u .$$

Онда дискрет кездейсоқ шама $\tilde{U}$ ның энтропиясы келесідей анықталады:

$$H(\tilde{U}) = -\sum_{i=1}^{n} p(u_i)\Delta u \log[p(u_i)\Delta u]$$

немесе: $H(\tilde{U}) = -\sum_{i=1}^{n} p(u_i)\Delta u \log[p(u_i)] - \sum_{i=1}^{n} p(u_i)\Delta u \log \Delta u$,

$\sum_{i=1}^{n} p(u_i)\Delta u = 1$ болғандықтан:

мынаны аламыз: $H(\tilde{U}) = -\sum_{i=1}^{n} p(u_i)\Delta u \log p(u_i) - \log \Delta u$.

Мұнда Δu кішірейген сайын $p(u_i \le u \le u_i + \Delta u)$ ықтималдығы $p(u_i)$ ықтималдығына жақындап, ал $\tilde{U}$ дискрет шамасының қасиеттері U үздіксіз кездейсоқ шаманың қасиеттеріне жақындай түседі.

$\Delta u \to 0$ дағы шекке өтіп, өздіксіз хабар көзінің энтропиясын $H(U)$ мына түрде аламыз:

$$H(U) = -\int_{-\infty}^{\infty} p(u)\log p(u)du - \lim_{\Delta u \to 0} \log \Delta u . \qquad (1.12)$$

Осы өрнектен “шексіз көп күйлердің энтропиясы да шексіз көп болады”- десек болады. Осы өрнектің **бірінші мүшесінің *мәні шекті болады;*** ол тек U үздіксіз ***кездейсоқ шаманың таралу заңына байланысты*** болып, оның ***кванттау қадамына байланысты болмайды***.

Ол дискрет хабар көзінің энтропиясы сияқты құрамға ие болады. Ал **екінші мүше**, керісінше, кездейсоқ шама U дың ***кванттау қадамына ғана байланысты болады***. Тек осы мүшенің саладарынан $H(U)$ шамасы шексіздікке ұмтылады.

Осы өрнекті хабар көзінің ***келтірілген энтропиясы*** деп атайды; оны талдауда екі жол бар: оның біріншісінде бірінші мүше ***үздіксіз хабар көзінің энтропиясын анықтайды***;

$$h(U) = -\int_{-\infty}^{\infty} p(u)\log p(u)du \quad , \qquad (1.13)$$

онда тек таралу нығыздығы болғандығы себепті оған – ***салыстырмалы дифференциал энтропия*** немесе тек ***дифференциал энтропия*** деп атайды.

Оның мағынасы – U кез келген заңмен таралған кездейсоқ шаманың басқа бірге тең аралықта біркелкі таралған кездейсоқ U' шаманың орташа энтропиясына салыстырғандағы орташа энтропияны айтамыз.

Осында U' кездейсоқ шама δ аралығында біркелкі таралған болса және $\delta = 1$ болса, онда:

$$H(U') = -\lim_{\Delta u' \to 0} \log \Delta u'$$

және $\Delta u = \Delta u'$ болғанда:

$$H(U) - H(U') = -\int_{-\infty}^{\infty} p(u) \log p(u) du = h(U).$$

Дәл осы жолмен кванттау және шекті өту жолымен үздіксіз хабар көзінің шартты энтропиясының өрнегін табамыз:

$$H_v(U) = -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(u,v) \log \frac{p(u,v)}{p(v)} du dv - \lim_{\Delta u \to 0} \log \Delta u . \quad (1.14)$$

Осының бірінші бөлімін келесідей таңбалаймыз:

$$h_v(U) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(u,v) \log \frac{p(u,v)}{p(v)} du dv . \quad (1.15)$$

Осы өрнек ***салыстырмалы дифференциалды шартты энтропия*** немесе тек ***дифференциалды шартты энтропия*** деп аталады.

Дифференциалды энтропияның қасиеттері:

1. Дифференциалды энтропияның дискрет хабар көзінің энтропиясынан айырмашылығы ол анықсыздықтың салыстырмалы өлшемі ғана болады. Оның мәні U кездейсоқ шаманың масштабына байланысты болады, сондай ақ ол шаманы өлшеу бірлігін таңдауға да байланысты болады.

Салыстырмалы дифференциалды энтропиядан шығатыны, оның мәні оң, кері және нөл болуы мүмкін.

1. Дифференциалдық энтропия U кездейсоқ шаманың айқын мәндеріне байланысты болмайды; мысалы, оның барлық мәндерін тұрақтыға өзгерткенде оның шамасы өзгермейді.

2. Қандай таралу заңдары максималды дифференциалды энтропияға ие болады?

а) Егерде үздіксіз кездейсоқ U шаманың жалғыз ғана шектеуі оның мүмкін болған мәндерінің өзгеру аймағы [α, β] болса, яғни оның дисперсиясы $\sigma^2 \to \infty$ шектелмеген болса (өте үлкен қуатты сигналдар), онда осы аймақта біркелкі таралған ықтималдықтар заңы максимал дифференциалдық энтропияға ие болады.

Мұнда мәселені шешуде мына функционалдың максимумы табылады: $h(U) = -\int_{-\alpha}^{\beta} p(u)\log\ p(u)du$.

Келесідей шектеуді есепке алып: $\int_{-\alpha}^{\beta} p(u)du = 1$ және Лагранждың анықсыз көбейткіштері жәрдемінде ***ықтималдықтың таралу заңын*** табамыз: $p(u) = 1/(\beta - \alpha), \alpha \le u \le \beta$

Осы функциядан энтропияны тапсақ төмендегідей болады және ол максимумға ие болатыны көрінеді, яғни ***экстремалды энтропия*** келесідей көрініс болады:

$$h(U) = \log(\beta - \alpha) \cdot$$

б) Егер кедергінің орташа қуаты шектелмеген болса (немесе өте үлкен болса), онда максимал нәтижелі кедергінің элементтерінің амплитудасы біркелкі ықтималдықтар заңы бойынша таралған болады.

в) Егер үздіксіз кездейсоқ шаманың өзгеру аймағы [α, β] шектелмеген болса және оның дисперсиясы (қуаты) шектелген болса, онда U кездейсоқ шамасының қалыпты таралған заңында дифференциалды энтропия максимал болады.

Мәселені шешуде функционалдың максимумы мына шектеулерде ізделеді:

$$\int_{-\infty}^{\infty} p(u)du = 1 \quad \text{және} \quad \int_{-\infty}^{\infty} u^2\ p\ (u\ )du = \sigma^2\ ,$$

мұнда σ – ортаквадраттық ауытқу болып, оның математикалық күтілімі:

$\bar{U}$ =0 (σ — берілген шектеу). Мұнда да Лагранждың анықсыз көбейткіштер әдісін қолданамыз. Тапқан функция Гаусстық болады, яғни мына түрде болады:

$$p(u) = \frac{1}{\sigma\sqrt{2\pi}} e^{-u^2/2\sigma^2}.$$

Мұнда екілік санақ жүйесінде ***экстремалды энтропия*** келесідей:

$h_{\max}(U) = \log_2 \sigma\sqrt{2\pi e}$ болады.

Амалда егер генератордың қуаты шектелген болса, онда максимал энтропиялы сигналдың амплитудасы қалыпты заңмен таралған болады.

г) Егер үздіксіз түрдегі кедергінің (бөгеуілдің) орташа қуаты шектелген болса, онда максимал нәтижелі кедергінің элементтерінің амплитудасы қалыпты заң бойынша таралған болады.

Зертханалық жұмыс 1.4.1

[α, β] аралығында біркелкі заңмен таралған кедергі көзі берілген болып, оны дәл сол аралықта әсер ететін, бірақ қалыпты заңмен таралған кедергі көзімен алмастырғанда қуат бойынша қанша ұту болады?

Мәселені шешуде екі түрлі таралу заңындағы энтропияларды теңестіріп, қуаттарының айырмашылығын табамыз.

$h_{\max}(U) = \log \sigma_g \sqrt{2\pi e}$, - Гаусс заңы үшін;

$h_{\max}(U) = \log(\beta - \alpha)$ - біркелкі таралу заңы үшін болса, онда екінші заң үшін дисперсия:

$$\sigma_r^2 = \int_\alpha^\beta \left(u - \frac{\alpha + \beta}{2} \right)^2 \frac{1}{\beta - \alpha} du = \frac{(\beta - \alpha)^2}{12}. \quad (1.16)$$

Энтропияларды теңеп:

$$\begin{aligned} &\log \sigma_g \sqrt{2\pi e} = \log(\beta - \alpha), \\ &\sigma_g \sqrt{2\pi e} = \beta - \alpha, \end{aligned} \quad . \quad (1.17)$$

Осыдан: $\sigma_r^2 = \frac{\pi e}{6} \sigma_g^2 = 1,42\ \sigma_g^2$, яғни қуаттан 42 % ұтыс аламыз.

***Зертханалық жұмыс* 1.4.2**

Сигналдың амплитудасы қалыпты заңға бойұсынады; оның қуаты х шамасымен өлшенеді. Бұл сигналды толық өшіру үшін біркелкі заңмен таралған ақ шуыл түріндегі кедергі қолданылған. Оның қуаты, ең кем дегенде қанша болуы керек?

***Зертханалық жұмыс* 1.4.3**

Кедергінің таралу заңы біркелкі болған кең жолақты шуыл қолданылып, оның қуаты Y болсын. Сонда осы кедергіден өту үшін тар жолақты сигналдың тарау заңы қалыпты болғанда оның қуаты қандай болуы керек?

***Зертханалық жұмыс* 1.4.4**

Радиошуыл жаратушы аспапда егер жаратылатын шуыл таржолақты болса және шуыл шығарушы аспаптың қуаты шектелген болса, онда нәтижелі кедергінің таралу заңы қандай болуы керек?

***Зертханалық жұмыс* 1.4.5**

Қалыпты заңмен таралған кездейсоқ шаманың дифференциалдық энтропиясын табу керек? Оның таралу заңы келесідей:

$p_X = \dfrac{1}{\sigma_X\sqrt{2\pi}} e^{-\frac{\left(x-\bar{x}\right)^2}{2\sigma_X^2}}$ болсын. Егер:

а) $\bar{x}$-орта мәннің шамасын, б) σ_X^2-дисперсияның шамасын екі есе арттырғанда дифференциал энтропия қандай өзгереді?

***Зертханалық жұмыс* 1.4.6**

Үздіксіз ақпарат көзінің шығуында сигнал қуаты $\sigma_U^{\ 2}$ шектелген; сигналдың максималды салыстырмалы энтропиясын беретін дифференциалды таралу заңын табу керек?

***Зертханалық жұмыс* 1.4.7**

Үздіксіз ақпарат көзінің шығуында сигнал қуаты $\sigma_U^{\ 2}$ шектелмеген; сигналдың орташа мәні нөлге тең болса, онда максималды салыстырмалы энтропия беретін дифференциалды таралу заңын табу керек?

***Зертханалық жұмыс* 1.4.8**

Кездейсоқ шаманың таралу заңы келесідей $F(x) = \begin{cases} 0,..x \le 0, \\ x^2,..0 \le x \le 1, \\ 1,...1 < x, \end{cases}$ болса,

онда оның дифференциалды энтропиясы қандай болады?

***Зертханалық жұмыс* 1.4.9**

Қалыпты заңмен таралған *m* кездейсоқ шамалар жүйесінің энтропиясын табыңдар.

***Зертханалық жұмыс* 1.4.10**

Қалыпты кездейсоқ шамалардың қосындысы үшін мына шартты дифференциал энтропияларды табыңдар:

$H_d(x/y) = ?, H_d(y/x) = ?$

***Зертханалық жұмыс* 1.4.11**

Энтропиялары тең болған әртүрлі заңмен таралған сигналдардың ішінде ең кем дисперсиялы заң қандай болады?

***Зертханалық жұмыс* 1.4.12**

Келесідей геометриялық заңмен таралған шаманың энтропиясын табу керек?

$$P(x_i = k) = \begin{cases} 0,\ldots -\infty \le x_i \le 0, \\ p(1-p)^{k-1},\ldots 0 < x_i < \infty. \end{cases}$$

***Зертханалық жұмыс* 1.4.13**

Келесідей биномиалдық заңмен таралған шаманың энтропиясын табу керек?

$$P(x_i = k) = \begin{cases} 0,\ldots -\infty \le x_i \le 0, \\ C_m^k p^k (1-p)^{m-k},\ldots 0 \le x_i \le m, \\ 0,\ldots\ldots\ldots\ldots\ldots m < x_i < \infty. \end{cases}$$

***Зертханалық жұмыс* 1.4.14**

[-W,+W] аралығында біркелкі таралған кездейсоқ сигналдың дифференциалдық энтропиясын табу керек.

***Зертханалық жұмыс* 1.4..15**

Үздіксіз ақпарат көзінің шығуында сигнал деңгейі келесідей шектелген: U_m, U_M болса, онда максимал салыстырмалы энтропияға ие болған сигналдың дифференциалды таралу заңын табу керек.

***Зертханалық жұмыс* 1.4.16**

Үздіксіз ақпарат көзінің шығуында сигнал қуаты бойынша σ_U^2 шектелген болса, онда максимал салыстырмалы энтропияға ие болған сигналдың дифференциалды таралу заңын табу керек.

1.4.2 Кездейсоқ шаманың эпсилон-энтропиясы

Амалда физикалық үдерісті өлшегенде оның анық мәнін табу мүмкін емес; егер физикалық үдеріс кездейсоқ үдеріс болса, оның өлшенген нүктелері өлшеу қателіктері әсерінен бір рет бұзылса, екінші рет ол нүктелерді жақындаушы (аппроксимациялаушы функциямен) тегістегенде және қателік болады.

Нәтижеде біз ешқашанда абсолютті анық функцияның мәнін алмаймыз.

Бірінші түрдегі қателікке келсек ол өлшеуіш аспаптың (датчиктер) мен түрлендіргіштердің (преобразователь) – сезімталдығының шектелгендігі мен шекті рұқсат етілген қабілетімен (конечная разрешающая способность) өлшенеді. Сондықтан амалда өлшенетін функциядан алатын ақпарат (энтропия) өзінің абсолютті шамасынан кемейген түрде алынады.

Қарапайым жағдайда ақпарат көзі кездейсоқ U шамасының байланыссыз нақты мәндері түрінде көрсетіледі.

Сонда кездейсоқ U шаманың орындалуының ансамблінің ықтималдықтарының таралу $p(u)$ теңдеуімен өлшенеді.

Алайда біз U шамасының анық мәнінің орнына басқа өлшемнен алынған кездейсоқ шама Z ті аламыз; онда оған қойылған талап – олардың арасындағы айырмашылық тіктеу шындығынан аспауы керек.

Осы жағдайда Z шамасы U шамасын тіктейді деп аталады.

Осы екі сигналдардың біріне бірі ***жақындығының сандық көрсеткіші -*** $\rho(z,u)$ теңдеуі ендіріледі. Онда ***шындық шарты V(Z, U)*** үшін $\rho(z,u)$ теңдеуінің z және u дың барлық мәндері бойынша алынған *орташа мәні* алынады: $V\left(ZU\right) = \iint p\left(zu\right)\rho\left(zu\right)dzdu$ (1.18)

мұнда $\rho(z, u)$ - шамаларының ықтималдықтарының бірге таралу нығыздығын береді. Көпшілік жағдайда орта квадраттық шарт істетіледі; мұнда $\rho(z, u)$ – тиісті кеңістіктегі нүктелер арасындағы Евклид қашықтығының квадраты болады. Осы жағдайда шындыққа қойылатын талап ***шындық шарты*** $\tilde{V}\left(ZU\right)$ арқылы көрсетіледі:

$$\tilde{V}\left(ZU\right) = \iint p\left(u\right)p_u\left(z\right)\left(z-u\right)^2 dudz \le \varepsilon^2 , \qquad (1.19)$$

мұнда $p_u\left(z\right)$ - шартты таралу нығыздығы – шындық теңдеуі

болып, *u* сигналы *z* сигналы түрінде қабылдануын көрсетеді; ал ε – шындықтың берілген мәні; *p(u)*- нығыздығы берілгендігі үшін жоғарыдағы шарт орындалғанда шартты таралу нығыздығы болған $p_u(z)$ - ті өзгерту мүмкін болады.

Егер кездейсоқ *Z* шамасы кездейсоқ *U* шамасын тіктейтін болса, *U* тіктеуіш шамасының *Z* тегі ақпарат саны мына түрде жазылады:

$$I(ZU) = \iint p(u)p_u(z)\log\frac{p_u(z)}{p(z)}, \qquad (1.20)$$

мұнда $p(z) = \int p(u)p_u(z)du$ *Z* - тіктеуіш шамасының нығыздығы. Тіктеудің талап етілген шындық орынында аталған ақпарат саны минимал болуы керек. Сондықтан көпшілік $p_u(z)$ қатыстарының ішінен ***I(ZU)- дың ең кеміне сәйкес*** келетінін таңдау керек болады.

U – шамасының *ε*-энтропиясы деп *U* туралы *Z* кездейсоқ шамасындағы минимал ақпарат санына айтамыз және ол келесідей $H_\varepsilon(U)$ болады:

$$H_\varepsilon(U) = \min_{(p_u(z))} I(ZU), \text{ мұнда } V(ZU) \le \varepsilon^2.$$

U шамасының шартты $h(U)$ және шартсыз $h_Z(U)$ дифференциалдық энтропияларын қолданып *ε* - энтропияны мына түрде көрсетсе болады:

$$H_\varepsilon(U) = h(U) - \max_{(p_z(u))} h_z(U),$$

мұнда $p_z(u)$ - *z* сигнал қабылданғанда *u* сигналы жіберілгендігінің шартты ықтималдығының нығыздығы болады.

***Зертханалық жұмыс* 1.5.1**

Хабар көзінің $H_\varepsilon(U)$ табу керек болып, оның күй ансамблі қалыпты таралған және дисперсиясы σ^2 кездейсоқ шама болып, ал тіктеу шындығы $V'(ZU) \le \varepsilon^2$ болсын.

Мұнда сигналға байланысты болмаған Ξ кедергі болып, оның параметрлері М [Ξ] =0 және М[Ξ^2] = ε^2 болсын.

Онда жіберілетін сигнал *u* тіктеуіш сигнал *z* пен кедергінің қосындысы $u=z+\xi$ түрінде қаралады.

$$H_\varepsilon(U) = h(U) - \max_{(p(\varepsilon))} h(\Xi),$$

мұнда $h(\Xi)$ - кедергінің дифференциалдық энтропиясы; $\rho(\xi)$

- кедергінің таралу теңдеуі. Жоғарыда көргеніміздей, кездейсоқ шаманың дисперсиясы шектелгенде максимал дифференциал энтропия қалыпты таралу заңында болатыны анықталған еді.

Сондықтан: $\max\limits_{(p\ (\xi))} h\ (\Xi) = \log \varepsilon\sqrt{2\pi e}$, .

$$H(U) \approx \log \sigma\sqrt{2\pi e}$$

Осыдан мынаны алса болады:

$$H_\varepsilon(U) = \log \sigma\sqrt{2\pi e} - \log \varepsilon\sqrt{2\pi e} = \frac{1}{2}\log\frac{\sigma^2}{\varepsilon^2}\cdot$$

Осы өрнекте σ^2 сигналдың орташа P^u қуатын, ал ε^2 — кедергінің ρ^{ξ} орташа қуатын Ξ көрсетсе, онда осы өрнек ***эпсилон – энтропияның сигнал/кедергі*** P_u / P_ξ ***қатысына байланыстылығын*** көрсетеді.

Егер сигнал/кедергі қатысы берілген болса, онда қалыпты таралған кездейсоқ шама үшін $H^\varepsilon(U)$ максимал болады.

Ал егер U кездейсоқ шама кез келген түрде таралған болса және сол шарт орындалып, ε кіші болса, онда мына қатыс орынды болады:

$$H_\varepsilon(U) \approx h(U) - \log \varepsilon\sqrt{2\pi e}\ .$$

Үздіксіз сигнал қуаты шектелген болып, оның амплитудасы қалыпты заңға бойсынатын Марков сигналы берілген болсын. Мұндай сигналды Котельников қадамымен дискреттегенде дискреттеу қателігінің энтропиясы табылсын.

Шешімі: Қалыпты Марков сигналының энтропиясын есептейміз; қалыпты заң үшін энтропия келесідей табылады (жоғарыда есептелген): $H(U) = h_{\max}(U) = \log \sigma_g\sqrt{2\pi e}$ және максимал шамаға ие болатынын көргенбіз. Дискреттеу үдерісінде Котельников шарты тек Марков үдерісінде толық орындалады, яғни $\Delta t = \frac{1}{2F_b}$ болғанда жоғарғы жиілікті гармоникалар болмайды. Осы қадаммен дискреттегенде дискретті үдерістің энтропиясы келесідей табылады: $H_d(U) = \log\left(\frac{\sigma_d\sqrt{2\pi e}}{\Delta u}\right)$, мұнда σ_d^2 - дискрет сигнал қуаты. Дискреттеу

қателігінің энтропиясы келесідей табылады: $\Delta H(U) = H(U) - H_d(U)$ болып, тек Марков үдерісінде ғана $\Delta u = 1$ орындалады; ал басқа үдерістерде $\Delta u > 1$ болады. Сондықтан қалыпты Марков үдерісінде Котельников шарты толық орындалып, дискреттеу қателігінің энтропиясы нөлге тең болады; яғни $\Delta H(U) = H(U) - H_d(U) = 0$ болады.

Зертханалық жұмыс 1.5.3

Үздіксіз сигнал қуаты шектелген болып, оның амплитудасы қалыпты заңға бойсынатын сигнал берілген болсын. Мұндай сигналды дискреттегенде дискреттеу қателігінің энтропиясы табылсын.

Дискреттеу қателігінің қуаты мына теңсіздіктен табылады:

$$\left|1 - \frac{1}{\sigma^2}\sum_{i=1}^{N} C^2[i]\right| \le \varepsilon^2,$$

мұнда $C[i]$ - дискретті үдерістің аппроксимациялаушы теңдеуінің салмақты еселіктері; ал σ^2 - үздіксіз сигналдың дисперсиясы.

Сонда дискрет сигналдың толық қуаты өрнектегі қосындының модуліне тең болады, яғни: $\sum_{i=1}^{N} C^2[i]$.

Дискрет сигналдың энтропиясы келесідей болады:

$$H_d(U) = \log\left(\sqrt{1-\varepsilon^2} \bullet \sigma \bullet \sqrt{2\pi e}\right).$$

Үзіксіз қалыпты сигналдың энтропиясы жоғарыда көргеніміздей келесідей: $H(U) = \log\left(\sigma\sqrt{2\pi e}\right)$. Сонымен дискреттеу қателігінің энтропиясын келесідей табамыз:

$\Delta H(U) = H(U) - H_d(U)$, $\Delta H(U) = -\frac{1}{2}\log\left(1-\varepsilon^2\right)$.

Сонда дискреттеу қателігінің қуаты: $|\sigma_d| \ge \left|\sqrt{1-\varepsilon^2}\right| * \sigma$ болады.

1.5 Ақпараттың мағыналық түрі; мазмұндылық, маңыздылық, мақсатқа сәйкес келетіндігі, тезаурус.

Ақпараттың түрлері және оның қасиеттері.

"Информацияны" келесідей түрлерге бөлсе болады:

Синтаксикалық, мағыналық, құндылықты (прагматикалық) және таңбалықты (сигматикалық) түрлерге бөлінеді.

Синтактикалық түрі – "Информацияның" бар-жоқтығын, көлемін, жазылу ережелерін білдіреді. Тілдің немесе сөйлемнің құрылымдық жағы қаралады.

Грек тілінде синтаксис құрамдас бөлімдері деген мағынаны білдіреді. Сөздер мен таңбалар арасындағы қатысты білдіреді. Тілдің құрылымдық тарабын көрсетеді.

Екілік есептеу жүйесіндегі өлшемі - (*bit*) бит, байт болса, үштік санақ жүйесінде - *tit* , натурал санақ жүйесінде - *nat,* ондық санақ жүйесінде – *det* деп өлшенеді.

Ақпарраттық технологияда ақпаратты кедергілерден қорғау үшін әртүрлі кодтар жаратуда қолданылады; мұнда кодтар нәтижелі (тиімді) және кедергіге шыдамды (артықшылығы бар) кодтарға бөлінеді.

Мағыналық түрі – информацияның мағынасын білдіріп, хабарлар түріне қарап әртүрлі бейнеленеді.

Грек тілінде семантика - мағынасы дегенді білдіріп, ол сөздер мен таңбалардың мағыналарын білдіреді. Тілдің мағыналық тарабын көрсетеді.

Осы кезде **бейнетану пәні** тек нысандарды жіктеп қана емес, қимыл әрекеттерді де нысан деп қарайды.

Жасанды интеллект немесе сарапшы (эксперт) жүйелері ғылымындарында білімдер негізінде тиісті білімдер жинақталады. Берілген сұрақты **жүйе** алдын синтаксикалық, кейін мағыналық талдап, сұрақтың мағынасын түсінеді. Мағыналық талдаумен бәйнетану пәні шұғылданады.

Бейнетану, мағынатану (логика), ойлау үдерісін үлгілеу де көне ғылым болып, Ерте Грек ғалымы Аристотелдің "Силлогизм" ғылымынан басталады.

Бұл ғылымда ойлау үдерісі сөйлемдер және сөздермен әртүрлі амалдар орындаумен амалға асырылатын болып, бұл пән лингвистикаға жақын қаралған болса, кейінгі дәуірде жасан-

ды интеллект математикалық ойлау жүйесіне байланысты болды. Мұнда Кантордың жиындар теориясын, Булдің ойлаужүйесі (логикалық) алгебрасын, Лейбництің екілік ойлау жүйесін, Пост, Тьюринг машиналарын, Черч тезистерін, Марковтың қалыпты бағдаржолдарын және осы кездегі атақты орыс ғылымы Никольскийдің математикалық ойлау жүйесіндегі еңбектерін атау керек болады.

Алайда ақырғы кезде ИТ және нейрофизиология ғылымдары дамып, ***информация ұғымы*** да, ***ойлау үдерісі*** де әдеуір ***өзгерді;*** анықсыз ойлау жүйесі, кейін гибридті ойлау жүйесі, нейрожелілер мен генетикалық бағдаржолдар жаратылды; ***мағына ұғымы*** да басқаша түрге келді.

Мысалы, **нейрожеліге** әтірдің әртүрлісін "иіскетіп", олардың нөмірлерін атасаңыз болғаны, солардың кез келгенін анық айтып бере алады. Мұнда сөздің мағынасы заттың (нысанның) параметрлері (таңбаларымен) анықталады; параметрлер қаншалықты көп болса, нысанның мағынасы да көлемді немесе бай болады.

Адамның миы да осыған ұқсас түрде істейді; сондықтан осы кезде мағына ұғымын да толығырақ мағынада түсінетін болдық. "Информацияның" мағынасын толық түсіну үшін нысанның барлық параметрлерін (көрінісін, дыбысын, иісін, дәмін, қаттылығын, температурасын, оның химиялық және т.б. құрамдарын, динамикалық сипаттамаларын және т.б.) толық зерттеумен амалға асыруға болады.

ИТ технологияда мағына келесідей анықталады;

ең төменгі **бірінші дәрежеде** - екілік санақ жүйесінде **әрбір биттің** мағынасы былай анықталады; **1 - ақиқат** немесе шын (**true**) деген мағынаны, ал **0** – **жалған** (**falsh**) деген мағынаны білдіреді. Бұл орындағы таңбалардың мағынасы мәтінді, дыбыстық және бейне хабарлардың барлығында да қатысады.

Екінші дәрежеде мағына әртүрлі көрсетіледі;

мәтінді хабарларда **бір байт** анық бір таңбаның мағынасын білдіріп, оның сандық нөмірі – үлгі түрдегі мағыналық информацияны білдіреді.

Мәтінді хабарларда екінші дәрежеде (әріптер, таңбалар) 1 байтқа 1 таңба, 1 әріп жазылады; мұнда таңбаның анық мағынасы болып, ондағы мағынаның үлгілі өлшемі – сол кодтағы кодтың нөмірімен өлшенеді; мысалы, КОИ-8, ASCII, және т.б. код нөмірлері 128-ге дейін өзгереді.

Үшінші дәрежеде сөздер сол таңбалардың **нөмірлерінің тізбегінен** құрылып, сандар тізбегі анық жалғыз (кейде бірнеше) мағынаны білдіреді.

Төртінші дәрежеде сөйлемдер құралады; олардың мағынасы әрбір табиғи тіл грамматикасының заңдылықтарына сәйкес сөйлемдер құрайды; соларға сәйкес бірнеше қарапайым сандар тізбектерінен күрделі тізбектер құралады.

Бұл тізбектер анық мағынаға ие болады.

Сөйлемдерді құрастыруда сол тілге байланысты грамматикалық, морфологиялық, синтаксикалық, және т.б. заңдылықтар қатал сақталғанымен, сөйлемдер және олардың тізбегін құрастыру жазушының сөз байлығына, оның сөйлем құрастыру шеберлігіне, оның парасатының дәрежесіне, көбінесе оның тәжрибесіне және талантына да байланысты болады.

Алайда бұл мәселені техникада шешіп болмайды деген дұрыс емес; зияткерлік технологияның дамуы бұл мәселені де шешуі мүмкін.

Қара сөздермен кейбір ақпаратты толық жеткізіп болмайды; оның дыбыстық және көрімдік түрін ғана жеткізеді; ал иісін, дәмін анық жеткізіп болмайды. Себебі иістің, дәмнің өлшемдері болмайды. Адамзат мыңдаған жылдар ақпаратты жазба түрде тек дыбыстық ақпаратты және сурет, мүсін түріндегі ақпаратты өрнектеп үйренген. Ал иісті, дәмді осы кезде де ИТ технологиясыз анық өрнектеп болмайды.

ИТ технологияның дамуы иіс, дәм сезу ақпаратын және де басқа түрдегі ақпараттарды (мысалы, жылуды, қатты-жұмсақты, тегіс-шотыр, және т.б.) да ***өлшеу және анық жазу мүмкіндігін*** берді. Осы кезде иісті де анық өлшеу құралдары өндірісте кең қолданылып келеді. Осындай екен, дәл осы кезде мағына ұғымына да жаңаша қарау керек болады; адамның бес мүшесіне әсер ететін барлық әсер, ықпалдарды (хабарларды) техника жәрдемінде өлшесе және анық өрнектесе болады және олардағы информацияның ***анық мағынасын "есептесе"*** болады.

Ал үздіксіз хабарларда (көбінесе ән-күйлік дыбыстар) мағынаның эквивалентін анықтау қиын болады; мысалы, телефон сигналдары 1 секунд аралығында 8000 ға бөлшектеніп, солардың әрбірі 1 байтпен өрнектеледі; сонда 1 секундта 64000 бит, яғни 64 Кбит екі жақтамалы арна бойынша хабар жіберіледі. Бұл жерде дыбыстың **бір артикуляциялық көрінісі -** бөлімі бөлектеп қаралып, оның мағынасы да бөлек түрде қаралады.

Алайда сол бөлім неше биттен тұратыны анық болмайды.

Мұнда жалғыз бір нәрсені анықтаса болады; сол дыбыстың бір бөлімінде қанша көп екілік сигналдар (бит) болса, сонша оның "мағынасы" арта береді. Мысалы, ұлы ақын Абайдың "...құлақтан кіріп, бойды алар..." деген сөздерін талдау жасайтын болсақ, ән-күйлік дыбыстың адамға күшті әсері туралы айтылғанын, яғни музыканың мағынасының өте бай екенін түсінеміз.

Алайда бұл мағына қабылдаушы нысан (адам) мұзыканы жақсы түсінгенде ғана пайда болады.

Дәм мен иістің мағынасын ешқандай сөз немесе сөйлемдермен анық жеткізіп болмайды; мысалы, "шырын" деген сөз жалпы сөз болып, оның ішінде өте көп мағыналы информация болуы мүмкін; оларды анық жеткізу тек информациялық технологияның жәрдемінде ғана орындалады.

Мұнда "информация" дегеніміз Абайдың айтқан "... бойды алары ..." болып, қабылдаушы нысан (адам) оны жақсы түсінгенде ғана ұлы ақынның сөздері орынды болады; ал музыканың өзі хабар, ақпарат күйінде қала береді.

Өмірде сөйлемдердің мағынасы былай түсініледі; сөздікке жазылған сөздер мен сөйлемдер жіктелуіна қарай ***олардың тезаурусы*** құрылады; яғни ***мағыналы сөздік*** (Толковый словарь) құрылады. Әрбір сөздің мағынасы толық түсіндіріледі.

Бұл сөздіктің кемшілігі - иіс, дәм және ән-күйлік бейнелердің еш қашан да анық мағынасын (параметрлерін) көрсетіп болмайды; олар тек салыстырмалы түрде ғана жазылады.

Бұл кемшілік қазіргі күнде ақпараттық технология жәрдемінде толық шешілген; яғни иісті де, дәмді де ***толық теңестіріп (идентификациялап)*** болады.

Ондай жабдықтар химия өндірісінде, ғылыми зерттеуде, азық-түлік өндірісінде, әтір жасау өндірісі, медицина мен қорғаныста кең қолданылып келеді.

Кешегі күнде мағынаны ***сөздіктегі тезауруспен*** түсіндірсек, бүгінде мағынаны түсіндіру үшін компьютерлік құрылғылар жасалып, олардың көмегімен ***иісті де, дәмді де түсіндірсе және анық өлшесе*** болады; мысалы, адамға "электронды" қалпақ кигізіп, оған тиісті электродтар қосылса болғаны. Мұндай тәжірибеде, мысалы, адам жемеген тамағының да дәмін сезе алады.

Мұндай тәжрибелер, мысалы, Ломоносов атындағы ММУ (МГУ)

де өткізіліп жатыр. Осы кезде жылжымалы телефонда иісті жеткізіп беру сынақтан өткен. Алайда мұндай телефондарды сатуға рұқсат берілмеген.

“Информацияның” философиялық тұжырымдамасында жоғарыда туындаған сұрақтарға келесідей жауап беріледі.

…Материя қандай түрде энергиядан құралған болып, энергиямен өлшенсе, тірі әлемдегі “Сана” да (сондай-ақ ақыл-ой да) сондай түрде “информациялардан” құралған болып, “информациямен” өлшенеді....

Мұнда: макромолекула молекуланың жоғары “ұйымдасқан” түрі, келбеті болса, ал “информация” энергияның тірі әлемдегі “ұйымдасқан” немесе векторлы голограммалық келбеті болып, тек тірі нысанда ғана пайда болады;

мағына ұғымы тірі мүшенің сыртқы әсерге таралған көлемді (немесе векторлы) ***голограммалық*** түрдегі ***тітіркенуі*** болып, ол тітіркену сол таралған көлемді түрде (голограмма түрінде) сақталып қала береді. Ал денеге жаңа әсер болғанда сол әсердің мида ***сақталған бейнелерге*** **(*параметрлері бойынша*)** ***сәйкес келу дәрежесі*** мағыналық ақпаратты білдіреді.

Мұнда сыртқы әсер мен мидағы сақталған бейне 100 пайыз сәйкес келуі шарт емес; адам миы ұқсастық қағидасымен істейді.

Бейнетану ғылымында бейнелерді таңбалармен ғана анықтасақ, ал табиғатта ол таңбалардың әрқайсысы бөлек сол жалғыз голограммалық бейнелердің құраушысы түрінде болады.

Голограмма кемінде бес (осы кезде 12) түрлі сигналдармен жасалады; визуал, дыбыстық, дәм, иістік, теріден келетін физикалық (жылулық, басымдық, және т.б.) сигналдармен жасалады.

Мағына адамның миындағы сақталған “бейнелермен” ғана анықталады.

Тілші ғалымдар мағынаны жалғыз тілге эквивалент етіп қарайды.

Бұл дұрыс емес; мағына ұғымы адамның сыртқы ортадан алған барлық ***сезімдерінің жинағымен*** өлшенеді; ол жинақ әрине әртүрлі тілде есіткен сөйлемдерге, көрген көріністерге, ән-күйлік дыбыстарға, иіс, дәм және т.б. ***әртүрлі сезімдерге*** байланысты болады.

Көп тілді білген, көпті көрген және сол салада көп жұмыс істеген адам, әрине үлкен тәжірибеге, білімге ие болып, бір түрлі хабардан алатын ***мағынасы*** да көбірек болады.

Атақты ғалымдардың өмірлеріне талдау жасасақ, олардың басым көпшілігі көп тілді меңгерген, көп кітаптарды оқыған және сол салада көп амалдық жұмыс істеген адамдар болып шығады.

Музыкантар ше; олардың ән-күй (музыка) әлемінен алған мағынасын жай адам ешқашан ала алмайды.

Зияткерлік жүйелерде сыртқы ортадан хабарлар алынып, олардың барлығы өңделіп, білімдер базасына жинақтала береді.

Егер берілген сұраққа ұқсас нысандар білімдер базасынан табылмаса, жүйе сұраққа жауап бере алмайды. Себебі берілген сұрақ түсініксіз немесе мағынасы жоқ болады.

Мұнан шығатын қорытынды***, "информация" әрқашан субьективті*** болады; ал хабар, ақпарат шын түрінде қала береді.

Құндылықты (прагматикалық) түрі – бұл да субъективті ұғым болып, адамның өзінің білімдер қорына бір жағынан байланысты болса, екіншіден, адамның сол білімді қолдана білу мүмкіншілігіне де байланысты болады.

Грек тілінде *практика* дегенді білдіріп, сөздер мен тілдің амалдық пайдалылығын білдіреді; яғни тілдің қолданулық тарабын білдіреді. "Информацияның" прагматикасын зерттеген ғалым, академик Харкевич А.А. болып, ол "информацияның" құндылығын уақытқа байланысты функция түрінде қараған; оны ***пайдалылық теңдеуі*** немесе ***айып теңдеуі*** деп атаған.

Арнайы желілерде, мысалы, қорғаныс жүйелерінде, желімен жіберілетін командалар мен ақпараттар құндылығы мен шапшаңдығына қарай әртүрлі дәрежелерге бөлінеді. Сонда ақпараттың дәрежесіне қарай оның құндылығы анықталады. Ал желі ақпараттың құндылығына қарай отырып оны өңдеу тәртібін өзгертіп отырады; сонда шапшаңдығы жоғары хабарлар кезекте жыдамырақ өңделіп, ал шапшаңдығы төмендеу хабарлар баяуырақ өңделеді.

Мұндай желілер мен жүйелер ***приоритттетті* (*басымдылықты*) *жүйелер*** деп аталады.

Сигматикалық түрі – грек тілінде **таңбалар** туралы ғылым болып, таңбалар, сөздер мен нысандар арасындағы қатысты білдіреді. Тілдің сөздік тарабын көрсетеді.

"Информацияны" хабарға айналдыруда әртүрлі таңбаларды қолдану ғылымы болып, бұл ғылымның да тарихы көне заманнан басталады.

Әрине, таңбалар таңдалғанда әртүрлі шарттар қолданылған бо-

лып, соларға қарай әртүрлі тілдердің әліпбилері, әртүрлі саладағы (математика, физика, астрономия, музыка, медицина, экономика, және т.б.) ғылымдарда қолданылатын таңбалар мен таңбалар қабылданды және қолданылып келеді. Осы аталған ғылымдардың жиыны **семиотика ғылымы** деп аталады.

Семиотика ғылымы немесе **оның теориясы болған "Ақпараттар теориясы"** көне ғылым болып, оны қай заманнан басталғанын анық айту қиын.

Алайда Хартли 1928 ж. "Ақпаратты ұзату" (арнамен) атты кітабында ***"информацияны" өлшеуді*** ұсынды; ол тең ықтималды оқиғалар үшін "информацияны" энтропиямен өлшеді де, энтропияның **логарифмдік өлшемін** ұсынды; ол мына көрініште болады:

$H(X) = log(N)$, мұндағы N - оқиғалар саны.

Алайда бұл теңдеу жалпы жағдайды көрсете алмады.

Орыс ғалымы Котельников В. 1933 ж. "Теория потенциальной помехоустойчивости" ("Потециалдық кедергіге орнықтылық теориясын") жаратты. Бұл теория өз ішіне ***сигналдар теориясын*** қамтып, кейіншелік барлық байланыс техникасының құрылуына негіз болды.

1947-48 ж. АҚШ ғалымы К.Э.Шеннон "Информация теориясындағы және кибернетикадағы еңбектер" атты кітабын жариялады; ол екі бөлімнен тұрады; "Байланыстың математикалық теориясы" және "Құпия жүйелердегі ақпараттарды қорғау" деп аталды.

Кітаптың екінші бөлімінде ол ақпаратты ***қасақана кедергілерге қарсы тұруды, яғни криптотұрақтылықты (криптостойкость)*** зерттеген.

Екінші дүниежүзілік соғыс уақытында ***криптожүйелер*** ақпаратты радиоарналармен ***құпия жіберуде*** қолданылды.

Шеннон ***абсолют криптотұрақтылық ұғымын*** ендірді.

Энтропия ұғымын физик Больцман газдардың энергиясын өлшеуде, термодинамиканың 2-теориясын жаратуда қолданған. Бұл теорияны жаратуда Максвелл мен Эйнштейннің еңбектерін атап кету керек.

Хаффмен энтропия қасиеттерін пайдалана отырып, ақпаратты сығымдаушы ***нәтижелі (нәтижеивті) кодтар*** жаратты.

Дәл осындай кодтарды Шеннон мен Фано да бір уақытта жаратты.

Бұл кодтар нәтижелі кодтар болып, ақпаратты мұрағаттауда сақтауда да сигналдардың көлемін қысқартуға мүмкіндік берді.

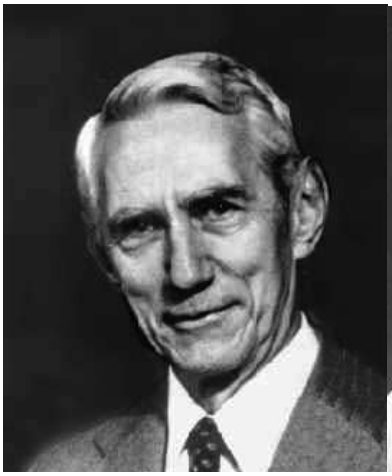
Ақпаратты сығымдауда Лемпель-Зив бағдаржолдары мәтінді хабарларды сығымдауда кең қолданылса, ал ***аудиохабарларды сығымдауда*** MPEG Audio, суретті ***бейнелерді сығымдауда*** бағдаржолдары JPEG үлгіттарында қолданып келеді.

Крипографиялық жүйелерде осы кезде ***жергілікті деректер қорында*** Шеннонның жаратқан бағдаржолы нәтижелі қолданылса, ал ***желілерде ашық кілтті жүйелер*** қолданылды; оларда негізінен осы кезде RSA (Ronald, Shamir, Adleman) бағдаржолы кең қолдану тапты.

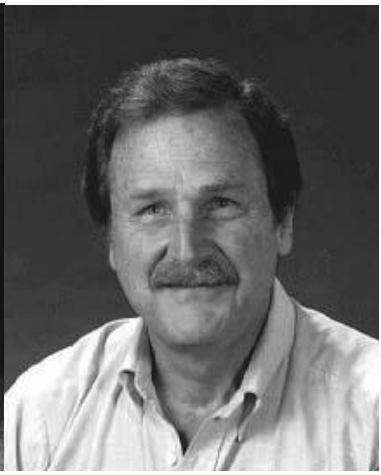
Осы саладағы атақты ғалым Хэмминг ***кедергіге орнықты кодтардың класын*** жаратты; оның кодттары ***жетілген кодтар класын*** құрайды.

Қателіктерді анықтап, түзетуші кодтары деректер қоры мен ішкі желілерде қолданылса, ал хабарлар ***жиынтығындағы (блогындағы) қателіктерді анықтаушы (циклдік) кодтар*** осы кездегі кең таралған Ғаламтор желілерінде қолданылады.

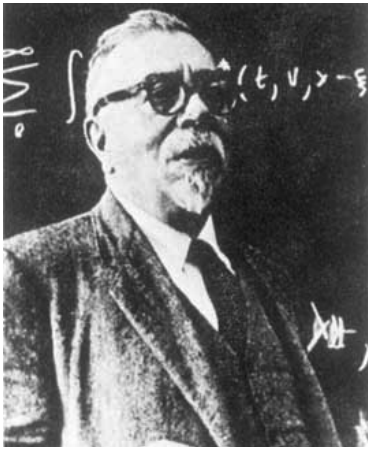
Төменде ақпараттар теориясында еңбек сіңірген ғалымдардың бейнелері көрсетілген.



Klod Shennon

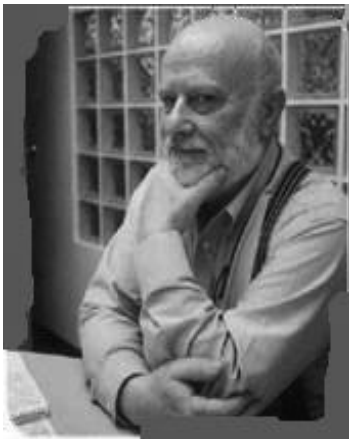


Dawid Haffmen



Norbert Winer

Donald Knut



Awraam Lemp

Richard Hamming

І тараудың бақылау және емтихан сұрақтары:

1) Қазақстанда осы кездегі жаңа философиялық бағыт қандай?

2) "Жасампаз көшбасшылық философиясының" маңызы неде?

3) Ақпарат (Информация) және кибернетика ғылымдарының тарихы, олардағы философиялық көзқарастар тарихы қандай болған?

4) Осы кездегі "информация" туралы қандай көзқарастар бар?

5) Информатика, кибернетика ғылымдарының табиғатқа байланысы; техносфера мен экосфераның, ноосфераның араларындағы байланыс қандай?

6) Ақпарат түрлері; өлшемдері; құрылымдық, геометриялық, комбинаторлық, аддитивтік (Хартли), санақтық (Шеннон) түрлері.

7) Тең ықтималды оқиғалар жүйесінде энтропия өлшемі. Информацияның аддитивтік немесе логарифмдік өлшемі. Хартли теңдеуі.

8) Ақпараттар теориясында біріне-бірі байланыссыз немесе қайталанушы оқиғалардағы ақпараттарды есептеу; Бернуллидің теңдеуімен ықтималдық есептеу.

9) Әртүрлі ықтималды оқиғалар жүйесінде энтропияны өлшеу.

10) Ақпараттың санақтық өлшемі. Шеннон теңдеуі.

11) Оқиғалар ансамблінің энтропиясы; шартсыз, шартты, өзара байланысты оқиғалар энтропиясы.

12) Энтропияның кейбір қасиеттері.

13) Энтропияны қосу ережесі, информацияның көлемін өлшеу; Тәуелді және тәуелсіз оқиғалар энтропиясы.

14) Өзара алмасу ақпараты; толық ықтималдық; Байесс теңдеуімен болжау бағдаржолы.

15) Кездейсоқ шаманың эпсилон-энтропиясы;

16) Үздіксіз хабар көзінің дифференциалдық энтропиясы; қасиеттері.

17) Кездейсоқ шаманың эпсилон-энтропиясы

18) Ақпараттың мағыналық түрі; мазмұндылық, маңыздылық, мақсатқа сайкес келетіндігі, тезаурус.

19) Ақпараттың түрлері және оның қасиеттері.

20) Дискрет оқиғалар энтропиясы.

21) Энтропияның қасиеттері.

Өзіндік жұмыстар (ӨЖ) тақырыптары:

1) Президент Н. Назарбаевтың “Жасампаз көшбасшылық философиясы” және оның осы кездегі дүниежүзілік үдерістерге әсері.

2) Өткен замандардағы ақпарат (Информация) туралы философиялық көзқарастар және осы кездегі философиялық көзқарастарды талдау.

3) Ақпараттар теориясының ақпараттық технологияның дамуындағы орны.

4) Ақпараттық технологияның инфосфера және ноосфера құрылысындағы орны.

5) Инфосфера, ноосфера, техносфера және “ғарыштық сана” тісініктерінің арасындағы байланысты талдау.

6) Ақпарат түрлері; өлшемдері.

7) Тең ықтималды оқиғалар жүйесінде энтропия өлшемі

8) Ақпараттар теориясында біріне бірі байланыссыз немесе қайталанушы оқиғалардағы ақпараттарды есептеу; Бернуллидің және Пуассон теңдеулері.

9) Ақпараттың санақтық өлшемі. Шеннон теңдеуі.

10) Оқиғалар ансамблінің энтропиясы; шартсыз, шартты, өзара байланысты оқиғалар энтропиясы.

11) Энтропияны қосу ережесі, информацияның көлемін өлшеу; Тәуелді және тәуелсіз оқиғалар энтропиясы.

12) Өзара алмасу ақпараты; толық ықтималдық; Байесс теңдеуі.

13) Кездейсоқ шаманың эпсилон-энтропиясы;

14) Үздіксіз хабар көзінің дифференциалдық энтропиясы; қасиеттері.

15) Ақпараттың мағыналық түрі; мазмұндылық, маңыздылық, мақсатқа сәйкес келетіндігі, тезаурус.

II ТАРАУ

СИГНАЛДАР МЕН ҮДЕРІСТЕРДІҢ ҮЛГІЛЕРІ

2.1 Сигнал түсінігі, үлгілері; сигналдың сипаттамалары; уақыттық, жиіліктік, векторлық (геометриялық) сипаттамалары

Сигнал деп жалпы жағдайда материалдық энергетикалық хабарларды тасушыларға айтамыз.

Сигналдарды табиғи және бір мақсатпен құрылған арнайы сигналдар деп бөлсе болады. Табиғи сигналдарға, мысал үшін, табиғи жарық сигналдарын жатқызса болады. Ал арнайы сигналдарға нысандардың күйін анықтау және өлшеу үшін қолдан жаратылған (эталондық) сигналдарға айтамыз.

Төменде тек қана арнайы сигналдар қаралып, олар ақпараттық жүйелерде хабарларды тасымалдау үшін ғана жаратылады.

Сигналдың негізін қандайдір бір физикалық нысан немесе үдеріс құрайды да оған хабар (ақпарат) тасушысы деп атайды.

Модуляция үдерісінде тасушы сигналға айланады. Мұнда тасушы параметрі жіберілетін хабарға сәйкес уақыт аралығында өзгеріп, ол **информативті** деп аталады.

Ақпарат тасушысы ретінде әртүрлі табиғатты тербелістер қолданылады, көбінесе гармоникалық, мысалы, өзгермес жиіліктегі тербелістер $(\omega = const)$. Техникалық ақпараттық жүйелерде электр кернеуі немесе тоғы түріндегі тасушылар кең қолдану тапты.

Сондықтан келешекте сигналдардың үлгісін қарастырғанда тек электр сигналдарын қарастырамыз. Мысалы, u(t) = const тасушысында тек бірғана информативтік параметр (кернеу деңгейі) бар.

Гармоникалық электр тербелісін қолданғанда информативтік параметр болып амплитуда, жиілік, фаза болуы мүмкін.

Мұнда тербелістер детерминделген және кездейсоқ болуы мүмкін. Детерминделген тербелістерде тербелістің параметрлері уақыт мезгілдерінде анық мәлім болады.

Ал кездейсоқ тербелістерде параметрлердің мәндері алды ала мәлім болмайды. Олар екі түрде ұшырайды; бізге керекті ақпаратты тасу үшін қолданылғанда кездейсоқ сигналдар түрінде

қарастырылса, ал біз бақылаған сигналдарға кедергі келтірсе, оларды кедергі (бөгеуіл) деп қараса болады.

Байланыс арналарын, сигналдарды, бөгеуідерді қарастырғанда олардың физикалық табиғатына, мағынасына және қолдануына көңіл бөлмейміз; тек олардың үлгілерін қарастырамыз.

Үлгі бұл нысанды, үдерісті, оқиғаны бейнелеу түрі болып, шешілетін мәселеге қажетті **әсер, ықпалдарды** көрсетеді.

Байланыс арналары мен ақпарат көзін сипаттайтын негізгі параметрлердің арасындағы сандық қатыстарды **орнатумен** ақпараттық жүйенің **нәтижелілігін арттыру мәселесі** шешіледі.

Сондықтан зерттеуде математикалық үлгілер қолданылады. Математикалық үлгілер әртүрлі әдістермен орындалады; бұл бізді қызықтыратын көрсеткіштерге байланысты болады.

Орнықты зерттеулер, негізінен, аналитикалық үлгілеуге негізделген болып, мұнда үлгі параметрлердің арасында математикалық байланыстар жиынымен көрсетілді. Мұнда көбінесе кейбір үлгілердің параметрлері нақты нысандардың физикалық қасиеттеріне сәйкес келмейді. Мысалы, сигнал үлгісі шексіз көп шектелмеген қатыстар (синусойдалар) жиыны түрінде көрсетіледі. Ал бұл нақты жағдайға сәйкес келе бермейді; себебі нақты арналардағы сигналдардың спектрлері әрқашанда шектелген болады. Сондықтан нақты жағдайда қолданылатын және анық нәтиже беретін үлгілер құру қажетті болады.

Нақты жағдайда хабар көзінен шығатын сигнал мәні кез келген уақытта қандай болатынын анықтау мүмкін болмайды, яғни ол кездейсоқ болады. Сондықтан сигналдың аналитикалық үлгісі тек кездейсоқ үдерістің ықтималды сипаттамасы түрінде көрсетіледі.

Детерминделеген сигналдарға детерминделген тербелістер сәйкес келеді; мұндай сигналдар алдын ала мәлім хабарларға сәйкес келіп, оларды байланыс арналармен жіберудің ешқандай мағынасы болмайды. Оған уақыт аралығында толық анықталған функция сәйкес келеді.

Детерминделген сигнал үлгілерін үйрену көптеген себептерге байланысты керек болады; мысалы, детерминделген сигналдардың нәтижелерін талдау өте күрделі кездейсоқ сигналдарды зерттеу мүмкіндігін береді. Бұл кездейсоқ үдерісті көптеген детерминделген қатыстардың жиыны түрінде қарасытруға мүмкіндік береді.

Сонда детерминделген тербелісті уақыт мезгілінде параметрлері

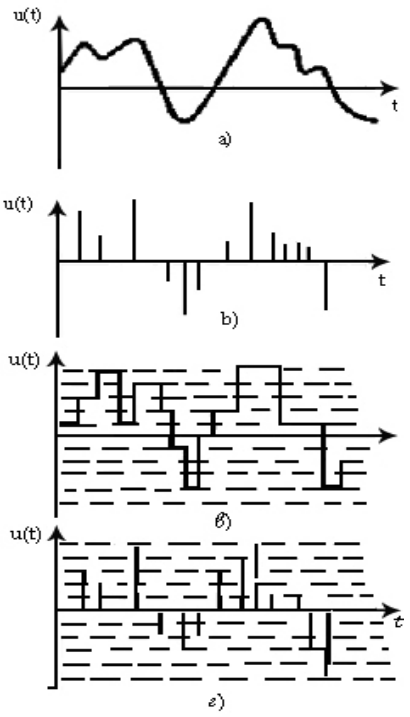
анықталған кездейсоқ үдерістің түрі деп қарастырылады. Бұдан тыс детерминделген сигналдардың өз алдына басқа да мақсатта қолданылуы да бар; ол ақпараттық техниканың нысандарін өлшеу, баптау, реттеу мақсатында да қолданылады.

Детерминделген сигналдарды көрсету келбеті.

Информациялық параметрдің құрылысына қарай сигналдар дискретті, үздіксіз және дискретті-үздіксіз деп бөлінеді. Егер сигналдың бірер параметрінің мәні шекті және санақты болса, онда берілген параметр бойынша сигнал **дискретті** деп аталады. Егер параметрдің мүмкін мәндері континуум құраса, онда сигнал осы параметр бойынша **үздіксіз** болады. Егер сигнал бір параметр бойынша дискретті,

екінші параметр бойынша – үздіксіз болса, онда сигнал **дискретті-үздіксіз** деп аталады.

Осыған орай детерминделген сигналдардың математикалық үлгілерінің келесідей түрлері болады:



(сурет 2.1.)

1. үздіксіз аргументтің үздіксіз теңдеуі, уақыт бойынша үздіксіз функция (сурет 2.1.а) ;

2. дискрет аргументтің үздіксіз теңдеуі, мысалы, функцияның мәндері тек анық бір мезгіліндерде саналады (сурет 2.1.б);

3. үздіксіз аргументтің дискретті теңдеуі, мысалы, уақыт бойынша кванталған функция (сурет 2.1.в) ;

4. дискрет аргументті дискрет функция, мысалы, анық уақыт мезгілдерінде функция мүмкін болған шекті мәндердің бірін қабылдайды (сурет 2.1.г).

Уақыт теңдеуі түрінде қаралған сигнал үлгілері бірінші кезекте сигнал келбетін талдауға арналған. Сигналдың байланыс арнасы арқылы өтуін

зерттеу мәселесін шешуді оңайлататын көрсету түрін табу керек болады.

Осы мақсатта күрделі сигналдар базистік элементер қатыстар жиыны түрінде көрсетіледі; бұл кейінгі талдауды оңайлатады.

Көп зерттелетін жүйелердің кең класы – бұл уақыт бойынша инвариантты сызықты жүйелер. Күрделі $u(t)$ сигналының осындай жүйеден өтуін талдауда сигналды $\varphi_k(t)$ базистік қатыстарының салмақты қосындылары (немесе оған сәйкес интегралы) түрінде көрсетсе болады:

$$u(t) = \sum c_k \varphi_k(t), \qquad t \in [t_1, t_2], \tag{2.1}$$

мұнда $[t_1, t_2]$ - сигналдың жарамдылық аймағы.

Базистік қатыстардың таңдалған (2.1) жиынында u(t) сигналы c_k өлшемсіз еселіктерінің жиынымен анықталады. Сандардың осындай жиынын сигналдың дискрет спектрі деп атайды. $[t^1, t^2]$ аралығында (2.1) өрнегі уақыт бойынша шектелмеген сигнал үшін де, шекті ұзындықтағы сигнал үшін де орынды болады. Алайда $[t^1, t^2]$ аралығының сыртында да шекті ұзындықтағы сигнал нөлге тең болмайды, себебі қосындының сыртында да сигнал кезеңді түрде жалғаса береді. Сондықтан уақыт бойынша шектелген сигналды кез келген мезгілінде көрсету үшін интегралды қолданған жөн болады:

$$u(t) = \int_{-\infty}^{\infty} S(\alpha)\varphi(\alpha, t)d\alpha, \tag{2.2}$$

мұнда $\varphi(\alpha, t)$ - α үздіксіз өзгеруші параметрлі базистік функция.

Осы жағдайда сигналдың үздіксіз спектрі $S(\alpha)$ спектралды тығыздық теңдеуімен көрсетіледі. Оның өлшемі α ның өлшеміне кері болады.

Өлшемсіз еселік c_k - ның ұқсасы $S(\alpha)d\alpha$ болады.

Сигналдарды (2.1) және (2.2) түрінде көрсету әдістерінің жиыны сигналдардың *жалпыланған спектралдық теориясы* деп аталады.

Сызықтық теория шеңберінде **спектрлер** сигналдарды аналитикалық түрде көрсетудің қолайлы түрі болады.

Теориялық талдау үшін $\varphi_k(t)$ базистік қатыстарын таңдауда мыналарға мән беру керек: (2.1) - қатардың кез келген $u(t)$ үшін жылдам жинақталуын қамтамасыз ететін қарапайым аналитикалық өрнек

болуы керек және ол өрнек c_k еселіктерін оңай есептеу мүмкіндігін беруі керек. Базисті қатыстар нақты болуы шарт емес, олардың саны да шексіз болуы мүмкін $(-\infty \geq k \geq \infty)$.

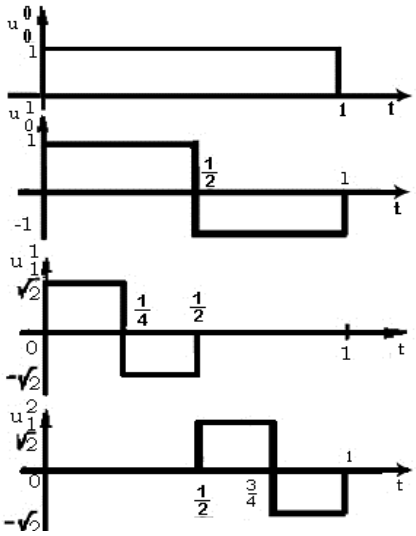
Амалдық жағдайларда нақты сигналдарды базистік сигналдармен аппроксимациялауда олардың техникалық орындалуы негізгі шешуші қызмет атқарады. Мұнда сигнал шекті санды $(0 \leq k \leq n)$ нақты сызықты байланыссыз базистік қатыстардың қосындысы түрінде көрсетіледі.

Сигналдардың ортогоналдық көрсетілуі.

Базис ретінде ортогонал қатыстар жүйесін таңдап алу сигналдың спектралдық құрамдастарын есептеуді әжептеуір оңайлатады.

$\psi_0(t)$, $\psi_1(t)$, ..., $\psi_k(t)$, ..., $\psi_j(t)$, ..., $\psi_n(t)$ қатыстар жүйесі $[t_a, t_b]$ кесіндісінде ортогонал деп аталады, егерде $k = j$ ден басқа барлық $k = \overline{0,n}$; $j = \overline{0,n}$ лерде мына шарт орындалса:

$$\int_{t_a}^{t_b} \psi_j^2(t)dt = \mu_j > 0, j = \overline{0,n}, \quad \int_{t_a}^{t_b} \psi_k(t)\psi_j(t)\,dt = 0. \tag{2.3}$$



(сурет 2.2.)

Осы қатыстар жүйесі ортоқалыптыланған (ортонормалданған) болады, егерде $j = \overline{0,n}$ - лердің барлығында төмендегі (2.4) шарт орынды болса:

$$\int_{t_a}^{t_b} \psi_j^2(t)\,dt = 1 \tag{2.4}$$

Егерде (2.4) қатысы орындалмаса, онда жүйені қалыптылау үшін $\psi_j(t)$ қатыстарын (қатыстарын) $1/\sqrt{\mu_j}$ на көбейту керек;

$u(t)$ сигналын ортоқалыптыланған қатыстар жиынымен көрсету үшін

c_k еселігін анықтаймыз:

$$u(t) = \sum_k c_k \psi_k(t), \; t \in [t_1, t_2] \qquad (2.5)$$

мұнда $[t_1, t_2]$ аралығы $[t_a, t_b]$ ортогоналдық кесіндісінің ішінде жатады деп ұйғарамыз. (2.5) теңдеуінің оң және сол жақтарын $\psi_j(t)$ ке көбейтеміз және есепке алмаймыз; сонда $[t_1, t_2]$ аралығында келесідей болады:

$$\int_{t_1}^{t_2} u(t)\psi_j(t)dt = \sum_k c_k \int_{t_1}^{t_2} \psi_j(t)\psi_k(t)dt \qquad (2.6)$$

(2.3) шарты орындалғандықтан (2.6) өрнегінің оң жағындағы барлық интегралдар $k \neq j$ болғанда 0 ге тең болады.

Ал $k = j$ болғанда (2.4) ке сәйкес интеграл 1 ге тең болады.

Сондықтан,

$$c_k = \int_{t_1}^{t_2} u(t)\psi_j(t)dt \qquad (2.7)$$

Теориялық зерттеулерде ортогонал қатыстардың толық жүйесі қолданылады; мұнда $u(t)$ үздіксіз теңдеуі қатардың мүшелер саны шексіз көбейгенде өзінің қатарынан айырмашылығы қалағанша кем болуы мүмкін;

осы айырмашылық мына шарт бойынша анықталады:

$$\delta = \int_{-\infty}^{\infty} \left[u(t) - \sum_k c_k \psi_k(t) \right]^2 dt \; . \qquad (2.8)$$

Мынаны $\sum_k c_k \psi_k(t)$ қатардың $u(t)$ теңдеуіна *орта квадраттық жинақталуы* деп атайды.

Кең таралған ***ортоқалыптыланған жүйе*** деп еселі аргументті тригонометриялы қатыстардың келесідей жиынын атаса болады:

$$\frac{1}{\sqrt{\pi}} \cos k\frac{2\pi}{T}t; \; \frac{1}{\sqrt{\pi}} \sin k\frac{2\pi}{T}t, k = 1,2,3,...$$

Ол мына $[-\pi, \pi]$ кесіндіде ортоқалыпты болады.

Осы қатарға жіктеу тарихи бірінші болған және *Фурье қатары* деп аталған; сондықтан (2.5) өрнегі Фурьенің *жалпыланған қатары* деп, ал $\tilde{n}_k$ - ны Фурьенің *жалпыланған еселіктері* деп аталады.

2.2 - суретте Хаар қатыстар жүйесі берілген; суретте оның 0-1 аралығында ортоқалыптылығы көрініп тұр.

Сигналдардың Котельников, Чебышев, Лаггер, Лежандр және т.б. ортогонал базистік көпмүшеліктер жиыны түрінде өрнектелуі мәлім.

Сондай ақ Лагранж, Тейлор және т.б. қатыстар бойынша **ортогонал болмаған** жіктеулер де мәлім.

Үдерістерді талдаудың айқын мәселелері үшін **базистік қатыстарды (функцияларды) дұрыс таңдау мәселесін** шешуді жалпы спектралды теория біршама жеңілдетеді; мұндай мәселелер сигналды қалыптастыруда және оның ақпараттық жүйенің кейбір бөлімінен өтуінде пайда болады.

Уақыт бойынша дискреттегенде әрбір t_i уақыт мезгілінде $x(t_i)$ санақ мәндерін Δt_i аралықтарында алынады; үздіксіз сигналды қайта тіктеген уақытта кейбір $V(t)$ *тіктеуіш теңдеуі* қолданылып, осы функция кейбір $f(t-t_k)$ қатыстар қатарының салмақталған қосындысы түрінде болады: $V(t)=\sum_k a_k f(t-t_k)$.

Осы жерде келесідей тиімділеу мәселесі келіп шығады; уақыт қадамын Δt_i кемейткенде, қайта тіктеу уақыты көбейеді.

Мұнда кванттау құрылымының жылдамдығы нөлге дейін кемейуі мүмкін болып, дискрет өлшемдердің артықшылығы шексіз өсуі мүмкін болады.

Осыдан шығатыны, дискреттеу қадамын $\Delta t_i \to \min$ минималдай отырып және тіктеуде талап етілген анықтықты қамтамасыз ете отырып, дискреттелген хабардың артықшылығын минималдау керек болады.

Мұнда **тіктеу анықтығын бағалау шарты** келесідей болуы мүмкін:

максималды, **орта квадратты**, **интегралды**, **ықтималды,** сондай ақ **қателіктің қуатымен** және **информациялық (энтропиялық)** өлшеммен өлшенуі мүмкін.

Ағымдағы қателіктің мәні $\xi(t)$ сигналдың мәндері $x(t)$ мен тіктеуші функцияның $V(t)$ мәндері арасындағы айырма түрінде анықталады: $\xi(t)=x(t)-V(t)$.

Дискреттеу және қайта тіктеу **қателіктерін бағалау шартын** сигналды қабылдаушының өзі таңдайды; оны дискрет сигналды алғандағы *мақсатқа* және *аспаптық, бағдарламалық орындалуына* байланысты түрде алады.

Дискреттеу аралығы $\Delta t_i = t_i - t_{i-1}$ арасында $V(t)$- ның $x(t)$- дан ауытқуы мына ***шарттармен*** бағаланады;

1) Сызықты метрикалық кеңістікте ***ең үлкен ауытқу шарты*** (Чебышев метрикасында):

$$\xi_v = \max_{t\in\Delta t_i}|\xi(t)| = \max_{t\in\Delta t_i}|x(t)-V(t)|.$$

Егерде сигнал туралы мәліметтер априор түрде Липшиц шарты бойынша анықталған болса, онда осы шартты қолдану қолайлы болады;

$$|x(t)-x(t')| \le \ell|t-t'| \text{ және } \left|x^n(t)-x^n(t')\right| \le \ell\left|t-t\ \right|,$$

мұнда ℓ - кейбір константа, ал $x^n(t)$- n-ші $x(t)$ функцияның туындысы.

2) Гильберттік кеңістіктегі ***орта квадраттық шарт***:

$$\overline{\xi}^2 = \sqrt{\frac{1}{\Delta t_i}\int_{\Delta t_i}\xi^2(t)dt} = \sqrt{\frac{1}{\Delta t_i}\int_{\Delta t_i}|x(t)-V(t)|^2\,dt} = \sqrt{\frac{1}{\Delta t_i}\int_{\Delta t_i}|x(t)-V(t)|^2\,dt}$$

$$(x,v) = \frac{1}{\Delta t_i}\int_{\Delta t_i}x(t)V(t)dt.$$

Мұнда,

Көбінесе мына түрдегі шарт қолданылады:

$$\overline{\xi}^2 = \sqrt{\int_{\Delta t_i}\xi^2(t)dt}.$$

Бұл шарт квадратта интегралданатын қатыстар үшін қолданылады, яғни:

$$\int_a x^2\,dt \prec \infty\left(-\infty \le a \prec b \prec \infty\right).$$

Әртүрлі дискреттеу қадамдарында аспаптың күрделенуінен бұл шартты қолдану мақсатқа сай емес;

3) Интегралдық шарты мына түрде болады:

$$\overline{\xi} = \int_{\Delta t_i} \xi(t)dt .$$

4) Ықтималдық шарты мына түрде болады:

$$P(\xi(t) \prec \xi_0) = P_0 .$$

Мұнда ξ_0 - қателіктің мүмкін мәні; P_0 - ықтималдықтың мүмкін мәні болып, ол қателік ξ_0 ден аспайды.

5) Қателіктің салмақтық бағасы шарты :

$$\overline{\xi}^2 = \sqrt{\frac{1}{\Delta t_i} \int_{\Delta t_i} P(t)\xi^2(t)dt} ,$$

мұнда $P(t)$ - салмақтық функция.

Кванттау қателігінің қуаты шарты:

Көптеген жағдайларда үздіксіз сигналдар Марковтік емес және спектрлері шектелмеген болады.

Мұндай сигналдарды кванттағанда қателіктің болуы сөзсіз болып, қателік мөлшері мүмкін болған қателік ε^2 қуатымен анықталады.

Амалдық мәселелерде салмақты еселіктердің және қосылғыштардың саны мына теңсіздіктен табылады:

$$\left|1 - \frac{1}{\sigma^2} \sum_{i=1}^{N} C^2[i]\right| \le \varepsilon^2 ,$$

мұнда $C[i]$ - бағдаржолдың кванттау еселіктері Фурьенің еселіктерімен сай келеді.

7) Кванттау ***қателігін*** бағалаудың ***энтропиялық шарты*** [70] :

энтропиялық қателік өлшемі сол қателіктің $\Delta H(X)$ энтропиясымен анықталады. Қателік энтропиясын келесідей тапса болады:

$$\Delta H(X) = H(X) - H_d(X),$$

$$\Delta H(X) = -\frac{1}{2}\log(1 - \varepsilon^2)$$

8) Қателіктің ***орта квадраттық ауытқуы***:

$$\Delta H(X) = -\frac{1}{2}\log(1 - \varepsilon^2)$$

9) Қателіктің ***орта квадраттық мәні***:

$\eta_E^2 = M\left[E^2(t_i)\right] = \sigma_E^2 + m_E^2$, мұнда $m_E = M\left[E(t_i)\right]$.

Берілген сигнал $x(t)$ ні оның дискрет мәндері $x(t_i)$ мен тіктеу уақытында жалпыланған көпмүшелік $V'(t) = \sum_{j=0}^{n} a_j \varphi_j(t)$, таңдап алынып, оның t_i санақ нүктелеріндегі мәндері $x(t)$ теңдеуінің мәндерімен сәйкес келеді.

Дискреттеу және қайта тіктеу мәселелерінде толық ортоқалыпты жүйелер кластары қолданылады: Фурье, Котельников қатарлары, Чебышев, Лежандр, орынды полиномдар, Лаггер, Лежандр, Чебышев, Уолш, Эрмит, Хаар, гипергеометриялық қатыстар және басқалар.

1) **Кешенді гармоникалық қатыстар.**

$T = [-1,+1], \omega(t) = 1$, мұнда T – уақыт аралығы, $\omega(t)$ – салмақты функция, кешенді гармоникалық қатыстар $\{\varepsilon^{j\pi nt}; n = 0, \pm 1, \pm 2, ...\}$, ортогоналды болып, Фурье қатарына $[-1,+1]$ кесіндіде 2 кезеңімен жіктегенде мына түрде болады: $x(t) \approx \frac{1}{\sqrt{2}} \sum_{k=-n}^{n} \alpha_k e^{j(\pi kt)}$, мұнда

$$\alpha_k = \int_{-1}^{+1} x(t) e^{-j(\pi kt)} dt \quad .$$

2) **Лежандр полиномы.**

Мына $T = [-1,+1], \omega(t) = 1$ болып, мына тізбек үшін $\{1, t, t^2, t^3, ...\}$ келесідей қалыптыланған полиномдар алынған:

$$\varphi_0(t) = \frac{1}{\sqrt{2}}, \varphi_1(t) = \sqrt{\frac{3}{2}} t, \varphi_2(t) = \sqrt{\frac{5}{2}}\left(\frac{3}{2}t^2 - \frac{1}{2}\right) ... \varphi_n(t) = \sqrt{\frac{2n+1}{2}} P_n(t),$$

мұнда $\{P_n(t)\}$ – Лежандр полиномы келесідей есептеледі:

$$P_n(t) = \frac{1}{2^n n!} \bullet \frac{d^n}{dt^n}(t^2 - 1)^n ,$$

$$nP_n(t) = (2n-1)tP_{n-1}(t) - (n-1)P_{n-2}(t).$$

Полиномның барлық n нөлдері $P_n(t)$ нақты болып, $[-1,+1]$ аралықтың ішінде жатады.

3) **Чебышев полиномы.**

Мына үшін $T = [-1,+1], \omega(t) = \left[1 - t^2\right]^{-\frac{1}{2}}$ төмендегі полиномдар $\varphi_n(t) = 2^n (2\pi)^{-\frac{1}{2}} T_n(t); n = 0,1,2,...$ ортогоналдық жүйе құрады.

Чебышев полиномдары төмендегідей беріледі:

$$T_0(t)=1; T_n(t)=\frac{1}{2^{n-1}}\bullet Cos\ (n * arc\ * Cos\ (t)); n \geq 1 .$$

Мына $n \geq 3$ үшін $T_n(t)$ рекуррентті теңдеумен есептеледі: .

$$T_n(t) = tT_{n-1}(t) - \frac{1}{4}T_{n-2}(t).$$

4) **Котельниковтың қатарлары мен функциялары.**

Котельниковтың санақтар теоремасында үздіксіз "ақ шуыл" $x(t)$ мына жиілікпен ω_c шектелген спектрлі болсын; онда оны өте анық түрде мына дискретті "ақ шуылмен" $x[n\Delta t]$ көрсетіп, оның параметрлері $(0,\sigma^2)$ болады. Дискрет $x[n\Delta t]$ "ақ шуыл" Котельников қатарымен мына түрде көрсетіледі:

$$x(t)=\sum_{-\infty}^{\infty} x[n]f_n(t), \text{мұнда}$$

$$f_n(t)=\frac{Sin\ [\omega_c(t-n\Delta t)]}{\omega_c(t-n\Delta t)},\ x[n]=x(n\Delta t).$$

Ақырында тіктеуші функция мына түрде болады:

$$x'[n]=\sum_{n=-\infty}^{\infty} C_0[k]x[n-k].$$

Мұндағы $C_0[k]$ - еселіктері $R_0(j\omega)$ теңдеуін $(-\omega_c,\omega_c)$ аралықта Фурье қатарына жіктегендегі Фурье еселіктеріне сәкес келеді.

Қосындының мүшелері шектелгенде мына түрде болады:

$$x'[n]\approx x^*[n]=\sum_{k=1}^{N} C_0[k]x[n-k],$$

мұнда $N=2P+1, C_k=C_0[k-P-1]$.

5) Лаггер полиномдары.

Мына үшін $T=[0,\infty], \omega(t)=e^{-t}$ төмендегі полиномдар ортоқалыпты жүйе құрады.

$L_{nn}(t)=e^t\frac{d^n}{dt^n}(t^n e^{-t})-$ Лаггер полиномы.

$L_{nn}(t)=(2n-1-t)L_{n-1}(t)-(n-1)^2 L_{n-2}(t).$

Лаггер қатыстары мына түрде болады: $\psi_n(t)=\frac{e^{-\frac{t}{2}}}{n!}L_n(t)$.

Олар $[0,\infty]$ аралықта бірлік салмақта ортогонал болады.

Оларды мына тізбекке Грамм-Шмидт шарасын қолданып шығарса болады: $\left\{t^n e^{-\frac{t}{2}}, n=0,1,2,...\right\}$.

Лаггер теңдеуінің жәрдемінде трансверсалді сүзгілер құрса болады да олардың шығуында кез келген үлгідегі серпіндік (импульстік) тітіркену (реакция) алса болады.

6) Лежандр фунциясы**.**

Мына түрде болады: $\pi_n(t) = \left[2P(2n+1)\right]^{\frac{1}{2}} e^{-pt} P_n\left(1-2e^{-2pt}\right)$ мына бірлік салмақты аралықта $[0,\infty]$ ортоқалыпты жүйе құрады;

мұнда p - қалауынша алынған оң нақты параметр.

Лежандр қатысын (фунциясын) Лежандр полиномынан келесідей қойылыммен алса болады: $\tau = 1-2e^{-2pt}$; мұнда τ үшін аралық $[-1,1]$ өзгеріп, мына түрге келеді: $[0,\infty]$.

7) Чебышев фунциясы**.**

Чебышев полиномынан келесідей өзгертулермен

$\tau = 1 - 2e^{-2pt}$

Чебышев қатысын алса болады:

$$\rho_n(t) = 2^n \left(\frac{p}{\pi}\right)^{\frac{1}{2}} T_n\left(1-2e^{-2pt}\right),$$

олар $[0,\infty]$-да мына салмақпен $\omega(t) = \left(e^{-2pt}-1\right)^{-\frac{1}{2}}$ ортоқалыпты болады.

8) Эрмит теңдеуі.

Келесідей

$T=[-\infty,\infty], \omega(t)=e^{-t^2}$ үшін $\varphi_n(t) = \left(2^n n!\sqrt{\pi}\right)^{-\frac{1}{2}} H_n(t), n=0,1,2,...$ полиномдары ортоқалыпты жүйе құрады. Эрмит полиномы мына түрде болады:

$H_n(t) = (-1)^n e^{t^2} \dfrac{d^n}{dt^n}\left(e^{-t^2}\right)$ және $H_n(t) = 2tH_{n-1}(t) - 2(n-1)H_{n-2}(t)$.

$\psi_n(t) = \left(2^n n!\sqrt{\pi}\right)^{-\frac{1}{2}} e^{-\frac{t^2}{2}} H_n(t)$ түрдегі Эрмит теңдеуі бірлік салмақта $[-\infty,\infty]$ ортоқалыпты болады.

9) Уолш теңдеуі.

Мына үшін толық ортоқалыпты қатыстар жүйесін құрса болады.

Сонда Уолш теңдеуі мына түрде болады:

$\varphi_0(t) = 1, 0 \le t \le 1;$ $\varphi_1(t) = \left\{ \begin{matrix} 1;\ 0 \le t \le \frac{1}{2} \\ -1;\ \frac{1}{2} < t \le 1 \end{matrix} \right\}$;

$$\varphi_2^{(1)}(t) = \left\{ \begin{matrix} 1;\ 0 \le t < \frac{1}{4};\ \frac{3}{4} < t \le 1; \\ -1;\ \frac{1}{2} < t < \frac{3}{4} \end{matrix} \right\}$$

$$\varphi_{m+1}^{(2k)}(t) = \left\{ \begin{array}{l} \varphi_m^{(k)}(2t);\ 0 \le t < \frac{1}{2}; \\ (-1)^k \varphi_m^{(k)}(2t-1);\ \frac{1}{2} < t \le 1; \end{array} \right\},$$

мұнда $m = 1,2,3,...$ және $k = 1,2,3,...,2^{m-1}$

Уолш теңдеулері (қатыстары) есептеу техникасында екілік ойлаужүйесі сұлбалар құруда және автоматиканың дискретті жүйелерінде үздіксіз-сандық түрлендірушілерде кең қолданылады

Сигналдың уақыт бойынша көрсетілуі.

Сигналдың уақыт бойынша өрнектеуде *u(t)* сигналының базистік теңдеуі ретінде бірлікті серпінді қатыс (функция) болған - дельта-серпін (импульс) қолданылады. Осындай қатыстың математикалық сипаттауы келесідей қатынаспен

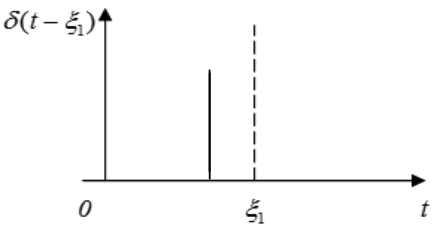
$$\delta(t) = \begin{cases} \infty,... = 0 \textit{ болғанда}, \\ 0,.... \neq 0 \textit{ болғанда}, \end{cases}$$

көрсетіледі:
$$\int_{-\infty}^{\infty} \delta(t)dt = 1, \qquad (2.9)$$

мұнда δ(t) — дельта-фунциясы болып, координат басында нөлден айырықты болады ($t = 0$ де). Ал егер уақыт мезгілі нөлден басқаша болса $t = \xi_1$ (төмендегі 2.3- сурет), келесідей болады:

$$\delta(t - \xi_1) = \left\{ \begin{array}{l} \infty,\ t = \xi_1, \\ 0,\ t \neq \xi_1, \end{array} \right.$$

$$\int_{-\infty}^{\infty} \delta(t - \xi_1)dt = 1.$$



2.3- Сурет (2.10)

Осындай математикалық үлгі шексіз кіші ұзындықтағы және шексіз үлкен амплитудалы абстракт серпінге сәйкес келеді.

Нақты сигналды бірден-бір анық көрсетуші параметр бұл оның әсер ету уақыты болып табылады. Алайды, (2.10) есепке ала отырып, дельта-фунция нақты $u(t)$ сигналының айқын уақыт мезгіліндегі мәнін білдіреді:

$$u(\xi_1) = \int_{-\infty}^{\infty} u(t)\delta(t - \xi_1)dt \qquad (2.11)$$

(2.11) теңдігі кез келген ағындағы t уақыт мезгілінде орынды болады. Осында ξ_1 ді t мен ауыстырып және интегралдау айнымалысы ретінде ξ ді қабылдап, мынаны аламыз:

$$u(t) = \int_{-\infty}^{\infty} u(\xi)\delta(\xi - t)d\xi = \int_{-\infty}^{\infty} u(\xi)\delta(t - \xi)d\xi \qquad (2.12)$$

Сөйтіп, $u(t)$ теңдеуі шексіз кіші ұзындықты бір-біріне тиіскен серпіндер жиыны түрінде көрсетіледі. Осындай серпіндердің ортогоналдығы көрініп тұр, себебі олар уақыт бойынша бір-бірімен қиылыспайды.

(2.12) жіктеуінің сызықты жүйелер теориясындағы мәні зор; осындайда кез келген үлгідегі сигналға жүйенің тітіркенуін табу үшін осы жүйенің кірудегі дельта-серпін түріндегі элементер сигналға тітіркенуін (тітіркенуін) (серпіндік өткізу теңдеуін) табу керек;

кез келген түрдегі берілген сигналға **жүйенің көрсеткен тітіркенуін** табу үшін аталған жолмен берілген сигналдың "ауданын" толық қамтитын шексіз көп біріне-бірі тиіскен дельта-серпіндер тізбегінен пайда болған жүйе тітіркенулерінің суперпозициясы табылады.

Дельта-серпін жәрдемінде идеал түрдегі деңгейі өзгермейтін немесе өзгеретін серпіндердің кезеңді тізбегін көрсету мүмкін.

$t = k\Delta t$ нүктелерінде $u^{\text{ї}}(t)$ теңдеуінің мәндері $u(k\Delta t)$ тең болып, басқа нүктелерде нөлге тең болады, сонымен:

$$u_n(t) = \sum_{k=-\infty}^{\infty} u(t)\delta(t - k\Delta t) \qquad (2.13)$$

мұнда Δt – серпіндер тізбегінің кезеңы.

$u(t)$ теңдеуін $t = k\Delta t$ мезгіліндегі мәндерін табу үшін $u(t)$ теңдеуін сол мезгілдерде дельта-серпінге көбейту керек.

Дәл осы жолмен $u(t)$ теңдеуінің біркелкі дискреттеуін $u_n(k\Delta t)$ түрінде көрсетсе болады.

Сигналды жиілік бойынша көрсетілуі.

Уақыт бойынша инвариантты сызықтық жүйелерді талдауда қандай қатыстарды базистік қатыс ретінде таңдау мақсатқа сай екендігін қарастырамыз.

Осындай жүйелерді зерттегенде шешімдер құрамында әрқашанда уақыт бойынша кешенді(комплексті) экспоненциалды қатыстар болады. Мұнда уақыт бойынша кешенді экспоненциалды қатыстармен сипатталатын детерминделген сигналдар уақыт бойынша инвариантты сызықтық жүйелерден өткенде өзінің сипатын өзгертпейді; мұның себебі дифференциалдау және интегралдау амалдарына қарағанда экспоненциалды қатыстар класы инвариантты болады.

Детерминделген сигналдарды көрсетуде e^{pt} түріндегі қатысының аргументі $\rho = \pm j\omega$ (Фурье түрлендіруі), сондай ақ келесідей $p = s \pm j\omega$ аргументте (жалпыланған Фурье түрлендіруі немесе атақты Лаплас түрлендіруі) өте кең қолданылады.

Осы кезге дейін біз базистік қатысының физикалық интерпретациясын қарастырған жоқпыз. Тек қана математикалық түрлендіру үшін оның қажеті де жоқ. Алайда осындай интерпретация сигналдың жүйеден өту кезіндегі физикалық құбылыстарды тереңірек түсіну мүмкіндігін береді.

Фурье түрлендіруінде кешенді-үйлескен паралы (параметр ω ның оң және кері мәндерінде) экспоненциал базистік қатысты қолданғанда Эйлер теңдеуіне: $e^{j\omega} + e^{-j\omega} = 2\cos\omega t$ (2.14)

сәйкес күрделі детерминделген сигналды гармоникалық құрамдастардың қосындысы түрінде көрсетсе болады.

Осында ω айналма жиілік мағынасын білдіргендіктен, осындай түрлендірудің нәтижесі ***сигналдың жиілік түрінде көрсетілуі*** деп аталады.

Жоғарыда айтылған абзалдықтарға байланысты сигналдардың гармоникалық базистік қатыстарға жіктелуі әртарапты кең зерттелген; осылардың негізінде атақты ***сигналдардың спектралды теориясы*** жаратылды.

2.2 Сигналды спектралды талдау тарихы.

Пифагор біздің дәуірімізге дейінгі VI ғасырда тәулік, ай, жылдың кезеңді екенін анықтады. Ішектің ұзындығы мен одан шығатын дыбыстың жиілігі арасындағы байланысты зерттеген. Сонда оның анықтағаны дыбыс гармониясын сандармен өрнектесе болатынын анықтаған. Дәл сондай-ақ оның: "...әлемді сандар билейді..."- деген атақты сөздері содан қалған. Дәл сол уақытта ол ән-күйлік дыбыстардың барлығын сегізге бөліп, ән-күйлік октаваны жаратты: до, ре, ми, ..., си, до.

Ньютон 1671 ж. күн нұрынан пайда болған кемпірқосақтың (радуга) нұрындығы жолақтарды Spektrum деп атады; мұнда spekter – бейне, таңба деген мағынаны білдіреді. Сөйтіп, Пифагордың тәжрибелерінде ол анықтаған құбылыстардың, яғни толқындық әрекеттердің математикалық түсінігін берді.

Ал толқындық теңдеудің музыкалық ішекке шешімін 1738 ж. Даниил Бернулли тапты. Оның жалпы түрі келесідей:

$u(x,t)=\sum_{k=1}^{\infty} Sinkx\left(A_k Coskct + B_k Sinkct\right)$, мұнда c - материалдың физикалық сипатамасын көрсететін еселік.

1755 ж. атақты Л. Эйлер теңдеудің еселіктерін тапты:

$A_k, B_{k:}$:

$$A_k = \frac{2}{\pi}\int_0^{\pi} u(x,0)Sinkxdx, B_k = \frac{2}{\pi}\int_0^{\pi} u(x,0)Coskxdx$$

Бұл өрнек Фурье қатары деп аталады.

1822 ж. Француз инженері Жан Батист Жозеф Фурье өзінің "Жылудың аналитикалық теориясында" кез келген қатысты (керек болса шекті үзілістері бар болған) шексіз көп синустық және косинустық мүшелер қосындысы түрінде көрсетсе болатындығын дәлелдеді:

$$u(x)=\sum_{k=1}^{\infty}\left(A_k Coskat + B_k Sinkat\right).$$

Математиканың осы қатыс мен оның еселіктерінің байланысын талдайтын бөлімі **гармоникалық талдау (анализ)** деп аталады.

Лорд Кельвин (Уйлям Томсон) гармоникалық **талдаушыны (анализаторды)** құрды; ал оның інісі Деймс Томсон өнертапқыш болып, оны амалға асырды.

Гармоникалық анализді одан ары дамытқан Хенрики, Шарп, Юл, Альберт Майкельсон, У. Стреттон т.б.

Майкелсон есептеуіш машинасы үшін Нобель силығына ие болды.

Томсон өзінің машинасында гармоникалық талдауды (Фурье қатарын қолданып) қатардың 80 артық еселіктерін тапты және 1866-72 жылдары теңіз толындарының тасуын болжап берді.

1882 ж. Уйлям Форрель (Смитсон, Вашингтон АҚШ тың Колумбия федералды аймағында (округінде)) 1883-1910 ж. аралығындағы теңіз толқындарының тасуының (прилив) кестесін құрды.

Орыс ғалымы Шустер А. периодограмма әдісін ұсынып, ол Фурье түрлендіру еселіктерін есептеп тапты; $S_k = A_k^2 + B_k^2$, мұнда $k = 2\pi / T_0$. Мұндағы еселіктер n бүтін кезеңдерден құралған кесіндіде анықталады. Шустер тәжрибелермен мынаны дәлелдеді: ақ жарыққа континуум (кезеңді жиын) жиіліктері сәйкес келеді.

Осы заңды 50 жылдан соң Н. Винер ақ жарықпен табылған заңды ақ шулы стохастикалық үдерістерге ұқсастық түрінде жалпылады; яғни сол заңды стохастикалық үдерістерге қолдануды ұсынды.

1927 ж. ағылшын статистигі Дж. Юл уақыт қатарын сызықтық регрессиялық теңдеумен үлгіледі; өзінің гармоникалық қисығын жалпылай отырып, регрессиялық талдауды ең кіші квадраттар әдісін қолданып мына үлгіге келді: $u(k) = b(1)u(k-1) + b(2)u(k-2) + \varepsilon(k)$, мұнда $b(1), b(2)$ - кез келген мәнге ие еселіктер; яғни авторегрессия теңдеуін ең кіші квадраттар әдісімен спектрал талдауға қолданды.

1930 ж. Н. Винер “Жалпыланған спектрал талдау” атты мақаласында спектрал талдауды кездейсоқ үдерістер теориясы негізінде трактаттады.

Ол тұрақты кездейсоқ үдерістер үшін автокорреляция және спектралды қуат тығыздығының қатыстарының анықтамасын берді.

Ол осы екі қатыс Фурьенің үздіксіз түрлендіруі арқылы байланысқандығын көрсетті. Бұл байланыс Винер-Хинчин теоремасымен көрсетіледі.

Мұнда Винер “ақ шуылдың” барлық жиіліктерде біркелкі спектрде болатындығын көрсетті. Бұл үдеріс “Винер үдерісі” деп аталады.

Жоғарыда берілген Юл теңдеуін сигналды алдын ала болжау теңдеуі деп қараса болады; мұнда сигнал мен кедергінің қосындысының нүктелері алдын ала саналған болады.

1938 ж. Вальд 7-теоремасын дәлелдеп, онда мынаны көрсетті:

...кез келген тұрақты үдерісті детерминделген құрамдас бөлігі және “ақ шуылмен” жаратылған жылжымалы орташа үдерісінің қосындысы түрінде көрсетсе болады.

Осы теореманың негізінде академик Колмогоров А. сызықты болжау мәселесін шешті.

1948 ж. Бартлет спектрді авторегрессия еселіктерімен есептеп тапты.

Одан кейін неміс Теплиц, Левинсон (Винердің әріптесі) Юл-Уолкер теңдеуін шешудің нәтижелі шарасын тапты.

Дж. Тьюки тәжрибелі спектралды талдау пионері болса, ал Н. Винер теориялық спектрлі талдау пионері болды.

1949 ж. Массачусетсте Тьюки корреляциялық қатыстың бағаларын сигналдың шекті уақыт санақтары арқылы тапты.

Ал Фурьенің жылдам түрлендіру бағдаржолдарын жаратқан да Дж.Кули мен Дж.Тьюки болды.

Жылдам бағдаржолдардың жаратылуы спектрал талдаудың әдістерін нақты уақытта қолдануға мүмкіндік берді.

Ақырғы уақыттағы салмақты зерттеулердің бірі - сигналдарды өңдеуде жылдам бағдаржолдарды іздеу болды. Осы салада көрінерлі зерттеулер деп Станфорд университетінің ғалымдары Морф пен Кайлат еңбектерін атаса болады.

Орыс ғалымдарының ішінде атақты **Марковтің** үдерістері мен тізбелері сигналдар теориясында кең орын алатын болса, ал академик **Колмогоровтің, Хинчиннің, Котельниковтің** еңбектерін ерекше атап өту керек.

Олардың жаратқан **теориялары** осы кезде **сандық ақпарат жүйелерінің негізі** десе болады.

Спектралды талдаудағы жылдам бағдаржолдар радиолокацияда, жылжымалы нысандарды басқаруда т.б. көптеген қолданбалары бар.

Осы кезде ***сигналдарды көп параметрлі талдауда спектралды талдаудың жылдам бағдаржолдары сүзгісүзгілеу теориясының негізі*** болып отыр. Осы кезде де біршама бағдаржолдар мәлім.

Жылжымалы нысанда УВЧ толқындарын қабылдайтын локаторлық антенналар болып, оның көптеген қабылдауыш элементтері кеңестікте орналасқан болады; олардың ара қашықтықтары толқын ұзындығынан табылады.

Қашықтан қабылдауда ДКМ, УКВ, УВЧ ауқымдарында

көпнұрлылық байқалып, бұл баяу федингті құбылысқа әкеледі; осындай жағдайда кеңістік-уақыт - КУ сигналдарын тиімді және нәтижелі қабылдау үшін оларды барлық кеңістікті өлшемдері (кеңістік өлшемдері) бойынша қабылдау керек болады: уақыт - *t,* жиілік – *f* және кеңістік – *r* бойынша.

Селектив кеңістік өлшемдері бойынша қабылдау нүктесінде сигнал жолдары толық ажыраған болса, онда сигнал тұрақты болады; мұнда ***ажыратылған қабылдау әдісі*** (разнесенный прием) қолданылып, КУ-ді тиімді өңдесе болады.

Ал селектив емес кеңістік өлшемдері бойынша сигнал тұрақты болмайды да, осы кеңістік өлшемдері бойынша әртүрлі бағдаржолдармен ***бейімделуші қабылдау*** орындалады.

Д. Кловскийдің, Е. Ф Камневтің, автордың [66-74,80] және басқалардың еңбектерінде КУ – арналарындағы сигналдарды бейімделуші өңдеу бағдаржолдары жаратылған; солардың ішінде, салмақтырақ тармақтарды таңдап алушы бағдаржол, ең салмақты тармақты таңдап алушы бағдаржол, ажралған тармақтардағы сигналдарды дискретті-салмақты өңдеу бағдаржолдары және т.б. атаса болады.

Ал селективті болмаған кеңістік өлшемдері бойынша әртүрлі қабылдау әдістері қолданылып, бұларда КУ- сигналдардың бұзылуын өтемдеуші әртүрлі бейімделуші сүзгілер қолданылады.

Ең көп нәтиже алу үшін КУ-сигналды бір уақытта барлық (*t,f,r*) кеңістік өлшемдері бойынша өңдеу керек; әрі селективті, әрі селективті болмаған кеңістік өлшемдері бойынша.

КУ- өрісін барлық кеңістік өлшемдері бойынша бір уақытта өңдеу үшін өте күрделі КУ-сүзгілер керек болады; бұларды құру және амалда қолдану осы уақытта да әлі толық шешілмеген болып, осы бөлімде осы мәселені шешудің кейбір бағдаржолдары мен әдістері қарастырылады.

Көп жағдайларда барлық кеңістік өлшемдері бойынша өңдеу амалда мүмкін емес. Оның үстіне жылжымалы нысандарда кейбір кеңістік өлшемдері бойынша қабылдау қиын немесе мүмкін де емес; мысалы, кеңістік өлшемдері бойынша антеннаның өлшемдері шекараланған болады.

Ал өте жедел хабарлар үшін уақыт кеңістік өлшемдері да шектелген. Кей жағдайда жиілік кеңістік өлшемдері да өте шектелген.

Сондықтан тиімді қабылдау үшін бейімделуші антенналар

жүйесінің – ААЖ қорларының барлық мүмкіншіліктерін максимал түрде қолдану керек.

Мұның үшін КУ- өрісінің корреляциялық теңдеуін (*t,f,r*)-дің жеке кеңістік өлшемдері бойынша **тәуелсіз жіктелу қасиетін** пайдаланамыз; яғни күрделі векторды бөлек кеңістік өлшемдері бойынша жіктейміз:

$$B\left(t,t^{/}\ ,f,f^{/}\ ,r,r^{/}\right)=B_1(t,t^{/})\bullet B_2(f,f^{/})\bullet B_3(r,r^{/})\ .$$

Бұл КУ- өрісін бөлек кеңістік өлшемдері бойынша өңдеу мүмкіншілігін береді.

ЖО (жылжымалы нысан)-да ААЖ-ның параметрлері мен өлшемдері, негізінде, ЖО-ның өлшемдерімен, оның жұмыс істеу режимдерімен (жер үстінде, су үстінде, су астында, әуеде, және т.б.), ажратылған КУ-арнасының корреляциялық-спектралдық сипаттамаларымен және оның жолағының кеңдігімен, сондай ақ жіберілген хабардың жеделдік дәрежесімен өлшенеді.

Жалпы алғанда, сигналдың КУ- өңдеудегі мүмкіншілігі (*F,T,R*) көлемімен анықталады; мұнда *F* – КУ- арнаны ұйымдастыру үшін керек болған жолақ кеңдігі; *T* – хабардың жеделдігін анықтайтын көрсеткіш; *R* – берілген режимдегі ЖО-ның өлшемдері және мүмкіншіліктерімен анықталады.

Әдетте ЖО-ның мүмкіншіліктерін өзгерту қиын болғандықтан, КУ-өрісінің корреляциялық теңдеуінің тәуелсіз жіктелуін есепке ала отырып, қабылдау нүктесінде барлық кеңістік өлшемдері бойынша максимал дәрежеде қабылдануы мүмкін болатын сигналды таңдау керек болады.

Айталық, КУ-арна кеңістік және жиілік бойынша селективті болсын, ал уақыт бойынша селективті болмасын. Мұнда, КУ-сигналды өңдеу кеңістікте орналасқан антенна элементері және өзара жиілік жолақтары қиылыспайтын элементар жиілікті сүзгілер жәрдемінде орындалады.

Мұндай жағдайда кіру әсері x_k^l *L* антеннасының элементтеріне К=1,2,3,…уақыт аралығында әсер етіп, $\overline{x_k}$ векторын құрады да, оның құрамдас бөліктері $\overline{x_k}=(x_k^1, x_k^2, x_k^3, \ldots, x_k^L)$ өзара байланысты болмайды.

Алайда уақыт бойынша x_k^l корреляцияланғандығы үшін осы кеңстік өлшемдері бойынша сүзгілеу теориясын қолдана отырып,

КУ-сигналдарының бұзылуын өтемдеу (компенсациялау) мақсатқа сай келеді.

Антеннаның әрбір элементі кіру сигналын көбейтуші $W_k^l, l = \overline{1,L}$ еселігіне ие болады. Осы еселіктер жиыны антенна жүйесінде салмақты еселіктер векторын – СЕВ құрады:

$$\overline{W_k^L} = \left(W_k^1, W_k^2, W_k^3, ..., W_k^L\right).$$

ААЖ де КУ-өрісін **бейімделуші өңдеу мәселесі** деп, СЕВ өлшемдерін дискретті бейімделуші сүзгілеуді айтамыз.

Автордың [66-70] еңбектерінде сигналдардың тәжрибелі өлшемдер бойынша СЕВ анықтау әдістемесі берілген.

Осы кезде ААЖ-де бейімделудің әртүрлі бағдаржолдары мәлім болып, амплитуда-фазалық таралуды басқару СЕВ ні өзгертумен орындалады.

Осы бағдаржолдар үш шартмен бағаланады: кедергі сигналдарын бәсеңдету дәрежесімен, бейімделу үдерісінің жинақталу жылдамдығымен және есептеу күрделілігімен. Осылардың кейбіреулерін талдаймыз:

1. Уидроу-Хофф бағдаржолы .

$\overline{W_k} = \overline{W_{k-1}} + \mu \bullet [Z_k - \overline{X_k^T} \bullet \overline{W_{k-1}}] \bullet \overline{X_k}$, мұнда:

$\overline{W_k}$ – t_k уақыт мезгіліндегі СЕВ нің мәндері;

k - итерация қадамы;

$\overline{X_k}$ – кіру әсерлерінің векторының мәндері;

Z_k – эталондық сигнал;

μ – бейімделу еселігі, жинақтылық жылдамдығын және бағдаржолдың тұрақтылығын көрсетеді;

T – транспондау индексі.

Бұл бағдаржолдың кемшілігі μ-дің мәнін дұрыс таңдамағанда төмен тұрақтылыққа ие болып, бейімделу үдерісінің баяу жинақтылық жылдамдығы.

2. Роббинс-Монро бағдаржолы :

$\overline{W_k} = \overline{W_{k-1}} + \mu_k \bullet [Z_k - X_k^T \bullet W_{k-1}] \bullet \overline{X_k}$, мұнда: $\mu_k = \mu / k,$

бейімделу еселігінің әр қадамда кемейтілуі жинақтылықты жылдамдатады.

3. Ньютон-Рафсон бағдаржолы .

$$\overline{W_k} = \overline{W_{k-1}} + [Y'(W_{k-1})]^{-1} \bullet [Z_k - \overline{X_k^T} \bullet \overline{W_{k-1}}] \bullet \overline{X_k} \ ,$$

мұнда $Y'(W_{k-1})-$ $Y_k = \overline{X_k^T} \bullet \overline{W_k}$ функциясының $W = W_{k-1}$ нүктедегі туындысы. СЕВ априор түрде беріліп, мақсат теңдеуінің квадратты екендігін көрсетеді: $W_0 = [1, 0.,...,0.]$.

4. Калман-Бьюси бағдаржолы .

$$\vec{W}_k F \vec{W}_{k,1} + \vec{\mu}_k \left[Z_k - \vec{X}_k^T \vec{W}_{k-1} \right]; \ \vec{\mu}_k = \frac{\left(FP_k F^T + GQ_k Q^T \right) \vec{X}_k}{\vec{X}_k^T \left(FP_k F^T + GQ_k G^T \right) X_k + \rho};$$

$$P_k = \left[I - \vec{\mu}_k \vec{X}_k^T \right] \left[FP_k F^T + GQ_k G^T \right],$$

осында F,G – жағдайлар және белсенділеу матрицалары; P_k, Q_k - СЕВ бағалау қателігінің дисперсиясының және белсенділеу кедергісінің үдемелілігінің (интенсивтігінің) матицалары.

5. Таңдаулы кооряциялық матрицаны бірден қайта өңдеу бағдаржолы :

$$\vec{W}_{opt} = R_{xx}^{-1} \vec{R}_{xz} \ ,$$

$$R_{xx} = E [\vec{X}_k \vec{X}_k^T] - \qquad \vec{X}_k$$

кіру әсерлер векторының корреляциялық матрицасы;

$\vec{R}_{xz} = E[Z_k \vec{X}_k]$ - кіру және эталондық сигналдардың корреляциялық векторы.

Анық емес корреляциялық матрицалар мен векторлар орнына

олардың максималды шындыққа ұқсас бағалары қолданылады:

$$\hat{R}_{xx} = 1 / N \sum_{k=1}^{N} \vec{x}_k \ , \qquad \hat{\vec{R}}_{xz} = 1 / N \sum_{k-1}^{N} Z_k \vec{x}_k$$

мұнда *N*- $\hat{R}_{xx}$ векторын қалыптастыру үшін керекті санақтар.

6**. Вудбери бағдаржолы (қайтарылушы матрицаны рекуррент есептеу)**

$$\vec{R}_{k+1} = \frac{k+1}{k} \hat{R}_k^{-1} - \frac{k+1}{k^2} [1 + \frac{1}{k} \vec{x}_{k+1}^T \hat{R}_k^{-1} \vec{x}_{k+1}]^{-1} \times \hat{R}_k^{-1} \vec{x}_{k+1} \vec{x}_{k+1}^T \hat{R}_k^{-1}$$

Ақырғы уақытта дискрет сүзгісүзгілеу саласында көптеген жаңалықтар болды; мысалы, Ли Дж., Митра С.К., Херц Д., Уидроу В.,

Папулис А. және т.б. лардың еңбектерінде жаңа сандық сүзгілер құрылып, олардың сипаттамалары төменде келтірілген [66-70] жұмыстардағыдан анағұрлым жақсы болды.

Бондьопадьхьяй П.К. еңбегінде бейімделуші сандық сүзгісүзгілеу әдісі жаратылған болып, ол Хартлидің (БДПХ) жүгіруші дискрет түрлендіруіне негізделген. Оның амалдық мәселелерді шешу мүмкіншілігі көрсетілген.

Мұнда $f[n]$ дискретті деректердің кіру ағыны болғанда, оның БДПХ-сы мына түрде көрсетіледі:

$$H[n,m] = \sum_{k-1}^{n-1} f[n-k]\left\{ Cos\left(\frac{2\pi}{N} \bullet km\right) + Sin\left(\frac{2\pi}{N} \bullet km\right)\right\},$$

мұнда N - мәлім болған бүтін сан, m - сүзгі ұзындығы.

Осы бағдаржолдар өте жоғары жылдамдыққа ие болып, нақты уақытта үдерістерді басқаруға арналған.

Аталған бағдаржолдарда жиынтықтар ұзындығы және ЖБЕК-бағдаржолдары ның жұмысшы сипаттамаларына қойылатын басқа да шектеулер есепке алынбаған болып, зерттеулерді талап етеді.

Бейімделуші антенна жүйелерінде және басқа да сигналдарды қабылдау, өңдеу құрылымдарында шешілетін мәселелердің типі мен талаптарына байланысты түрде бейімделуші сүзгінің айқын типін таңдау мақсатқа сай келеді.

2.3 Детерминделген сигналдар: кезеңді, кезеңсіз сигналдар

Сигнал спектрі бойынша энергияның таралуы;
Серпін ұзындығы мен ені арасындағы қатынас

А) Кезеңді сигналдардың спектрі

Нақты жағдайда сигналдың басы мен ақыры болғандықтан оның математикалық үлгісін құрып болмайды; алайда орнықты жағдайда олар өте көп уақытта жарамды болып, оның математикалық үлгісі ретінде уақыт бойынша кезеңді қатысты (функцияны) алса болады. Төменде осындай қатыстарды экспоненциалды құрамдастардың қосындысы немесе гармоникалар қосындысы түрінде қарастырамыз.

Айталық қатыс $u(t)$ мына уақыт аралығында $t_1 \le t \le t_2$ берілген болып, Дирихле шартын қанағаттандыратын болсын; және $-\infty$ до $+\infty$ уақытта мынау $T = 2\pi / \omega_1 = t_2 - t_1$ кезеңмен қайталанатын болсын.

Дирихле шарттары: кез келген шекті аралықта қатыс үздіксіз болуы керек немесе шекті бірінші текті үзіліс нүктелеріне ие болуы керек, сондай ақ шекті экстремал нүктелер санына ие болуы керек. Үзіліс нүктелерінде $u(t)$ теңдеуі тең болады деп есептеу керек.

$$u(t_0) = 0,5\left[u(t_0 + 0) + u(t_0 - 0)\right]$$

Егер базистік деп экспоненталық қатысты алсақ, онда (2.5) теңдеуі келесідей жазылады:

$$u(t_0) = 0,5\left[u(t_0 + 0) + u(t_0 - 0)\right]$$

$$A(jk\omega_1) = \frac{2}{T}\int_{t_1}^{t_2} u(t)e^{-jk\omega_1 t}\,dt \quad (2.15; 2.16)$$

(2.5) қатысы Фурье қатарының кешенді түрі болып, оң және кері ω параметрлі экспоненциалдық қатыстардан құралған болады (екі жақтамалы жиілікті көрсетілуі). Кері жиілікті құрамдастарының болуы нақты қатыстардың кешенді түрде жазылуының салдары деп түсіну керек.

$A(j\omega)$ теңдеуін $u(t)$ кезеңді сигналының ***кешенді (комплексті) спектрі*** деп аталады. Бұл спектр дискретті болады; себебі бұл $A(jk\omega_1)$ теңдеуі сан оғында k-ның бүтін мәндерінде ғана анықталған.

Берілген *k*-ның айқын мәндерінде $A(jk\omega_1)$ теңдеуінің мәні ***кешенді амплитуда*** деп аталады.

$A(j\omega)$ спектрінің сыртқы тегістеушісі (огибающая) мына түрде болады:

$$A(j\omega) = \frac{2}{T}\int_{t_1}^{t_2} u(t)e^{-j\omega t}dt \qquad (2.17)$$

Сонда кешенді спектрді мына түрде жазамыз:

$$A(j\kappa\omega) = A(\kappa\omega_1)e^{-j\varphi(\kappa\omega_1)} \qquad (2.18)$$

Кешенді спектрдің модулі $A(k\omega_1)$-ны **амплитудалар спектрі**, ал $\varphi(k\omega_1)$ теңдеуі – **фазалар спектрі** деп аталады.

Егерде сигналдың **амплитудалар спектрі және фазалар спектрі мәлім болса, онда** (2.15)-ке сәйкес ол бірмәнді анық түрде қайта қалпына келтіріледі. Амалдық мәселелерде амплитудалар спектрі маңызды болып, ал фазалар туралы ақпарат оншалықты маңызы болмайды.

$A(k\omega_1)$ және $\varphi(k\omega_1)$-лар *k*-ның тек бүтін мәндерінде ғана нөлден айырмашылығы болғандықтан кезеңді сигналдың амплитудалары мен фазаларының спектрлері **дискретті** болады.

Эйлердің $e^{-jk\omega t} = \cos k\omega t - j\sin k\omega t$, теңдеуін қолданып, $A(jk\omega_1)$ ның кешенді спектрін нақты және алмағайып (мнимый) бөліктер түрінде көрсетеміз:

$$A(jk\omega_1) = \frac{2}{T}\left[\int_{t_1}^{t_2} u(t)\cos k\omega_1 t dt - j\int_{t_1}^{t_2} u(t)\sin k\omega_1 t dt\right] = A_k - jB_k \qquad (2.19)$$

Мұнда
$$\frac{2}{T}\int_{t_1}^{t_2} u(t)\cos k\omega_1 t dt = A_k \qquad (2.20;\ 2.21)$$
$$\frac{2}{T}\int_{t_1}^{t_2} u(t)\sin k\omega_1 t dt = B_k$$

Амплитудалар спектрі $A(k\omega_1) = \sqrt{A_k^2 + B_k^2}$ (2.22)

К жұп теңдеуі болады, яғни

$$A(k\omega_1) = A(-k\omega_1) \tag{2.23}$$

A_k және B_k лардың жұптығы қарама-қарсы болғандықтан, фазалар спектрі

$\varphi(k\omega_1) = arctg\frac{B_k}{A_k}$ тақ функция болады, яғни

$$\varphi(k\omega_1) = -\varphi(-k\omega_1) \tag{2.24}$$

k = 0 болғанда тұрақты құраушысын табамыз:

$$\frac{A_0}{2} = \frac{1}{T}\int_{t_1}^{t_2} u(t)dt \tag{2.25}$$

Екі жақты спектралды көрсетуден оңай түрде біржақты көрсетуге өтуге болады (мұнда кері жиіліктер болмайды); бұл кешенді-үйлесімді құрамдастарын біріктірумен амалға асырылады [(2.14) ті қара].

Бұл жағдайда Фурье қатарының тригонометриялық түрін аламыз.

Расында да, (2.15)- ның тұрақты $A_0/2$ бөлімін ажыратып және симметриялы жиіліктер болған ω және –ω құрамдастарын қосып, мынаны аламыз:

$$u(t)\frac{A_0}{2} + 0{,}5\sum_{k=1}^{\infty}\left[A(jk\omega_1)e^{jk\omega_1 t}\right] + A(-jk\omega_1)e^{-jk\omega_1 t} \tag{2.26}$$

(1.15) және (1.16) қатыстарын есепке ала отырып, мынаны жаза аламыз:

$$u(t) = \frac{A_0}{2} + 0{,}5\sum_{k=1}^{\infty}\left[A(k\omega_1)e^{-j\varphi(k\omega_1)}e^{jk\omega_1 t} + A(k\omega_1)e^{j\varphi(k\omega_1)}e^{-jk\omega_1 t}\right]$$

$$u(t) = A_0/2 + \sum_{k=1}^{\infty}\left[A(k\omega_1)\left(\frac{e^{j(k\omega_1 t-\varphi(k\omega_1))} + e^{-j[k\omega_1 t-\varphi(k\omega_1)]}}{2}\right)\right]$$

Эйлердің (2.14) теңдеуін қолдана отырып және $\varphi(k\omega_1)$ - ны келесідей φ_k таңбалап біткен түрде мынаны аламыз:

$$u(t) = \frac{A_0}{2} + \sum_{k=1}^{\infty} A(k\omega_1)\cos\left(k\omega_1 t - \varphi_k\right) \qquad (2.27)$$

Сондай ақ Фурье қатарының басқа да тригонометриялық түрі кең таралған болып, ол мына түрде болады:

$$u(t) = \frac{A_0}{2} + \sum_{k=1}^{\infty} \left(A_k \cos\left(k\omega_1 t\right) + B_k \sin\left(k\omega_1 t\right)\right) \qquad (2.28)$$

Алайда оны амалда қолдану қолайсыз.

(2.23) және (2.24) лердің бөлек құраушылары **гармоникалар** деп аталады.

Кезеңді сигналдың амплитудалар және фазалар спектрлерін спектралдық диаграммалар түрінде көрсету қолайлы болады.

Амплитудалар спектрінің диаграммасында әрбір гармоникаға тік кесінді сәйкес келеді де оның ұзындығы амплитудаға сәйкес келеді; ал оның абсцисса оғындағы орны осы гармониканың жиілігіне сәйкес келеді.

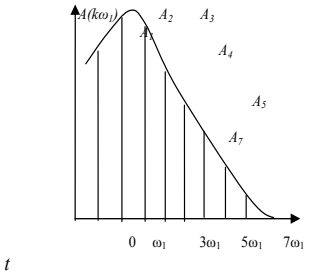
Дәл осындай фазалар спектрінің диаграммасында гармоникалардың фазаларының мәндері көрсетіледі.

Спектрлер тік сызықтармен көрсетілгендігі себепті оларды **сызықты диаграммалар** деп атайды.

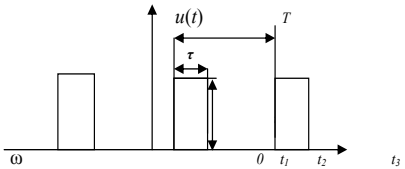
Атап кететін жай, дискретті сызықты спектр тек кезеңді сигналға сәйкес келуі шарт емес; кезеңді сигналдардың спектрі ω_1 негізгі жиілікке ретті (кратный) гармоникалар жиынынан тұратын болуы керек.

Ретті болмаған жиіліктердегі гармоникалардың спектрі кезеңдіге жақын сигналдарға сәйкес келеді.

Кезеңді сигналдың амплитудаларының спектрінің диаграммалары 2.4 суретте көрсетілген. Осы амплитудалар спектрінің тегістеушісін (огибающая) алу үшін $A(k\omega_1)$ дағы $k\omega_1$ ны ω мен алмастырамыз, мұндағы k - гармоникасы үшін $\omega = k\omega_1$.



2.4-сурет



2.5-сурет

***Зертханалық жұмыс* 2.1.** Кезеңді тікбұрышты серпіндер берілген болып, олардың ұзындығы τ , ал амплитудасы u_0 болып, олардың жиілігі $\omega_1 = 2\pi/T$ болсын. Олардың амплитудалары мен фазаларының спектрін табу керек (2.5-сурет). Осындай серпіндерді кезеңде сипаттайтын $u(t)$ теңдеуі мына түрде көрсетіледі:

$$u(t) = \begin{cases} u_0, t_1 \le t \le t_2 = t_1 + \tau, \\ 0, t_2 < t < t_3 = t_1 + T \end{cases}$$

(2.16) ге сәйкес келесідей болады:

$$A\left(jk\,\omega_1\right) = \frac{2u_0\left[e^{-j\omega_1 t_1} - e^{-jk\omega_1(t_1+\tau)}\right]}{T \ldots 2j\left(k\omega_1/2\right)}$$

немесе

$$A\left(jk\,\omega_1\right) = \frac{2u_0\tau}{T}\frac{\sin\left(k\omega_1\tau/2\right)}{k\omega_1\tau/2}e^{-jk\omega_1(t-\tau/2)}. \qquad (2.29)$$

Гармоникалардың амплитудасы, соның ішінде тұрақты және мынаған $A_0/2$ тең болғаны да бар болып, келесідей анықталады:

$$A(\omega) = \frac{2u_0\tau}{T}\left|\frac{\sin\left(\omega\tau/2\right)}{\omega\tau/2}\right|, \qquad (2.31)$$

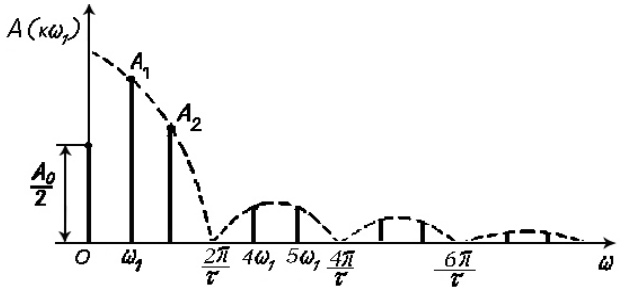
ω = 0 болғанда

$$A_0 = 2u_{0\tau}/T\ . \qquad (2.32)$$

Амплитудалардың өзгеруі *sin x/x* теңдеуімен көрсетіледі және серпіндердің тізбегінің жиілігіне байланысты болмайды. $2\pi/\tau$ ге ретті болған жиіліктерде спектр тегістеушісі нөлге тең болады.

2.6 - суретінде амплитудалар спектрінің диаграммасы мына жағдайға $T/\tau = 3[\omega_1 = 2\pi/(3\tau)]$ берілген. Спектрде құраушылар саны шексіз көп.

Серпін жақтарының тіктігі осы спектрде негізгі ω_1 жиілігінен әжептеуір артатын жиіліктердің бар екендігінен болады.



2.6-сурет

(2.29) теңдеуіне сүйеніп және $\sin(k\omega_1\tau/2)$ теңдеуінің таңбалары $\Delta\omega = 2\pi/\tau$ жиілік аралықтарының тізбегінде кезекті түрде өзгеріп отырады; сондықтан фазалар спектрі үшін мынаны жазамыз:

$$\varphi_k = k\omega_1\left(t_1 + \tau/2\right) + \left(n-1\right)\pi\,, \qquad (2.33)$$

мұнда n — жиіліктер аралығының нөмірі $\Delta\omega = 2\pi/\tau$ болып, ол $\omega = 0$ ден бастап саналады. Фазалар спектрі санақтың басталу нүктесіне байланысты болады. Егер тікбұрышты серпіндер тізбегінің алдыңғы жағы уақыт бойынша санақ басына сәйкес келсе, онда әрбір $\Delta\omega = 2\pi/\tau$ аралықта құраушылар фазасы сызықты түрде өседі.

2.3.1 *Сигнал спектрі бойынша энергияның таралуы*

Серпін ұзындығы мен спектр ені арасындағы қатынас.

$u(t)$ күрделі кезеңді сигналдың энергиясының оның спектралды құраушылары бойынша таралуын көрейік.

$u(t)$ ның уақытты теңдеуі деп 1 Ом кедергідегі шағы T- ға тең уақытта ажыралған Энергия W_T мөлшері айтылады:

$$W_T = \int_0^T \left[u\left(t\right)\right]^2 dt \quad . \qquad (2.34)$$

$u(t)$ ның спектрал көрсетуі үшін (2.15)-тегі Фурье қатары түрін қолданып, мынаны аламыз:

$$W_T = \frac{1}{4}\left[\sum_{k=-\infty}^{\infty}\sum_{t=-\infty}^{\infty} A\left(jk\,\omega_1\right)A\left(jl\,\omega\omega_1\right)\int_0^T e^{j\frac{2\pi\left(k+l\right)t}{T}}dt\right]. \qquad (2.35)$$

(2.35) өрнегіндегі интегралдар мәнін анықтаймыз:

$$\int_0^T e^{j\frac{2\pi(k+l)t}{T}} dt = = T\frac{\sin 2\pi(k+l)}{2\pi(k+l)} = \begin{cases} 0, k+l \neq 0, \\ T, k = -l \end{cases} . \qquad (2.36)$$

$A(jk\omega_1)$ және $A(-jk\omega_l)$-лар кешенді-үйлесмді болғандықтан келесідей болады:

$$A(jk\omega_1)A(-jk\omega_1) = |A(k\omega_1)|^2 . \qquad (2.37)$$

(2.28) және (2.29)-лерді есепке алып, W_T өрнегі әжептеуір оңтайланады:

$$W_T = \frac{T}{2}\left[\frac{A_0^2}{2} + \sum_{k=1}^{\infty} |A(k\omega_1)|^2\right] . \qquad (2.38)$$

Ақырғы (2.38) өрнектен мынаны көрсек болады; күрделі кезеңді сигналдың бір кезеңдегі энергиясы әрбір гармониканың 1 Ом кедергіде ажыратқан энергияларының орташасының қосындысына тең болады (тұрақты құраушысын қоскқанда). Уақыт өтуімен ажыралатын энергия шексіз артады. Мұнда орташа энергия қалыпты түрде өзгермейді:

$$P_{ср} = \frac{A_0^2}{4} + \frac{1}{2}\sum_{k=1}^{\infty} |A(k\omega_1)|^2 . \qquad (2.39)$$

Осында айтып кететін жай, орташа энергия бөлек гармоникаларының фазаларына байланысты болмайды; сигнал келбетін өзгерткенде өзінің мәнін сақтап қалады. Келбетінің өзгеруі спектр гармоникаларының арақатысы өзгеруінен болады.

***Зертханалық жұмыс* 2.2**

Б) Кезеңсіз сигналдар спектрлері.

Кез келген физикалық нақты сигнал уақытта шектелген және шекті энергияға ие болады. Нақты сигналдарды көрсететін қатыстар Дирихле шарттарын қанағаттандырады және абсолютті интегралданады, яғни

$$\int_{-\infty}^{\infty} |u(t)|dt \leq M , \qquad (2.40)$$

мұнда M — шекті өлшем.

Осындай сигналдардың үлгісі (2.2) өрнегінде көрсетілгендей гармоникалық құраушылар түрінде көрсетілуі мүмкін.

Кезеңсіз сигналда спектрал түрлендірудің айқын түрін шығарып алу үшін кезеңді $u_1(t)$ серпіндер тізбегінің спектрінде болып өтетін өзгерістерді олардың қайталау кезеңін үлкейте отырып зерттеу керек.

T кезеңінің кез келген мәні үшін рас болатын (2.30) теңдеуіне сәйкес (2.27) дегі спектрал құраушылардың амплитудаларының абсолютті мәндері кезең үлкейгенде кемейеді.

Спектр құраушыларының жиіліктері негізгі жиілікке еселі болғандықтан, оның кемейгенінде спектрал диаграмманың сызықтары жақындай түседі.

Бірлік серпін $u(t)$ тің спектралды көрінісін алу үшін $u_1(t)$ сигналының кезеңын шексіз көбейтумен оның спектрінің көрінісін алу керек.

Кезеңді қатыс $u_1(t)$ үшін Фурьенің қос түрлендіруін (2.15) және (2.16) түрінде жазамыз:

$$u_1(t) = \frac{1}{2}\sum_{k=-\infty}^{\infty} A(jk\omega_1)e^{jk\omega_1 t}$$

$$A(jk\omega_1) = \frac{2}{T}\int_{t_1}^{t_2} u_1(t)e^{-jk\omega_1 t}dt$$

.

Кезең $T\to\infty$- ғанда $u_1(t)$ теңдеуі $u(t)$-ге айналады, ал жиілік ω_1 кемейіп $d\omega$-ға, ал $k\omega_1$ ағындағы жиілікке ω айналады. Сонда қосындылауды интегралдаумен алмастырып, табамыз:

$$u(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\left[\int_{-\infty}^{\infty} u(t)e^{-j\omega t}dt\right]e^{j\omega}d\omega$$

Квадратты жақшадағы интегралды келесідей таңбалап $S(j\omega)$, Фурьенің тура және кері түрлендіру теңдеулерін аламыз:

$$S(j\omega) = \int_{-\infty}^{\infty} u(t)e^{-j\omega t}dt \quad , \tag{2.41}$$

$$u(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} S(j\omega)e^{j\omega t}d\omega \quad . \tag{2.42}$$

$S(j\omega)$ мәнін ***кешенді спектрал тығыздық теңдеуі*** немесе ***спектралды сипаттама*** деп атайды. Оның өлшемі [амплитуда/жиілік].

Әрбір айқын жиілікте осы құраушының амплитудасы нөлге тең болады. (2.15) және (2.42) өрнектерді салыстырып, шексіз кіші $d\omega$ аралығына шексіз кіші кешенді амплитудалы $dA(j\omega)$ құраушысы сәйкес келеді.

$$dA\left(j\omega\right) = \frac{1}{\pi} S\left(j\omega\right) d\omega \ . \tag{2.43}$$

$t_1 \le t \le t_2$ уақыт аралығында берілген $u(t)$ теңдеуінің спектрал сипаттамасы үшін (2.41) өрнегін сол қатыстың уақыт бойынша кезеңді кешенді спектрінің (2.17) өрнегімен салыстырғанда, олар тек көбейткішпен ғана ажыралатынын көреміз:

$$A(j\omega) = \frac{2}{T} S(j\omega). \tag{2.44}$$

Сондықтан мәлім болған бірлік серпіннің спектралдық сипаттамасы арқылы олардың кезеңді тізбегінің сызықты спектрін құрса болады.

(2.44) өрнегінен келесідей дәлелді көрсе болады; спектрал сипаттаманың әртүрлі көрінісі үшін (2.18) — (2.24) терге өте ұқсас теңдеулар табылады.

Кешенді шама сияқты спектралды сипаттаманы мына түрде жазса болады:

$$S(j\omega) = S(\omega) e^{-j\varphi(\omega)} . \tag{2.45}$$

Мұнда $S(\omega)= |S(j\omega)|$ ***амплитуданың спектралды тығыздығы*** немесе ***кезеңсіз сигналдың спектрі*** деп аталады.

Кезеңсіз сигналдың құраушылары барлық жиіліктерде болғандықтан, оның спектрі үздіксіз болады. Спектралды сипаттама нақты және мауқым (мнимая часть) бөліктерден тұрады:

$$S(j\omega) = A(\omega) - jB\left(\omega\right) , \tag{2.46}$$

мұнда

$$A(\omega) = \int_{-\infty}^{\infty} u(t) \cos \omega t dt , \tag{2.47}$$

$$B(\omega) = \int_{-\infty}^{\infty} u(t) \sin \omega t dt . \tag{2.48}$$

Спектрал $S(\omega)$ сипаттаманың мөлшері (модулі) келесідей анықталады:

$$S(\omega) = \sqrt{|A(\omega)|^2 + |B(\omega)|^2} \qquad (2.49)$$

және жиіліктің жұп функциясы болады.

$S(j\omega)$ спектрал сипаттамасының фазасы келесідей болады:

$$\varphi(\omega) = arctg\frac{B\omega}{A(\omega)} \qquad (2.50)$$

(2.42) және (2.43) мынаны көрсе болады: $A(\omega)$ – жиіліктің жұп функция, ал $B(\omega)$ – тақ функция, $\varphi(\omega)$ – теңдеуі жиілікке қарағанда тақ функция болады.

Фурьенің интегралдық түрлендіруінің кешенді түрі тригонометриялық түрге оңай келеді:

$$u(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} S(\omega)e^{j[\omega t-\varphi(\omega)]}d\omega = \frac{1}{2\pi}\int_{-\infty}^{\infty} S(\omega)\cos[\omega t-\varphi(\omega)]d\omega + \frac{j}{2\pi}\int_{-\infty}^{\infty} S(\omega)\sin[\omega t-\varphi(\omega)]d\omega$$

Интеграл астындағы екінші мүшенің тақ болғандығынан нөлге айналады:

Сонымен соңында мынаған келеміз:

$$u(t) = \frac{1}{\pi}\int_{0}^{\infty} S(\omega)\cos[\omega t-\varphi(\omega)]d\omega \qquad (2.51)$$

Фурье-түрлендіруінің тригонометриялық түрде жазылуының абзалдығы - қиялдау (идеалдау) жәрдемінде оны физикалық талқылау мүмкін болады.

***Зертханалық жұмыс* 2.3**

Уақыт теңдеуі төмендегідей берілген болса, тікбұрышты серпіндің спектрін табу керек (2.7-сурет):

$$u(t) = \begin{cases} u_0,, t_1 \le t \le t_2 = t_1 + \tau_0, \\ 0, t_2 < t < t_1 \end{cases}.$$

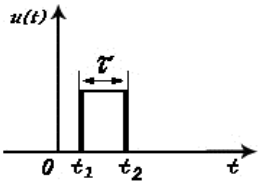
(2.41) ге сәйкес амплитудалардың спектралды сипаттамасының өрнегі келесідей болады:

$$S(j\omega)=\int_{t_1}^{t_1+\tau}u_0e^{-j\omega t}dt=\frac{u_0}{j\omega}\left[e^{-j\omega t_1}-e^{j\omega(t_1+\tau)}\right]=\frac{2u_0}{\omega}\sin\frac{\omega\tau}{2}e^{-j\omega\left(t_1+\frac{\tau}{2}\right)}.$$

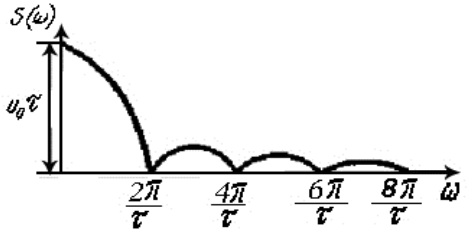
Сонда іздеп отырған спектріміз осы өрнектің мөлшері (модулі) болады:

$$S(\omega)=u_0\tau\left|\frac{\sin(\omega\tau/2)}{\omega\tau/2}\right| . \qquad (2.52)$$

Дара тікбұрышты серпіндің спектрі (2.8-сурет) (2.44) те көрсетілген осындай серпіндердің кезеңді тізбегінің спектріндей болады (2.6-сурет).



2.7-сурет



2.8-сурет

***Зертханалық жұмыс* 2.4** Дельта-функцияның спектрін табу керек: [(2.10) қатысын және 2.3 суретін қара].

ξ_1 нүктесінде жинақталған дельта-функцияның $S_\delta(j\omega)$ спектралды сипатты үшін мына өрнекті жазамыз:

$$S_\delta(j\omega)=\int_{-\infty}^{\infty}\delta(t-\xi_1)e^{-j\omega t}dt .$$

(2.41) -ге сәйкес мынаны аламыз:

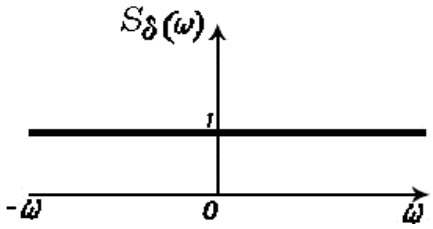
$$S_\delta(j\omega)=e^{-j\omega\xi} ;$$

осыдан спектрал сипаттаманың модулі келесідей болады:

$$S_\delta(\omega)=1 . \qquad (2.53)$$

Осыдан шығатыны, дельта-функциябіртегіс үздіксіз спектрі болып, ол шексіз үлкен жиілікті құраушылардан тұрады (2.9- сурет).

$\xi_1 = 0$ болғанда, барлық құраушылардың бастапқы фазасы нөлге тең болады.



2.9-сурет

Онда осы резистордан алынатын энергия келесідей болады:

$$W = \int_{-\infty}^{\infty} u^2(t)dt . \qquad (2.54)$$

(2.54) интегралы жинақталады деп ұйғарып, $u(t)$ сигналының энергиясын спектралды $S(\omega)$ сипаттамасының мөлшері (модулі) арқылы көрсетеміз.

Онда ол модулдің квадратын мына түрде жазамыз:

$$|S(\omega)|^2 = S(j\omega)S(-j\omega) \qquad (2.55)$$

мұнда:

$$S(-j\omega) = \int_{-\infty}^{\infty} u(t)e^{j\omega k}dt$$

теңдеуі $u(t)$ сигналдың $S(j\omega)$ спектралды сипаттамасына кешенді-үйлесімді болады. Онда

$$\int_{-\infty}^{\infty} |S(\omega)|^2 d\omega = \int_{-\infty}^{\infty} S(j\omega)\int_{-\infty}^{\infty} u(t)e^{j\omega t}dtd\omega .$$

Интегралдау кезегін өзгерткен соң және (2.42) Фурьенің кері түрлендіруін қолданып мынаны алса болады:

$$\int_{-\infty}^{\infty} u(t)\left[\int_{-\infty}^{\infty} S(j\omega)e^{j\omega t}d\omega\right]dt = 2\pi\int_{-\infty}^{\infty}|u(t)|^2 dt .$$

Ең соңында мынаны аламыз:

$$\int_{-\infty}^{\infty}|u(t)|^2 dt = \frac{1}{2\pi}\int_{-\infty}^{\infty}|S(\omega)|^2 d\omega = \frac{1}{\pi}\int_{-\infty}^{\infty}|S(\omega)|^2 d\omega \qquad (2.56)$$

Ақырғы (2.56) теңдік **Парсеваль теңдігі** деген атпен танылған.

Осыдан шығатыны, кезеңсіз сигналдың нақты уақыт аралығындағы энергиясы оның спектралды сипаттамасының

модулінің квадратының жиіліктер аралығындағы интегралына тең болады.

2.3.2 Серпін ұзындығы мен спектр ені арасындағы қатнас.

Бірлік тікбұрышты серпіннің спектрін (2.8 суретті қара), талдай отырып, келесідей тоқтамға келсе болады; серпіннің τ ұзындығын 0 ден ∞ дейін үлкейткенде оның спектрі шексізден (дельта-функцияның) координат басындағы бір ғана спектрлік сызыққа дейін қысқарады; бұл сызық сигналдың тұрақты мәніне сәйкес келеді.

Бұл қасиет, яғни сигнал ұзындығы артқанда оның спектр енінің кішірею қасиеті немесе керісінше, сигнал ұзындығы кемейгенде оның спектр енінің арту қасиеті сигналдың кез келген түрі үшін орынды болады.

Бұл қасиет Фурьенің дұрыс және кері интегралдық түрлендіруінің өзгешеліктерінен келіп шығады; оларда интеграл астындағы өрнектерде экспоненциалдық қатыстың орынында t және ω айнымалылары көбейтінді түрінде болады.

Анық уақыт мерзімінде (аралығында) берілген $u(t)$ теңдеуін және $\lambda>1$ болғанда λ есе кіші уақыт мерзімінде болатын $u(\lambda t)$ теңдеуін қарастырайық; $u(t)$ ның спектралды сипаттамасы $S(j\omega)$ болғанда, $u(\lambda t)$ үшін $S_\lambda(j\omega)$ сәйкес сипаттамасын табамыз:

$$S_\lambda(j\omega)=\int_{-\infty}^{\infty}u(\lambda t)e^{-j\omega t}dt=\frac{1}{\lambda}\int_{-\infty}^{\infty}u(t')e^{-j\frac{\omega t'}{\lambda}}dt'=\frac{1}{\lambda}S\left(j\frac{\omega}{\lambda}\right), \qquad (2.57)$$

мұнда $t'=\lambda t$. Сондықтан **λ есе қысқарған сигналдың спектрі λ есе кең болады.** Ал $S(j\omega/\lambda)$ алдындағы $1/\lambda$ **еселігі гармоникалық құраушылардың амплитудаларын ғана өзгертіп, сигнал спектріне әсер етпейді.**

Бұдан басқа тағы бір салмақты келесідей қорытынды бар; ол да Фурьенің түрлендіруінен тура келіп шығады;

сигнал ұзындығы мен оның спектрінің ені бір уақытта шекті аралықтармен шекарауы мүмкін емес; яғни егер сигнал ұзындығы шектелген болса, оның спектрі шектелмеген болады; және, керісінше, шекті спектрлі сигнал шексіз ұзындықта болады. Осыдан келесідей қатыс орынды болады:

$$\Delta t\Delta f = C\,. \qquad (2.58)$$

Мұнда Δt – серпін ұзындығы, Δf – серпін спектрінің ені,

C — серпін түріне байланысты тұрақты сан болып, шамамен бағалағанда C=1 болады.

Нақты сигналдар уақыт аралығында шекараланған болып, екпінділік элементтері (мысалы, электр тізбегінде сыймдылықтар және индуктивтіктері) бар құрылғылармен генерацияланады және жіберіледі; сондықтан кез келгенше жоғары жиіліктегі гармоникалық құраушылары болмайды.

Сондықтан шектелген ұзындықтағы немесе шектелген спектрлі сигнал үлгісін қарастыруда өзгерістер ендіру керек болады; мұнда қандайда бір шартпен қосымша спектр ені, немесе сигнал ұзындығы, немесе екі параметр де бірге шекараланады. Осындай шарт деп **энергетикалық шартты** алса болады; сонда амалдық сигнал ұзындығы T_n мен амалдық спектр енін T_n таңдауда **сигнал энергиясының басым бөлігі** соларда болатындай етіп алынады.

t_0 = 0 уақыт мезгілінде басталатын сигналдар үшін амалдық ұзындық келесідей қатыстан анықталады:

$$\int_0^{T_n} |u(t)|^2 dt = \eta \int_0^{\infty} |u(t)|^2 dt , \tag{2.59}$$

мұнда η – 1-ге жетерлі дәрежеде жақын еселік (0,9 дан 0,99 дейін, сигналды қайта тіктеуге қойылатын талаптарға байланысты).

Парсевалдің (2.56) теңдігін ескере отырып, сигнал спектрінің амалдық ені үшін мынаны табамыз:

$$\frac{1}{\pi} \int_0^{\omega_n} |S(\omega)|^2 \, d\omega = \frac{\eta}{\pi} \int_0^{\infty} |S(\omega)|^2 d\omega . \tag{2.60}$$

2.4 Детерминделген сигнал қуатының спектрлік тығыздығы.

$\frac{1}{\pi}|S(\omega)|^2$ шамасы сигнал энергиясының сигнал спектрі бойынша таралуын көрсетіп, тек қана шексіз уақыт аралығында энергиясы шектелген сигналдарға ғана орынды болады; оларға Фурье түрлендіруін қолданса болады.

Уақыт аралығында сөнбейтін сигналдарға энергия шексіз үлкен болады және интеграл (2.54) жинақсыз болады. Осындайда амплитуда спектрін көрсету мүмкін болмайды. Бірақ та төмендегі қатыспен көрсетілетін орташа қуат шекті болады:

$$P_{cp} = \lim_{T \to \infty} \frac{1}{2T} \int_{-T}^{T} |u(t)|^2 dt . \tag{2.61}$$

Сондықтан оған қарағанда кеңірек болған “қуаттың спектралдық нығыздығы” деген түсінік қолданалады. Оны табу үшін сигналдың орташа қуатынан жиілік бойынша туынды аламыз және оны келесідей таңбалаймыз:

$$P_{kcp} = \int_0^{\infty} P_k(\omega)\, d\omega . \qquad (2.62)$$

Осындағы k индексі қуаттың спектралды нығыздығы детерминделеген $u(t)$ теңдеуінің сипаттамасы ретінде қаралатынын көрсетеді, ал функция сигнал орындалуын береді.

Бұл сипаттама амплитудалар спектрінің нығыздығына қарағанда мазмұнсыздау келеді, себебі мұнда фазалық информация болмайды.

Сондықтан да оның жәрдемінде берілген сигналдың орындалуын қайта тіктеу мүмкін емес.

Алайда фазалық информацияның жоқтығы осындай түсініктерді фазасы анықталмаған сигналдарға қолдану мүмкіндігін береді.

Спектралдық $P_k(\omega)$ нығыздық пен амплитудалық спектр арасындағы байланысты анықтау үшін шекараланған ($-T < t < T$) уақыт аралығында анық болған $u(t)$ сигналын қолданамыз.

Осындай сигнал үшін Парсевал теңдігі (2.56) орынды болады. (2.62) теңдеуін (2.56) теңдігінің оң жағымен салыстырып, мынаны аламыз:

$$P_k^T(\omega) = \frac{|S(\omega)|^2}{2\pi T} , \qquad (2.63)$$

мұнда $P_k^T(\omega)$ - уақыт аралығында шектелген сигналдың қуатының спектралды нығыздығы.

Осы сипаттаманы көптеген нақты мәндері бойынша орташалай отырып, кездейсоқ үдерістердің үлкен класы үшін қуаттың спектралды нығыздығын шығарып алса болады.

2.5 Детерминделген сигналдың автокорреляциялық функциясы.

Жиіліктер аймағында екі сипаттама бар: спектрілік сипаттама және қуаттың спектрлік нығыздығы. $u(t)$ сигнал туралы толық информацияны беретін спектралды сипаттама ретінде уақыт функциясы түрінде көрсетілген Фурье түрлендіруін алса болады.

Фазалық информациясы болмаған уақыт аймағындағы қуаттың спектралдық нығыздығы нені көрсететіндігін анықтап алайық; мұнда бір ғана қуаттың спектралдық нығыздығына фазалары әртүрлі болған көптеген уақыт функциялары сәйкес келетінін көреміз.

Кеңес одағының ғалымы Хинчин Л. Я. және американ ғалымы Н.Винер бір уақытта қуаттың спектралдық нығыздығына Фурьенің кері түрлендіруін тапты:

$$r(\tau)=\frac{1}{2}\int_{-\infty}^{\infty}P_k(\omega)e^{j\omega\tau}d\omega=\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{\tau}[u(t)-u_0][u(t+\tau)-u_0]dt\ ,$$

$$\text{мұнда}\quad u_0=\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}u(t)dt\,. \tag{2.64}$$

Фазалық информациясы жоқ болған $r(\tau)$ жалпыланған уақыт теңдеуін уақыт бойынша *автокорреляциялық функция* деп атаймыз.

Ол $u(t)$ теңдеуінің τ уақыт аралығымен ажыратылған мәндерінің арасындағы байланыстың дәрежесін көрсетеді; оны санақтық теориядан корреляциялық еселік түсінігін дамыту арқылы алса болады.

Айта кететін жай, бұл функцияны анықтауда уақыт бойынша орташалау жетерлі дәрежеде үлкен болған уақыт арасындағы бір ғана нақты мәндерінен табылады.

Дәл осындай ақ, Фурьенің қос түрлендіруі үшін алынған екінші интегралдық қатыс та орынды болады:

$$P_k(\omega)=\frac{1}{\pi}\int_{-T}^{T}r(\tau)e^{-j\omega\tau}d\tau\ . \tag{2.65}$$

***Зертханалық жұмыс* 2.5** Гармоникалық сигнал $u(t) = u_0\,cos(\omega t-\varphi)$ ның автокорреляциялық уақытты функциясын табу керек. (2.64) ке сәйкес:

$$r_u(\tau)=\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}u_0\cos(\omega t-\varphi)u_0\cos(\omega t+\omega\tau-\varphi)dt\ .$$

Өзгерістер ендіріп, оңтайлаған соң мынаны аламыз:

$$r_u(\tau)u_0^2\cos\omega\tau/2\,. \tag{2.66}$$

Күткеніміздей, $r_u(\tau)$ φ-ге байланысты болмайды; сондықтан, (2.66) теңдігі фазалары әртүрлі бірқатар гармоникалар жиыны үшін орынды болады.

2.6 Стохастикалық (кездейсоқ) үдеріс сигналдың үлгіссі түрінде; оның ықтималдық сипаттамалары

Жоғарыда қарастырылған детерминделген сигналдардың математикалық үлгілері анық мәлім болған уақыт қатыстары түрінде көріледі.

Оларды қолдану айқын жүйенің кіруіндегі берілген сигналға тітіркенуін (әсерінен өзгеруін) анықтауға байланысты мәселелерді шешу мүмкіндігін береді.

Нақты жағдайда кіру сигналындағы кездейсоқ құраушылары өте кішкене деп, олар назарға алынбайды.

Амалдық жағдайлардың көпшілігінде сигнал кездейсоқ үдеріс түрінде ұшырайды; мысалы, ақпарат өткізуші арнаның шығуындағы сигналдар әрқашанда кездейоқ үдеріс болып, оның сипаттамасы арнаның сипатын білдіреді.

Сонда арнамен сигнал өтуінде сигналға әсер етуші бөгеуілдер (кедергілер) де кездейсоқ үдеріс түрінде болады.

Сонда бөгеуілдің сипаты оның параметрлерімен және оның таралу заңымен анықталып, олар тәжрибелі зерттеулерден табылады.

Кедергілердің ықтималды сипаттары пайдалы сигналдың қасиеттерінен ерекше болады; осыны пайдалана отырып оларды бірінен бірін ажыратса болады. Ақпараттар теориясының орнықты шешімдері негізінен сигнал мен бөгеуілдердің санақтық сипаттамаларына негізделген; мұнда кездейсоқ үдерісті сигналдың үлгісі деп қарап, оның негізгі сипатттамасын анықтаймыз.

Кездейсоқ үдеріс деп уақыт бойынша кездейсоқ $U(t)$ қатысты айтамыз; оның әрбір уақыт мезгіліндегі мәні кездейсоқ болады. Жалғыз бір өткізілген тәжірибе түріндегі кездейсоқ үдеріс осы ***үдерістің орындалуы*** деп аталады.

Кейінгі тәжірибеде қандай орындалуын болжау мүмкін емес.

Мүмкін болған нақты мәндері жиыны ***ансамбль*** деп аталып, оны сипаттаушы санақтық деректерді анықтау мүмкін болады.

Мұндай үлгілердің қымбаттылығы - олардың жәрдемінде жалғыз орындалуға тиісті жүйенің іс-әрекетін анықтап қана қоймастан, барлық мүмкін болған нақты мәндері үшін жүйенің іс-әрекетін анықтау мүмкін болады.

Кездейсоқ үдерістердің түрлерге бөлудің негізгі таңбалары: күй

кеңістігі, уақыт параметрі, әртүрлі t_i уақыт мезгілдеріндегі $U(t_i)$ кездейсоқ шамаларының арасындағы санақтық байланыстар.

Күй кеңістігі деп кездейсоқ шама $U(t_i)$-дің мүмкін болған мәндерінің жиынын айтады. Күйлер жиыны континуум болып, ал күйінің өзгеруі кез келген уақыт мезгілінде мүмкін болса, онда кездейсоқ үдеріс үздіксіз деп аталады.

Ал егер күй өзгеруі тек шекті және санақты уақыт мезгілдерінде өтетін болса, онда үздіксіз кездейсоқ тізбек болады.

Егер кездейсоқ үдерісте күйлер жиыны шекті болса және олар кез келген уақыт мезгілінде өзгерсе, онда үдеріс дискретті-кездейсоқ үдеріс деп аталады.

Ал егер күйлердің өзгеруі тек шекті санақты уақыт мезгілдерінде болса, онда дискретті-кездейсоқ тізбектер деп аталады.

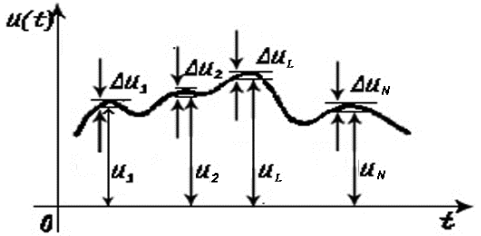
Аталған кездейсоқ үдерістер нақты мәндері 2.1-суретінде көрсетілген.

Заманауй ақпараттық жүйелерде ақпаратты жіберу және өңдеуде сандық әдістер қолданылады; сондықтан датчиктердегі ақпараттар дискретті түрде қаралып, олар дискретті кездейсоқ тізбектер түрінде қаралады.

Осындай кездейсоқ үдерістер ішінде бізді қызықтыратыны - санақтық байланыстары шектелген $к$ тізбектелген мәндеріне дейін жететін үдерістер болып, олар жалпыланған $к$ - орынды **Марков үдерістері** деп аталады.

2.6.1 Кездейсоқ үдерістердің ықтималды сипаттамалары

Анықтамаға сәйкес кездейсоқ $U(t)$ үдерісі бұл бір біріне байланысты болған және әртүрлі уақыт $t_1...t_i...t_N$ мезгілдерінде берілген $U_1 = U(t_1)$, ..., $U_i = U(t_i)$, ..., $U_N = U(t_N)$ кездейсоқ шамалардың N жүйесімен сипатталады. N ді шексіз үлкейткенде



2.10 - сурет

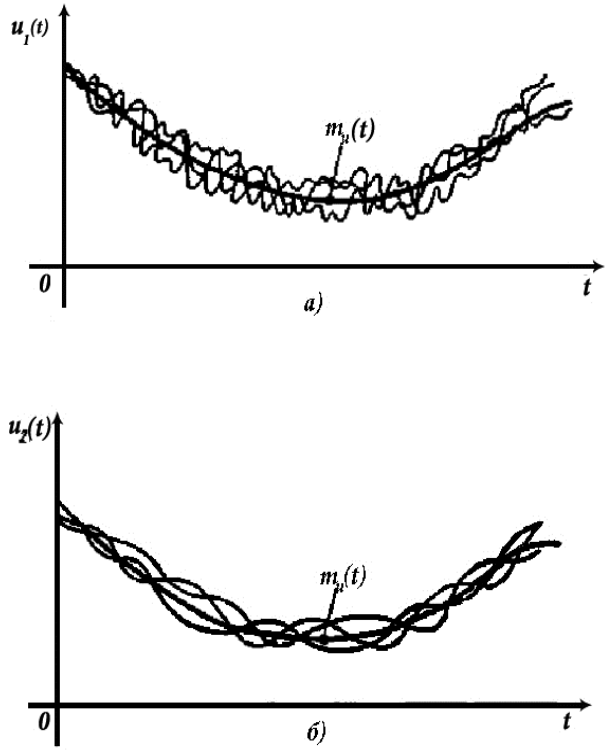
мұндай жүйе қаралып отырған $U(t)$ кездейсоқ үдерісіне эквивалент болады.

Осы жүйенің толық сипаттамасы бұл N өлшемді ықтималдықтардың нығыздық теңдеуі $p_N(U_1, ..., U_i, ..., U_N; t_1, ..., t_N)$ болады.

Осы функцияның $t_1, t_2, ..., t_N$ уақыт мезгіліндегі P_N нақты мәндері $(u_1, u_1+\Delta u_1),...,(u_i, u_i+\Delta u_i), ..., (u_N, u_N+\Delta u_N)$ аралықтарда жатады;

мұнда $u_i (1 \le i \le N)$ - U_i кездейсоқ шамасының мәндері (2.10-сурет).

Егер Δu_i жетерлі дәрежеде кіші етіп алынса, онда келесідей қатынас орынды болады: $P_N \approx p_N(u_1,...,u_N;t_1,...,t_N)\Delta u_1,...,\Delta u_N$.



2.11-сурет

N - өлшемді ықтималдықтардың тығыздық теңдеуін тәжрибемен алу үшін біріне бірі ұқсас болған көптеген кездейсоқ үдерістер көздерінің нақты мәндерін өңдеу керек болады.

N - үлкен болғанда бұл өте қиын және қымбат жұмыс болады; ал

оның нәтижелерін қолдану одан бетер математикалық қиындықтар тудырады.

Амалда мұндай толық сипаттаудың керегі болмайды.

Сондықтан әдетте бір- немесе екі- өлшемді ықтималдықтардың нығыздық теңдеуімен шектеледі.

$U(t)$ кездейсоқ үдерісінің бірөлшемді нығыздық теңдеуі $p_1(U_1; t_1)$ бір ғана кездейсоқ U_1 шамасының t_1 уақыт мезгіліндегі таралу заңын көрсетеді.

Алайда ол кездейсоқ шаманың әртүрлі уақыт мезгіліндегі байланыстылықты көрсетпейді.

Екі өлшемді $p_2 = p_2(U_1, U_2; t_1, t_2)$ нығыздық теңдеуі U_1 и U_2 кездейсоқ шамаларының t_1 и t_2 уақыт мезгілдеріндегі кез келген екі мәндерінің бір уақыттағы орындалуының ықтималдығын көрсетеді; сондықтан, ол кездейсоқ үдерістің динамикасын көрсетеді. $U(t)$ кездейсоқ үдерістің бірөлшемді нығыздық ықтималдығын екі өлшемдік нығыздықтан келесідей қатысты қолданып алса болады:

$$p_1(U_1;t_1) = \int_{-\infty}^{\infty} p_2(U_1,U_2;t_1,t_2)dU_2 \,. \qquad (2.67)$$

Амалда төменгі орынды нығыздық функциясын қолданудың өзі де күрделі есептеулерді қажет етеді.

Сондықтан көп жағдайларда кездейсоқ үдерістің ең қарапайым сипаттамалары қолданылады; мысалы, олардың сандық сипаттамалары сияқты.

Олардың ішінде кең таралғаны бірінші және екінші орынды мезгілдік (моменттік) қатыстар (функциялар), сондай ақ корреляциялық функция.

$U(t)$ кездейсоқ үдерістің **математикалық күтілімі** $m_u(t_1)$ - бұл уақыттың кез келген t_1 аргументі бойынша кездейсоқ болмаған теңдеуі болып, $U(t_1)$ кездейсоқ шамасының барлық мүмкін болған нақты мәндері бойынша алынған орташасына тең болады:

$$p_1(U_1;t_1) = \int_{-\infty}^{\infty} p_2(U_1,U_2;t_1,t_2)dU_2 \,. \qquad (2.68)$$

$U(t_1)$ кездейсоқ үдерісінің өзінің орташа $m_u(t_1)$ мәнінен t_1 дегі шеттеу дәрежесі **дисперсиямен** сипатталады:

$$D_u(t_1) = M\left\{\left[U(t_{1u}) - m_u(t_1)\right]^2\right\} = M\left\{\left[\overset{0}{U}(t_1)\right]^2\right\}, \qquad (2.69)$$

мұнда $\overset{\circ}{U}(t_1) = U(t_1) - m_u(t_1)$ орташаланған кездейсоқ шама.

Әрбір t_1 уақыт мезгіліндегі $Du(t_1)$ дисперсия $\sigma_u(t_1)$ **ортаквадраттық ауытқуға** тең болады: $D_u(t_1) = \sigma_u^2(t_1)$. (2.70)

Кездейсоқ үдерістердің математикалық күтілімдері мен дисперсиялары біртүрлі болуы мүмкін болып, олардың мәндері уақыт аралығында әртүрлі жылдамдықта өзгеруі мүмкін (2.11-сурет, а, б).

$U(t)$ үдерісінің кезкелген t_1 және t_2 уақыт мезгілдеріндегі мәндерінің санақтық байланыстық дәрежесін бағалау үшін осы аргументердің кездейсоқ болмаған теңдеуі $R_u(t_1, t_2)$ қолданылады; бұл функция **автокорреляциялық** немесе тек **корреляциялық** функция деп аталады.

Айқын аргументтер болған t_1 және t_2 лерде осы қатыс $U(t_1)$ және $U(t_2)$ үдерістер мәндерінің корреляциялық мезгіліне (моментіне) тең болады:

$$R_u(t_1 t_2) = M\left[\overset{0}{U}(t_1)\overset{0}{U}(t_2)\right]. \qquad (2.71)$$

(2.71) өрнекті екі өлшемді ықтималдықтар нығыздығы түрінде көрсетсек келесідей болады: (2.71) өрнекті екі өлшемді ықтималдықтар нығыздығы түрінде көрсетсек келесідей:

$$R_u(t_1 t_2) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left[\overset{0}{U}(t_1)\overset{0}{U}(t_2)\right] p_2(U_1, U_2; t_1, t_2)\, dU_1 dU_2 . \qquad (2.72)$$

Бұл теңдеу аргументеріне байланысты симметриялы болғандықтан мына теңдік орынды болады:

$$R_u(t_1 t_2) = R(t_2 t_1). \qquad (2.73)$$

Әртүрлі кездейсоқ үдерістерді салыстыру үшін бұл қатыстық орнына автокорреляцияның қалыптыланған функциясын қолданған жөн болады:

$$\rho_u = \frac{R_u(t_1 t_2)}{\sigma_u(t_1)\sigma_u(t_2)} . \qquad (2.74)$$

(2.69) және (2.70)-лерді салыстыра отырып, кез келген t_1, t_2 үшін $t_1 = t_2$ болғанда автокорреляциялық функция дисперсияға айланатынын көрсе болады:

$$R_u(t_1 t_1) = D_u(t_1) \,. \tag{2.75}$$

Ал қалыптыданған автокорреляциялық функция бірге тең болатынын көрсе болады:

$$\rho_u = \frac{R(t_1 t_1)}{\sigma_u(t_1)\sigma_u(t_1)} = 1 \,. \tag{2.76}$$

Сонымен, кездейсоқ үдерістің дисперсиясын оның автокорреляциялық функцияның кез келген уақыт мезгіліндегі жеке мәні деп қарау мүмкін болады. Осы сияқты екі кездейсоқ $U(t)$ және $V(t)$ үдерістер арасындағы байланысты өлшесе болады; оны өзара корреляциялық функция деп атайды:

$$R_{uv}(t_1 t_2) M\left\{\left[\overset{0}{U}(t_1)\overset{0}{V}(t_2)\right]\right\}. \tag{2.77}$$

2.6.2 Стохастикалық және эргодикалық үдерістер; олардың спектрлік және жиіліктік сипаттамалары.

Кездейсоқ үдерістер уақыт бойынша біртектілігімен ерекшеленеді; егер кездейсоқ үдерістің параметрлері мен сипаттамалары уақыт мезгіліне байланысты болса, ондай үдерістер ***бейтұрақты*** болады.

Бейтұрақты үдерістің математикалық үлгісі жалпы жағдайға сай келгенімен өте күрделі болғандықтан қолдану қолайсыз болады.

Зерттеуде математикалық аспапты ықшамдау үшін кездейсоқ үдерістің тұрақтығы туралы ұғымды ендіреміз.

Кездейсоқ үдеріс тар мағынада тұрақты болады, егер нығыздық ықтималдықтары үшін өрнек уақыт бойынша санақ басына байланысты болмаса; яғни мына қатыс орынды болса:

$$p_N(U_1,...,U_N;t_1,...,t_N) = p_N\left(U_1^{\tau},...,U_N^{\tau};t_1+\tau,...,t_N+\tau\right); \tag{2.78}$$

мұнда U_i^{τ} –кездейсоқ үдерістің $t = t_i + \tau$ (τ — кез келген сан) уақыт мезгіліндегі кездейсоқ мәні. Басқаша айтқанда, үдерістің тұрақтығы оның $-\infty$ ден $+\infty$ уақыт ауқымында санақтық біртекті болуын көрсетеді.

Алайда бұл нақты сигналдардың физикалық қасиеттеріне тура келмейді; себебі әрқандай нақты сигнал шекті уақыт аралығында

ғана өмір сүреді.

Дегенмен тұрақтанған детерминделген үдерістер сияқты кейбір жүйенің тұрақтанған жағдайында және сыртқы әсерлер де тұрақты болған жағдайда үдерісті жуық түрде **тұрақты** деп қарау мүмкін болады.

Көптеген техникалық мәселелерді шешуде кездейсоқ үдерісті кең мағынада тұрақты деп қарастырса болады; мұнда $U(t)$ үдерісі кең мағынада **тұрақты** болады, егерде оның математикалық күтілімі мен дисперсиясы тұрақты болып, ал корреляциялық теңдеуі уақыт мезгіліне байланысты болмастан, тек уақыт аралығына $\tau = t_2 - t_1$ байланысты болса, яғни

$$\begin{aligned} m_u(t_1) &= m_u = const, \\ D_u(t_1) &= D_u = const, \\ R_u(t_1, t_1 + \tau) &= R_u(\tau). \end{aligned} \qquad (2.79 - 2.81)$$

Дисперсияның тұрақты болуы корреляциялық функцияның $\tau = 0$ болғандағы жеке жағдайына қойылған талап болады:

$$D_u(t_1) = R_u(t_1, t_1) = R_u(0) = const\ ;$$

сондықтан (2.79) және (2.81) қатыстарының орындалуы $U(t)$ кездейсоқ үдерісінің **тұрақты** болуына жетерлі болады.

Тұрақты істейтін нақты үдерістерде корреляция уақыты әрқашанда шектелген болады. Сондықтан амалда ұшырайтын тұрақты үдерістер үшін мына қатыс орынды болады:

$$\lim_{\tau \to \infty} R_u(\tau) = 0\ . \qquad (2.82)$$

Егер де кездейсоқ үдерісте (2.79), (2.81) теңдіктері орындалмаса, бірақ бізді қызықтыратын аралықта (интевалдарда) аталған параметрлердің өзгеруін есепке алынбаса, онда үдерісті ***квазитұрақты*** деп атайды.

Егер үдерістің бір орындалуының өте үлкен уақыт аралығында табылған сандық сипаттамалары сол үдерістің ансамбліндегі басқа нақты мәндері бойынша табылған сандық сипаттамаларына жуықты түрде тең болса үдеріс ***эргодикалық үдеріс*** болады.

Эргодикалық үдерісте кездейсоқ үдерістің жалғыз бір орында-

луынан үдерістің басқа да орындалулары туралы толық ақпарат алса болады. Сондықтан тұрақты эргодикалық үдеріс үшін келесідей қатыстар орынды болады:

$$m_u = \lim_{T\to\infty} \int_0^T u(t)dt = u_0,$$

$$D_u = \lim \frac{1}{T} \int_0^T [u(t) - u_0]^2 \, dt, \qquad (2.83\text{-}2.85)$$

$$R_u(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_0^T [u(t) - u_0][u(t+\tau) - u_0]dt,$$

мұнда $u(t)$ - $U(t)$ кездейсоқ үдерістің айқын нақты орындалуының мәндері болады.

(2.85) ке сәйкес корреляциялық қатыстарды амалда анықтау үшін арнайы есептеу құрылымдары – ***корреляторлар*** жаратылған.

Кездейсоқ сигналдардың спектрлік көрсетілуі.

Жоғарыда детерминделген сигналдардың сызықты жүйелерден өтуін зерттеуді оңайлату үшін оларды элементер базисті сигналдармен өрнектеген едік. Кездейсоқ үдерістерді зерттеуде де дәл сондай әдісті қолданса болады.

Математикалық күтілімі $m_u(t)$ болатын $U(t)$ кездейсоқ үдерісті қарастырайық. Оның орташаланған түрі $\overset{\circ}{U}(t)$ болса, кез келген t_1 уақыт мезгіліндегі шамасы орташаланған $\overset{\circ}{U}(t_1)$: кездейсоқ шама болады:

$$U(t) = m_u(t) + \overset{0}{U}(t). \qquad (2.86)$$

Сонда орташаланған кездейсоқ үдеріс $\overset{\circ}{U}(t)$-ны ортогонал құраушылардың шекті немесе шексіз қосындысы түрінде жазып, мұнда олар кездейсоқ болмаған базисті функция $\varphi_k(t)$-мен оның кездейсоқ еселігі C_k-нен тұрады:

$$\overset{0}{U}(t) = \sum_k C_k \varphi_k(t). \qquad (2.87)$$

Кездейсоқ C_k шамалары жіктеу еселіктері деп аталады. Жалпы жағдайда олар санақтық байланысты болады және корреляциялық еселіктер $\|R_{kl}\|$ матрицасымен беріледі.

Жіктеу еселіктерінің математикалық күтілімі нөлге тең болады. Кездейсоқ болмаған базистік қатыстарды (функцияларды) координатты қатыстар (функциялар) деп атайды. Айқын орындалуы үшін жіктеу еселіктері (1.7) теңдеуімен анықталады.

Келесідей шартта $\int_{-T}^{T} m_u^2(t)dt < \infty,$

(2.86) дегі $m_u(t)$ теңдеуін —$T<t< T$ аралықта $\varphi_k(t)$ қатыстары бойынша мына түрде жіктеу мүмкін болады:

$$m_u(t) = \sum_k m_{uk}\varphi_k(t); \quad m_{uk} = \int_{-T}^{T} m_u(t)\varphi_k(t)dt. \quad (2.87а, 2.87b)$$

Орта мәні нөлге тең болмаған $U(t)$ кездейсоқ үдерісі үшін (2.87а) және (2.87б)- лерді (2.86)- ге қойып, мынаны алса болады:

$$U(t) = \sum (C_k + m_{uk})\varphi_k(t). \quad (2.87в)$$

Кездейсоқ үдерістің осы түрде жазылуы оны сызықты түрлендіруін әжептеуір оңайлатады; себебі ондайда түрлендіру тек детерминделген $[m_u(t), \sum_k \varphi_k(t)]$, функцияларды түрлендіруге келтіріледі де, ал жіктеу еселіктері кездейсоқ шамалар болғандықтан өзгермей қала береді.

Корреляциялық функцияларға қойылатын талаптарды анықтау үшін $\overset{\circ}{U}(t)$ үдерісінің корреляциялық функциясын қарастырамыз:

$$R_u(t_1t_2) = M\left[\overset{0}{U}(t_1)\overset{0}{U}(t_2)\right] = M\left[\sum_k C_k\varphi_k(t_1)\sum_l C_l\varphi_l(t_2)\right] = \sum_{k.l} M[C_kC_l]\varphi_k(t_1)\varphi_l(t_2)$$

Осында келесідей болғандықтан:

$$M[C_kC_l] = \begin{cases} D_k, k = l, \\ R_{kl}, k \neq l \end{cases}$$

келесідей болады:

$$R_u(t_1t_2) = \sum_k \varphi_k(t_1)\varphi_k(t_2)D_k + \sum_{k\neq l} \varphi_k(t_1)\varphi_l(t_2)R_{kl}. \quad (2.88)$$

Егерде корреляциялық еселіктер корреляцияланбаған ($R_{kl} = 0$,

келесідейда: $k \neq 1$, $R_{kl} = 1$, келесідейда: $k = 1$) болса, онда (2.88) өрнегі қысқа түрге келеді:

$$R_u(t_1 t_2) = \sum \varphi_k(t_1)\varphi_k(t_2)D_k \ . \qquad (2.89)$$

Мұнда $t_1 = t_2 = t$ болғанда $U(t)$ кездейсоқ үдерістің дисперсиясын аламыз:

$$D_u(t) = \sum_k [\varphi_k(t)]^2 D_k \ . \qquad (2.90)$$

$\{C_k\}$ кездейсоқ шамаларының санақтық байланыссыз болуын қамтамасыз ететін кеңістік өлшемдерін (координат) функцияларын таңдап алу мақсатқа сай келеді. Осы шартты қанағаттандыратын жіктеу канондық жіктеу деп аталады.

Егер кездейсоқ үдерістің корреляциялық теңдеуінің канондық жіктеуі мәлім болса, онда оның кеңістік өлшемдерінің қатыстары арқылы кездейсоқ үдерістің де канондық жіктеуін жазса болады; мұнда осы үдерісті жіктеу еселіктерінің дисперсиясы корреляциялық қатыстың жіктеу еселіктерінің дисперсиясына тең болады.

Сөйтіп, координаттық қатыстар (функциялар) таңдап алынғанда орташаланған кездейсоқ үдеріс жіктеу еселіктерінің дисперсиялар жиынымен сипатталады және оны кездейсоқ үдерістің жалпыланған спектрі деп қарау мүмкін болады.

(2.87) түріндегі канондық жіктеуде осы спектр дискрет (сызықтық) түрде болып, шекті немесе шексіз мүшелері (сызықтары) болуы мүмкін.

Алайда (2.2) түріндегі интегралдық канондық жіктеу де қолданылады. Кездейсоқ үдерістердің канондық жіктеулерінің амалда кең қолданылмауына негізгі себеп кеңістік өлшемдерінің қатыстарының табу шарасының қиындығы болады. Алайда бірқатар тұрақты кездейсоқ үдерістер үшін бұл мәселенің шешімі бар.

2.6.3 Тұрақты кездейсоқ сигналдардың жиілікті көрсетілуі

Дискретті спектрлер

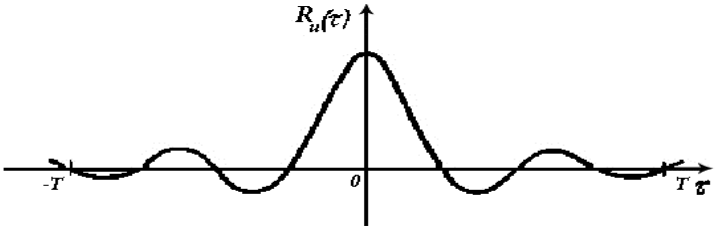
Кездейсоқ тұрақты үдерістің корреляциялық функциясы $R_u(\tau)$ (2.12 - сурет) шекті уақыт $[-T, T]$ аралығында Фурье қатарына (2.15) жіктесе болады; мұнда үдеріс шартты түрде $4T$ (мұнда —$T < t_1, t_2 < T$, $-2T < \tau < 2T$) кезеңімен қайталанады деп есептелінеді:

$$R_u(\tau) = \frac{1}{2}\sum_{k=-\infty}^{\infty} D_k e^{j\omega_k \tau} \quad . \tag{2.91}$$

Мұнда

$$\omega_k = k\omega_i, \omega_i = \pi/(2T);$$
$$D_k = \frac{1}{2T}\int_{-2T}^{2T} R_u(\tau) e^{-j\omega_k \tau} d\tau (k = 0, \pm 1, \pm 2, ...) \cdot \tag{2.92}$$

2.12-сурет



$R_u(t)$ жұп функция екенін есепке ала отырып, мынаны алса болады:

$$D_k = \frac{1}{T}\int_{T}^{2T} R_u(\tau) e^{-j\omega_k \tau} d\tau \, . \tag{2.93}$$

$\tau = t_1 - t_2$ деп таңбалап, мынаны аламыз:

$$R_u(t_1 - t_2) = \frac{1}{2}\sum_{-\infty}^{\infty} D_k e^{j\omega_k t_1} e^{-j\omega_k t_2} \; ; \tag{2.94}$$

бұл (1.89) ға сәйкес корреляциялық функцияның канондық жіктеуі болады. Осы арқылы кездейсоқ үдерістің канондық жіктеуін алса болады:

$$\overset{0}{U}(t) = \frac{1}{2}\sum_{k=\infty}^{\infty} C_k e^{j\omega_k t} \, , \tag{2.95}$$

мұнда $D[C_k] = D_k$. (2.96)

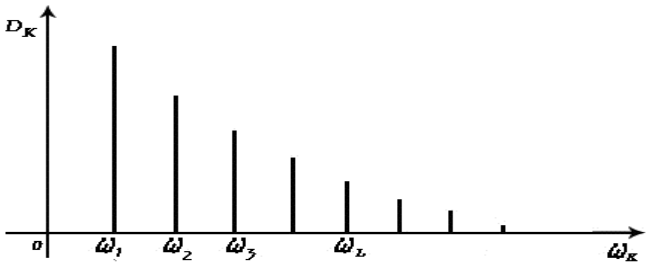
(2.95) теңдеуде кездейсоқ үдеріс тұрақты бөлімі нөлге тең болып, ол көптеген нақты сигналдарға тән болады. Ал жалпы жағдайда осы өрнектің оң жағына кездейсоқ үдерістің математикалық күтілімін (m_u) қосу керек. Мұнда корреляция өзгермейді.

(2.95) канондық жіктеуін тригонометриялық түрге келтіру үшін оның экспоненциал құраушыларын k оң және кері индекстері бойынша жұптап қосылады. Сөйтіп, шекараланған уақыт аралықтарында тұрақты кездейсоқ үдерісті әртүрлі жиілікті гармоникалық құраушылар жиынынан тұрады деп, олардың амплитудалары кездейсоқ корреляцияланбаған сандардан құралған болып, олардың математикалық күтілімі нөлге тең болады:

$$U(t) = m_u + \sum_{k=1}^{\infty} (a_k \cos k\omega_1 t + b_k \sin k\omega_1 t), \qquad (2.96а)$$

Мұнда: $\omega_1 = \pi/(2T); m_u = M[U(t)]; M[a_k] = M[b_k] = 0;$
$M[a_k^2] = M[b_k^2] = D_k.$

Осындай үдерістің спектралды диаграммасында әрбір гармоникаға сәйкес тік кесінді қойылып, оның ұзындығы гармониканың амплитудасының дисперсиясына сәйкес келеді, ал абсциссасы гармониканың жиілігіне сәйкес келеді (2.13-сурет).



2.13-сурет

Ал егер тұрақты кездейоқ үдерістің $-\infty < t < \infty$ уақыт аралығының кез келген мезгіліндегі мәнін табу үшін оның интегралдық канондық жіктеуіне өту керек болады.

Үздіксіз спектрлер.

Кездейсоқ үдерісті бақылау уақыты көбейгенде оның дисперсиясының мәні кемейеді және спектралды сызықтар арасындағы қашықтық та кемейеді; бұл (2.92)-ден көрініп тұр:

$$\Delta\omega = \omega_{k+1} - \omega_k = \pi/(2T); \qquad (2.97)$$

Жетерлі дәрежеде үлкен, бірақ шектелген T үшін дисперсияның жиілік бойынша таралуының орташа нығыздығы үшін мына өрнекті жазса болады:

$$S^T_{uu}(\omega_k) = D_k/(\Delta\omega) = 2D_kT/\pi \ \ (k = 0,\pm 1, \pm 2, ..). \qquad (2.98)$$

Мұнда $S^T_{uu}(\omega_k)$ - ω_k жиілігіне жақын болған учаскідегі дисперсияның орташа нығыздығы.

Енді (2.94) және (2.98) формулаларды мына түрге келтіру мүмкін:

$$R_u(\tau) = \frac{1}{2}\sum S^T_{uu}(\omega_k)e^{j\omega_k\tau}\Delta\omega, \qquad (2.99\text{-}2.100)$$

$$S^T_{uu}(\omega_k) = \frac{1}{\pi}\int_{-2T}^{2T} R_u(\tau)e^{-j\omega_k\tau}.$$

Олардың $T \to \infty$ болғандағы шекті түрі келесідей:

$$R_u(\tau) = \frac{1}{2}\int_{-\infty}^{\infty} S_{uu}(\omega)e^{j\omega\tau}d\omega, \qquad (2.101)$$

мұнда $S_{uu} = \frac{1}{\pi}\int_{-\infty}^{\infty} R_u(\tau)e^{-j\omega\tau}d\omega.$ (2.102)

$S_{uu}(\omega)$ теңдеуі кездейсоқ үдерістің дисперсияларының жиіліктері бойынша таралуын көрсетеді және $U(t)$ тұрақты кездейсоқ үдерісінің спектралды нығыздығы деп аталады.

(2.101) теңдеуінде $\tau = t_1 - t_2$ қойып, $R_u(\tau)$ корреляциялық функциясыныңинтегралдық канондық жіктеуінің өрнегін табамыз:

$$R_u(t_1 - t_2) = \frac{1}{2}\int_{-\infty}^{\infty} S_{uu}(\omega)e^{j\omega t_1}e^{-j\omega t_2}. \qquad (2.103)$$

$G^T(\omega) = C_k/(\Delta\omega)$ деп таңбалап және (2.95) қатысы үшін $T \to \infty$ дегі шекті түрлендіру шарасын қайталап, $U(t)$ тұрақты кездейсоқ функциясының канондық жіктеуін табамыз:

$$U(t) = \int_{-\infty}^{\infty} G(\omega)e^{j\omega t}d\omega, \qquad (2.104)$$

мұнда $G(\omega)d\omega$ кездейсоқ функциясының дисперсиясы болып $S_{uu}(\omega)d\omega$ функциясы болады.

Спектрлік нығыздықтың негізгі қасиеттері

Айта кететін жай**,** (2.101) және (2.102) формулаларда $S_{uu}(\omega)$ оң және кері жиіліктерде де анықталған. Енді тек оң жиіліктермен ғана шектелеміз. Эйлер теңдеуін қолданып, (2.102) қатысын екі қосынды түрінде көрсетеміз:

$$S_{uu}(\omega) = \frac{1}{\pi}\int_{-\infty}^{\infty} R_u(\tau)\cos\omega\tau d\tau - \frac{1}{\pi}\int_{-\infty}^{\infty} R_u(\tau)\sin\omega\tau d\tau .$$

$S_{uu}(\omega)$ формуласының жұп екенін есепке ала отырып және екінші қосылғыш нөл деп, ал біріншісін мына түрде жазса болады:

$$S_{uu}(\omega) = \frac{2}{\pi}\int_{0}^{\infty} R_u(\tau)\cos\omega\tau d\tau . \qquad (2.105)$$

Осыдан $S_{uu}(\omega)$ нақты және жұп функция екені көрінеді:

$$S_{uu}(\omega) = S_{uu}(-\omega). \qquad (2.106)$$

Сондықтан (2.101) де тек оң жиіліктермен ғана шектелеміз:

$$R_u(\tau) = \int_{0}^{\infty} S_{uu}(\omega)\cos\omega t d\omega . \qquad (2.107)$$

(2.101) және (2.102), сондай-ақ (2.105) және (2.107) қатыстары Фурьенің интегралды түрлендіру параметрлері болып, ал осылардан (2.105) және (2.107) лері жұп қатыс үшін орынды болады. Сондықтан корреляциялық функция мен спектрлік нығыздық келесідей заңдылыққа бойсынады: $S_{uu}(\omega)$ қисығы қаншалықты ұзынырақ болса, оның корреляциялық $R_u(\tau)$ (соншалық корреляция уақыты кемірек болады), және керісінше.

Спектралды диаграммада $S_{uu}(\omega)$ үздіксіз қисығымен шектелген аудан кездейсоқ $U(t)$ үдерісінің D_u дисперсиясына тең болады.

Расында, (2.107) теңдеуінде $\tau = 0$ деп қойып, мынаны аламыз:

$$R_u(0) = D_u = \int_{0}^{\infty} S_{uu}(\omega)d\omega . \qquad (2.108)$$

Осында кездейсоқ $U(t)$ үдерісі деп кернеуді түсінсек, онда D_u деп 1 Ом резисторда ажыралып шығатын орташа қуатты айтса болады;

$$\bar{D_u} = M\left[U^2\right] = P_u \ . \tag{2.109}$$

Сондай ақ мына шама:

$$dP_u = S_{ш}(\omega)d\omega\,, \tag{2.110}$$

осы орта қуаттың бір бөлігі болып, оны $(\omega,\ \omega + d\omega)$ жиілік аралығына сәйкес келетін спектр құраушысы бөліп шығарады. $S_{ш}(\omega)$ энергия өлшемімен өлшенгендігі үшін кездейсоқ үдерістің **энергетикалық спектрі** деп немесе **қуаттың спектралдық нығыздығы** деп те аталады.

Қуаттың спектралдық нығыздығы көптеген орындалған нақты мәндердің орта шамасы болғандықтан оны табу үшін көптеген $P_k(\omega)$ нақты мәндердің спектралды қуатын (2.62) орташалап та тапса болады.

$P_k^T(\omega)$ орташа мәнін $к$ нақты мәндері жиынынан табамыз:

$$P^T(\omega) = \frac{1}{2\pi T}\int_{-T}^{T}\int_{-T} R_u(t_1 t_2)e^{-j\omega(t_1 - t_2)}dt_1 dt_2\,. \tag{2.113}$$

Егер кездейсоқ үдеріс $U(t)$ тұрақты болса, онда

$$R_u(t_1 t_2) = R(t_1 - t_2) = R_u(\tau)\,, \tag{2.114}$$

мұнда $t_1 - t_2 = \tau$ шарты орындалғанда (2.113) өрнегі үшін $T \to \infty$ болғанда келесідей шек табылады:

$$\lim_{T\to\infty} P^T(\omega) = \frac{1}{\pi}\int_{-\infty}^{\infty} R_u(\tau)e^{-j\omega\tau}d\tau = S_{ш}(\omega). \tag{2.115}$$

II тараудың бақылау және емтихан сұрақтары:

1. Дискреттеу мен кванттау үдерістерінің мағынасы неде?
2. Дискретті және сандық ақпаратты ұзатудың абзалдығын сипаттаңдар.
3. Дискреттеу мәселесінің жалпы қойылуын қалыптастыру керек.
4. Сигнал кеңістік өлшемдерін алудың негізгі әдістері қандай?
5. Сигналды тіктеудің интерполяциялық және экстраполяциялық әдістерін салыстырыңдар.
6. Сигналды тіктеудің ортаквадраттық шарты деп нені түсінеміз?
7. Котельников теоремасын түсіндіріңіз.
8. Спектрі шектелген үздіксіз қатысты санақтар жиынымен көрсетудің физикалық мүмкіндіктерін түсіндіріңіз.
9. Спектрі шектелген қатыстарды сигнал үлгісі ретінде көрсетудің қолайсыз жақтары неде?
10. Үздіксіз сигналдарды ұзатудың Котельников теоремасына негізделгенде техникалық орындалуының қиындығы неде?
11. Ең үлкен ауытқу шартында біркелкі дискреттеу шарасы қандай?
12. Бейімделуші дискреттеудің абзалдығы мен кемшіліктері неде?
13. Біркелкі кванттаудың ортаквадраттық қателігі қандай өрнекпен табылады?
14. Кванттау шуылы деп неге айтамыз?
15. Кедергі болғанда сигналды кванттау қадамы қалай табылады?
16. Геометриялық көрсетуде сигналдың қандай кеңістік өлшемдері жиыны қолданылады?
17. Сигналдарды геометриялық көрсетудің амалдық маңызы неде?

Өзіндік жұмыстар (СӨЖ) тақырыптыры

1. Сандық түрдегі сигналдардың абзалдығы.
2. Дискреттеу және кванттау; олардың сандық жүйелерде қолданылуы.
3. Кванттау шуылы. Бөгеуіл бар болғандағы кванттау.
4. Дискреттеу; ақпаратты дискреттеу және қалпына келтіруде сапа шарттары.
5. Таңдау құралы бойынша дискреттеу.

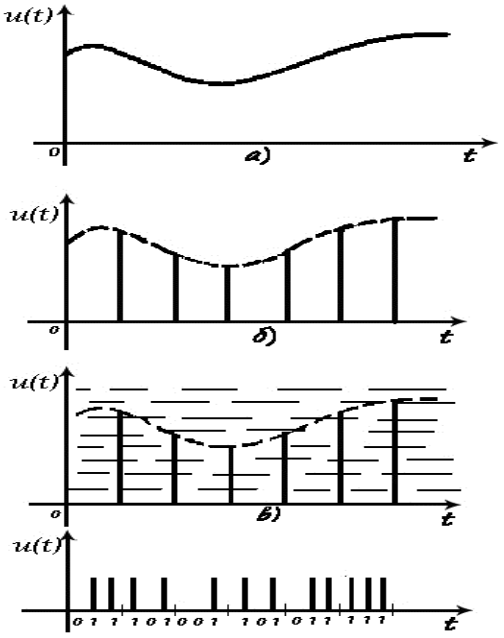
6. Бірқалапты дискреттеу. Котельников теоремасы.
7. Котельников теоремасының амалдық маңызы.
8. Ең үлкен ауытқу бойынша дискреттеу.
9. Дискреттеудің энтропиялық, экстраполяциялық әдістері.
10. Тейлордың экстраполяциялық көпмүшелігімен дискреттеу.
11. Бейімделуші дискреттеу.
12.Сигналдардың көрсетілуінің геометриялық келбеті.

III ТАРАУ.

ҮЗДІКСІЗ СИГНАЛДАРДЫ ДИСКРЕТТЕУ

3.1 Сандық түрдегі сигналдардың абзалдығы

Кез келген ақпараттық жүйеге ақпарат сигналдар түрінде келіп түседі. Мұнда физикалық үдерістердің параметрлері датчиктер (өлшеуіш асбаптар) арқылы электр сигналдарына айлантырады.



3.1- сурет

Әдетте, олар уақыт аралығында өзгеретін кернеу болады; алайда импульсті сигналдар да қолданылады, мысалы, радиолокацияда. Баспа мәтінді әріптер, цифралар және басқада таңбалармен көрсетіледі.

Әрине, сигналдардың екі түрін де қолдану мүмкін болса да, осы күні ақпараттық техниканың дамуы сандық сигналдарға орын беріп отыр.

Сондықтан, сигналдар дискрет түрге айналдырылады. Осы мақсатта үздіксіз сигналдар баған бойынша кванттау және уақыт бойынша дискреттеу амалдарынан өтеді. Мұнда **дискреттеу** деп үздіксіз уақыт теңдеуін дискрет уақыт теңдеуіне айналдыруды айтамыз; ал алынған кеңістік өлшемдері жиыны арқылы үздіксіз функция (қатыс) берілген анықтықпен қайта тіктеледі.

Кеңістік өлшемдері қызметін анық бір уақыт мезгілдерінде анықталған қатыстың (функцияның) лездік мәндері атқарады.

Ал **кванттау** деп үздіксіз қатыстың үздіксіз мәндерін берілген шәкіл бойынша дискрет мәндерге айналдыруды айтамыз.

Мұнда қатыстың кез келген лездік мәні оған сәйкес келген кванттау деңгейімен алмастырылады.

$u(t)$ (сурет 3.1, а) сигналын дискреттеуден кейінгі түрі 3.1,б-суретінде, ал дискреттеу және кванттауды бірге өткізгендегі түрі 3.1,в суретте көрсетілген. $u(t)$ (3.1, а-сурет) сигналдың сандық түрі 3.1,г суретінде көрсетілген.

Мұнда сегіз деңгей үшін үш екілік орын (разряд) жеткілікті болады.

Жоғары орындағы серпіндер сол жақ шетте орналасқан болады.

Ақпараттың дискретті сандық түрге өткізілу себебі мынада;

берілген нысанды зерттеу және басқару үшін датчиктерден келіп түскен үздіксіз хабарға қарағанда әжептеуір **кем ақпарат** керек болады.

Сигналдар туралы априор ақпаратты есепке алу және оны қолдану мақсаттарын алдын ала білу сигналдарды **қысқарту мүмкіншілігін** тудырады; яғни сигналдарды тек кейбір уақыт мезгілдерінде ғана алуға мүмкіндік береді.

Өлшенетін параметрлердің флуктуациясы мен өлшеу құралдарының қателік деңгейі шектелгендігінен кванттау деңгейі де шектелген болып шығады. Шешілетін мәселенің түріне қарай отырып, сигналды кванттау деңгейін тағы да кемейтсе болады.

Көп жағдайда ақпарат сандық техника жәрдемінде алынады және ұзатылады; бірінші орында ЭЕМ және микропроцессорлар жәрдемінде.

Кванттау және дискреттеу амалдарының рационал түрде орындалуы әжептеуір **экономикалық** үнемге жеткізеді; бұл ақпаратты өңдеуге және сақтауға кететін уақыттың қысқаруы есебінен болады. Ал бұл басқарудың **анықтығы** мен **шапшаңдығын** да **арттырады.**

Ақпаратты сандық түрде өңдеу мен ұзатуда **қателіктер**

ықтималдығын кез келген **дәрежеге дейін кемейту** мүмкін болады; бұл әртүрлі кодттау амалдарымен орындалады.

Екіншіден, ұқсастық сигналдарына тән ***қателіктің*** немесе **бұзылудың жинақталуын** болдырмау мүмкін болады.

Ақпаратты сандық түрде көрсету оны түрлендірудің барлық этаптарында түрлендірулерді **унификациялау** мүмкіндігін береді.

Типтік түйіндер мен жиынтықтарды **массалық түрде** дайындау, оларды **баптаудың оңайлығы**, пайдалану уақытында **баптаудың керек болмауы**, және ең керегі, құруда және пайдалану уақытында құ**ны төмен** және **сенімділігі жоғары** болады.

Өте үлен интегралдық сұлбалардың **төмен құны** мен **жоғары сенімділігі** сандық сигналдардың одан ары да қолданылуына **үлкен стимул** жаратты.

Дискреттеу мәселесінің жалпы қойылуы.

$u(t)$ үздіксіз сигналын T аралығында (c_1, c_2, ..., c_N) кеңістік өлшемдері жиынымен көрсетудің жалпы түрі келесідей болады:

$$(c_1, c_2, ..., c_N) = A[u(t)], \tag{3.1}$$

мұнда A - сигналды дискрет түрде көрсету операторы болып, дискретизатор мен нақты мәнге жетіледі.

Осы (c_1, c_2, ..., c_N) кеңістік өлшемдері жиынымен берілген сигналды біршама жақындау қателігімен $\delta(t) = u(t) - u^*(t)$ көрсететін үздіксіз қатыс болған $u^*(t)$ (тіктеуші қатыс) арқылы тіктесе болады:

$$u^{\bullet}(t) = B[(c_1, c_2, ..., c_N)], \tag{3.2}$$

мұнда, B - тіктеу операторы, оны сигналды тіктеуіш құрылымы орындайды.

Математикалық түрде дискреттеу мәселесі тиісті тіктеу анықтығын беретін A және B қос **операторын таңдап алуға** келеді.

Қолданылатын A және В операторларының түрлері мен сигналды тіктеу анықтығын бағалау шарттарын қарастырайық.

Техникалық орындалуы оңай болғандығы үшін көбінесе сызықтық операторлар кең қолданылады.

Сигналдардың кеңістік өлшемдерін анықтауда мына қатыс қолданылады:

$$c_j = \int_T \xi_j(t) u(t) dt = Au(t) \tag{3.3}$$

мұнда $\{\xi_j(t)\}_{j=1}^{N}$ - қатыстар жиыны ***салмақты функция*** деп аталады.

Тіктеуіш қатыс келесідей аппроксимациялаушы полиноммен көрсетіледі:

$$u^*(t) = \sum_{j=1}^{N} c_j \varphi_j(t) = B(c_1, c_2 ..., c_N) \ , \qquad (3.4)$$

мұнда $\{\varphi_j(t)\}_{j=1}^{N}$ - базистік функциялар жүйесі.

Дискреттеу әдісі сигнал кеңістік өлшемдерін шығарып алу әдісіне байланысты түрде ажыралады.

Егерде салмақты функция ретінде базистік функция [$\xi_j(t) = \varphi_j(t)$] істетілсе, онда $u(t)$ сигналының $c_1, c_2, ..., c_N$ кеңістік өлшемдері T уақыт аралығында сигналды "салмақты" интегралдау арқылы табылады.

Онда мына шарттар орындалуы керек: базистік функциялар ортогоналды болуы керек және олар $N \to \infty$ да (3.4) ортаквадраттық қатардың $u(t)$ ға жинақталуын қамтамасыз етуі керек; бұл берілген тіктеу қателігіне сай кеңістік өлшемдері санын шектеуге мүмкіндік береді.

Дискреттеу операциясы берілген айқын түрдегі кездейсоқ үдеріске, демек детерминделген үдеріске өткізіледі; алайда басқа да нақты мәндерге де сол дискреттеу бағдаржолы өзгеріссіз істетіледі.

Сондықтан кездейсоқ үдерістің үлгісі берілген сигнал үлгісі деп қаралуы керек. Амалда дискреттеу әдісін таңдау оның техникалық орындау мүмкіндігіне байланысты болады.

Ал теориялық зерттеуде берілген тіктеу қателігінде кеңістік өлшемдер (координат) санын минималдайтын дискреттеу әдісін табу болады. Оларды **тиімді** немесе **шекті дискреттеу әдісі** деп атайды.

Нақты жағдайда көбінесе бейтұрақты кездейсоқ үдеріс берілген болса, онда осы **үдерісті канондық жіктеу** олардың кеңістік өлшемдерінің коореляцияланбайтындығын, сондай ақ олардың минимал болуын қамтамасыз етеді.

Мұнда базистік функция $\varphi_j(t)$ ретінде координаттық қатыстар (функция) қолданылады. Жіктеу кеңістік өлшемдері c_k ізделіп отырған кеңістік өлшемдері болады. Бейтұрақты үдерісті дискреттеудің координаттық қатыстарын табу күрделілігі себепті инженерлік амалда кем қолданылады.

Кеңістік өлшемдері корреляцияланбайтын болуы үшін тек

канондық жіктеулер қолданылатын болса, мұндай жағдайға тура келетін, мысалы, тригонометриялық функциялар болады.

Егер үдеріс шектелген уақыт аралығында анықталған болса және ол уақыт корреляция аралығынан артық болса, онда Фурье қатарын қолдану мүмкін болады; оның еселіктері – кездейсоқ шамалар (2.95) түріндегі координаттар болады.

Егерде кеңістік өлшемдерінің **корреляцияланбау талабы** қойылмаса, онда кездейсоқ үдерісті **кез келген толық ортогонал функциялар жүйесімен** жіктеуге болады.

Мұнда нақты мәннің кеңістік өлшемдері ретінде Фурьенің жалпыланған еселіктері алынады.

Осы жағдайда кеңстік өлшемдері өрнегі интегралдау операциясымен орындалғандығы себепті дискреттеу бағдаржолдары жоғары кедергіге шыдамдылығымен ерекшеленеді.

Дискреттеу мақсатында Лежандр, Уолш, Хаар қатыстары қолданылатыны мәлім.

Алайда кеңістік өлшемдеріды табу және сигналды қайта тіктеуде техникалық орындалуының күрделілігі, сигналдың уақыт аралығында іркілуі себепті сигналды “салмақты” интегралдау негізінде оның кеңістік өлшемдерін табу әдісі тек қана серпінді кедергілердің жоғары орынында ғана қолданылады.

Амалда кеңірек таралған дискреттеу әдісінде $u(t)$ сигналы оның лездік $u(t_j)$ мәндерінің жиынымен алмастырылады; ол мәндер анықталған $t_j(j=1,2, ..., N(t)$ уақыт мезгілдерінде алынады; олар **таңдаулар** немесе **санақтар** деп аталады.

Мұнда (3.3) қатысындағы ***салмақты қатыс*** $\xi_j(t)$ қызметін Дирактың дельта-функциясы атқарады.

(2.11) ге сәйкес $c_1, c_2, ..., c_N$ кеңістік өлшемдері болып, $u(t_j)[\xi_j(t) = \delta(t - t_j)]$ таңдаулары немесе көрші таңдаулардың айырмасы $\Delta u(t_j) = u(t_j) — u(t — t_j)[\delta_j(t)= \delta(t - t_j) – \delta(t - t_{j-1})]$ көрінеді.

Дельта-функция техникада орындалмайтындығы үшін таңдау ұзындығы шекті болады. Сондықтан санақты бір нүктеде емес, кілтті құрылымның басқарушы серпінінің ұзындығына байланысты кішкене бір уақыт аралығына тең етіп алынады.

Егер серпін ұзындығы дискреттеу қадамынан әжептеуір кем болса, онда таңдаулар қысқа серпін (имульс) болып, олардың амплитудалары сигналдың лездік мәндеріне өлшемдес (пропорционал) болады.

Көрші таңдаулар арасындағы уақыт $\Delta t_j = t_j — t_{j-1}$ кесіндісін **дискреттеу қадамы** деп атайды.

Егер ол түрлендірудің ақырына дейін болса, **дискреттеу біркелкі** болады. Техникалық орындалуы оңай болғандықтан дискреттеудің бұл түрі амалда кең қолданылады.

Алайда дискреттеудің кейбір жерлерінде санақтардың жиілігінен **санақтардың артықшылығына** алып келеді.

Ал егер дискреттеу қадамы сигналдың өтпелі сипатына қарай өзгеріп отырса, онда ***дискреттеу біркелкі емес*** деп аталады.

Кейбір жағдайда сигнал кеңістік өлшемдері ретінде $u(t_j)$ сигналдың таңдауларымен бірге сигналдың t_j уақыт мезгілдеріндегі $u(t)$ сигналының N-дәрежеге дейін туындылары да қолданылады. Алайда көбінесе таңдаулар бойынша дискреттеу қолданылады.

Үздіксіз сигналды қайта тіктеу әдісі.

Таңдау бойынша сигналды тіктеуді ортогонал, сондай-ақ ортогонал болмаған базисті қатыстар негізінде орындаса болады; олар аппроксимациялаушы полиномның түрін және жақындау қағидасын анықтайды.

Жақындау қағидасы келесідей болады: интерполяциялық, экстраполяциялық және қисындастыруылық.

Ортогонал болмаған сигнал көрінісінде көбінесе алгебралық полиномдар қолданылады:

$$u^*(t) = \sum_{j=0}^{N} a_j t^l \tag{3.5}$$

немесе

$$u^*(t) = \sum_{j=0}^{N} a_j (t - t_0)^j, \tag{3.6}$$

мұнда α_j - нақты еселіктер.

Егер сигнал координаттары таңдаулар айырмасы түрінде берілген болса, онда оны тіктеуде алдын таңдаулар тізбегі есептеліп, кейін солар арқылы аппроксимациялаушы полином $u^*(t)$-ды құрады.

Аппроксимациялаушы полиномның $u^*(t)$ құрамындағы **базистік функциялар жүйесін таңдау** көбінесе сигналды дискреттеу және тіктеудің аспаптық және бағдарламалық құрылымдарының техникалық орындалуының **қарапайымдығына** қойылатын **талаптармен** анықталады.

Егер базистік қатыстарды таңдауда аппроксимациялаушы полином мәндері қатыстың санақ мезгілдеріне сәйкес келсе, ондай ***полином интерполяциялық*** деп аталады.

Санақтар санын қысқарту жағынан қарайтын болсақ интерполяциялық әдіс абзал болады.

Алайда мұнда сигнал интерполяция уақытына іркіледі. Ал нақты уақыт масштабында істейтін жүйелер үшін бұл жағдай мүмкін емес болады. Сондықтан, мұндай жүйелерде экстраполяция әдістері қолданылып, мұнда таңдау мәндерін анықтауда және сигналдарды тіктеуде сигнал іркілмейді.

3.1.а Бөгеуіл бар болғандағы кванттау; кванттау шуылы

Үздіксіз сигналдың математикалық үлгісі ретінде келесідей кездейсоқ үдерісті $U(t)$ түсінетін болсақ, онда оның мезеттік мәні $U = U(t_i)$ кездейсоқ шама болады. Оның өзгеру ауқымы сигналдың мезеттік мәнінің үздіксіз өзгеру шәкілі деп аталып, ол мына мәндермен шекараланған u_{min} және u_{max} болады; ол сигналдың физикалық орындалуы мүмкіндігін білдіреді.

Сигналдың мезеттік мәнінің үздіксіз шәкілін $u_n = u_{max} - u_{min}$ n аралықтарға бөліп, оларды ***кванттау қадамдары*** деп атайды.

Кванттау қадамының мәндері $u_0 = u_{min}$, u_1, ..., u_{n-1}, $u_n = u_{max}$.

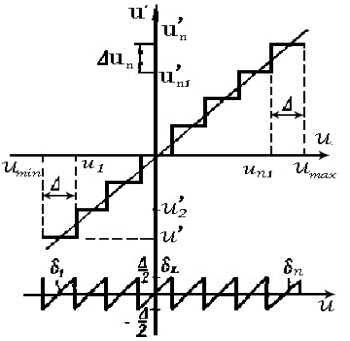
Сигналдың көптеген мәндерінің ішінде *i*- кванттау қадамына сәйкес келетін $(u_{i-1} \le u < u_i)$, тек қана бір ғана мәні u'_i ғана рұқсат етілген (*i* - кванттау деңгейі) болады.

Сигналдың басқа кез келген мәндері осы u'_i мәніне жуықталады.

Келесідей мәндер жиыны $u'_i (i=1, 2, ..., n)$ кванттау деңгейінің дискрет шәкілін құрайды.

Егер осы шәкіл (шкала) біркелкі болса, яғни мәндер айырмашылығы $\Delta u'_i = u'_i - u'_{i-1}$ сигналдың үздіксіз шәкілінің барлық ұзындығы бойынша өзгермейтін болса, кванттауды ***біркелкі*** деп аталады.

Ал егерде $\Delta u'_i$ өзгеруші болса, онда кванттау ***біркелкі емес*** болады.



3.2 Сурет

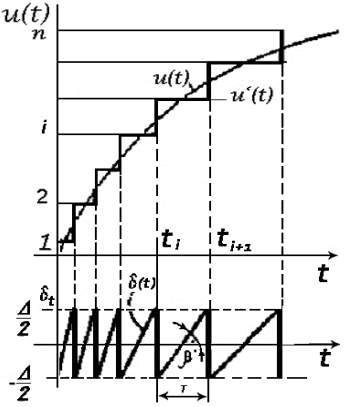
Техникалық орындауоңай болғандығы себепті ***біркелкі*** кванттау кең қолдану тапты.

U сигналының мезеттік мәндерін кванттаудың сәйкес u'_i деңгейлерімен алмастырғанда келесідей қателік пайда болады: $\delta_i = u - u'_i$, оны ***кванттау қателігі*** дейді. Осы қателік кездейсоқ шама болады.

Бізді қызықтыратын нәрсе оның максимал мәні: $\delta_M = max|\delta_i|$ және сигналдың мезеттік мәнінен ортаквадраттық ауытқу σ барлық өлшеу ауқымында есептеледі;

$$\delta_{Mc} = \delta_M /(u_{\max} - u_{\min}),$$
$$\sigma_0 = \sigma /(u_{\max} - u_{\min}).$$

Сондай-ақ олардың келтірілген мәндері қолданылады.



3.3-сурет

Кванттау қателігін минималдау мақсатында сигналдың үздіксіз кванттау ауқымын n біртүрлі кванттау қадамына бөлу керек: $\Delta = (u_{max} — u_{min})/n$ және кванттау деңгейін әрбір қадамның ортасына орналастыру керек болады (3.3-сурет). Мұнда кванттаудың максимал қателігі 0.5Δ дан аспайды.

Ал егер де кванттау деңгейін кванттау қадамының бір шетіне қойсақ, онда максимал қателік Δ дейін артуы мүмкін.

i - қадамы үшін кванттау қателігінің ортаквадраттық ауытқуы σ_i тек қана қадам үлкендігі Δi және ондағы i - кванттау деңгейіне ғана байланысты болмастан, сонымен қатар осы қадамда сигналдың лездік мәндерінің таралу заңына да байланысты болады:

$$\sigma_i = \sqrt{\int_{u_i-1}^{u} (u - u_l')^2 \, p(u) du}, \tag{3.7}$$

мұнда $p(u)$ – U сигналының лездік мәндерінің ықтималдықтарының нығыздық теңдеуі.

Сигналдың өзгеру ауқымына қарағанда кванттау қадамы өте кіші деп қарасақ, онда қадамның ішінде $p(u)$ нығыздығын өзгермес және оның орта мәні $p(u'_i)$ тең деп алсақ болады.

Осындай таңбалеулерден кейін минимал ортаквадраттық қателік σ_i кванттау деңгейін қадамның ортасына орналастырғанда ғана болады:

$$\sigma_i = \sqrt{p(u_i')\frac{\Delta_i^3}{12}} \tag{3.8}$$

Түбір астындағы өрнекті мына түрге келтіріп:

$$\sigma_i^2 = \left[p(u_i')\right]\frac{\Delta_i^2}{12}, \tag{3.9}$$

i - қадамындағы кванттау қателігінің дисперсиясы табылады: $\Delta^2_i/12$;

ол сигнал осы қадамда біркелкі таралғанда оның осы қадамға түсу ықтималдығын $p(u'_i)\Delta_i$ қадам ұзындығына көбейтіндісіне тең болады.

Сигналдың барлық ауқымында кванттау қателігінің толық дисперсиясы σ^2 әр қадамдағы $\Delta^2_i/12$ дисперсияның математикалық күтілімі ретінде табылады, яғни:

$$\sigma^2 = \sum_{i=1}^{n} \sigma_i^2 = \frac{1}{12}\sum_{l=1}^{n} p(u_l')\Delta_i^3 \quad . \tag{3.10}$$

Егер кванттау қадамы бірдей болса ($\Delta_i = \Delta$), онда:

$$\sigma^2 = \frac{\Delta^2}{12}\sum_{l=1}^{n} p(u_l')\Delta \tag{3.11}$$

Егер келесідей қабылдасақ:

$$\sum_{l=1}^{n} p(u_i')\Delta = 1, \text{ онда: } \sigma^2 = \Delta^2/12 \quad . \tag{3.12}$$

Сөйтіп, біртүрлі қадаммен кванттауда және кванттау деңгейін

қадам ортасына орналастырғанда (біртегіс кванттау) кванттау қателігінің ортаквадраттық ауытқуы, біртегіс кванттауда да, басқа әртүрлі таралу заңдарында да бірдей болып, мынаған тең болады:
$\sigma = \Delta / 2\sqrt{3}$. (3.13)

Кванттау шуылы

Сигналдың деңгейі бойынша кванттағанда кездейсоқ үдеріс текшелі байланыспен алмастырылады $U'(u)$.

Уақыт бойынша өзгеруші кванттау қателігі $\delta(u)$ де кездейсоқ үдеріс болып, **кванттау шуылы** деп аталады:

$$\delta(t) = U(t) - U'(t). \tag{3.14}$$

Алдыңғы ендірілген шектеулерді (кванттау қадамы кіші болып, ондағы сигналдың мәні өзгермес) ескере отырып және кездейсоқ үдерістерді $U(t)$ және $\delta(t)$ эргодикалық деп, біртегіс кванттаудың ортаквадраттық қателігін σ оның келесідей $\delta_1(t)$ (3.3-сурет) нақты мәндерімен анықтаса болады.

Бір кванттау қадамының Δ ішінде қателіктің өзгеру заңдылығы $\delta_1(t)$ түзу сызық деп және $t \times tg\beta_1$ алмастырамыз; мұндағы β – түзудің көлбеулік бұрышы. Кванттау деңгейін қадамның ортасына орналастырғанда кванттау қателігінің математикалық күтілімі нөлге тең болады; ал оның ортаквадраттық мәні келесідей анықталады:

$$\sigma = \sqrt{\frac{1}{T}\int_{-T/2}^{T/2} (t \cdot tg\beta)^2 dt}. \tag{3.15}$$

Мұнда:

$$tg\ \beta\ =\ \Delta\ /\ T\ ,\ _1\sigma\ =\ \Delta\ /\ 2\sqrt{3}\ .$$

Мүмкін болған кванттаудың ортаквадраттық қателігі берілген болса және кедергі жоқ болса, онда кванттау деңгейінің санын келесідей табамыз:

$$n = (u_{\max} - u_{\min}) / (2\sqrt{3\sigma}). \tag{3.16}$$

Алайда сигналдың лездік мәндерінің біртегіс болмауы кванттаудың бірдей қадамды болуы тиімді болмауына әкеледі; мұнда тиімділік қателіктің σ ортаквадраттық ауытқуының минимумы шарты бойынша табылады.

Осы шарт бойынша σ одан әрі кемейту үшін сигналдың ықтималдығы кем учаскелерде кванттау қадамын үлкейту керек болады.

3.1. *Зертханалық жұмыс*

Берілген сигнал $u(t)$, оны кванттау қателігінің нығыздық теңдеуі $p(u)$ болсын; мұнда кванттау қадамы Δ өзгермес және сигнал $u(t)$ өзгеру ауқымынан әлдеқайда кем болса және кванттау деңгейі қадамның ортасында орналасқан болса, онда кванттау қателігінің ортаквадраттық ауытқуы σ өзінің минимумына жетеді.

Кванттау қателігінің дисперсиясы i - қадамының ішінде болғанда, (3.7) сәйкес келесідей жазылады:

$$\sigma^2 = p(u_l^{'}) \int_{u_l - 1}^{u_l} (u - u_l^{'}) du = p(u_l^{'}) \frac{1}{3} \left[(u_l - u_l^{'})^3 - (u_{l-1} - u_l^{'})^3 \right],$$

мұнда u'_i – i-нші кванттау деңгейі.

Осы өрнектің туындысын нөлге теңеп, минимум шартын табамыз:

$$\partial[\sigma^2] / \partial u_l = p(u_l^{'})[(u_l - u_l^{'})^2 - (u_l - u_{l-1}^{'})^2] = 0_1$$

осыдан $\pm (u_l - u_l^{'}) = \pm (u_{l-1} - u_l^{'})$ және біртүрлі таңбаларде $u_i = u_{i-1}$;

алайда мұндай болуы мүмкін емес; себебі мұнда дискреттеу болмайды; яғни: (Δ = 0). Сондықтан әртүрлі таңбаларды қабылдап, мынаны аламыз: $u_l^{'} = (u_1 - u_{l-1)} / 2$.

3.1. б Бөгеуіл бар болғандағы кванттау

Нақты жағдайда кванталатын сигналға әрқашанда кедергі әсер етеді.

Сондықтан кванттаудың минимал қадамын кедергінің ықтималды сипаттамасын есепке алып отырып табылады.

Айталық, кедергі (бөгеуіл) аддитивті болсын.

Онда сигналдың лездік мәні кванттау қадамының i-қадамына сәйкес келетін болса және ол u'_i кванттау деңгейіне сәйкестендірілетін болса, кедергі әсерінен мына мән $u + \xi$ қабылданады; ал ол басқа кванттау деңгейіне сәйкестендіріледі.

Мұндай болуы ақпараттың бұзылуына әкеледі; ал оның ықтималдығы мүмкін болған мәннен аспауы керек.

$p_i(k)$ – деп сигналдың мәнін u'_k кванттау деңгейіне (u'_i орнына) сәйкестендірудің ықтималдығы десек, мұнда u кванттаудың i- қадамына сәйкес келеді. Кедергі бар болғанда $p_i(k)>0$, ал $p_i(i)<1$ болады.

Сонда мына $u + \xi$ мәні i - кванттау қадамында қалатындығының ықтималдығы:

$$p_i = p_i(i) \int_{u_i - 1}^{u_i} p(u)du\,, \tag{3.17}$$

p_i - ықтималдығын екі u және ξ кездейсоқ шамалар жүйесінің $f(u, \xi)$ – ықтималдықтар нығыздығын қолданып тапса болады:

$$p_i = \iint_S f(u,\xi)dud\xi \tag{3.18}$$

мұнда S — интегралдау аймағы.

U ды интегралдау шекаралары u_i және u_{i-1} болып, олар сигналдың лездік мәндерінің i - кванттау қадамына сәйкес келеді.

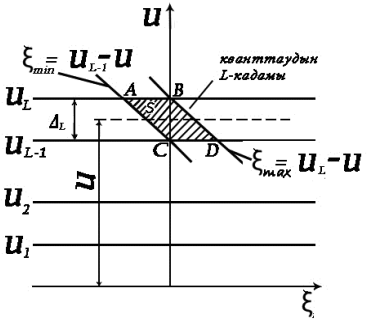
Ал ξ бойынша интегралдауда жоғары ξ_{max} және төменгі ξ_{min} шекаралары келесідей шарттардан табылады; сигнал және кедергінің алгебралық қосындысы i - кванттау қадамының шектерінен шықпауы керек:

$$u + \xi_{\max} = u_i, \ldots u + \xi_{\min} = u_{i-1} \tag{3.19}$$

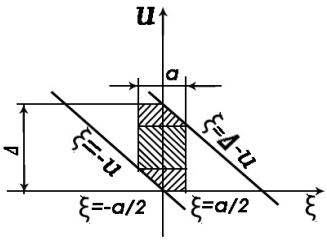
осыдан

$$\xi_{\max} = u_t - u, \ldots\ldots\ldots \xi_{\min} = u_{i-1} - u\,. \tag{3.20}$$

Сөйтіп, интегралдау шекаралары параллелограмм ABCD (3.4-сурет) түрінде болады:



3.4-сурет



3.5-сурет

Кедергі сигналмен байланысты болмағанда келесідей жазса болады:

$$p_i(i) = \frac{\int_{u_{i-1}}^{u_i} \int_{\xi_{\min}}^{\xi_{\max}} p(u)p(\xi)dud\xi}{\int_{u_{i-1}}^{u_i} p(u)du},$$

мұнда $p(\xi)$ — кедергінің таралу заңы.

Сигналдарды біркелкі кванттағанда оның лездік мәндері u_{min} дан u_{max} шейін біртегіс таралған болады: $p(u) = 1/(u_{\max} - u_{\min})$. (3.21)

$p_i(i)$-ді анықтауды алдын кедергі біркелкі заңды нығыздықпен таралған кедергі әсерінде қарастырамыз; $p(\xi) = 1/a$,

мұнда $a/2$ – кедергінің амплитудасы сигналдың лездік мәніне симметриялы болған жағдай. Осы шарттарда есептеу нәтижелері кванттау қадамына қарағанда инвариантты болады және a және $\Delta = \Delta_i$ қатыстарына байланысты болады; $\alpha<\Delta$ болғанда $p_i(i)$- ді табамыз.

Интегралдау аймағын (3.5-сурет) жеке бөлшектерге ажыратамыз және интегралдау шектерін қоямыз; мұнда (3.20) дің бөлімі мынаған $\Delta/(u_{max} - u_{min})$ тең болады. Сонда

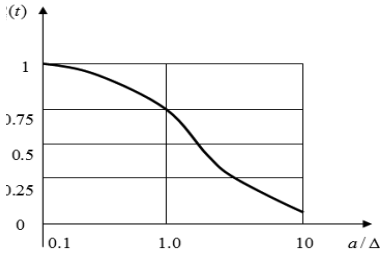
$$P_i(i) = \int_0^{\Delta} \frac{1}{\Delta} \int_{\xi_{\min}}^{\xi_{\max}} \frac{1}{a} d\xi du = \int_0^{a/2} \frac{1}{\Delta} \int_{-a}^{a/2} \frac{1}{a} d\xi du + \int_{a/2}^{\Delta-a/2} \frac{1}{\Delta} \int_{-a/2}^{a/2} \frac{1}{a} d\xi du + \int_{\Delta-a/2}^{\Delta} \frac{1}{\Delta} \int_{-a/2}^{\Delta-a} \frac{1}{a} d\xi du = 1 - \frac{a}{4\Delta}$$

(3.22)

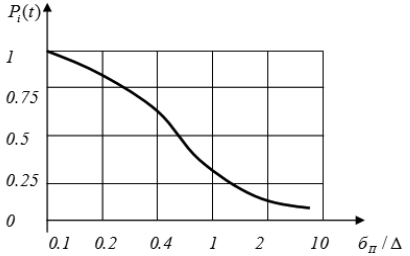
Дәл сондай жолмен интегралдау аймағын құрып, $\Delta<a<2\Delta$ және $a>2\Delta$ болғанда $p_i(i)$- ді табу мүмкін болады:

$$\begin{aligned} p_i(i) &= 1 - a/(4\Delta), .. \Delta < a \le 2\Delta; \\ p_i(i) &= \Delta / a, ... a \ge 2\Delta. \end{aligned} \quad . \qquad (3.23)$$

3.6-суретінде $p_i(i) = f(a/\Delta)$ графигі берілген болып, одан көрінетіні, Δ ның шамасын a дан кем алмау керек; себебі $a/\Delta>1$ болғанда, сигналдың дұрыс кванталмау ықтималдығы күрт артады.



3.6-сурет



3.7-сурет

Дәл осындай жолмен $p_i(i) = f(\sigma_n/\Delta)$ (3.7-сурет) байланыстылықты табамыз; мұнда сигналға қалыпты заңмен таралған кедергі әсер етеді:

$$p\ (\xi\ ) = \frac{1}{\sigma_{\ n}\sqrt{2}} e^{-\xi^2/(2\sigma_n^2)}, \qquad (3.24)$$

мұнда σ_n — ξ кедергінің ортаквадраттық ауытқуы.

Осы графиктерді талдай келе мынаны көрсе болады:

$a = 3\sigma_n$ болғанда, кванттау кедергісінің қалыпты таралу заңы мен біркелкі таралу заңындағы кедергілердің дұрыс кванттау ықтималдығы тұрғысынан қарағанда олар эквивалентті болады.

3.2 Дискреттеу; хабарды дискреттеу және қалпына келтіруде сапа шарттары.

Тіктеу анықтығы әдетте ақпаратты қолданушысы анықтайды. Қолдану мақсатына сай $u^*(t)$-нің $u(t)$-ге жуықтау анықтығының әртүрлі шарттары қолданылады. Біркелкі тіктеу шартында (ең үлкен шеттеу шарты деп те аталады) мүмкін болған қателіктің абсолют мәні орнатылады:

$$\delta_{\ Д}\ \geq\ \delta_{\ m}\ =\ \max_{t\ \in\ \Delta_{\ i}} \left|\delta_{\ u}\ (t)\right|, \qquad (3.25)$$

мұнда δ_m жуықтаудың максимал қателігі; Δ_i - аппроксимациялау бөлшегі; $\delta_u(t) = u(t) - u^*(t)$ - ағындағы жуықтау қателігі. Егер сигнал барлық мүмкін болған нақты мәндерімен берілген болса, онда мүмкін болаған ең үлкен қателік Δ_m барлық $u(t)$ және $u^*(t)$- лардың орындалуының жиыны үшін орнатылады:

$$\Delta_m = \sup\{|\delta_m|\}. \qquad (3.26)$$

Мұндай шарт берілген сигналдың кез келген ауытқуын сезу керек болса, әсіресе, егер ол ауытқу нысанның апатты тәртібіне сәйкес келетін болғанда қолданылады.

Сондай ақ ортаквадраттық жақындау шарты де кең қолданылады:

$$\delta_{Д} \geq \sigma = \sqrt{\frac{1}{\Delta_i}\int_{\Delta_i}\delta^2(t)dt}, \qquad (3.27)$$

мұнда $\delta_{Д}$ - жақындаудың мүмкін болған ортаквадраттық қателігі, σ - жақындаудың ортаквадраттық қателігі. Сигналдың көптеген мүмкін болаған нақты мәндерінде σ шамасы оның ықтималдықтарына қарай орташаланады. Техникалық орындалуында ортаквадраттық жақынадау шарты бойынша беркелкі емес дискреттеу біркелкі жақындау шартына қарағанда анағұрлым күрделірек болады. Интегралдық жақындау шарты келесідей қатыспен анықталады:

$$\varepsilon_{Д} \geq \varepsilon = \frac{1}{\Delta_i}\int_{\Delta_i}\delta_u(t)dt, \qquad (3.28)$$

мұнда $\varepsilon_{Д}$ - жақындаудың мүмкін болған орташа қателігі; ε - жақындаудың орташа қателігі. Амалда **ықтималды шарт** де кең қолданылады. Мұнда ағындағы жақындау қателігі $\delta(t)$ алдын ала берілген ықтималдықтың анық мәні δ_0 -ден аспау ықтималдығының мүмкін мәні $p_{Д}$ – беріледі:

$$P_{Д} \leq p\{\delta(t) \leq \delta_0\}. \qquad (3.29)$$

3.3 Таңдау құралы бойынша дискреттеу әдістері

Дискреттеу әдісін таңдауда санақтарды таңдау шартын анықтау, санақтар арқылы сигналды қалпына келтіру шарасын орнату және осындағы қателіктің шамасын анықтау мәселелері толық шешілуі керек.

Осылардың ішінде ең кең қолданылатын әдіс біркелкі дискреттеудегі қадамның үлкендігін табу болып, мұнда бірнеше әдістер бар.

Теориялық зерттеулерде ең көп тарағаны сигналдың үлгісін квазитұрақты кездейсоқ үдеріс түрінде қаралады; мұнда әрбір орындалуы шектелген спектрлі қатыс болады. Дискреттеу қадамының мәні спектрдің ең үлкен мәніне байланысты болады. Осындай *санақтарды табу шарты* **жиілікті** деп аталады. Дискреттеу қадамын таңдауда санақтардың корреляцияланбағандық дәрежесіне қарау мүмкін.

Мұнан басқа үлгіде сигнал үлгісі үшін T уақытымен шектелген кездейсоқ үдеріс алынып, жиіліктің оғы бойынша нөлден бастап барлық жиіліктерде оның спектрі нөлден ерекше деп есептеледі. Мұнда $\tau_0 << T$ деп, сигналдың анықталған корреляциялық теңдеуі бойынша табылатын τ_0 ***корреляция аралығы*** арқылы таңдаулар алынады. Осындай түрде таңдаулардың табылуы **корреляциялық** деп аталады. Алайда ол инженерлік амалда қолдану табпады.

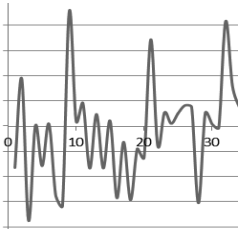
Мұнда артықшылық минимал болғанымен, сигналдың жоғары жиілікті гармоникалары есептелмейді; сондықтан сигнал өз қасиетін толық жоғалтады және қайта тіктелмейді [автор]. Ал Котельников теоремасында сигналдың корреляциялық теңдеуінің ең жоғарғы (ең жоғарғы гармоникасына тура келетін) мәні алынады; сондықтан сигнал толық қайта тіктеледі. Мұнда әрине артықшылық максимал дәрежеде болады [автор].

Біркелкі дискреттеуде сигналдың максималды гармоникаларына қарай дискреттеу қадамы таңдалады; ал сигналдың көптеген бөліктерінде сигнал жылдам өзгермейді және санақтар артықша болады [автор].

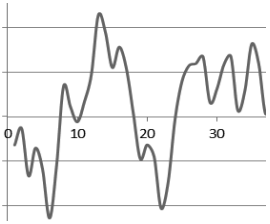
Осындайда бейімделуші біркелкі болмаған дискреттеу санақтардың артықшылығын жояды. Мұнда дискреттеу қадамы сигнал орындалуының ағындағы параметрлеріне байланысты өзгеріп отырады. Сигналды тіктеу қателігі жойылмайды; сондықтан оның максимал мәні негізгі шарт болады.

Мұнда сигналды тіктеу қателігі анық бір мәнге жеткенде ғана санақтар жүргізіледі.

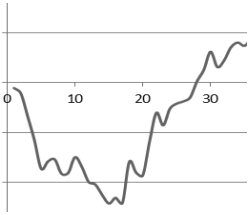
3.4 Бірқалыпты дискреттеу. Котельников теоремасы



3.8 а)-сурет



3.8 б)-сурет



3.8 в)-сурет

Біртүрлі қадаммен дискреттеуде ең кіші қадамды таңдап алу мәселесі анық түрде акад. Котельников теоремасында шешілген. Мұнда жиілікті шарт бойынша дискреттеу өткізіледі.

Котельников теоремасы: ***Детерминделген қатыстың спектрі шектелген болса, онда шекті бір аралықтармен алынған өзінің мәндері арқылы оны толық түрде тіктеу мүмкін болады.***

Теорема мына түрде көрінеді:

u*(*t*) *теңдеуінің Фурье түрлендіруі мүмкін болса және үздіксіз спектрге ие болып, оның жиілік жолағы келесідей* 0 *ден* $F_c = \omega_c/(2\pi)$ *аралығында шектелген болса, онда ол қатыс өзінің уақыт аралықтарында өлшенген

$$\Delta t = 1/(2F_c) \quad (3.30)$$ ***дискретті лездік мәндерімен толық анықталады.***

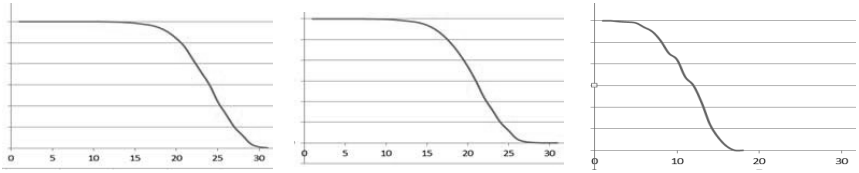
Теореманың физикалық мағынасын қатыстың түрі мен оның спектрінің ені арасындағы байланыстан түсінсе болады.

Тек қатыстың спектрі шексіз болғанда ғана біріне-бірі жақын нүктелер корреляцияланбаған болады; амалда бұл жағдай тек ақ шуылда ғана болады.

Жоғары жиілікті спектрдің бөлімі жоқ болуы және спектрдің ω_1 шектелуі одан жоғары гармоникалырдың жоқ екені және өткір қырлы бөлімдердің болмауын білдіреді (3.8, а-сурет).

Одан да кіші шекаралы жиілікте ω_2 (3.8, б-сурет) және ω_3 (3.8, в-сурет) одан да тегістелген уақыт теңдеуін аламыз.

Мұнда $\omega_{1>>}\omega_{2>>}\omega_3$.



Осы графиктерде жоғарыдағы аталған сигналдардың спектрлері көрсетілген болып, мұнда сигналдар тегістелген сайын олардың спектрі кішірейе беретіні көрінеді.

Осы қатыстардың $u(t_1)$ және $u(t_1+\Delta t)$ уақыт мезгілдерінде кейбір Δt аралығында өте жылдам үлкен өзгеріс болмайтыны және сол қатыстың мәндерінің аргументі Δt (санақтары) нан аспайтыны анық болады.

Дәлелдеу:

$u(t)$ теңдеуімен берілген сигнал болсын. Оның спектрі $S(j\omega)$ келесідей болсын:

$$S(jw) = 0\text{, мұнда } |w| > w_c \text{ ,} \tag{3.31}$$

мұнда ω_c - сигналдың ең жоғарғы спектрі болсын.

Ақырында келесідей теңдеуге келеміз:

$$u(t) = \sum_{n=-\infty}^{\infty} u(n\Delta t)\frac{\sin\omega_c(t - n\Delta t)}{\omega_c(t - n\Delta t)}. \tag{3.32}$$

$u(t)$ теңдеуі оның $t_n = n\Delta t = n\pi/\omega_c$ уақыт мезгілдерінде алынған дискретті мәндерімен берілген.

Сонда кез келген бүтін k және n үшін мына қатыстар орынды болады:

$$\omega_c(k\Delta t - n\Delta t) = (k - n)\omega_c\Delta t = (k - n)\pi,$$

$$\text{онда} \qquad \frac{\sin\omega_c(t - n\Delta t)}{\omega_c(t - n\Delta t)} = \begin{cases} 1, t = n\Delta t, \\ 0, t = k\Delta t, k \neq n \end{cases}. \tag{3.33}$$

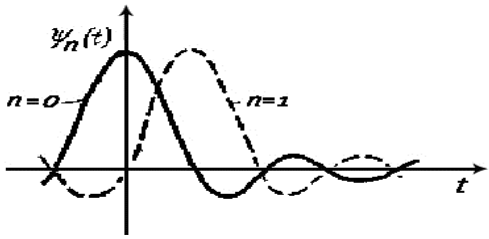
Ақырғы қасиеттен $u(k)$ теңдеуінің $tn = n\Delta t$ мезгілдеріндегі мәндері сол нүктелердегі оның ***санақталған (өлшенген) мәндерінің өзі*** болады.

$u(t)$ қатыстың (3.32) ***(Котельников қатары)*** түрінде көрінуі оның (2.1) жіктелуінің меншікті түрі екені көрінеді.

Осында C_k еселігінің *қызметін* $u(t)$ теңдеуінің $u(n\Delta t)$ санақтары орындайды. Ал **базистік функция** қызметін мынау атқарады:

$$\psi_n(t) = \frac{\sin\omega_c(t - n\Delta t)}{\omega_c(t - n\Delta t)} \text{ .} \tag{3.34}$$

Ол ***санақтар теңдеуі*** (функциясы) немесе ***Котельников теңдеуі*** деп аталады.



3.9-сурет

Осы қатыстың графиктері n = 0 және n = 1 де 3.9-суретте көрсетілген.

Әрбір $\psi_n(t)$ қатыс уақыт бойынша шектелмеген болып, өзінің ең үлкен мәні бірге тең болатын уақыт мезгілі $t = n\pi/\omega_c$; осы мезгілге салыстырғанда ол симметриялы болады.

Ал басқа уақыт мезгілдерінде $t=r\pi/\omega_c$ болады, мұнда $k \neq n$ қатыс нөлге айналады.

Барлық қатыстар (функциялар) шексіз уақыт аралығында ортогонал болады; бұл интегралды есептеумен оңай табылады:

$$\int_{-\infty}^{\infty} \frac{\sin\omega_c(t-n\Delta t)}{\omega_c(t-n\Delta t)} \frac{\sin\omega_c(t-k\Delta t)}{\omega_c(t-k\Delta t)} dt = \begin{cases} \pi/\omega_c, k \\ 0, k \neq n. \end{cases} \qquad (3.35)$$

Әрбір санақ теңдеуін F_c шекті жиілікпен шектелген төменгі жиіліктегі сүзгінің дельта-серпінге көрсеткен жауабы деп қарау керек; мұнда дельта–серпіндер $t_n = n\Delta t$ уақыт мезгілдерінде келеді және ауданы мынаған тең болады: $u(n\Delta t)$.

Котельников теоремасы ортаквадраттық мағынада үздіксіз болған және энергетикалқ спектрі шектелген ($S_n(\omega) = 0$ және $|\omega|>\omega_П = 2\pi F_П$) тұрақты кездейсоқ үдеріс үшін орынды болады. Амалдық сигналдың көпшілігі осындай болады [автор]. Мұндай үдеріс квазидетерминделген үдерістер қосындысы түрінде көрсетіліп, оның ортогонал детерминделген теңдеуінің қызметін санақтар теңдеуі орындайды; ал кездейсоқ еселіктер қызметін - таңдаулар мәні анықтайды:

$$U(t) = \sum_{n=-P}^{P} U(n\Delta t) \frac{\sin\omega_n(t-n\Delta t)}{\omega_n(t-n\Delta t)} = \sum_{n=0}^{N} U(n\Delta t) \frac{\sin\omega_n(t-n\Delta t)}{\omega_n(t-n\Delta t)}, \qquad (3.36)$$

мұнда $N=2P$, $\Delta t = \pi/\omega_n = 1/(2F_n)$.

Сөйтіп, кездейсоқ үдеріс толығымен кездейсоқ сандардың санақты жиынымен анықталады; мұндағы кездейсоқ сандар - үдерістің кеңістік өлшемдері болады.

***Зертханалық жұмыс* 3.2**

Берілген детерминделеген қатыс

$$u(t)=\begin{cases}2e^{-t}, t\ge 0,\\ 0, t\le 0\end{cases}$$

үшін Котельников теоремасымен дискреттеу қадамын анықтаңыз.

Шешімі:

Онда спектрдің амалдық ені (2.60) η = 0,95 пен (2 42) теңдеумен спектрлік сипатты табамыз:

$$S(j\omega)=2\int_0^{\infty}e^{-1}e^{-j\omega}dt=\frac{2}{1+j\omega},\quad \text{осыдан}\quad S(\omega)=2/\sqrt{1+\omega^2}\,.$$

(2.60) қатысты қолданып амалдық спектр енін табамыз:

$$\frac{1}{\pi}\int_0^{\omega_n}\frac{4}{1+\omega^2}d\omega=\frac{0.95}{\pi}\int_0^{\infty}\frac{4}{1+\omega^2}d\omega\,.$$

Келесідей болғандықтан, $\int_0^{\infty}\frac{1}{1+\omega^2}d\omega=arctg\ \omega\Big|_0^{\infty}=\frac{\pi}{2}$

мынаны табамыз: $arctg\omega_0=0{,}95\pi/2=1{,}49$.

Тангенстер кестесінен: $\omega_0=13{,}11/c$.

Сөйтіп, $\Delta t=\pi/\omega_{\pi}=0{,}24c$ болады.

3.5 Котельников теоремасының амалдық маңызы

Котельников теоремасының теориялық қолданылуында біз біршама математикалық абстракцияларға жол қоямыз; мысалы, қатыстың спектрі шектелген болуы үшін оның уақыт бойынша ұзындығы шексіз болуы керек және санақтар саны да шексіз болуы керек қой.

Ондай болса оның энергиясыда шексіз болуы керек емес пе?

Ал мұндай жағдай амалда мүмкін емес; амалда сигналдың спектрі де, оның қуаты да әрқашанда шектелген болады.

Сигнал жіберуші тарапта берілген үздіксіз сигнал $u(t)$ ның Δt

уақыт аралықтарындағы мәндері $u(n\Delta t)$ өлшеніп, байланыс арналарына A_n амплитудалы және τ шексіз кіші ұзындықтағы δ-серпіндер түрінде жіберіледі; олар $A_n\tau$ болып, ауданы $u(n\Delta t)$ тең болады.

Қабылдаушы жағында осындай серпіндер тізбегі төменгі жиіліктегі идеал сүзгіден өткізіледі; оның ең жоғары жиілігі F_c тең болады.

Осындай сигналды көп уақыт жіберілсе, онда сүзгінің шығуында $u(t)$ үздіксіз сигналы толық қайта тіктелген болар еді.

Алайда осы айтылғандардың техникалық орындалуы бірқатар қиыншылықтар туындайды.

Біріншіден, нақты сигнал шекті T ұзындыққа ие болады, сондықтан, оны жиілікті аймақта көрсеткенде оның спектрі шексіз болады. Алайда амалдық жағдайда нақты сигнал көзінің қуаты шектелгендіктен және нақты арнаның өткізу жолағының шектелгендігі себепті сигналдың **спектрін** қандайда бір анықтықпен алынған F_m - шекті ***жиілікпен шектелген*** десе болады. Әдетте ол энергетикалық шарт негізінде анықталады.

Мұнда сигнал спектрі жиіліктің 0 ден F_m-ге дейінгі аймақпен шектеледі; осы аймақта сигнал энергиясының (80—95%) жинақталады. Осындай шектеулер табиғи түрде сигналдың бұзылуына әкеледі. Сигнал тіктелуінің салыстырмалы анықтығы мына қатыспен анықталады:

$$\gamma = \frac{\int\limits_{\omega_c}^{\infty} S^2(\omega)}{\int\limits_{0}^{\infty} S^2(\omega)} = \frac{P_\varepsilon(\omega)}{P_c(\omega)}\ , \qquad (3.37)$$

мұнда P_ε сигналдың қырқып тасталған жоғары жиілікті бөлігінің энергиясы; Pc – сигналдың толық энергиясы.

Сондықтан, уақыт бойынша өте қысқа сигналдың Котельников теоремасы бойынша алынған санақтары бойынша қайта тіктелуі, сигнал ***спектрі шектелмегенде*** тек қана ***жорымалды*** болады.

Мұнда сигнал спектрінің шектелуі T уақыт аралығындағы санақтар көлемінің шектелуіне әкеледі; ал Котельников теоремасында санақтар саны $2F_cT$. Сондықтан кейбір авторлардың спектр шектелмегенде қателік себебі екі түрлі болады: біріншісі - спектрдің шектелуінен, ал екіншісі - санақтар санының кемеюінен дегені дұрыс болмайды; себебі спектрдің шектелуі санақтар санының кемеиуіне

әкеледі; қиылған жоғары гармоникалар санақтан тыс қалады [автор].

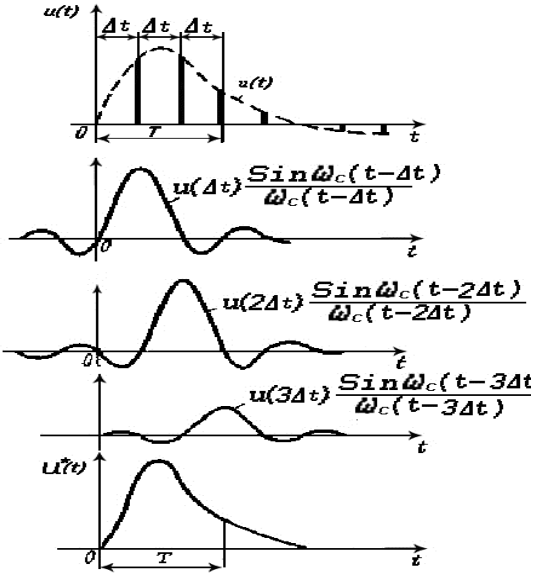
Сонымен өте қысқа сигналдардың (мысалы, шуылды сигналдар-шумоподобные сигналы) жоғарғы жиілігін өлшеу қиын немесе анық болмайды; сондықтан олардың жоғарғы жиіліктерін қиып тастап, негізгі жиіліктері алынады. Мұнда алынған гармоникалар қосындысы сигналдың жалпы қуатының 0,9 нан, яғни 90 пайызынан кем болмауы керек. Яғни Котельников теоремасын тек шуылды сигналдарды дискреттегенде ғана жуықтап қолданылады. Басқа амалда қолданылатын үздіксіз тар жолақты сигналдардың барлығында ***Теорманы*** толық түрде қатесіз қолданса болады.

Осы орайда айта кететін жай, дискретті сигналдың келбетін тиімді түрде таңдап алумен оның спектрін кемейтіп, арнаның өткізу жолағына сәйкестендірумен сигналдың арнамен өткенде бұзылу жағдайын мүлде жою мүмкін. Бұл Котельников теоремасының амалда қолданылуына мысал болады [80, автор].

Осы жерде айта кететін жай, егер дискретті сигналдың келбеті жарты синусойда немесе қиылған қоңырау (90 градусқа жылжыған толық синусойда) түрінде алынатын болса, онда сигнал спектрі максимал дәрежеде қысқарады [80]; яғни сигналдың түрін тиімді таңдап алумен оның спектрін қысқарту мүмкін болады.

Бұл әсіресе тар жолақты (төменгі жылдамдықты) арналармен сигналдарды жіберудегі негізгі мәселелердің бірі болып, сигнал келбетін таңдаумен сигналды арнамен келістіру мүмкін болады. Мұнда сигналдың қуатын максимал дәрежеде көбейту және оның спектрін минималдау мүмкіншілігі туылады.

Бұл мәселені шешуге арналған автордың және басқа ғалымдардың еңбектерін атаса болады [80,81].



3.10- сурет

Потенциал кедергіге шыдамдылық теориясы.

Акад. Котельников В. А. 1933 ж. "***О пропускной способности эфира, проволоки и радиосвязи"***, 1956 ж. ***"Теория потенциальной помехоустойчивости***" кітаптарында бұл теорияны толық негіздеді.

1-**Теорема: Спектрі** f_m **жиілігімен шектелген функция өзінің** $F_0 = 2f_m$ **жиілігімен алынған дискретті мәндерімен толық анықталады; мұнда** f_m **- берілген** x_i **сигналының** $S(j\omega)$ **спектріндегі максимал жиілігі (Найквист теоремасы).** Теореманы басқаша айтқанда былай болады:

2-Теорема. Егерде уақыт бойынша үздіксіз x_i **сигналы өзінің Фурье бойынша** $S(j\omega)$ **спектрімен беріліп және ол спектр W жиілікпен шектелген болса, онда бұл функция өзінің** $\Delta t = \frac{1}{2W}$ **уақыт аралықтарында алынған дискретті мәндерімен толық анықталады. (Санақтар немесе Котельников теоремасы).**

Бақылау аралығы Т және санақтар саны (өлшемдер көлемі)

$$n = \frac{T}{\Delta t} = 2WT$$ **болады.**

Бұл теорема **санақтар теоремасы** деп аталып, осы кездегі барлық аудио-бейне сандық ақпарат байланыс жүйелерінің **негізін** қалады.

Котельниковтің санақтар функциясы мына түрде болады:

$$\varphi(t)=\frac{Sin\,\omega_m(t-k\Delta t)}{\omega_m(t-k\Delta t)}=\frac{Sin\,\omega_m\tau}{\omega_m\tau}.$$

Бұл функция дискретті серпінді түрдегі сигналдарды үздіксіз түрге қайта келтіруде қолданылады; яғни санды-үздіксіз түрлендірушілерде интерполяциялау үшін қолданылады.

Ал түрлендіру операциясы толығымен мына түрде жазылады:

$$x(t)=\sum_{k=\infty}^{\infty}x(k\Delta t)\frac{Sin\,\omega_m(t-k\Delta t)}{\omega_m(t-k\Delta t)}, \qquad (3.38)$$

мұнда уақыт аралықтары $\Delta t=\frac{1}{2F_m}=\frac{\pi}{\omega_m}$ болады.

(3.38) өрнек ***Котельников қатары*** деп те аталады.

Қасиеттері:

1) $t=k\Delta t$ ***мезгілінде*** $\varphi(t)_{\max}=1$ ***болады, яғни тек сол мезгіліндерде ғана сигналдың қуыты максимал дәрежеде болады;***

2) $t=(k\pm z)\Delta t, z=1,2,3,...,$ ***болғанда,*** $\varphi(t)=0$ ***болады. Яғни, аргументтің аралық міндерінде қатыстың мәндері*** **0** ***ге тең болады.***

3) Мұндай селектив жүйенің шығуында ең қысқа серпін ұзындығы $\frac{1}{W}=\frac{1}{F_m}$ ***болады.***

4) Санақтар функциясы шексіз үлкен уақыт аралықта **(1** ***ге тең ауырлықпен) ортогонал болады.***

(3.38) теңдеу $x(t)$ сигналды ***қайта тіктеу*** **(*интерполяциялау*)** ***теңдеуі*** деп аталады. Осы теңдеу идеал сүзгінің шығуындағы сигнал түрі болады.

Сүзгі *П* типіндегі жоғары жиілігі ω_m болған δ серпін беріледі.

Нақты сигналдардың ұзындығы шектелген, ал спектрі - теорияда шексіз болғанымен, амалда шексіз болмайды. Амалдық сигналдардың көпшілігінің спектрі шектелген болады. Шуылды сигналдардың да спектрі шексіз деп болмайды.

Мысал үшін, телефон арналарында сигнал спектрі шектелген (4

кГц) болып, сигнал үздіксіз болғандығы үшін оның ұзындығы шектелмеген десек болады. Алайда кейбір ән-күйлік дыбыстар жиілігі 4 кГц тен анағұрлым асып кетеді (скрипка дыбысы 10 кГцтен де асады). Мұндайда шектеулер қойылады.

Нақты сигналдардың спектрі арнаның өткізу жолағынан үлкен болған жағдайда Котельников теоремасын істеткенде мәлім дәрежеде қателік болып, ол қателік инженер есебінің шартына жауап беруі керек болады.

Мұнда максимал жиілік амалда сигнал спектрін қысқарту жолымен табылады; сонда алынған сигнал спектрінің қуаты толық сигналдың қуатының 0,9 нан, яғни 90 пайызынан кем болмауы керек.

Сонда жіктеудегі қосылғыштар саны да шектеліп, қалған сигналмен өлшенеді; себебі спектр шектелген соң соған сәйкес санақтар да қысқарады. Демек, спектрдің қысқаруы санақтар санының да қысқаруына әкеледі. Ал Котельников теоремасында максималды жиілік шектелгендігінен, сигналдың толық спектрін санақты гармоникалармен толық көрсетсе болады; мұнда еш қандай қателік болмайды.

Қателік жоғарғы жиілікті анық өлшеп болмағандығы себепті тек шексіз немесе иррационал спектрлі немесе өте кең жолақты (шумоподобные сигналы) сигналдарда ғана болады.

Алайда амалдық жүйелердің барлығында үздіксіз сигналдың жоғары спектрі шектелген немесе спектрі рационал болады. Сондықтан, амалда көп сигналдарға да Котельников теоремасын қолдану мүмкін. Бірақ кең жолақты сигналдарға бұл теореманы қолдану нәтижелі болмайды. Себебі мұндай сигналдың жоғарғы жиілігін анық өлшеп болмайды.

Сонымен, сигнал ***спектрі шексіз*** болғанда немесе өте жоғары болып, ***арнаның өткізу жолағы одан кем*** болғанда Котельников теоремасы жуықталған түрде істетіледі [80, автор].

Кейбір авторлар "...амалда жиілікті шарттан гөрі корреляциялық шарт кең қолданылады; мұнда дискреттеу қадамы ең жақын корреляциясыз нүктелер деп қаралады...,"- деген. Бұл пікір дұрыс емес.

Алайда мұндай корреляциясыз нүктелерден өлшемдер алынғанда сигнал кездейсоқ сандар тізбегіне айналып, өзінің барлық қасиеттерін (корреляциялық және т.б.) жоғалтады және қайта тіктелмейді [80, автор].

Котельников теоремасының салдары.

1) ***x*(*t*) *үздіксіз хабарлар берілген болса, жиіліктер жолағы шектелген болса, онда осы сигналды байланыс арнасымен сандық түрде бұзбастан жіберу мүмкін; Мұның үшін***

$\Delta t = t_k = \frac{k}{2W}, k = 1,2,3\ldots$ ***нүктелерінде сигналдың*** $x(t_k)$ ***өлшемдері*** $x\left(\frac{1}{2W}\right), x\left(\frac{1}{2W}\right), \cdots$ ***табылған болып, олар екілік байтпен кодталады және екілік сигналдар) түрінде арнамен жіберіледі.***

Арнаның шығуында амплитудасы сол сандарға тең болған дельта-серпіндер генерацияланады; $s_1(t), s_2(t), \ldots$.

Бұл сигналдар Котельниковтың қатыстарына коньюнктивті көбейтіліп, сумматорда қосылғаннан кейін бастапқы сигнал қалпына келтіріледі.

2.а) ***Егер*** $x(t)$ ***сигнал берілген болса,*** $\int_{-\infty}^{\infty} x^2(t)dt$ ***сигналдың квадраттық нәтижесі деп аталады; оның мөлшері энергияның мөлшеріне тең болады:***

$$\int_{-\infty}^{\infty} x^2(t)dt = \frac{1}{2F_m} \sum_{k=1}^{2F_m T} x^2\left(\frac{k}{2F_m}\right). \quad (3.39)$$

Бұл телекодтық сигналдарды құруда олардың қуатын өлшеу үшін өте қолайлы болады.

2.б) ***Егер f(t) функция F спектрімен шектелген және уақыт бойынша да T мен шектелген болса, онда ол функция*** $m = 2kFT = \frac{T}{\Delta t} = 2n$ ***нүктелерімен толық анықталады;***

А) $\Delta t = t_k = \frac{k}{2W}, k = 1,2,3\ldots$ ***аралықтарындағы нүктелерде функция дискрет нүктелерімен толық анықталады;***

Б) Фурье қатарының A_k ***спектрлік еселіктерімен толық анықталады. Жоғарғы екі жағдайда да ол нүктелер саны m = 2n болады.***

Зертханалық жұмыстарға есептер:

1-*есеп.* Адамның құлағы 20 кГц тен кем жиіліктерді қабылдай алады. Сонда дыбысты қандай жиіліктерде дискреттеп, CD-R ге жазу керек болады?

Шешімі: Найквист теңдеуін қолдана отырып, табатынымыз дискреттеу жиіліктері есіту жиілігінен екі есе ден көп немесе тең болуы керек, яғни 40 кГц -тен көп немесе тең болуы керек.

Үздіксіз-сандық (Analog-Digital Converter-ADC) немесе (Digital to Analog Converter-DAC) түрлендірушісінің жиілігі 40 кГц болуы керек.

3.3 ***Зертханалық жұмыс*** МР-2 плейерде дискреттеу жиілігі 48 кГц; Сонда оған жазылатын дыбыстың максималды жиілігі қандай?

Шешімі: Найквист теңдеуін қолдансақ:

$$f_{\max} \le f_{diskret} / 2 = 48 / 2 = 24 \text{ кГц.}$$

3.4 ***Зертханалық жұмыс*** Кадрда N=600*625=375000 пикселдер бар. Информация көлемін табу керек.

Шешімі: $I(X) = \log 8^N = \log 2^{3\times N} = 3 \times Nbit$

3.5 ***Зертханалық жұмыс*** Ән-күйлі дыбыс спектрі

$\Delta F = 16 \div 28$ *кгц* болса, үздіксіз-сандық түрлендіргіштің (АЦТ) генераторының жиілігі қандай болуы керек?

Шешімі: Найквист теоремасы бойынша дискреттеу жиілігі сигнал спектрінің жоғарғы жиілігінен екі есе көп болуы керек, яғни:

$$f_d = 2 f_{\max} = 56\,кГц \quad \text{болады.}$$

3.6 Ең үлкен ауытқу бойынша дискреттеу

Дискреттеу үдерісінде үздіксіз $u(t)$ қатыстың $(n+1)$ шектелген туындысы болса, ол n- орынды көпмүшелікпен аппроксимацияланады.

Қайта тіктеу әдісіне қарай ол интерполяциялық немесе экстраполяциялық болуы мүмкін.

Сигналды тіктеуде минимал қателіктің табылу мәселесі қойылмайды. Әдетте оның мүмкін болған немесе рұқсат етілген мәні ε_0 көрсетіледі. $u(t)$ қатыстың $u^*(t)$ көпмүшелігімен тіктеу қателігі $\delta_u(t)$ аппроксимацияның әрбір қадамында $L_n(t)$ қалдықты мүшемен анықталады:

$$\delta_u(t) = L_n(t) = u(t) - u^*(t). \qquad (3.40)$$

Сондықтан, дискреттеу қадамы мына $Ln(t) \le \varepsilon_0$ шарттан таңдалуы керек. Кемірек рұқсат етілген ε_0 қателікте аппроксимациялау үшін жоғарырақ орынды полиномды таңдап алу санақтар санын кемейткенімен, әдістің техникалық орындалуының күрделілігі күрт жоғарылайды.

Сондықтан әдетте көпмүшеліктің нөлінші, бірінші, екінші дәрежелерімен шектеледі (тікбұрышты, сызықты және параболалық аппроксимациялар).

Интерполяциялау үшін көбінесе Лагранж көпмүшелігі, ал экстраполяция- лау үшін - Тейлор көпмүшелігі қолданылады.

3.7.а Лагранждың интерполяциялық көпмүшелігімен дискреттеу.

Біртегіс дискреттеуде интерполяциялаушы Лагранж көпмүшелігі мына түрде жазылуы мүмкін:

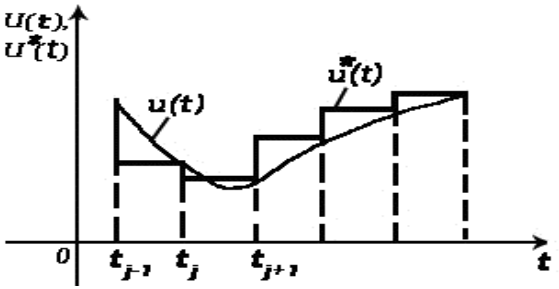
$$u_n^{\bullet}(t) = (-1)^n \frac{\lambda(\lambda-1)...(\lambda-n)}{n!} \sum_{j=0}^{n} (-1)^j \frac{C_n^j u(t_j)}{\lambda - j}, \qquad (3.41)$$

мұнда $\lambda = (t - t_0)/\Delta, .. \Delta = t_j - t_{j-1}, .. j = 0, ... n$

Қалдықты мүшенің $L_n(t)$ мәні:

$$L_n(t) \le \frac{M_{n+1}}{(n+1)!} \prod_{k=0}^{n} (t - t_k), \qquad (3.42)$$

мұнда M_{n+1} — $u(t)$ сигналының $(n+1)$ - туындысының барлық түрлендіру аралығындағы максимал модулі.



3.11-сурет

3.6 ***Зертханалық жұмыс***

Нөлінші орынды Лагранждың интерполяциялық көпмүшелігі негізінде біртегіс дискреттеу қадамын табу керек.

Шешімі: 3.11-суретте көрсетілгендей $u^*(t)$ тіктеуші қатыстың мәні $t_{j-1} \le t \le t_j$ дің әрбір j-аралығының кез келген t уақыт мезгілінде $u(t_j)$ санағына тең етіп алынады. (3.42) қатысы қалдықты мүше үшін мына өрнекті табуға мүмкіндік береді:

$$L_0(t) \le M_1 |t - t_0| \tag{3.43}$$

Оның максимал мәні дискреттеу қадамына пропорционал болады.

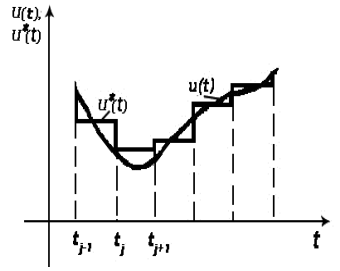
Ол ε_0 ден аспауы керек. Осыдан дискреттеу қадамын анықтайтын шарт:

$$\Delta \le \varepsilon_0 / M_1 \tag{3.44}$$

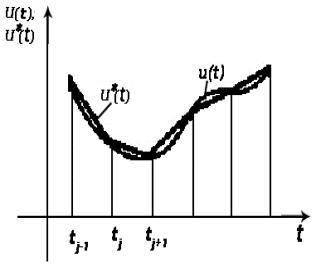
Егер $u(t)$ сигналын тіктеуді екі нүкте арқылы жүргізетін болсақ, мына қатыстарды қолданамыз (3.12-сурет):

$$u^*(t) = \left[u(t_j) + u(t_{j-1})\right]/2, t \in \left[t_{j-1}, t_j\right]. \tag{3.45}$$

Онда дискреттеудің осындай қадамында да тіктеу қателігі екі рет кемейеді.



3.12-сурет



3.13-сурет

3.7. Зертханалық жұмыс

Бірінші орынды Лагранждың интерполяциялық көпмүшелігімен біркелкі дискреттеу қателігін табу керек.

Шешімі: Берілген сигнал $u(t)$ ны әрбір уақыт $[t_{j-1}, t_j]$ аралығында екі $u(t_j)$ және $u(t_{j-1})$ санақ өлшемдері істетіледі.

Олар түзу сызықпен (3.13-сурет) біріктіріледі. Қалдықты мүшенің $L^n_{1\max}$ максимал мәнін табуда оның туындысын нөлге теңейміз:

$$L^{n}_{1\max} = \frac{M_2}{2}\left|\frac{(t_1 - t_0)(t_0 - t_1)}{4} = \frac{M_2\Delta^2}{8},\right| \quad (3.46)$$

осыдан рұқсат етілген дискреттеу қадамы:

$$\Delta \le 2\sqrt{2\varepsilon_0 / M_2}\ . \quad (3.47)$$

3.7 б. Тейлордың экстраполяциялық көпмүшелігімен дискреттеу

Тейлордың экстраполяциялық көпмүшелігі келесідей өрнекпен көрсетіледі:

$$u*(t) = u(t_0) + \frac{u'(t_0)(t - t_0)}{1!} + \ldots + \frac{u^n(t_0)(t - t_0)^n}{n!}, \quad (3.48)$$

мұнда $u^n(t_0)$ — U(t) сигналының t_0 уақыт мезгіліндегі n -нші орынды туындысы. Қалдықты мүше үшін төменгі баға келесідей болады:

$$L^{T}_{n}(t) \le \frac{\bar{M}_{n+1}}{n+1}\left|t - t_{j-1}\right|^{n+1} \quad t \in \left[t_{j-1}, t_j\right]. \quad (3.49)$$

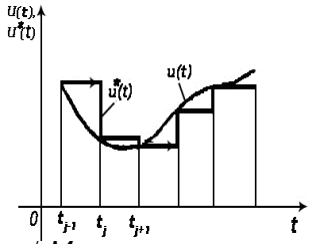
3.8 ***Зертханалық жұмыс***

Нөлінші орынды Тейлор көпмүшелігімен біркелкі дискреттеу қадамын табу керек.

Шешімі: Тіктеуші *u*(t)* қатыстың кез келген *t* уақыт мезгілінде және әрбір *j* - аралығындағы $t_{j-1} \le t \le t_j$ мәндерін мынаған $u(t_{j-1})$ тең деп аламыз (3.14-сурет). Қалдықты мүшенің мәні $L^{T}_{0\max}$ аралығының ақырында (мына мәнде $t = t_j$) максимумға ие болады:

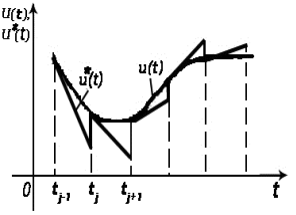
$$L^{T}_{0\max} \le M_1\left|t_j - t_{j-l}\right|. \quad (3.50)$$

Сондықтан дискреттеу қадамы мына шартқа жауап беруі керек:



$\Delta \le \varepsilon_0 / M_1$.

3.14-*с*урет



3.15-сурет

3.9 ***Зертханалық жұмыс***

Бірінші орынды Тейлор көпмүшелігі жәрдемінде біркелкі дискреттеу қадамын табыңыз.

Шешімі*:* $u(t)$ сигналын тіктеуде $u(t_0)$ санағынан басқа соның t_0 уақыт мезгіліндегі $u'(t$о) бірінші орынды туындысы қолданылады.

Қалдықты мүшенің мәнінің максимумына

$$L_{1\max}^{T} \le \left(M_2 / 2\right)\left|t - t_{i-1}\right|^2 \qquad (3.51)$$

$t = t_j$ -де жетеді. Соған сәйкес дискреттеу қадамын табу өрнегін аламыз:

$$\Delta \le \sqrt{2\varepsilon_0 / M_2}\ . \qquad (3.52)$$

Мұнда сигналдың тіктелуі уақыт бойынша іркілусіз өткізіледі (3.15-сурет). Алайда интерполяциялық әдіспен салыстырғанда бұған екі есе көп санақтар қажет болады.

3.8 Бейімделуші дискреттеу

Алдын көрілген дискреттеу әдістері сигналдардың барлық мүмкін болған нақты мәндері жиынына негізделген болып, оның динамикалық сипаттамаларының шекті мәндеріне сүйенген едік; ал бейімделуші дискреттеуде біз сигналдың айқын орындалуына негізделіп, тиісті анықтықпен сигналды тіктеуде минималды таңдаулар санына сүйенеміз.

Бейімделуші дискреттеудің негізінде сигналды тіктеудің ағындық қателігін ε үздіксіз зерттеу жатады.

Мұнда дискреттеу бағдаржолдарының ішінде ең кең тарағаны – аппроксимациялау ***аралығының ұзындығы*** бойынша ***бейімдеу.***

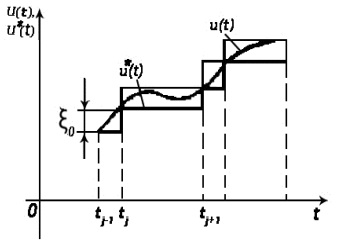
Мұнда аппроксимация аралығы үздіксіз түрде ұзартып отырылады және $u(t)$ сигналы оны тіктеуші қатыс $u^*(t)$-мен салыстырылып отырылады; мұнда ***тіктеуші қатыс*** сигналдың ***ағындық динамикалық сипаттамаларын есептеумен*** табылады.

Тіктеу қателігі берілген мәнге ε_0 жеткенде аралықты ұзарту тоқтатылады да, санақ жүргізіледі. Мұнда санақтар арасындағы аралықтар (интервалдар) кез келген түрде болады. Тіктеуші қатыс түрінде көбінесе бірінші және екінші орынды ***алгебралық полиномдар*** қолданылады. Мұнда бейімделуші дискреттеудің ***интерполяциялық*** және ***экстраполяциялық әдістері*** қолданылуы мүмкін.

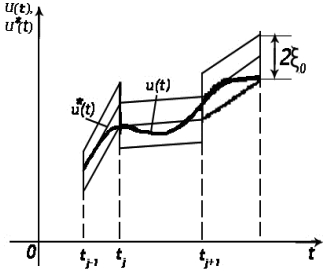
Осы кезде интерполяциялық әдістер көп қолдану таппады. Оның себебі аппроксимациялау аралығында сигналдың көптеген нүктелерін есте сақтап, үлкен есептеу амалдарын орындауға әкеледі. Сондықтан экстраполяция негізінде аппроксимациялауды қарастырамыз.

3.10 *Зертханалық жұмыс*

$u(t)$ сигналының бейімделуші дискреттеудің орындалуын нөлінші орынды аппроксимациялаушы көпмүшелік жәрдемінде жүргізу керек.



3.16-сурет



3.17-сурет

Әрбір аппроксимациялаушы аралықтың басында t_j мезгілінде $u^*(t)$ полиномы $u(t_j)$ мәнін алады және мына айырма есептеледі $\Delta u(t)=u(t) - u^*(t_j)$; ол ε_0 мен салыстырылады. Мына теңдеудің $|\Delta u(t)| = \varepsilon_0$ орындалуы аралықтың ақырындағы t_{j+1} мезгіліне сәйкес келеді және келесі санақтың басталуын көрсетеді.

3.11 ***Зертханалық жұмыс***

$u(t)$ сигналының бейімделуші дискреттеудің орындалуын бірінші орынды аппроксимациялаушы көпмүшелік жәрдемінде жүргізу керек. Мұнда ең үлкен рұқсат етілген ауытқу ε_0 болсын.

Шешімі: Әрбір аппроксимациялаушы аралықтың басында t_j мезгілінде:

$$u^*(t) = u(t_j) + u'(t_j) \times t,$$

мұнда $u'(t_j)$ — $u(t)$ сигналының t_j мезгіліндегі туындысы.

Кейінгі санақ мезгілі мына теңдеудің орындалуымен табылады:

$$\Delta u(t) = u(t) - u(t_j) - u'(t_j) \times t = \varepsilon_0 .$$

Дискреттеу нәтижесі 3.16, 3.17-суреттерде көрсетілген.

Бұл бағдаржолды қолданғанда дифференциалдау операциясы орындалғандығы себепті жоғары жиілікті кедергілер болғанда қолдану нәтижелі емес.

3.9 Сигналдардың көрсетілуінің геометриялық келбеті

Жалпыланған сигналдар теориясына сәйкес ортоқалыптыланған қатыстар жиыны $\psi_k (1 \le k \le N)$ таңдалған болса, шектелген уақыт T аралығында $u(t)$ сигналы өлшемсіз еселіктер жиыны C_1, ..., C_k, ..., C_N мен толық анықталады. Бұл еселіктер N өлшемді геометриялық кеңістіктегі нүктенің кеңістік өлшемдері болып, ол кеңістіктің оқтары озара перпендикуляр және ψ_1, ..., ψ_k, ..., ψ_N таңбаланған. Мұндай көпөлшемді кеңістік ***сигналдар кеңістігі*** деп аталады. Егер C_1, ..., C_k, ..., C_N жиындағы әрбір санды оған сәйкес оқтың орт-на (векторлық бірлік) көбейтсек, онда $u(t)$ сигнал векторының кеңістік өлшемдерін N - өлшемді ***векторлық эвклидтік кеңістігін*** аламыз.

Мұнда бірлік сигнал немесе (норма $||u||$) вектордың 1 ұзындығы деп бірлік сигнал ұшынан кеңістік өлшемдері басына дейінгі қашықтықты білдіріп, ол былай табылады:

$$\|u\| = l = \sqrt{\sum_{k=1}^{N} c_k^2} . \qquad (3.53)$$

Мына C_1, ..., C_k, ..., C_N және C'_1, ..., C'_k, ..., C'_N кеңістік

өлшемдерімен берілген екі нүктенің арасындағы d қашықтық келесідей табылады:

$$d = \sqrt{\sum_{k=1}^{N} \left(c_k - c'_k\right)^2} . \qquad (3.54)$$

F_c – шекті спектрлі үздіксіз сигнал $u_c(t)$ уақыт Tc аралығында берілген болып, оның кеңістік өлшемдері ретінде Котельников теоремасы негізінде табылған $N = 2FcT_c$ санақтар жиыны қолданылады.

Алайда кеңістіктің өлшемдер саны өте үлкен болады.

Егер сигнал өлшемі кернеу (немесе ток) болса, онда вектордың ұзындығының квадраты сигналдың салыстырмалы энергиясын көрсетеді (1 Ом кедергілі резисторда ажыралатын).

Сигнал қуатын келесідей табамыз:

$$W \approx \frac{1}{2F_c} \sum_{k=1}^{N} u_c^2 (k\Delta t)$$

немесе: $\sum_{k=1}^{N} u_c^2 (k\Delta t) = 2F_c T_c P_c = NP_c$, (3.55)

мұнда P_c — сигналдың орташа қуаты.

$u_c(k\Delta t)$ - сигнал кеңістік өлшемдері деп қабылданғандығы үшін осы өрнектің сол жағы сигнал векторының квадратына тең болып, мынаны аламыз:

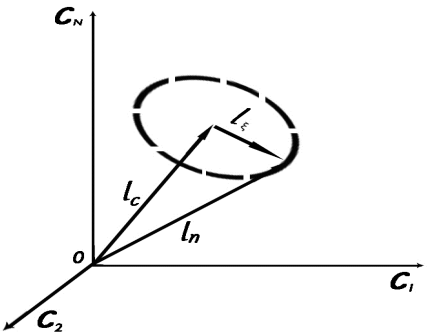
$$l_c = \sqrt{\sum_{k=1}^{N} u_c^2 (k\Delta t)} = \sqrt{2F_c T_c P_c} . \qquad (3.56)$$

Егерде сигналға спектрі шектелген ақ кедергі аддитивті түрде әсер етсе, онда сигнал векторы қандай өзгереді?

Кедергі кездейсоқ вектор болып, оның кеңістік өлшемдері кездейсоқ сандар болады.

Оның кеңістікте анық күйі берілген болмаса, алайда оның кеңістік өлшемдерінің таралу заңы берілген болса, онда кедергі векторының ұшының берілген кеңістік көлеміне түсу ықтималдығын анықтаса болады.

Егер кедергінің ұзындығы мен спектрінің ені Tс және Fс болса, онда оны N - өлшемді сигналдар кеңістігінде көрсетсе болады.



3.18 - сурет

Амалда кедергі нөлдік орта мәнді қалыпты заңмен таралған түрде болады.

Осы заң барлық санақтар нүктесіне де бірдей болады.

Онда кедергі векторының барлық бағыты тең ықтималды болады.

Осындай жағдайда кедергі векторының ұшының орналасатын ең ықтималды аймағы N - өлшемді өрісітк (сфера) болып, оның радиусы келесідей болады:

$$l_\xi = \sqrt{2 T_c F_c P_\xi},$$

мұнда P_ξ — кедергінің T_c уақытындағы орташа қуаты.

Егер сигнал мен кедергі корреляцияланбаған болса, онда кедергі векторы сигнал векторына көбінесе перпендикуляр болады. 3.18- суретте айтылған векторлар үш өлшемді кеңістікте көрсетілген.

Мұнда нәтижелі вектордың ұшы сигнал векторына перпендикуляр болған шеңбердің бір нүктесінде болады.

Нәтижелі вектордың ұзындығы келесідей болады:

$$l_ï = \sqrt{2F_cT_c\left(P_c + P_\xi\right)}. \qquad (3.57)$$

Сонымен, кедергі әсерінен нәтижелі вектордың күйі анық болмай қалады. Себебі кедергінің таралуы шектелмеген болады. Сондықтан оның ұшы кез келген жерде болуы мүмкін. Егер жіберуде сигналдардың орташа қуаты анықталған болса, онда жіберілетін

сигналдар (код) векторының жиынын таңдау кедергі сипаты мен қойылатын шындыққа байланысты болады.

Сигналдар кеңістігінде әрбір берілген векторға өзіне меншікті кеңістік аймағы таңбаланған болып, осы вектордың ұшының сол аймақтың сыртына шығып кету ықтималдығы берілген деңгейден кем болады.

Дискретті-үздіксіз сигналдардың евклидтік кеңістікте геометриялық көрсетілуі сияқты үздіксіз $u(t)$ сигналдары да гильберттік кеңістікте көрсетіледі.

Оның шексіз көп өлшемдері болады және [0,T] аралығында берілген барлық үздіксіз уақыт қатыстарын көрсетуі мүмкін болады.

Осы кеңістіктегі бірлік вектор (норма) келесідей табылады:

$$l_n = \sqrt{2F_cT_c\left(P_c + P_\xi\right)}. \qquad (3.58)$$

Екі векторлар $u(t)$ және $\upsilon(t)$ арасындағы қашықтық келесідей болады:

$$d_r(u, v) = \sqrt{\frac{1}{T}\int_0^T [u(t) - v(t)]^2\, dt}\ . \qquad (3.59)$$

Кедергілер, бұрынғыдай, векторлармен көрсетіледі.

Дискреттеу және кванттау жолымен алынатын дискрет сигналдарды геометриялық көрсету үшін дискреттік сызықтық векторық кеңістіктер қолданылады.

Кеңістік өлшемдері санақтар санына сәйкес келеді. Сигнал координаттары шекті мәнге ие болып, квант мәніне Δ ретті болады.

Сондықтан сигнал векторларының ұштары дұрыс нүктелі тордың ұштарында болады.

Осындай тордың жеке жағдайы N - өлшемді бірлік куб болып, Хэмминг кеңістігінде екілік кодтың қисындастыруылар жиынын көрсетеді.

Байланыс арнасы арқылы сигнал өткенде олар әртүрлі түрленуге түседі (дискреттеу, модуляциялау және т.б.).

Сондықтан сигналдың әртүрлі кеңістіктердегі көрінісі қолданылады (хабарлар кеңістігі, жіберілетін сигналдар кеңістігі, модуляцияланған сигналдар кеңістігі, қабылданатын сигналдар кеңістігі).

Мұнда сигналдардың түрленуін бір вектор кеңістігінің басқа бір вектор кеңістігімен бейнеленуі деп қарау керек.

Ақпараттар теориясында сигналдардың геометриялық кескінделуі маңызды қызмет атқарады. Ол жіберілетін сигналға кедергінің әсер ету үдерісін көрнекі түрде бейнелеу мүмкіншілігін береді; осындай әсердің нәтижесін жоюдың жолдарын талдау мүмкіндігін, сигнал мен арнаның негізгі параметрлерінің арасындағы орнықты қатыстарды зерттеу мүмкіндігін береді.

III тараудың бақылау және емтихан сұрақтары:

1. Дискреттеу мен кванттау үдерістерінің мағынасы неде?
2. Дискретті және сандық ақпаратты ұзатудың абзалдығын сипаттаңдар.
3. Дискреттеу мәселесінің жалпы қойылуын қалыптастыру керек.
4. Сигнал кеңістік өлшемдерін алудың негізгі әдістері қандай?
5. Сигналды тіктеудің интерполяциялық және экстраполяциялық әдістерін салыстырыңдар.
6. Сигналды тіктеудің ортаквадраттық шарты деп нені түсінеміз?
7. Котельников теоремасын түсіндіріңіз.
8. Спектрі шектелген үздіксіз қатысты санақтар жиынымен көрсетудің физикалық мүмкіндіктерін түсіндіріңіз.
9. Спектрі шектелген қатыстарды сигнал үлгісі ретінде көрсетудің қолайсыз жақтары неде?
10. Үздіксіз сигналдарды ұзатудың Котельников теоремасына негізделгенде техникалық орындалуының қиындығы неде?
11. Ең үлкен ауытқу шартында біркелкі дискреттеу шарасы қандай?
12. Бейімделуші дискреттеудің абзалдығы мен кемшіліктері неде?
13. Біркелкі кванттаудың ортаквадраттық қателігі қандай өрнекпен табылады?
14. Кванттау шуылы деп неге айтамыз?
15. Кедергі болғанда сигналды кванттау қадамы қалай табылады?
16. Геометриялық көрсетуде сигналдың қандай кеңістік өлшемдері жиыны қолданылады?
17. Сигналдарды геометриялық көрсетудің амалдық маңызы неде?

Өзіндік жұмыс (СӨЖ) тақырыптыры.

1. Сандық түрдегі сигналдардың абзалдығы.
2. Дискреттеу және кванттау; олардың сандық жүйелерде қолданылуы.
3. Кванттау шуылы. Бөгеуіл бар болғандағы кванттау.
4. Дискреттеу; ақпаратты дискреттеу және қалпына келтіруде сапа шарттары.
5. Таңдау құралы бойынша дискреттеу.
6. Бірқалапты дискреттеу. Котельников теоремасы.
7. Котельников теоремасының амалдық маңызы.
8. Ең үлкен ауытқу бойынша дискреттеу.
9. Дискреттеудің энтропиялық, экстраполяциялық әдістері.
10. Тейлордың экстраполяциялық көпмүшелігімен дискреттеу.
11. Бейімделуші дискреттеу.
12. Сигналдардың көрсетілуінің геометриялық келбеті.

IV ТАРАУ.
ХАБАР КӨЗІНІҢ ЖӘНЕ БАЙЛАНЫС АРНАСЫНЫҢ АҚПАРАТТЫҚ СИПАТТАМАЛАРЫ

4.1 Дискрет хабар көзінің ақпараттық сипаттамалары; үлгілері, өнімділігі; артықшылық

Сигналдардың үлгілік сипаттамасы мен ендірілген ақпараттың көлемдік өлшеміне таянып, хабар көздері мен байланыс арналарының ақпараттық сипаттамаларын қарастырайық; бұлар ақпаратты ұзату жүйелерінің нәтижелілігін арттыру жолдарын табу мүмкіндігін береді. Мысалы үшін, айтылғандар байланыс арналармен кедергі бар немесе жоқ болған жағдайларда хабарларды ұзатудың максималды жылдамдығына жету мүмкін болған шарттарды анықтау мүмкіндігін береді.

Хабар көздері мен байланыс арналары ақпаратты ұзату жүйелерінде өзінің құрамы және физикалық табиғатының әртүрлілігімен ерекшеленеді.

Мұнда механикалық, акустикалық, оптикалық, электрлі және радиоарналар қолданылады. Жалпы заңдылықтарды анықтау үшін олардың физикалық табиғатын абстракттау жолымен хабар көзі мен байланыс арналарының үлгіленген түсініктерін қолдану керек.

Мұнда дискрет хабарлар көзі элементар хабарлардың шегараланған санынан дискрет тізбектерді қалыптастырады. Ал үздіксіз хабар көзінің шығуында үздіксіз хабарлар бейнеленеді.

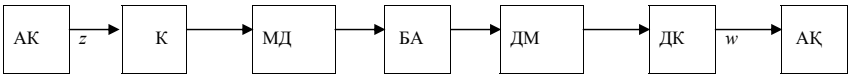
Ақпараттар теориясында хабарлар көзі ол қалыптастыратын хабарлардың санақтық сипаттамаларымен толық анықталады.

Байланыс арнасы ретінде құрылымдар мен физикалық ортаның жиынын түсініп, ол хабарлардың бір жерден басқа жерге (бір уақыт мезгілінен басқа уақыт мезгіліне) өтуін қамтамасыз етеді.

Егер арна дискрет хабар үшін қолданылса, ол **дискрет арна** деп аталады. Ал үздіксіз хабарларға арналған болса, **үздіксіз арна** деп аталады.

Егер хабар көзі мен хабар қабылдаушысы дискретті болса, онда модулятордың шығуынан демодулятордың кіруіне дейін үздіксіз арна болады (4.1-сурет); ал осыған хабар жіберуші жағында модуляторды, ал хабарды қабылдаушы жағында демодуляторды қоссақ, дискрет арнаны аламыз. Мұнда қабылдаудағы бірінші шешуші сұлба демодулятордың құрамында деп есептейміз.

Дискрет арна кірудегі *z* және шығудағы *w* таңбалар жиынымен сипатталады.



4.1- сурет Дискретті байланыс арнасы

Жүйенің сипаттарын жақсату үшін дискретті арнаға кодер және декодер құрылымдары ендіріледі. Мұнда құрылған дискретті арнаның кіруіне *z* хабары түсіп, ал шығуында *w* хабарлары адресатқа беріледі. Мұнда келесідей таңбалеулер істетілген: АК-ақпарат көзі; К- кодер; МД- модулятор; БА- байланыс арнасы; ДМ-демодулятор; ДК-декодер; АҚ-ақпарат қабылдаушысы.

Айта кететін жай, үздіксіз $z(t)$ хабарлары дискреттеу және кванттау жолымен дискретті түрге өткізіледі. Егер арнада кедергілердің әсерін елемесек, онда арнаны мақсатты (идеал) түрде қарап, оны ***бөгеуілсіз (кедергісіз) арна*** деп қараса болады.

Осындай мақсатты арналарда кірудегі әрбір хабарға шығуда анық бір хабар сәйкес келеді және керісінше. Амалда мұндай болмайды.

Егерде кедергі деңгейі жоғары болып, оны ескермеу мүмкін болмаса және *z* және *w* арасында біртаңбалі сәйкестік болмаса, онда күрделі үлгі болған ***бөгеуілді арна*** қолданылады.

Егер арнаға жетіп барған хабар туралы ақпарат алу үшін кері байланысты арна орнатылса, онда оған ***кері байланысты арна*** деп аталады.

Дискрет хабар көзінің ақпараттық сипаттамалары.

Дискрет хабар көзінің үлгілері

Хабар көзінің көптеген мүмкін болған амалдық көріністерінің математикалық үлгісі үздіксіз немесе дискретті кездейсоқ шамалар түрінде көрсетіледі.

Алайда бұл тек хабар көзінің бір ғана жағдайын көрсетеді.

Үлкен уақыт аралығында хабар көзінің жағдайлары да үздіксіз немесе дискрет түрде өзгеріп отырады; сондықтан, осындай хабарларды сипаттау үшін үздіксіз немесе дискрет кездейсоқ үдерістер түріндегі математикалық үлгілер қолданылады.

Мұндай үлгіні құру үшін хабарларды қалыптастыратын хабар көзі ($z_1, z_2, \ldots, z_l$) таңбалар әліпбиінің l көлемін білуі қажетті болады; және бөлек таңбаларды жаратудың ықтималдығын және

олардың арасындағы мүмкін болған байланыстың ықтималдықтарын білуі қажетті болады.

Шеннонның ақпараттар теориясының негізгі ережелерін дәлелдеуде ***эргодикалық хабар көздері*** атты үлгі қолданылған.

Осында құрылған хабарлар математикалық жағынан эргодикалық кездейсоқ тізбектер түрінде көрінеді. Осындай тізбектер тұрақтық және эргодикалық шарттарын толық қанағаттандырады.

Бірінші шарт бойынша, жеке таңбалар мен олардың әртүрлі орын алмасқан топтарының ықтималдықтары хабар ұзындығы бойынша өзгермейді.

Екінші шарт бойынша, өте ұзын хабар үшін алынған санақтық заңдылықтар бірге жақын ықтималдықпен осы хабар көзі жаратқан барлық хабарлар үшін орынды болады.

Санақтық сипаттамалардан бізді қызықтыратыны тізбектің бір таңбасына тура келетін орташа анықсыздық болады.

Алайда амалда хабар көзі шығаратын таңбалар өзара байланысты болады; яғни әрбір таңба өзінен алдыңғы таңбаға санақтық байланысты болады.

Бұл байланыс алдыңғы бірнеше таңбаға дейін (жадысы бар хабар көздері) болады. Осындай хабар көзінің үлгісі ретінде ***Марковтің тізбектерін*** қолдану орынды болады.

N деңгейлі Марков тізбегі оқиғалар тізбегін сипаттап, олардың әрбірінің ықтималдығы одан алдын болған *n оқиғаларға* байланысты болады. Сол *n* болып өткен айқын оқиғалар хабар көзінің күйін анықтайды; және ол кезектегі таңбалы шығаруда осы күйде болады.

Таңбалар әліпбиінің көлемі *l* болғанда хабар көзінің күйлер саны *R* болып, ол l^n - нен аспайды. Осы күйлерді $S_1 \ldots S_q \ldots S_R$, таңбалаймыз;

S_q күйінде z_i таңбасын таңдау ықтималдығын $p_q(z_i)$ деп таңбалаймыз. Осы ықтималдықты $p_q(z_i)$ анықтауда келесідей деу орынды болады;

- осы кезектегі таңбалы шығару мезгілінде осыдан алдын жаратылған барлық таңбалар мәлім деп есептелінеді.

Егер ақпарат көзі S_q күйде болса, оның меншікті энтропиясы $H(S_q)$ мына түрде анықталады:

$$H(S_q) = -\sum_{i=1}^{l} p_q(z_i) \log p_q(z_i) \,. \qquad (4.1)$$

Осында кездейсоқ $H(S_q)$ шаманың барлық мүмкін болған күйлерінде $q = \overline{1,R}$, орташалап хабар көзінің энтропиясын табамыз:

$$H(Z) = -\sum_{q=1}^{R} p(S_q) \sum_{i=1}^{l} p_q(z_i) \log p_q(z_i), \qquad (4.2)$$

мұнда $p\ (S_q)$ – ақпарат көзінің S_q күйінде болуының ықтималдығы; $H(Z)$ – хабар көзінің бір таңбаға тура келетін анықсыздығының орташа мәні болады.

Бірнеше меншікті күйлер үшін хабар көзінің анықсыздығын табайық.

Егерде таңбалар арасында **санақтық байланыс болмаса**, онда хабар көзі z_i таңбалы таңдаған соң, оның күйі өзгермейді (R = 1). Сондықтан, $p(S_1)$= 1, хабар көзінің энтропиясы үшін мына өрнек орынды болады:

$$H(Z) = -\sum_{i=1}^{l} p\ (z_i) \log p\ (z_i) \cdot$$

Егер корреляциялық байланыс тек екі таңба арасында болса (қарапайым Марков тізбегі), хабар көзінің күйлерінің максималды саны әліпби көлеміне тең болады. Сондықтан, $R = l$ және $p_q(z_i) = p(z_i / z_q)$, мұнда $q = \overline{1,l}$.

Осыдан (4.2) өрнегі мына түрге келеді:

$$H(Z) = -\sum_{q=1}^{l} p(z_q) \sum_{i=1}^{l} p\ (z_i / z_q) \log p\ (z_i / z_q) \qquad (4.3)$$

Ал егерде таңбалар арасындағы корреляциялық байланыс үш таңбаға таралса, онда хабар көзінің күйі алдынғы өткен екі таңбамен анықталады. Сондықтан хабар көзінің кез келген S_q күйі үшін екі төменгі телгіні (индексті) таңбалы қолдану қолайлы болады: $S_{k,h}$, мұнда $k = \overline{1,l}$ және $h = \overline{1,l}$.

Онда $p(S_q) = p(S_{k,h}) = p(z_k, z_h)\ \ p_q(z_i) = p(z_i / z_k z_h)$

Осыны (4.2) ге қойып, мынаны табамыз:

$$H(Z) = -\sum_{k=1}^{l} \sum_{h=1}^{l} p(z_k z_h) \sum_{i=1}^{l} p\ (z_i / z_k z_h) \times \log p\ (z_i / z_k z_h) \qquad (4.4)$$

Осындай жолмен таңбалар арасындағы корреляциялық

байланыстардың ұзынырақ болған жағдайларына да арнап хабар көзінің энтропиясын тапса болады.

4.1 ***Зертханалық жұмыс***

Стационарлы дискрет хабар көзі берілген болып, оның әліпбиі төрт таңбаден тұрады: z_1 z_2 z_3 және z_4.

Олардың шартсыз ықтималдықтары бірдей, яғни:

$[\, p(z_1) = p(z_2) = p(z_3) = p(z_4) = 1/4\,]$, ал шартты ықтималдықтары $p(z_i / z_q)$ 4.1 кестеде көрсетілген.

4.1-кесте

		z_2	z_3	z_4
z_1	1/3	1/3	1/3	0
z_2	1/3	1/3	1/3	0
z_3	1/3	1/3	1/3	0
z_4	0	0	0	1

Кестені талдау жасасақ, хабар көзі екі режимде істеуін көреміз.

Алдын ¾ ықтималдықпен z_1, z_2 немесе z_3 таңбалардың бірі таңдалады; және хабар көзі сол таңбаларды қолданып, тізбектерді қалыптастыра бастайды. Егер бірінші болып z_4 таңбасы таңдалса (осындай оқиғаның ықтималдығы $1/4$ ге тең болады), онда генерацияланатын тізбекте тек z_4 таңбалары болады.

Ансамбль бойынша орташалауда көптеген бір типті көздері бар деп ұйғарылады; осының шамамен төрттен үші бірінші режимде, ал төрттен бірі - екінші режимде істейді.

Мұнда (4.3) ке сәйкес хабар көзінің энтропиясы

$$H(Z) = -\frac{3}{4}\log_2\frac{1}{3} - \frac{1}{4}\log_2 1 = 1{,}19 \text{ ек.өлшем.}$$

Уақыт бойынша орташасын есептеуде айқын тізбек қолданылады; сондықтан, хабар көзінің жұмыс істеуі жұмыс тәртіптеріне (тәртібіне) байланысты болады.

Бірінші режимде жетерлі дәрежеде үлкен болған тізбектің бір таңбасына тура келетін анықсыздық (тізбектің энтропиясы) 1,586 екілік өлшемге, ал екінші режимде - нөлге тең болады.

Құрылып отырған тізбектердің энтропиялары хабар көзінің энтропиясына сәйкес келмегендіктен, ол эргодикалық болмайды.

Бірақ айтып кететін жай, кез келген тұрақты хабар көзі бірнеше әртүрлі эргодикалық көздер арқылы көрсетілуі мүмкін.

Эргодикалық таңбалар тізбегінің қасиеттері.

Нақты хабар көзінің қалыптастыратын тізбектерінің сипаты ондағы Таңбалардың ықтималдығының әртүрлі болуы және ол таңбалар арасындағы коореляциялық байланыстардың болуында. Мысалы, эргодикалық хабар көзі тізбектеп z_1, z_2, z_3 таңбаларын келесідей 0,1; 0,3; 0,6 ықтималдықтармен шығаратын болсын делік. Онда жетерлі дәрежеде ұзын болған таңбалар тізбегінде әрбір z_1 таңбасына үш z_2 және алты z_3 таңбасы сәйкес келетін болады.

Алайда тізбектегі таңбалар саны шектелгенде осы тізбекте келесідей оқиғалар ықтималдықтары мүмкін болады:

тек қана z_1 таңбалар (немесе z_2 немесе z_3) болады;

тек қана z_1 таңбалары және бір таңба z_2 немесе z_3;

тек қана z_2 таңбалары және бір таңба z_1 немесе z_3;

тек қана z_3 таңбалары және бір таңба z_1 немесе z_2;

тек қана z_1 таңбалары және бір таңба z_2 немесе z_3 және сол сияқты.

Тізбектің элементтері көбейген сайын жоғарыда аталғандай тізбектердің ықтималдығы да кемейе бастайды.

Эргодикалық хабар көзінің ұзын таңбалар тізбегін құрудағы орнықты қасиеттерін көрсететін келесідей теорема бар:

жетерлі дәрежеде үлкен болған N, қаншалықты да кіші болған екі δ>0 және μ>0 үшін барлық тізбектер екі топқа бөлінеді.

Бірінші топты көпшілік тізбектер құрап, олардың әрбірі өте кіші ықтималдыққа ие болады; осындай тізбектердің барлығының бірге алғандағы ықтималдықтарының қосындысы өте кіші болады және N жетерлі дәрежеде үлкен болғанда ол ықтималдық қалағанша кіші болған δ санынан да кіші болады.

Осындай тізбектерді ***типтік болмаған тізбектер*** деп аталады.

Екінші топ өз ішіне типтік тізбектерді алып, олар *N* жетерлі дәрежеде үлкен болғанда олардың ықтималдықтары амалда өзара тең болады;

онда олардың кез келгенінің ықтималдығы *p* мына теңсіздікті қанағаттандырады:

$$\left|\log(1/p)/N - H(Z)\right| < \mu, \qquad (4.5)$$

мұнда *H(Z)* — хабар көзінің энтропиясы.

Осы қатыс ұзын тізбектердің ***ассимптотикалық біртегістік*** қасиеті деп аталады.

Егер $N \to \infty$ болса, онда хабар көзі қалағанша бірге жақын ықтималдықпен тек типтік тізбектерді шығарып береді.

Осындай тізбектердің ықтималдықтары $1/p$ болады.

Осындай тізбектердің пайда болуындағы анықсыздық олардың тең ықтималды екенін ескерсек келесідей болады: $\log(1/p)$.

Онда әрбір таңбаға тура келетін анықсыздық $\log(1/p)/N$ болады.

Осы мән хабар көзінің энтропиясынан амалда шеттемеуі керек болып, ол (4.5) қатысынан көрінеді.

Осы теореманы қарапайым эргодикалық жадысыз хабар көзіне дәлелдейік. Ол үлкен сандар теоремасынан шығады.

l l l әліпбиінің ($z_1, z_2, \ldots, z_l$) N элементтерінен құралған ұзын тізбекте Np_1 элементтері z_1 болады; Np_2 элементтері z_2 болады және сол сияқты; мұнда олардың ықтималдықтары $p_1, p_2, \ldots, p_l$ болады; онда кез келген типтік тізбектің орындалуының ықтималдығы p мына мәнге жақын болады:

$$p = p_1^{p_1 N} p_2^{p_2 N} \ldots p_l^{p_l N} . \qquad (4.6)$$

Осының оң және сол бөлімін логарифмдеп мынаны табамыз:

$$\log p = N \sum_{i=1}^{N} p_i \log p_i .$$

Осыдан өте үлкен N үшін мына теңдеуді аламыз:

$$\log(1/p)/N = H(Z) \cdot$$

Жалпы жағдай үшін теорема **Марковтің тізбектерін** қолданумен дәлелденеді.

Енді әріптер бір түрлі ықтималды және өзара байланысты болмаған жағдайдан басқа жағдайларды қарастырайық. Онда типтік болмаған тізбектер болмайды.

Қарастыратын жағдайларымызда N жетерлі дәрежеде үлкен болғанда типтік тізбектер барлық тізбектер санының кішкене ғана (болмашы) бөлімін құрайды. Хабар көзінің әліпбиінің көлемі l және тізбектегі таңбалар саны N болғанда барлық тізбектер саны:

$$n_l = l^N = 2^{N[\log_2 l]}. \qquad (4.7)$$

Типтік тізбектер саны $n_2 = 2^{NH(Z)}$ болғанда, мына қатысты табамыз:

$$n_{12} / n_1 = 2^{175} / 2^{200} = 1/2^{25} \approx 1/30 \bullet 10^6 \ .$$

$H(Z) < \log_2 l$ болғандықтан келесідей: $n_2 < n_1$ болады.

Осы теңсіздік *N* үлкейгенде, күшейе түседі.

Осы қасиеттерді қолданып, ақпаратты нәтижелі кодтау мүмкіндігін Шеннон дәлелдеген.

4.2 ***Зертханалық жұмыс***

Эргодикалық хабар көзінің параметрлері*:* l = 16, $H(Z)$ = 3,5 бит , ал N = 50. Барлық мүмкін болған тізбектердің ішінде типтік тізбектердің үлесін табу керек.

Шешімі:

(4.7) және (4.8)-дерден мынаны табамыз:

$n_1 = 16^{50} = 2^{200}; n_2 = 2^{50 \bullet 3,5} = 2^{175}$.

Осыдан $n_{12} / n_1 = 2^{175} / 2^{200} = 1/2^{25} \approx 1/30 \bullet 10^6$.

Демек, барлық мүмкін болған тізбектердің 30 миллионнан бір бөлігі ғана типтік болады.

Хабар көзінің **артықшылық өлшемі** осы көздің ***әрбір таңбасы қаншалықты жақсы*** қолданылатынын көрсетеді және келесідей табылады:

$$D = [H_{\max}(Z) - H(Z)]/[H_{\max}(Z)], \qquad (4.9)$$

мұнда $H_{\max}(Z)$ – $\log l$ ге тең болған максимал мүмкін болған энтропия;

$H(Z)$ – хабар көзінің энтропиясы.

Егер ақтықшылық нөлге тең болса, онда ол қалыптастыратын хабарлар тиімді (тиімді) болады және ақпаратты ең көп өзімен алатын болады. Осындайда кедергі жоқ болғанда I көлеміндегі ақпаратты жіберу үшін керек болған таңбалар саны $k^1 = I/[H_{\max}(Z)]$ болады.

Нақты хабар көзі қалыптастыратын хабарлардың артықшылығы бар болғандықтан оның энтропиясы максималдан кем болып, сол I

көлеміндегі ақпаратты жіберу үшін көбірек таңбалар керек болады, яғни $k_2 = I/H(Z) > k^1$.

Онда хабардағы әріптердің (белгілердің) артықшылығы немесе хабардың артықшылығы туралы айтылып, оны да сол параметрмен сипаттаймыз D: $D = (k_2 - k_1)/k_2 = [H_{\max}(Z) - H(Z)]/[H_{\max}(Z)]$.

Артықшылықты хабар көзінің ***кемшілігі*** деп қарау керек емес.

Әдетте ол табиғи тілдің өзгешелігіне байланысты болады.

Артықшылықтың бар болуы, бір тараптан, ***хабардың көлемін арттырып***, оны өңдеуге және жіберуге кететін шығындарды көбейтсе, екіншіден, хабардағы артықшылық оның ***кедергілерге шыдамдығын арттырады***.

Мысалы, табиғи тілдегі артықшылықтың болуы оны қолданатын адамдардың тілінде көптеген деффекттер мен акценттер болғанда да адамдар сенімді немесе түсінікті түрде сөйлесе алады.

Алайда автоматты жүйелерде **табиғи артықшылықты жою** керек болады.

Ал қателіктермен күресу үшін рационал түрде артықшылық ендіріледі де, ол артықшылық ең көп ұшырайтын қәуіпті қәтеліктерді анықтап түзетеді.

Арнада кедергі деңгейі төмен болғанда артықшылықты кемейту немесе жою ақпаратты ұзату жылдамдығын арттырып, әжептеуір экономикалық нәтиже береді.

4.3 ***Зертханалық жұмыс***

Орыс тілінде жазылған мәтінді ұзатуда артықшылықты жоюдан болатын нәтижеті анықтау керек.

Шешімі: Орыс тілінің мәтіндінің максимал энтропиясы 5 бит.

Ал әрбір әріптің ықтималдықтарын есептегенде энтропиясы - 4,42 бит.

Әріптер арасындағы корреляцияны есептегенде - 3,5 бит.

Сөздер арасындағы корреляцияны есептегенде - 1,5 бит-ке жуық болады. Сонымен орыс тілінің артықшылығы –

$$D = [H_{\max}(Z) - H(Z)]/[H_{\max}(Z)] = (5 - 1{,}5)/5 = 0{,}7$$

Бұны басқаша түсіндірсек былай болады; егер орыс әліпбиімен ақпаратты жібергенде барлық әріптерді бір-біріне байланыссыз таңбалар деп есептеп, кедергісіз арнамен ақпарат жібергенде оның тек 30 % қолданылады, яғни табиғи тілде тестті жібергенде ақпараттың 70 пайызы артықша болады.

Ал егер осы артықшылықты жоятын болсақ, онда жүйенің нәтижелігі 3 есе артады.

4.1.1 Сигналдар мен хабарлардың артықшылығын есептеу. Сигналдарды энтропия бойынша оңтайландыру. Сығымдау еселіктері

Дискрет түрдегі сигналдарда (хабарларда) хабарлар тиімді болуы үшін олардың әрбірінде энтропия максимал болуы керек; мұның үшін олардың әрбірінің ықтималдығы өзара тең болуы керек.

$$H = -\sum_{k=1}^{m} P_k \log P_k ; P_k = P_1 = P_2 = ... = \frac{1}{m}; H_{\max} = \log m.$$

Хабар (сигнал) **үздіксіз** болғанда оның тиімді болуы жоғарыда баяндалған;

яғни сигналдың қуаты шектелген болса, оның амплитудасының таралу теңдеуі қалыпты (нормал) болуы керек.

Ал егер сигналдың қуаты шектелмеген жағдайда немесе өте үлкен болған жағдайда, оның амплитудасының таралу теңдеуі біркелкі болуы керек.

Ал сигналдың таралу теңдеуі (функциясы) басқа түрде болса, оның таралу теңдеуін сызықсыз түрлендірушілер жәрдемінде қалыпты (нормал) түрге келтіріледі.

Мұндай жағдайда оның келтірілген энтропиясы келесідей анықталады:

$$H(X) = -\int_{-\infty}^{\infty} \omega(x) \log \{\omega(x) \Delta x\} dx \cdot$$

Нақты жағдайда дискрет хабарда да, үздіксіз хабарда да энтропия максималдан анағұрлым кем болады;

$$H_{real} \le H_{\max}; H(X) \le H_{\max}(X).$$

Сығымдау еселігі дискрет хабар үшін мына түрде болады:

$$\mu_d = \frac{H}{H_{\max}}.$$

Ал үздіксіз хабар үшін мына түрде жазса болады:

$$\mu_u = \frac{H(X)}{H_{\max}(X)}.$$

Егерде тиімді хабардағы информация көлемін нақты хабарға тең деп алсақ, онда тиімді хабардағы таңбалар саны

$$n_{\min} < n_{real}, I_{opt} = I_{real}$$ болады.

Осыны есепке алып, мынаны жазса болады:

$$I_0 = n_{real} H = n_{\min} H_{\max}.$$

Онда сығымдау еселігін мына түрде жазса болады:

$$\mu_u = \frac{H(X)}{H_{\max}(X)} = \frac{n_{\min}}{n_{real}}.$$

Артықшылық еселігі сығымдау еселігін бірге толтырады, яғни оны келесідей есептесе болады:

$$r = 1 - \mu = \frac{H_{\max} - H}{H_{\max}} = \frac{n_{real} - n_{\min}}{n_{real}}.$$

Артықшылық еселігі 0 мен 1 аралығында өзгереді, яғни $0 < r \le 1$.

r = 0 болғанда, хабар көзі максимал дәрежеде информативті болып, әрбір таңба тең ықтималды болады; ал r =1 болғанда, хабарлардың информативтігі 0 болады.

4.4 ***Зертханалық жұмыс***

10 дискрет хабары берілген болсын; 1 таңбасының ықтималдығы 0,5; ал 0 таңбасының ықтималдығы да 0,5 болсын; осы кодтың артықшылық еселігін табу керек.

Шешімі:

Барлық мүмкін болған қисындастыруылар (комбинациялар) мыналар: 10, 00, 01, 11.

Әрқайсысының энтропиясын табу керек; олардың ішінде ең үлкен энтропиялысын тауып, берілген хабардың энтропиясымен айырмасын табу керек; яғни мынаны табу керек:

$$r = \frac{H_{\max} - H_{10}}{H_{\max}}.$$

$H_0 = H_0 = ... = -0{,}5\log 0{,}5 = -0{,}5\log 0{,}5 = ... = 0{,}5$, яғни барлық қисындастыруылардың энтропиялары бірдей болады; сондықтан: $r = 0$ болады.

Мұны энтропияның қасиеттеріне сүйене отырып, есептеместен ақ тапса болар еді.

Бұл мысалда 1 таңбасы мен 0 таңбасының ықтималдықтары тең болғандықтан, олардың энтропиялары максимал болады; яғни код қисындастыруы да тиімді болғандықтан артықшылық еселігі 0 ге тең болады.

4.5 ***Зертханалық жұмыс***

Орыс әліпбиі 32 таңбадан тұрады; егер олардың әрбірінің санақтық ықтималдығы өзара тең болғанда, яғни

$P_1 = P_2 = ... = P_{32} = \frac{1}{32}$ болар еді; орыс әліпбиіндегі артықшылықты табу керек.

Шешімі: 1) $H_{\max}(X) = \log_2 32 = 5bit$ болады.

Алайда таңбалардың ықтималдығы тең емес; сондықтан олардың нақты ықтималдықтарын есепке алсақ, энтропия төмендегідей есептеледі.

2) Егер таңбалардың әрбірінің санақтық ықтималдығын есептесек, онда $H_1(X) = -\sum_{i=1}^{32} P(x_i)\log P(x_i) = 4{,}39bit$ болады.

Бұл әріптер арасында байланыс болмағандағы энтропия; ал әріптер арасындағы корреляцияны есептесек, энтропия кемейеді.

3) Екі әріптер арасындағы байланыстарды есептесек, онда :

$$H_2(X) = -\frac{1}{2}\sum_{i=1}^{32}\sum_{j=1}^{32} P(x_i x_j)\log P(x_i x_j) = 3{,}41\,bit$$ болады.

4) Үш әріптер арасындағы байланыстарды есептесек энтропия одан ары төмендейді:

$$H_3(X) = -\frac{1}{3}\sum_{i=1}^{32}\sum_{j=1}^{32}\sum_{k=1}^{32} P(x_i x_j x_k)\log P(x_i x_j x_k) = 3\,bit$$ болады.

Ақырғы жағдай үшін артықшылық еселігін есептесек, онда:

$r = \frac{5-3}{5} = \frac{2}{5} = 0{,}4$, яғни артықшылық 40 % болады.

4.1.2 Үздіксіз хабарлардың энтропиясы және оның максимумын табу

Көп жағдайларда хабарлар үздіксіз түрде болады; дыбыстық хабарлар (радио, телефон, теледидар, және т.б.). Мұндай жағадайда олардың энтропиясы қалай табылады?

Егер үздіксіз хабар оның дискрет нүктелерімен $x_1, x_2, ..., x_n$ ауыстырсақ, олардың элементар ықтималдығы: $P_k = \omega(x_k)\Delta x$ болады. Энтропияны есептейміз:

$$H = -\sum_{k=1}^{m} \omega(x_k)\Delta x \log\{\omega(x_k)\Delta x\} = -\sum_{k=1}^{m} \omega(x_k)\Delta x \log \omega(x_k) - \sum_{k=1}^{m} \omega(x_k)\Delta x \log \Delta x$$

Екінші интегралда $\int_{-\infty}^{\infty} \omega(x_k)dx = 1$ болғандығы үшін екінші

қосындыдан тек мына қалады: $-\log \Delta x$.

Сонда ***келтірілген энтропия*** келесідей болады:

$$H^* = \int_{-\infty}^{\infty} \omega(x_k) \log \omega(x_k)dx - \log \Delta x .$$

Келтірілген энтропияда оң жақтағы қосылғыш дискреттеу қателігін көрсетеді. Егер дискреттеу қадамын Котельников бойынша тапсақ, онда оны $\Delta x = 1$ деп алса болады; мұндай жағдайда қателік болмайды. Мұндай шарт тек Марков сигналдарында немесе тиімді (ра···ионал) спектрлі сигналдарда ғана орындалады [автор].

Кездейсоқ үздіксіз сигналдарды қалай тиімділесе болады?

Олардың таралу теңдеуін (функциясын) таңдап алумен олардың энтропиясын максималдауға болады.

Келесідей жағдайларды қарастырамыз:

біріншісінде - сигналдың дисперсиясы шектелген және $D_x = \sigma^2 = const, M_x = 0$ тең болсын.

Екінші жағдайда сигнал қуаты $[a,b]$ аралығында шектелмеген болсын; $D_x = \infty, M_x = 0$.

Зерттеудің ***қорытындысы*** мынаны көрсетеді:

1. Егер үздіксіз кездейсоқ сигналдың қуаты $D_x = \sigma^2 = const, M_x = 0$ шектелген болса, онда **энтропия максимал** болуы үшін оның таралу теңдеуі қалыпты болуы керек.

2. Кедергінің орта қуаты берілген болса, онда кедергі **максимал нәтижелі** болуы үшін оның таралу заңы қалыпты болуы керек.

3. Егер **сигнал қуаты** $[a,b]$ аралығында **шектелмеген** болса: $D_x = \infty, M_x = 0$, онда оның таралу теңдеуі (функциясы) сол аралықта **біркелкі таралған** болуы керек; онда оның таралу теңдеуі келесідей болады: $\omega(x) = \frac{1}{b-a}$.

4. Мұндай жағдайда **кедергі нәтижелі** болуы үшін оның таралу теңдеуі (функциясы) **біркелкі** болуы керек.

Осы заңдылықтардағы сигналдың энтропиясын табайық:

1. Қалыпты заң үшін келесідей болады: $H_n(X) = \log\left(\frac{\sigma}{\Delta x}\sqrt{2\pi e}\right)$.

2. Біркелкі таралған заңды сигналдың энтропиясы: $H_d(X) = \log\frac{b-a}{\Delta x}$.

4.1.3 Дискрет хабар көзінің өнімділігі.

Хабар көзінің өнімділігі деп хабар көзінің уақыт бірлігінде өндіретін ақпарат көлеміне айтады. Оны басқаша хабар құру жылдамдығы немесе ақпараттың кіру жылдамдығы деп атайды. Оны хабар көзінің бірлік уақытқа тура келетін энтропиясымен өлшесе де болады.

z_i таңбасын хабар көзі S^q күйінде қалыптастырған уақыты τ_{qz_i} болсын.

Онда бір таңбалы хабар көзінің орташа шығару уақыты:

$$\tau_u = \sum_{q=1}^{R} p(S_q) \sum_{i=1}^{l} p_q(z_i) \times \tau_{qz_i} \qquad (4.10)$$

Хабар көзінің өнімділігін $\bar{I}(z)$ мына теңдеумен (формуламен) көрсетсе болады:

$$\bar{I}(Z) = H(Z)/\tau_u. \qquad (4.11)$$

Ақырғы теңдеуден көрініп тұрғандай хабар көзін тиімділегенде оның энтропиясын асыра тұрып, ал әрбір таңбаның сол уақыттағы ұзындығын оның ықтималдығына кері пропорционал түрде өзгерту керек.

Егер ол өзгермесе, онда

$$\bar{I}(Z) = H(Z)/\tau \ , \tau_{\grave{e}} \approx \tau \quad . \qquad (4.12)$$

Ең үлкен өнімділік максималды энтропияда болады.

4.2 Дискрет байланыс арнасының ақпараттық сипаттамалары

Үлгілері; жіберу жылдамдығы

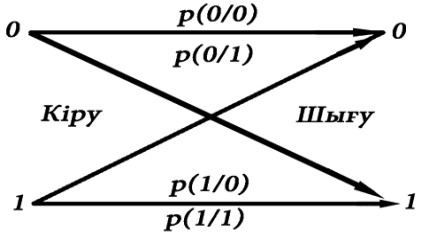
Дискретті арналар үлгісі.

Дискретті арналар деп дискрет сигналдарды ұзату құрылымдарының жиынына айтамыз. Осындай арналар, мысалы, деректерді ұзатуда, телеграфияда, радиолокацияда қолданылады.

Хабар көзінің таңбалар l әліпбиінен (бірінші әліпби таңбалары $z_1, z_2, ..., z_l$) таңбалар тізбегі түрінде дискретті хабарлар құрылады.

Оларды екілік таңбалар тізбегіне кодтаушы құрылым (кодер) айналдырады. Екінші әліпбидің таңбалар m көлемі (екінші әліпби таңбалары $u_1, u_2, ..., u_m$) әдетте l таңбалары m нен көп болуы мүмкін; бірақ тең болуы да мүмкін.

Кедергілі ақпараттық арнаның үлгісі оның кіруіндегі және шығуындағы таңбалар жиыны және жеке таңбалардың ұзатудағы ықтималдық қасиеттерімен



4.2-сурет

көрсетіледі. Жалпы жағдайда арнаның көптеген жағдайлары болып, уақыт арасында бір жағдайдан басқа жағдайға өтуі де мүмкін; сондай ақ ол жіберілетін таңбалар тізбегіне де байланысты өзгеруі мүмкін болады.

Әрбір жағдайда арна шартты ықтималдықтардың матрицасымен $p(v_j / u_i)$ көрсетіліп, мұнда әрбір жіберілген таңба u_i арна шығуында таңба v_j болып қабылданады.

Нақты арналардағы ықтималдықтардың мәндері әртүрлі әсер, ықпалдарға байланысты болады: сигналдардың қасиетіне, арнаға әсер етуші кедергілердің үдемелілігіне (интенсивтігі) мен сипатына, сигналды қабылдау тарапында қабылдау әдісіне байланысты болады.

Егерде арнадан өтуде уақыт аралығында арна сипаттары өзгеретін болса, ал бұл нақты арнаның көпшілігіне тән қасиет, ондай арналар ***бейтұрақты арна*** деп аталады. Алайда бейтұрақты арна ажыратылған аралықтарда жергілікті тұрақты бөліктерге ажыратылуы және ***жергілікті тұрақты*** деп аталуы да мүмкін.

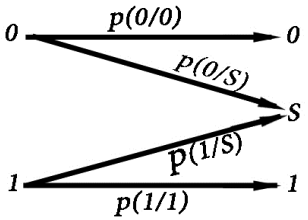
Егер оның осы күйдегі өткелдік ықтималдықтары оның алдыңғы күйлеріне байланысты болса, арна "жадысы бар" деп аталады.

Ал егер өткелдік ықтималдықтары өзгермес болса, яғни арна тек бір күйде болса, ол ***"тұрақты жадысыз арна"*** деп аталады.

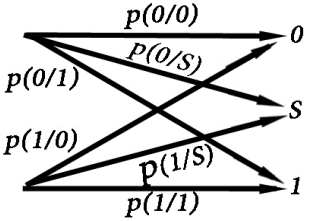
Егер оның кірудегі және шығудағы әртүрлі таңбалар саны бірдей және *к*-ге тең болса, онда арна ***"к - негізде"*** деп аталады.

Тұрақты дискретті екілік жадысыз арна төрт шартты ықтималдықтармен анықталады: $p(0/0)$, $p(1/0)$, $p(0/1)$, $p(1/1)$.

Арнаның осындай үлгісі граф түрінде көрсетіледі (4.2-сурет). Мұнда $p(0/0)$ және $p(1/1)$ — таңбалардың бұзылмай өткізу ықтималдықтары; ал $p(0/1)$ және $p(1/0)$ — таңбалардың 0 және 1 бұзылу (транформация) ықтималдықтары.



4.3,а-сурет



4.3,б-сурет

Егер арнаның шартты ықтималдықтары тең: $p(0/1) \approx p(1/0) = q$ болса, онда арна ***екілік симметриялы*** деп аталады.

Ал егер $p(0/1) \neq p(1/0)$ болса, арна ***симметриясыз*** деп аталады.

Оның шығуында таңбалар *p* ықтималдығымен дұрыс қабылданады; және *1—p = q* ықтималдығымен қате қабылданады.

Арнаның осы үлгісінің кең қолданылуына негізгі себеп оның қарапайымдығы болды. Алайда көптеген арналар бұл үлгімен өте жуықталған түрде көрсетіледі.

Бұдан басқа осы кезде кең қолданылып келе жатқан арна үлгісі - бұл ***өшіруі бар дискретті арна.*** Оның негізгі өзгешелігі – кірудегі таңбалар әліпбиі шығудағы әліпбиден өзгеше болады. Мұнда кіруде 0 және 1 таңбалары болса, ал шығуда 0 және 1 ден өзгеше ***өшіру S таңбасы*** да бар. Бұған негізгі себеп - транформация болған таңбаның қате екенін табу қиын болып, ал өшірілген таңбаның қате екенін табу оп оңай болады.

4.3-суретте осындай арнаның үлгісі граф түрінде көрсетілген. Мұнда біріншісінде транформациясы жоқ арна (4.3.а-сурет), ал екіншісінде транформациясы бар арна (4.3.б-сурет) үлгілері көрсетілген.

4.2.1 Дискрет арнамен ақпаратты жіберу жылдамдығы

Дискрет арнада жылдамдықтар екіге бөлінеді: техникалық және ақпараттық (информациялық) деп. ***Техникалық V_T ұзату жылдамдығы*** немесе ***манипуляция жылдамдығы*** деп элементар таңбалардың уақыт бірлігінде жіберу санына айтады. Ол байланыс арнасының қасиеттеріне және арна аспапсының жылдамдығына байланысты болады. Таңбалар ұзындығы әртүрлі болғанда осы жылдамдық келесідей болады:

$$V_\tau = 1/\tau_{ср}, \qquad (4.13)$$

мұнда $\tau_{ср}$ – таңбалардың орташа ұзындығы. Олар біртүрлі болғанда $\tau_{ср} = \tau$ болады. Осындай жылдамдықтың өлшем бірлігі болып қабылданған ***бод*** – бір секундта бір таңба ұзатылатын (жіберілетін) жылдамдықты білдіреді.

Ақпараттық (информациялық) жылдамдық немесе ***ақпарат ұзату жылдамдығы*** уақыт бірлігінде арнамен жіберілген ақпараттың орта мәнімен анықталады. Ол ***байланыс арнасының сипаттарына*** байланысты болады; *қолданатын таңбалар әліпбиіне, оларды жіберудегі техникалық жылдамдыққа, линиядағы кедергілердің санақтық қасиеттеріне, кіруге келіп түсетін таңбалардың*

ықтималдығына және олардың өзара санақтық байланысына, т.б. байланысты болады.

Манипуляция жылдамдығы V_T анықталған болса, онда ***ақпаратты жіберу Ī(V,U) жылдамдығы*** мына қатыспен табылады:

$$\bar{I}(V,U) = V_\tau I(V,U) \qquad (4.14)$$

мұнда $I(V,U)$ — бір таңбаның орташа ақпарат тасу көлемі.

4.2.2 Бөгеуілсіз дискрет арнаның өткізу қабілеті; бөгеуілді дискрет арнаның өткізу қабілетігі.

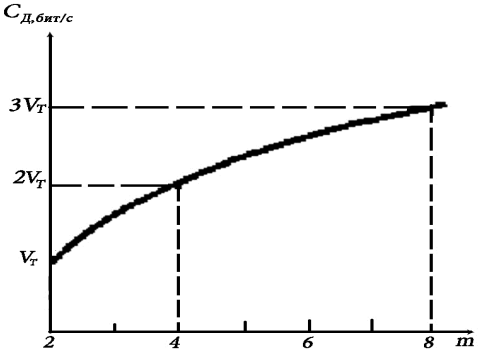
Кедергісіз дискрет арнаның өткізу қабілеті

Теорияда және амалда берілген арна бойынша қандай шекке дейін ақпарат өткізу мүмкін және жылдамдықты қандай жолдармен арттыру мүмкін болатынын зерттеу маңызды мәселе. Арнаның шекті мүмкіндіктері оның өткізу қабілетімен анықталады.

Арнаның өткізу қабілеті $C_д$ осы арнамен ақпаратты жіберудің максимал шамасына тең болады және бұл жылдамдықта жіберу және қабылдаудың ең дамыған әдістерін қолданумен қол жеткізіледі:

$$C_Д = \max \bar{I}(V,U) = \max V_\tau I(V,U). \qquad (4.15)$$

Таңбалардың әліпбиі берілген болса және негізгі сипаттамалары



4.4 - сурет

(мысалы, өткізу жолағы, сигнал жіберушісінің орташа және пиктік қуаты) таңбаланған болса, осы арнамен элементар сигнал-

дарды ең үлкен жылдамдықпен жіберетіндей етіп басқа сипаттарын таңдау керек; яғни V_T максималды мәнін қамтамасыз ететін болуы керек.

Қабылданған сигналдың бір таңбасына сәйкес келетін *I(V,U),* ақпараттың орташа мәнінің максимумы $u_1 \ldots u_i \ldots u_m$ таңбалар арасындағы ықтималдықтардың таралу жиынымен анықталады.

Арнаның өткізу қабілеті, арнаның жылдамдығы сияқты, бір секундта ақпараттың екілік өлшем санымен өлшенеді (екілік өлшем/с). **Кедергі жоқ болғанда** арнаның кіруіндегі $\{v\}$ таңбалар саны мен арнаның шығуындағы $\{u\}$ таңбалар саны арасында **қатал байланыс** болады. Онда $I(V,U) = I(U,V) = H(U)$.

Бір таңбаға тура келетін мүмкін болған максимал ақпарат мынаған тең:

$$C_Д = V_\tau \log m . \tag{4.16}$$

Сөйтіп, кедергісіз дискретті арнада жіберу жылдамдығын арттырып, өткізу қабілетіне жақындату үшін кодердегі хабардың әріптер тізбегін келесідей талаптар орындалатын түрде өзгерту керек;

шығу тізбегіндегі әртүрлі әріптер мүмкін болғанша біртүрлі ықтималдықта болуы керек; ал ***олардың арасындағы санақтық байланыстар жоқ болуы*** керек.

Бұл қағида кез келген ***эргодикалық әріптер тізбегі*** үшін дәлелденген болып, мұнда кодтаудағы жиынтықтардың ұзындығы үшін ***ассимптотикалық тең ықтималдылық теоремасы*** орынды болуы керек.

Таңбалар әліпбиінің m көлемін кеңейту арнаның өткізу сипаттамасын арттырады (4.4-сурет); алайда мұнда техникалық орындалуының күрделілігі де артады.

Кедергілі дискретті арнаның өткізу қабілеті.

Арнада **кедергі болғанда** арнаның кіруі мен шығуындағы таңбалар жиындары арасында **байланыс қатал болмайды.**

Онда арна бойынша бір таңба арқылы жіберілетін орташа ақпарат көлемі $I(V,U)$, осындай жағдайда келесідей анықталады:

$$I(VU) = H(V) - H_U(V) = H(U) - H_V(U) \tag{4.17}$$

Егер таңбалар арасында санақтық байланыстар болмаса, онда байланыс арнасының шығуында сигнал энтропиясы келесідей болады:

$$H(V) = -\sum_{j=1}^{m} p(v_j) \log p(v_j) \qquad (4.18)$$

Санақтық байланыс болғанда энтропияны Марков тізбегі жәрдемінде анықтайды. Осындай анықтаудың бағдаржолы мәлім болғандықтан күрделі теңдеулерді (формулаларды) жазудың қажеті қалмайды; сондықтан, байланыс жоқ болған жағдайларды қарастырамыз.

Апостериор энтропия жіберілген ақпараттың қателіктер әсерінен кемейуін сипаттайды. Ол арнаға келіп түскен таңбалар тізбегінің санақтық сипаттарына және кедергінің әсерін көрсетуші ықтималдықтарға да байланысты болады. Егер кірудегі *и* таңбалар көлемі m_1, ал шығудағы таңбалар υ көлемі m_2 болса, онда

$$H_U(V) = -\sum_{i=1}^{m_1} \sum_{j=1}^{m_2} p(v_j u_i) \log p(v_j / u_i). \qquad (4.19)$$

(4.18) және (4.19) өрнектерін (4.17) қойып және біршама түрлендіруден кейін мынаны аламыз:

$$I(V,U) = -\sum_{i=1}^{m_1} \sum_{j=1}^{m_2} p(v_j u_i) \log \frac{p(v_j u_i)}{p(v_j) p(u_i)}. \qquad (4.20)$$

Кедергілі арнадағы ақпаратты жіберу жылдамдығы

$$\overline{I}(V,U) = V_T \sum_{i=1}^{m_1} \sum_{j=1}^{m_2} p(v_j u_i) \log \frac{p(v_j u_i)}{p(v_j) p(u_i)}. \qquad (4.21)$$

Арнаның берілген техникалық сипаттарында манипуляциялау V_T жылдамдығы мүмкін болған шекте деп, мына $I(V,U)$ мәнін максималдау мүмкін;

бұл арна кіруіндегі арнаның кодерінде (түрлендірушісінде) таңбалар тізбегінің санақтық қасиетін өзгерте отырып орындалады.

Мұнда арнамен ақпарат ұзату жылдамдығының қол жеткізілетін шекті мәні

$C_Д$ – кедергілі дискретті байланыс арнасының ***өткізу қабілеті*** деп аталады.

$$C_Д = \max_{p(u)} V_T \bar{I}(VU), \tag{4.22}$$

мұнда $p\{u\}$ – кіру сигналдарының ықтималдықтарының таралуының мүмкін болған жиыны.

Кедергі бар болғанда арнаның өткізу қабілеті бір уақыт өлшемінде арнамен өтетін ең үлкен ақпарат санын көрсетеді; олар қателіктің қалағанша кіші ықтималдығымен өтеді.

Амалда бұл өткізу қабілетіне жету мүмкін бе?

Хабар көзінің әріптерінің эргодикалық тізбегін ұзын жиынтықтармен кодтайтын болайық; ондағы жиынтық ұзындығы үшін ұзын тізбектердің тең ықтималдықты ассимптотикалық теоремасы орынды болсын.

Осында айтатын жай, қателіктің қалағанша кіші ықтималдығын тек жиынтықтардың шексіз арттыру жолымен ғана алса болады.

Алайда кодталатын жиынтықтарды ұзартқанда кодтаушы және декодтаушы құрылымдардың техникалық орындалуы артады және хабарларды жіберуде жиынтықтағы әріптерді жинақтау үшін көп уақыт кету себебінен үлкен іркілістер пайда болады.

Амалда кодттаудың мүмкін болған күрделіліктерінде екі түрлі мәселе қойылады: **біріншісінде,** ақпаратты берілген жіберу жылдамдығында қателіктердің ықтималдығын минималдау мәселесі шешілсе, ал **екінші** мәселеде, берілген қателіктердің ықтималдығында жіберу жылдамдығын өткізу қабілетіне жақындату мәселесі шешіледі.

Арнаның барлық мүмкіншіліктері еш уақытта толық істетілмейді.

Оның жүктелу дәрежесі ***арнаның істетілу еселігімен*** сипатталады:

$$\lambda = \bar{I}(Z) / C_Д . \tag{4.23}$$

мұнда $\bar{I}(Z)$ – хабар көзінің өнімділігі; $C_Д$ – байланыс арнасының өткізу қабілеті.

Егер мына шарттар орындалса, арнаның қалыпты істеуі мүмкін болады:

- егер хабар көзінің өнімділігі мына шектерде болса: $0 \le \bar{I}(Z) \le C_Д$;
- арнаның істетілу λ еселігі 0 ден 1- ге дейін болса.

4.4 ***Зертханалық жұмыс***

Екілік симметриялы арнаның өткізу қабілетін табу керек; мұнда ондағы манипуляциялау жылдамдығы V_T берілген және ұзатылатын таңбалар өзара байланысты емес.

Шешімі: (4.19) өрнегін келесідей жазамыз:

$$H_U(V) = -\sum_{i=1}^{2} p(u_i) \sum_{j=1}^{2} p(v_j u_i) \log_2 p(v_j / u_i).$$

Графтағы таңбалеулерді қолданып (4.5-сурет), мынаны жазса болады:

$$H_U(V) = -p(0)\left[(1-p)\log_2(1-p) + p\log_2 p\right] - \\ - p(1)\left[p\log_2 p + (1-p)\log_2(1-p)\right] =$$

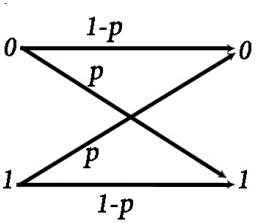
$p(0) + p(1) = 1$; осындай болғандығы себепті келесідей болады:

$$H_U(V) = -p\log_2 p - (1-p)\log_2(1-p).$$

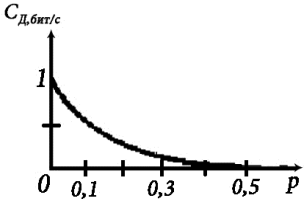
Мына мән $H_U(V)$ кіру таңбаларының ықтималдығына байланысты емес; ол арнаның симметриялы екендігінің салдарынан болады.

Сондықтан, өткізу қабілеті

$$C_Д = V_T\left[\max H(V) + p\log_2 p + (1-p)\log_2(1-p)\right] \quad \text{болып,}$$



4.5-сурет



4.6-сурет

таңбалардың ықтималдықтары тең болғанда $H(V)$ максимумға жетіп, 1-ге тең болады. Осыдан:

$$C_Д = V_T\left[1 + p\log_2 p + (1-p)\log_2(1-p)\right]. \qquad (4.24)$$

Дискрет екілік симметриялы арнаның өткізу қабілетінің p на байланыстылығы 4.6-суретте көрсетілген. Осы суретте таңбалардың

транформация ықтималдығы 0 ден ½ көбейгенде, өткізу қабілеті $C_Д(p)$ 1- ден 0- ге дейін кемейетінін көреміз.

Егер $p = 0$ болса, онда арнада шуыл болмайды және оның өткізу қабілеті 1- ге тең болады. Ал $p = 1/2$ болғанда арнаның өткізу қабілеті нөлге тең болып, арна пайдасыз болады.

4.3 Үздіксіз хабар көзінің ақпараттық сипаттары; үлгілері, жіберу жылдамдығы

Үздіксіз хабар көзінің өнімділігі; эпсилон энтропия

Үздіксіз хабар $z_T(t)$ деп ұзындығы T- ға тең болған кездейсоқ үдерістің қандай да бір орындалуын айтамыз.

Үздіксіз хабар көзі оның нақты мәндерінің ансамблімен сипатталады.

Үздіксіз хабар үлгісі көбінесе эргодикалық кездейсоқ үдеріс түрінде көрінеді. Үздіксіз хабар көзінің өнімділігін анықтау үшін кездейсоқ шаманың ε-энтропия анықтамасын қолданамыз.

Үздіксіз хабар көзінің ***ε-өнімділігі $H_ε(z)$ - кез келген*** $z_T(t)$ орындалу мәнін берілген ықтималдық ε-мен қайта тіктеу үшін керек болған минималды ақпарат өлшемі болып, оны ақпарат көзі бірлік уақытта құруы керек болады.

Айталық, $z_T(t)$ $u_T(t)$ орындалу мәнімен қайта тіктеледі.

Бақылынатын нақты мәндерді жетерлі дәрежеде кең F шекараланған спектрі бар сигналдар деп қарастыруымыз керек.

T ның жетерлі дәрежеде үлкен болған ұзындығында $z_T(t)$, сондайақ $u_T(t)$- да N-өлшемді ($N = 2FT$) векторлар $(z_1, z_2, ..., z_N)$ және $(u_1, u_2, ..., u_N)$ деп, олардың кеңістік өлшемдері болып санақтар көрінеді.

$\{z_T(t)\}$ хабарларының және $\{u_T(t)\}$ тіктеуіш сигналдардың ансамблдері N-өлшемді кездейсоқ векторлармен Z және U сипатталып, олардың құраушылары Z_1, Z_2, .., Z_N және U_1, U_2, .., U_N кездейсоқ шамалар болады.

Ансамблдің әрбірінің санақтық анықтамасы N-өлшемді ықтималдықтардың таралу нығыздығымен $p(Z) = p(z_1, z_2, ..., z_N)$ және $p(U) = p(u_1, u_2, ..., u_N)$ беріледі. Ансамблдер арасындағы байланыстарды шартты таралу нығыздығы көрсетеді:

$p_u(Z) = p(z_1, z_2, ..., z_N / u_1, u_2, ..., u_N)$ және $p_z(U) = p(u_1, u_2, ..., u_N / z_1, z_2, ..., z_N)$,

сондай-ақ ықтималдықтар таралуының біргелікті нығыздығымен көрсетіледі: $p(Z,U) = p(z_1, z_2, ..., z_N; u_1, u_2, ..., u_N)$.

N-өлшемді кездейсоқ Z және U векторлары біріне салыстырғанда екіншісі үшін ақпарат көлемі келесідей:

$$I(Z,U) = \int_{ZU} \int p(Z,U) \log \frac{p(Z,U)}{p(Z)p(U)} dZdU \quad . \quad (4.25)$$

Мұнда интегралдар N- өлшемді болады.

Ортаквадраттық шындық $\theta(Z,U)$ шарты осы мысалда келесідей:

$$\theta(Z,U) = \int_Z \int_U p(Z) p_z(U) \rho(Z,U) dZdU \ ,$$

мұнда $p(Z,U)$ ZU арақашықтықтың $l(Z,U)$ квадраты болып, N - өлшемді эвклидтің кеңістігінде өлшенеді.

$Z_T(t)$ және $U_T(t)$ дискреттелген сигналдардың бір санағына тура келетін ақпарат саны келесідей табылады:

$$I(Z,U) = \frac{1}{N} \int_Z \int_U p(Z,U) \log \frac{p(Z,U)}{p(Z)p(U)} dZdU \ .$$

Үздіксіз хабарлар көзінің ε-пропорционалдық анықтамасына сәйкес $H_\varepsilon(Z)$ келесідей болады: $H_U(Z) = v \min_{T \to \infty} \bar{I}(VU)$. (4.26)

Мына шарт орындалғанда: $\theta(Z,U) \le \varepsilon^2$, хабар көзінің санақтарды қалыптастыру v жылдамдығы: ($v = 2F$) болады.

4.4 Үздіксіз байланыс арнасының өткізу қабілеттілігі. Үздіксіз байланыс арнасының үлгілері

Үздіксіз сигналдарды тасушы арналар ***үздіксіз арналар*** деп аталады.

Осы кезде радиохабарлар, телефондық хабарлар, телекөрсетулер ж.т.б.лар үздіксіз арналармен таратылады.

Нақты үздіксіз арналар күрделі екпінділік сызықсыз нысандар болып, сипаттамалары уақыт аралығында кездейсоқ түрде өзгереді.

Көптеген үлгілер жаратылған болып, ең кең таралған түрі – бұл ***гаусстық арналардың*** әр түрдегі көріністері.

Гаусстық арна деп нақты арнаның келесідей шектеулердегі математикалық үлгісіне айтамыз:

1. арнаның негізгі физикалық параметрлері мәлім болған детерминделген шамалар болады;

2. арнаның өткізу жолағы F_K герц жолақпен шектелген;

3. арнада аддитивті гаусстық ақ шуыл әсер етеді - қуаты шектелген аддитивті флуктуациялық кедергі болып, оның жиілік спектрі біртегіс, ал амплитудаларының таралуы қалыпты заңға бойсынады.

Сондай ақ арнамен жіберілетін сигналдардың орташа қуаты тұрақты, сигнал мен кедергі арасындағы санақтық байланыстар жоқ, сигнал мен кедергілердің спектрлері арнаның өткізу жолағымен шектелген.

Үздіксіз арнамен ақпарат жіберу жылдамдығы

Арнаның өткізу жолағы әрқашан шектелген болғандығынан үздіксіз хабарларды әжептеуір үлкен T уақыт аралықтарында мәлім қателікпен санақтар тізбегімен көрсетсе болады. Санақтар арасындағы кооряляциялық байланысты және кедергіден болатын тіктеудегі шекті шындықты есепке ала отырып, дискрет сигналдың орташа ақпарат ұзату жылдамдығы $\bar{I}(VU)$ келесідей болады:

$$\bar{I}(VU) = I(VU)/T \ , \qquad (4.27)$$

мұнда $I(VU)$ (4.25)- ке ұқсас өрнекпен анықталады.

$T \to \infty$ болғанда N - өлшемді таралуы шексіз өлшемдіге айналады және үздіксіз арнамен ақпаратты ұзату жылдамдығын анықтайды.

$T \to \infty$ шекке өту $i \quad \bar{I}(VU) = \lim_{T\to\infty} \bar{I}(VU)$ жылдамдықты барлық мүмкін болған сигналдар бойынша орташалауды білдіреді.

Мәлім болған санақтық сипаттамасы бар кедергілердің әртүрлі кіру сигналдарының ансамблдеріне көрсеткен зиян дәрежесі әртүрлі болады. Сондықтан ақпаратты жіберу жылдамдығы да әртүрлі болады.

Үздіксіз байланыс арнасының өткізу қабілеті

Техникалық сипаттары мәлім болғанда үздіксіз арнамен максималды мүмкін болған өткізу жылдамдығы ***үздіксіз арнаның өткізу қабілеті*** *деп аталады:*

$$C_H = \max_{\{p(u)\}} \bar{I}(VU). \qquad (4.28)$$

Мұнда максимумды кіру сигналдарының барлық мүмкін ансамблдерінен табады. Гаусс арнасы үшін ақпаратты жіберу жылдамдығын табайық.

Айталық Гаусс арнасымен үздіксіз $u_T(t)$ сигналы қуаты P_u, дисперсиясы σ_u^2 болған $\{u_T(t)\}$ ансамльдің ішінен алынған болсын; арнаның шығуында $\{v_T(t)\}$ ансамблінен алынған сигнал $v_T(t)$ болып, ол орташа қуаты $P_\xi (P_\xi = \sigma_\xi^2)$ болған $\xi(t)$ кедергісімен бұзылған болсын.

Мұнда $u_T(t)$ сигналының ұзындығы жетерлі дәрежеде үлкен болып, мүмкін болған орындағы қателікпен $u_m(t)$ және $v_m(t)$ ларды $\Delta t = 1/(2F_к)$ аралықтары арқылы алынған санақтар тізбегімен ауыстыру мүмкін болсын; мұнда $F_к$ - арнаның өткізу жолағы.

(4.17)- ге сәйкес $v_T(t)$ сигналымен берілетін орташа ақпарат саны үшін өрнек мына түрде болады: $I(V,U) = H(V) - H_U(V)$, (4.29)

мұнда $H(V)$ және $H_U(V)$ – N - өлшемді кездейсоқ вектор V болып, оның құраушылары $V_1, V_2, ..., V_N$ кездейсоқ шамалар болады.

Арнадағы кедергі аддитивті және кірудегі сигналмен санақтық байланыста болмағандықтан келесідей теңдік орынды болады:

$$H_U(V) = H_U(U + \Xi) = H(\Xi). \qquad (4.30)$$

Осы теңдіктегі $H(\Xi)$ N - өлшемді кездейсоқ Ξ кедергінің энтропиясы болып, оның құраушылары $\Xi_1, \Xi_2, ..., E_N$ кездейсоқ шамалар болсын.

Осында ақ шуылдың санақ мезгілдеріндегі мәндері корреляцияланбаған деп, мынаны аламыз:

$$H(\Xi) = 2F_k Th(\xi) . \qquad (4.31)$$

Мұнда $h(\xi)$ – кедергінің бір санағындағы **дифференциалдық энтропиясы.** Егер кедергі қалыпты заңмен таралған және дисперсиясы σ^ξ болса, онда оның **дифференциалдық энтропиясы** келесідей болады:

$$h(\xi) = \log \sigma_\xi \sqrt{2\pi e} = \frac{1}{2} \log 2\pi e P_\xi \quad . \qquad (4.32)$$

Мұндайда $u_T(t)$ теңдеуінің санақты мәндері байланыссыз деп санаймыз. Оларға кедергілердің байланыссыз мәндері әсер еткенде, шығу $V_T(t)$ сигналдарының санақты мәндері де байланыссыз болады.

Онда $H(V)$ны шығу сигналының бір санағының дифференциалдық $h(V)$ энтропиясы арқылы жазса болады:

$$H(V) = 2F_k T h(V). \tag{4.33}$$

(4.32) және (4.33)- ді мынаған (4.29) қойып, мынаны аламыз:

$$I(VU) = 2F_k T\left[h(V) - \frac{1}{2}\log 2\pi e\sigma_\xi^2\right]. \tag{4.34}$$

Сонымен үздіксіз арнамен ақпараты жіберу жылдамдығы келесідей болады:

$$I(VU) = 2F_k T\left[h(V) - \frac{1}{2}\log 2\pi e\sigma_\xi^2\right]. \tag{4.35}$$

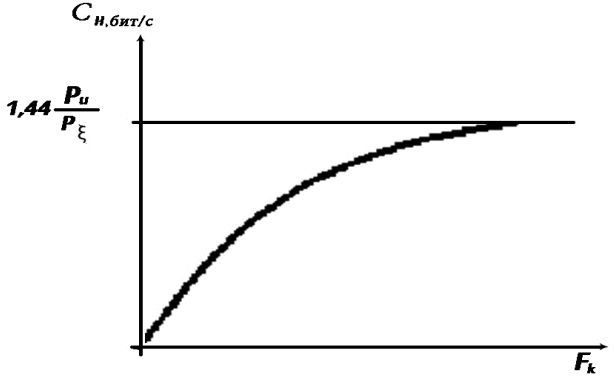
Гаусстық арнаның өткізу қабілетін табу үшін ақырғы өрнектегі $h(V)$ ны максимумға жеткізетін кіру сигналдарының ансамблін табамыз.

Шығудағы сигналдар кірудегі сигналдар мен кедергілерді қосу нәтижесінде табылады; ал олардың орташа қуаты шектелгендігі себепті шығудағы сигнал қуаты да шектелген болады.

Осындай сигналдар үшін ***h(V) ның ең үлкен шамасына V қалыпты заңмен таралған*** жағдайда ғана қол жеткізуге болатынын жоғарыда көргенбіз. Сондай ақ екі қалыпты заңмен таралған кездейсоқ шамаларды қосындысы да қалыпты заңмен таралған болып, оның ***дисперсиясы қосылушыларың дисперсияларының қосындысына*** тең болады.

Осыдан, егерде қалыпты заңмен таралған ξ кедергіде кірудегі u сигналы тек қалыпты заңмен таралған жағдайда ғана шығудағы V сигналы қалыпты заңмен таралған болады.

$h(V)$-ның энтропиясының ең үлкен мәніне, сондай ақ, ақпараттың ***максималды ұзату жылдамдығына тек қалыптыланған орташаланған кездейсоқ сигналдарды қолданғанда ғана*** қол жеткізуге болады.



4.7-сурет

Орташа қуат берілген болса, сигналдың орташаланғандығы дисперсияның максимал мәніне сәйкес келеді.

Олар да *біртегіс таралған* және *кең энергетикалық спектрге ие* болуы керек; себебі тек осы жағдайда ғана санақтардың байланыссыздығы туралы сөйлессе болады.

Мұндай жағдай ***шуылға ұқсас*** сигналдарды қолданғанда ғана болады. Мұнда дифференциал энтропияның максимал шамасы:

$$h(V) = -\log 2\pi e\left(\sigma_u^2 + \sigma_\xi^2\right) = \frac{1}{2}\log 2\pi e\left(P_u + P_\xi\right).$$

(4.36) өрнегін (4.35)-ке қойып, гаусстық арнаның өткізу қабілетін көрсететін өрнек аламыз:

$$C_H = F_k\left[\log 2\pi e\left(P_u + P_\xi\right) - \log 2\pi e P_\xi\right] = F_k \log\left(1 + P_u / P_\xi\right). \qquad (4.37)$$

Гаусс арнасында өткізу қабілеті өткізу F_K жолағына қандай байланысты болатынын қарастырайық.

Ақ шуылдың спектрінің біртегістігін есепке ала отырып, оның қуатын P^ξ бірлік жиілікке сәйкес келетін P_0 меншікті қуаты арқылы өрнектейміз. Онда ақырғы (4.37) өрнегі мына түрге келеді:

$$C_H = F_k \log_2\left[1 + P_u /\left(P_0 F_k\right)\right].$$

Арнаның өткізу жолағын шексіз кеңейткенде оның өткізу қабілеті C_M мен шектелген болады: $C_M = \lim\limits_{F_k \to \infty} C_H = \lim\limits_{F_k \to \infty} \dfrac{\log_2\left[1 + P_u /\left(P_0 F_k\right)\right]}{1/F_k}$.

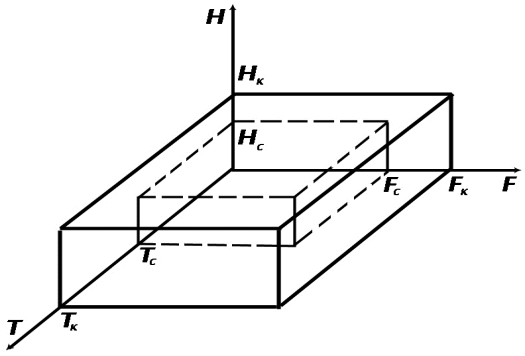
Келесідей таңбалап $\gamma = 1/F_k$, Лопиталь ережесімен $C_н$ шегін $\gamma \to 0$ болғанда табамыз: $C_M = 1{,}443 P_u / P_0$.

$C_н$ нің өткізу жолағының еніне F_K байланыстылығын 4.7-суреттен көрсе болады.

4.5 Байланыс арнасымен сигналдың физикалық сипаттарының келісуі; сигнал көлемі мен байланыс арнасының сиымдылығы.

Берілген арна мәлім бір физикалық параметрлерге ие болып, осыларға сигналдың өткізу қабілеті байланысты болады.

Қолдану шарттарына байланысты болмаған түрде үздіксіз арна үш негізгі параметрлерімен сипатталады: сигналды ұзату уақыты - $T_к$, сигналды өткізу жолағының ені - F_K және арнадағы кедергінің деңгейінен сигналдың артып кетуі мүмкін болған шамасы - $H_к$. Осы шама логарифмдік өлшемде арнадағы максималды мүмкін болған $P_{u\,max}$ сигнал мен кедергі деңгейінің P^{ξ} айырмасымен



4.8-сурет

өлшенеді. Сымды арналар үшін артып кету шамасы сым қорғауын бұзып кету кернеуімен және көлденең кедергілер деңгейімен өлшенеді; ал радиоарналарда тиісті қашықтықтарда сигналды анықтай алу мүмкіндігімен өлшенеді.

Арнаның аталған үш негізгі параметрлерінің көбейтіндісі ***арнаның көлемі*** (***сыймдылығы***) деп аталады және келесідей *таңбаланады* V_K:

$$V_k = T_k F_k H_k \ . \qquad (4.38)$$

Сигналды арнамен жіберуді бағалауда да сигналдың негізгі үш параметрлері шектеледі: оның уақыт бойынша ұзындығы - T_c, спектрінің ені - F_c, және сигналдың кедергіден артып кетуі- H_c.

Мұнда $H_\varepsilon = \log\left(P_u / P_\xi\right)$ болады; P_u - жіберілетін сигналдың орташа қуаты; ал P^{ξ} - арнадағы кедергінің орташа қуаты.

Параметр H_c сигнал жіберуші құрылымдар мен сигнал жіберу қашықтығына байланысты болады. Осы шама қаншалықты көп болса, соншалықты қателіктердің ықтималдығы аз болады.

Арнаның көлемі сияқты ***сигналдың*** да ***көлемі*** V_c ***(сыймдылығы)*** деген түсінік ендіріледі: $V_c = T_c F_c H_c$. (4.40)

Сигналдың көлемі де, арнаның көлемі де үш өлшемді кеңістікте *T, F, H* кеңістік өлшемдерімен көрсетіледі (4.8-сурет). Осы арна бойынша сигнал бұзылмастан өтуі үшін мына шарт орындалуы керек:

$$V_c \le V_k \tag{4.41}$$

Бұның үшін мына шарттар орындалуы керек болады:

$$T_c \le T_k, F_c \le F_k, H_c \le H_k . \tag{4.42}$$

Егерде арнаның өткізу жолағы сигналдың спектрінен кем болса, осы сигналды уақыт бойынша ұзындығын ұзарту арқылы оның спектрін кемейту мүмкін болады. Мұнда сигнал көлемі өзгермейді.

Амалда бұны орындау қиын емес; сигналды магнит лентасына жазуда жоғары жылдамдықта жазып, оны оқығанда баяу оқу керек болады.

Сонда оның спектрі арнаның өткізу жолағына тең болуы керек. Ал егер арна кең жолақты болып, оның істеу уақыты кем болса, онда сигналдың спектрін кеңейту керек. Бұл тәжірибеде сигналды магнит лентасына баяу жазып, жылдам оқумен сигналдың спектрін кеңейтсе болады.

Ал арнада сигналдың кедергіден артып кету мүмкіндігі кем болса, онда мұны сигналдың уақыт бойынша ұзындығын арттыру немесе көп рет қайталау жолымен орындаса болады. Басқа да сигналды түрлендіру жолдары болуы мүмкін.

Ал енді арнаның көлемі мен ол арқылы өтетін ақпараттың мөлшері арасында қандай байланыс бар?

(4.37) өрнегіне сәйкес $T_к$ уақытында байланыс арнасымен ***жіберілетін ақпараттың шектік саны*** келесідей болады:

$$I_{\max}(V,U) = T_k F_k \log(1 + P_u / P_\xi).$$

Осыдан келесідей шешімге келсе болады; $P_u/P^{\xi} >> 1$ болғанда, сигналды түрлендіру жолымен арнаның физикалық мүмкіндіктерін толық қолдану мүмкін болады; онда осы ***сигналдан алынатын ақпараттың максимал саны арнаның сиымдылығына жақын*** болады:

$$I_{\max}(V,U) = V_k = T_k F_k \log(1 + P_{u\max} / P_\xi).$$

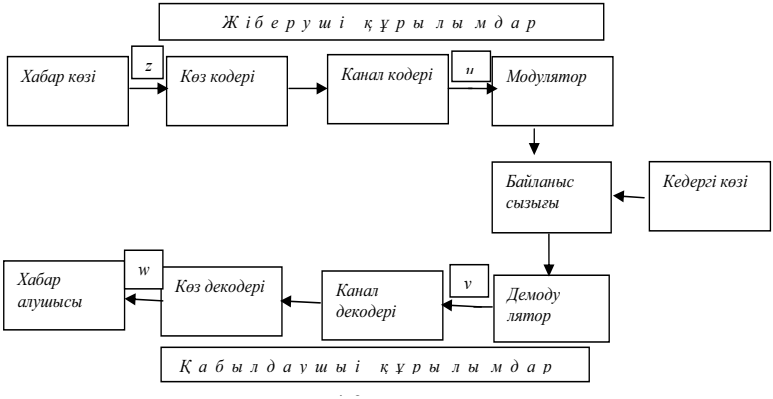
4.5.1 Хабар көзі мен байланыс арнасының санақтық қасиеттерін келістіру

Хабар көзі мен байланыс арнасының санақтық қасиеттерін келістіру ақпарат ұзатудың сипатын жақсарту мақсатында жүргізіледі. Мұнда сипатты бағалау үш көрсеткіш бойынша орындалады: шындық көрсеткіші, орташа ұзату жылдамдығы және жүйенің техникалық орындалу күрделілігі болып, ақырғысы жүйенің бағасы және сенімділігімен анықталады.

Амалда техникалық орындалуының күрделілігі шешуші қызмет атқарғанымен, көбінесе, жүйені шектік мүмкіншіліктерін анықтау да керек болады; мұндайда бірінші екі көрсеткішпен шектелген жөн.

Дискрет арнаның шындығы (достоверность) жеке алынған таңбаның (элементар сигнал) қате қабылдану ықтималдығымен өлшенеді.

Үздіксіз хабарды ұзатуда шындықты табу хабарды тіктеудің



4.9-сурет

ортаквадраттық қателігінің мәнімен өлшенеді:

$$M\left[\varepsilon^2\right] = M\left[\left(w(t) - z(t)\right)^2\right].$$

Мұнда $w(t)$ — арнаның шығуындағы хабар; $z(t)$ — арнаның кіруіндегі хабар.

Шындық ақпараттық жүйенің кедергіге шыдамдылығын сипаттайды.

Егерде ұзатушы жүйеде ұзату жылдамдығы мен үлкен шындыққа талап қойылмаса, онда хабар көзі мен байланыс арнасының санақтық сипаттарын келістіру өте қажетті емес.

Хабарды сигналдарға айналдыруда екі мақсат қойылады:

біріншісі, үздіксіз хабарды дискрет түрге келтіру (кодтау) және оның кедергіге шыдамдылығын арттыру; бұл үздіксіз-сандық түрлендірушілермен амалға асырылады.

Ал **екіншісі,** оған рұқсатсыз қол жеткізбеуді амалға асыру. Бұл түрлендіру ***шифрлеу*** деп аталады. Ол екілік таңбалар деңгейінде немесе әріптер (белгілер) деңгейінде орындалуы мүмкін.

Осындай санақтық келісудің қажеті болмаса, онда жүйенің істеу сипатын арттыру дискрет арна үшін модулятордың кіруінен демодулятордың шығуына дейін орындалады.

Модуляторға түсетін таңбалар тең ықтималды және олардың арасындағы байланыс жоқ деп есептеледі.

Қуат пен жиілік тарапынан берілген шектеулерге толық жауап

беретін және аддитивті гаусс кедергісі әсер ететін сигналдардың ішінен ең жоғары шындық беретін жеке таңба табылады.

Сонымен бір уақытта тиімді қабылдаушының құрамы да анықталады. Мұндай мәселелер екілік жүйедегі дискрет арналары үшін толық шешілген.

Ақпаратты ұзату жүйесінің нәтижелігі мен кедергіге шыдамдылығын арттыруды, Шеннон көрсеткендей, байланыс арналарына кодттаушы және декодтаушыларды ендірумен орындаса болады; ондағы мақсат – хабар көзі мен байланыс арнасын санақтық келістіру.

Шеннон дәлелдеген теоремада келесідей деген:

Байланыс арнасының өткізу қабілетіне кез келгенше жақын болған ақпаратты ұзату жылдамдығына қол жеткізу мүмкін болатын тиімді кодтау әдісін тапса болады.

Мұнда кодтау әдісі деп хабарларды сигналдарға түрлендіру амалдары және керісінше, сигнал мен кедергілердің қоспасын сигналға түрлендіру түсініледі.

Өкінішке орай аталған теоремалар тиімді кодтау әдістерінің орындалуы жолдарына сай ***ұсыныстар бермейді***.

Сол себепті байланыстың (тиімдіды) тиімді жүйесінің құрылысы мен арна үлгілері біршама оңтайланғанымен де, ***осы күнге дейін бұл мәселе толық шешілмеген.***

Мәселені оңайлату үшін ***жүйені тиімділеуді бөлшектеп жүргізеді***;

мұнда арнаның «модулятор-демодулятор» бөлігі үшін ең жақсы код табылады.

Сонымен бірге **хабар көзінің** санақтық қасиеттерін есепке алатын кодтау шарасын бір бөлек, ал **байланыс арнасының** санақтық қасиеттерін есепке алатын кодтауды басқа бір бөлек жүргізіледі.

Бұл кодтаушы және декодтаушы құрылымдарды екіге бөліп қарауға мүмкіндік береді**: *хабар көзінің кодтаушысы - ХКК, арнаның кодтаушысы - КК, хабар көзінің декодтаушысы - ХКД, арнаның декодтаушысы - КД.***

Егер дискрет хабар көзінің артықшылығы болмаса, ал арна кедергілі болса, онда хабар көзінің кодерінің керегі болмайды.

Мұнда арнадағы хабарға артықшылық ендіріп, қателіктің әсерін максимал дәрежеде кемейту керек болады; мұнда арнадағы кедергінің санақтық қасиеттеріне қарай отырып, артықшылық ендіріледі.

Шеннонның кедергілі дискретті арнаға арналған теоремасынан күтпеген әрі орнықты келесідей қорытынды шығады;

- арнадағы кедергілер өткізу шындығына ешқандай шектеу қоймайды. Ал ***шектеу тек қана өткізу жылдамдығына*** қойылады; мұнда ***кез келгенше үлкен шындыққа қол жеткізсе болады.***

Жылдамдық кедергілі дискрет арнаның өткізу қабілетінен аспауы керек. Сонда артықшылығы жоқ хабарға шындықты арттыру үшін **қосылатын артықша ақпарат** оншалықты көп емес болып, ол кедергілер әсерінен болатын **ақпараттың жоғалған бөлігіне тең** болады.

Жіберудің әжептеуір шындығын арттырудың техникалық орындалуы арнаның кодері мен декодері арқылы амалға асырылады.

Осындай кодтау ***кедергіге орнықты (помехоустойчивое кодирование) кодттау*** деп аталады.

Жалпы жағдайда, хабар көзінің құрған хабарларында артықшылық бар болса және арнада кедергі бар болса, онда хабар көзінің кодері мен декодерін ендірген жөн болады; ал арнада оның кодері мен декодерін бөлек түрде ендірген дұрыс болады.

Көпшілік жағдайларда хабарлардың артықшылығы арнадағы кедергінің статистикаларына байланысты болмайды. Сондықтан көп жағдайда хабарларды алдын нәтижелі кодтаумен кодтап, кейін кедергіге шыдамды кодпен кодтайды; яғни ***хабар екі рет кодталады***.

Кедергісіз арнамен үздіксіз сигналды жіберу теориялық планда қарастырылмайды. Сондықтан, үздіксіз хабар көзінің үздіксіз кедергілі арнамен санақтық келістіруді қарастырайық.

Ақпаратты ұзатудың шекті мүмкіндіктері **Шеннонның мына теоремасымен** анықталады:

- үздіксіз хабар көзінің ε-өнімділігі $\overline{H}_{\varepsilon}(Z)$ ***үздіксіз арна көзінің өткізу қабілетінен*** C_u ***аспайды; онда кез келгенше бірге жақын ықтималдықпен қандайда бір жіберу әдісін тапса болатын болып, мұнда қабылданған кез келген хабардың жіберілген хабардан тек қайта тіктеу шындығының бағасы аумағындай ғана айырмашылығы болады.***

Бұған кері болған төмендегідей қағида да бекітілген.

Келесідей шартта, $H_{\xi}(Z) > C_u$ ***хабарды ұзатуды ешқандай әдіспен орындап болмайды.***

Осыны дәлелдеместен сигналдардың геометриялық түрін қолданып осындай жіберу әдісін түсіндірейік.

Егер хабар анық бір шындықпен тіктелуі керек болса, онда шексіз көп ұзындығы T-ға тең болған үздіксіз хабарлардың ішінен тек тіктеуші хабарлардың санақты жиынын жіберу керек болады.

Онда кодтау үдерісі келесідей болады; хабар көзінен алынған хабарға ең жақын болған тіктеуіш табылып, оған рұқсат етілген сигналдар жиынынан айқын сигнал таңдауда кедергінің әсері есепке алынады.

Ал декодтауда қабылданған сигнал ең жақын рұқсат етілген сигналмен теңестіріледі.

Егерде қабылданған сигнал векторының ұшы гильберт кеңістігінде осыған тиісті рұқсат етілген сигналдың меншікті аймағына түсетін болса, осындай жағдайда қателік болмайды.

Осы аймақтың өлшемдері кедергінің орташа қуатына тең болады.

Бұл шарт рұқсат етілген векторлардың ұштарының ара қашықтығына шектеу қояды. Сөйтіп, ұзатылатын сигналдардың орташа қуатының деңгейіне сәйкес келетін гиперсфераның бетіне рұқсат етілген сигналдардың тек шектелген саны ғана сиятын болады. Осы сан шекті ұзату жылдамдығын көрсетіп, мұнда тиісті шындық дәрежесі қамтамасыз етіледі.

Кедергінің кез келген дәрежесі болуы мүмкін болғандықтан, басқа рұқсат етілген сигналдың тіктелу ықтималдығы нөлге тең болмайды.

Алайда ұзатылатын сигналдың ұзындығы шексіз артқанда ол ықтималдық нөлге ұмтылады.

4.5.2 Үздіксіз хабарлардың энтропиясы және оның максимумын табу.

Көп жағдайларда хабарлар үздіксіз түрде болады; дыбыстық хабарлар (радио, телефон, теледидар, т.б.). Мұндай жағдайда олардың энтропиясы қалай табылады?

Егер үздіксіз хабар оның дискрет $x_1, x_2, ..., x_n$ нүктелерімен ауыстырылса және олардың элементар ықтималдығы $P_k = \omega(x_k)\Delta x$ деп таңбаласақ, онда энтропияны келесідей есептейміз:

$$H = -\sum_{k=1}^{m} \omega(x_k)\Delta x \log\{\omega(x_k)\Delta x\} = -\sum_{k=1}^{m} \omega(x_k)\Delta x \log \omega(x_k) - \sum_{k=1}^{m} \omega(x_k)\Delta x \log \Delta x .$$

Екінші интегралда $\int_{-\infty}^{\infty} \omega(x_k)dx = 1$ болғандығы үшін екінші қосындыдан тек мынау қалады:

$H^* = \int_{-\infty}^{\infty} \omega(x_k) \log \omega(x_k)dx - \log \Delta x$. Сонда ***келтірілген энтропия*** келесідей болады: .

Келтірілген энтропияда оң жақтағы қосылғыш дискреттеу қателігін көрсетеді. Егер Марков сигналдарында дискреттеу қадамын Котельников бойынша тапсақ, онда $\Delta x = 1$ деп алса болады; мұндай жағдайда қателік болмайды.

Мұндай шарт сигналдың ең жоғарғы гармоникасындағы синусойданың амплитудасы оның кезеңінің жартысына тең болғанда орындалады. Ал бұл тек Котельников шарты орындалғанда мүмкін болады [автор].

4.1 ***Зертханалық жұмыс*** Кездейсоқ үздіксіз сигналдың дисперсиясы шектелген және $D_x = \sigma^2 = const, M_x = 0$ тең болсын.

Кездейсоқ үздіксіз сигналдарды қалай тиімділеу (оңтайландыру) керек.

Шешімі:

Олардың таралу теңдеуін таңдап алумен олардың энтропиясын максималдауға болады.

Сигналдың дисперсиясы шектелген және $D_x = \sigma^2 = const, M_x = 0$ тең болғанда, зерттеудің ***қорытындысы*** мынаны көрсетеді:

1. Егер үздіксіз кездейсоқ сигналдың қуаты $D_x = \sigma^2 = const, M_x = 0$ шектелген болса, онда **энтропия максимал** болуы үшін оның амплитудасының таралу теңдеуі **қалыпты** болуы керек.

2. Кедергінің орта қуаты берілген болса, онда ол **максимал нәтижелі** болуы үшін оның амплитудасының таралу заңы **қалыпты** болуы керек.

Осы заңдылықтарда солардың энтропиясын табайық:

1. Қалыпты заң үшін энтропия келесідей болады: $H_n(X) = \log\left(\frac{\sigma}{\Delta x}\sqrt{2\pi e}\right)$.

4.2 ***Зертханалық жұмыс***

Кездейсоқ үздіксіз сигналдың дисперсиясы **сигнал қуаты** $[a,b]$ аралығында **шектелмеген** болса: $D_x = \infty, M_x = 0$.

Шешімі: Онда **энтропия максимал** болуы үшін оның амплитудасының таралу теңдеуі сол аралықта **біркелкі таралған** болады және оның таралу теңдеуі келесідей болады: $\omega(x) = \frac{1}{b-a}$.

Мұндай жағдайда **кедергі нәтижелі** болуы үшін оның амплитудасының таралу теңдеуі **біркелкі** болуы керек, яғни $\omega(x) = \frac{1}{b-a}$ болады.

Осы заңдылықта солардың энтропиясын табайық:

2. Амплитудасының біркелкі таралған заңды сигналдың энтропиясы: $H_d(X) = \log\frac{b-a}{\Delta x}$ болады.

4.5.3 Арналарды хабарлармен санақтық келістіру. Хабардың таралу заңын өзгертумен оны оңтайландыру

Үздіксіз хабардың энтропиясы және тығыздық қатыстары келесідей болсын: $H(X), \omega(x)$.

Бұл сигналды оңтайландыру үшін оның тығыздық теңдеуін тиімді түрге келтіру керек; мысал үшін қалыпты заңға немесе соған жақын квадраттық $\psi(y)$ қатысқа келтіру керек; мұнда сигналдың энтропиясы да келесідей өзгереді: $H(X) \to H(Y), H(Y) > H(X)$ болады.

Мұнда қисық сызықты түрлендіруші істетіліп, оның өткізу теңдеуі қисық сызықты дәл біз іздеген қатысқа жақын немесе тең болады; яғни $y = F(x)$. Осыған кері қатыс құрамыз: $x = \varphi(y)$.

Сонда біз іздеген тиімді тығыздық теңдеуі келесідей табылады: $\psi(y)dy = \omega(x)dx$; мұнда *dx*- ті жоғарыдағы *x* мәнін дифференциалдап табамыз, яғни: $dx = \varphi'(y)dy$. Орнына қойып, қысқартып, мынаны аламыз: $\psi(y) = \omega[\varphi(y)]\varphi'(y)$.

Осы қатыс субтиімді қатыс болып, оның энтропиясы максимумға жақын болады.

4.3 ***Зертханалық жұмыс***

Айталық тиімді болмаған заңмен таралған элементтерден құралған келесідей хабарлар көзі берілген болсын; $\omega(x) = \begin{cases} e^{-x}, x \geq 0, \\ 0, x < 0. \end{cases}$

Шешімі: Қисық сызықты түрлендірушінің өткізу теңдеуін келесідей етіп: $y = F(x) = \left|\sqrt[4]{x}\right|$ таңдап аламыз.

Бұл қатыстың кері теңдеуі келесідей болады:

$$x = \varphi(y) = y^4; x' = 4y^3;\ \psi(y) = \omega[\varphi(y)]\varphi'(y) = 4y^3 e^{-y^4}.$$

Бұл түрлендірушінің шығуындағы сигналдардың таралу заңы тиімдіге (қалыпты заңға) жақын балып, ал оның энтропиясы максимумға жақын болады.

4.5.4. Хабар көзі мен байланыс арнасының ақпараттық сипаттамалары. Кедергілі байланыс арнаның өткізу қабілеті. Хабар және арна көлемдері. Котельников теоремасының қолданылуы.

$y(t) = x(t) + n(t)$ бұл арна шығуындағы сигналдар жиыны болсын; ондағы бірінші қосылғыш – сигнал, ал екіншісі - кедергі.

Котельников теоремасын қолдана отырып, арнаның шығуындағы максимал информацияны табайық; яғни $I(Y, X) = ?$

Мұндағы X арнаның кіруіндегі сигнал болса, ал $У$ - оның шығуындағы сигнал. Сонда оны келесідей жазса болады:

$$I(Y, X) = H(Y) - H(Y / X) = H(Y) - H(N).$$

Мұнда X пен N өзара байланыссыз жиындар.

Котельников теоремасынан $n = 2WT; \Delta t = \frac{1}{2W}$ болады.

Осыларды қолданып, максимал жылдамдықты немесе өткізу қаблетін табамыз;

$$r = \frac{I(Y, X)}{T} = \frac{H(Y) - H(N)}{T}$$

хабар жылдамдығы болса, ал арнаның өткізу қаблеті келесідей болады:

$$C = r_{\max} = \lim_{T \to \infty} \frac{I_{\max}(Y, X)}{T} = \lim_{T \to \infty} \frac{H(Y) - H(N)}{T}.$$

IV Тараудың бақылау және емтихан сұрақтары:

1. Хабар көзінің негізгі ақпараттық сипаттамаларын атаңыз.
2. Эргодикалық хабар көзі түсінігінің маңызы.
3. Жадысы бар дискрет хабар көзінің энтропиясы қалай есептеледі?
4. Ұзын таңбалар тізбегінің ассимптотикалық теңықтималдық теоремасын қалыптастырыңыз.
5. Хабар көзінің әліпбиінің артықшылығы деп нені түсінеміз?
6. Хабардағы артықшылықтың себебі неде?
7. Дискрет хабарлар көзінің өнімділігін анықтаңыз және оны арттыру жолдарын атаңыз.
8. Дискрет арнаның негізгі сипаттамасын атаңыз.
9. Кедергілі арнаның ақпараттық үлгісін құру үшін керек болаған бастапқы деректер қандай?
10. Жадысыз екілік симметриялы арнаны сипаттаңыз.
11. Техникалқ және ақпараттық жіберу жылдамдықтары арасындағы айырмашылық?
12. Арнаның өткізу қабілеті түсінігінің маңызы.
13. Кедергілі және кедергісіз дискрет арнаның өткізу қабілетін көрсететін өрнекті жазыңыз.
14. Үздіксіз хабар көзінің ε- өнімділігі деп нені түсінеміз?
15. Гаусстық арна үлгісінде қандай жуықтаулар қолданылған?
16. Үздіксіз арнаның өткізу жылдамдығы мен өткізу қаблеті қандай анықталады?
17. Гаус арнасы үшін өткізу қаблетінің өрнегін жазып түсіндіріңіз.
18. Сигнал мен арнаның көлемі деп нені түсінеміз?
19. Сигналдың арнамен бұзылмай өтуінің шарттарын анықтаңыз.
20. Кедергілі үздіксіз арна Шеннонның кодтау теоремасын қалыптастырыңыз.
21. Кодтаудың негізгі мақсаттарын атаңыз.

Өзіндік жұмыстар (СӨЖ) тақырыптары

1. Дискрет хабар көзінің ақпараттық сипаттамалары; үлгілері, өнімділігі.
2. Ақпараттың сипаттамалары; үлгілері, артықшылық ұғымы.

3. Сигналдар мен хабарлардың артықшылығын есептеу.
4. Сигналдарды энтропия бойынша оңтайландыру.
5. Сигналдарды энтропия бойынша қысқарту; қысқарту еселіктері.
6. Үздіксіз хабарлардың энтропиясы және оның максимумын табу.
7. Дискрет хабар көзінің өнімділігі.
8. Дискрет байланыс арнасының ақпараттық сипаттамалары; үлгілері.
9. Дискрет арнамен ақпаратты жіберу жылдамдығы.
10. Бөгеуілсіз дискрет арнаның өткізу қабілеті.
11. Бөгеуілді дискрет арнаның өткізу қабілеттілігі.
12. Үздіксіз хабар көзінің ақпараттық сипаттары; үлгілері, жіберу жылдамдығы.
13. Үздіксіз байланыс арнасының өткізу қабілеттілігі;
14. Дифференциалды энтропия.
15. Байланыс арнасы мен сигналдың физикалық сипаттарының келісуі.
16. Сигнал көлемі мен байланыс арнасының сыймдылығы.
17. Хабар көзі мен байланыс арнасының санақтық келісуі.
18. Үздіксіз хабарлардың энтропиясы және оның максимумын табу.
19. Арналарды хабарлармен санақтық келістіру.
20. Үздіксіз хабардың таралу заңын өзгертумен оны оңтайландыру.
21. Кедергілі байланыс арнасының өткізу қабілеті.
22. Хабар және арна көлемдері.
23. Котельников теоремасының қолданылуы.

V ТАРАУ.
БӨГЕУІЛСІЗ ДИСКРЕТ БАЙЛАНЫС АРНАСЫ БОЙЫНША ХАБАР ЖІБЕРУ КЕЗІНДЕГІ АҚПАРАТТАРДЫ КОДТАУ

5.1 Бөгеуілсіз арна үшін Шеннонның кодтау туралы негізгі теоремасы

Қарапайым (бөгеуіл орнықсыз) кодтар.

Бөгеуілсіз дискрет байланыс арнасы бойынша хабар жіберу кезіндегі ақпараттарды кодттау да дискрет хабарға немесе таңбаға сәйкес бір нөмір беру мүмкін. Ал егер үздіксіз хабар болса, алдын ол дискретке түрлендіріледі. Сөйтіп, дискрет хабарлармен амалдар орындау (сақтау, арнамен жіберу, т.с.с.) үшін оны санды түрге өткізіліп, сол сандармен амалдар орындалады. Ал сандар кез келген санақ жүйесінде болуы мүмкін. Алайда амалда тек екілік жүйедегі сандар қолданылады. Санақ жүйесінің негізі m болса, кез келген жүйеден басқа жүйеге өту теңдеуі келесідей болады:

$$Q = \sum_{i=1}^{l} a_{i-l+1} m^{i-l} = a_i m^{i-1} + a_{i-1} m^{i-2} + \ldots + a_2 m^1 + a_1 m^0$$

мұнда i — осы санның дәрежесінің (дәрежесіның) нөмірі; l — дәрежелер саны; a_i - көбейткіш болып, ол 0-ден m-1-ге дейін өзгереді де осы *i*- орынында қанша сан бар екенін көрсетеді. Осыдан қаншалықты санақ жүйесінің негізі жоғары болса, соншалықты ондағы дәрежелер саны кем болады; яғни оны жіберу уақыты да кем болады. Алайда санақ негізі артқанда байланыс жолына және элементар сигналдарды тану және жіберу аспапсына талап та арта түседі.

Ғылыми зерттеу жұмыстарының нәтижесінде ең нәтижелі санақ жүйесі ретінде негізі натурал логарифмнің негізі (яғни e=2,71..) табылған; ал амалда оған жақын екі сан бар - бірі 2 саны, екінішісі - 3 саны табылған. Ал физикалық орындалуы жағынан ең нәтижелісі екілік санақ жүйесі болды. Бұл жүйеде қосу, айыру, көбейту бар болғаны төрт теңдікпен амалға асырылады. Ең кең таралған ойлаужүйесі операциясы болып, екі модулінде қосу операциясын атаса болады; ол да төрт теңдеумен көрсетіледі:

$$0 \oplus 0 = 0 \quad 1 \oplus 1 = 0$$

$$0 \oplus 1 = 1 \quad 1 \oplus 0 = 1$$

Екілік жүйеден сегіздік, екілік-ондық, он алтылық жүйеге өту қиын емес.

Сегіздік жүйеде үш екілік дәреже бір сегіздік санды көрсетеді. Кең қолданатын код - екілік-ондық код.

5.1-кесте

	Салмақтармен алынған екілік-ондық код 8-4-2-1	Салмақтармен алынған екілік-ондық код 5-4-2-1	Салмақтармен алынған екілік-ондық код 2-4-2-1
0	0000 0000	0000 0000	0000 0000
1	0000 0001	0000 0001	0000 0001
2	0000 0010	0000 0010	0000 0010
3	0000 0011	0000 0011	0000 0011
4	0000 0100	0000 0111	0000 0100
5	0000 0101	0000 1000	0000 1011
6	0000 0110	0000 1001	0000 1100
7	0000 0111	0000 1010	0000 1101
8	0000 1000	0000 1011	0000 1110
9	0000 1001	0000 1111	0000 1111
10	0001 0000	0001 0000	0001 0000

Амалда бір саннан басқа санға өткенде тек бір дәрежесі өзгеретін кодтар кең қолданылады; осындай кодтар ішінен кең тарағаны Грей коды болып, ол циклдік немесе рефлексті-екілік код деп аталады. Осы код үздіксіз-сандық түрлендіру техникасында қолданылып, санақтағы теңсіздік қателігін кіші дәреже бірлігіне әкелуге мүмкіндік береді. Грей коды төменгі 5.2-кестеде берілген.

5.2-кесте

Ондық сан	Грей коды	Ондық сан	Грей коды	Ондық сан	Грей коды
0	0000	6	0101	11	1110
1	0001	7	0100	12	1010
2	0011	8	1100	13	1011
3	0010	9	1101	14	1001
4	0110	10	1111	15	1000
5	0111				

Грей кодынан жай екілікке өткізу төменде көрсетілген.

5.2 Үздіксіз-санды түрлендірушіде Грей, Уолш, Рademахер кодтарын (түрлендіру бағдаржолдарын) қолдану

Уолш қатыстар жүйесін сандық ұзату жүйелеріндегі үздіксіз хабарларды түрлендіру бағдаржолдарын жарату мәселелері қаралған.

Қазіргі заманда сандық ақпараттарды ұзату жүйелері (аудио, бейне, мәтінді және басқада) кең қолданылуда. Мысалы, сандық интегралдық қызмет көрсету жүйелерінде (ISDN - Integrated Servises Digital Network) дыбысты жіберу үшін 4 кГц диапазон ажыратылады. Ал кодтау үшін ИКМ - серпінді-кодты модуляциясының (PCM – Pulse Code Modulation) сегіз немесе жеті биті істетіліп, жіберу жылдамдығы 64 Кбит/с немесе 56 Кбит/с болады [23,24].

V.32 протоколында істейтін модемдер жылдамдығы мына аралықта болады: 2,4-тен 28,8 Кбит/с шейін.

V.90 и X.2 протоколдарында құрылған модемдердің жылдамдығы – 56 кбит/с болады. X.75 үлгіқалыбында және G.703 рекомендациясында 64 Кбит/с жылдамдығы да есепке алынған. ITU-T үлгіқалыбында жіберу жылдамдықтары 2096 Мбит/с ке дейін жеткізілген.

Тоналдық (ТЧ) жиіліктерде құрылған телефон арналары үшін ISDN желілерінде DSO типіндегі арна келесідей жалдамдаққа ие - 64 Кбит/с; ал олардың бір T1(DS1) тобы DSO типіндегі 24 ТЧ арнасына ие болады және оның жалпы жылдамығы - 1554 Кбит/с. Ал ISDN (Broadband ISDN) кеңжолақты арналарда жылдамдықтар 2048 Кбит/с ке дейін жетеді.

Компьютердің шығуында шеткі құрылым сипатында UART (Universal Asynchronous Reseiver /Transmitter) микросұлбасы қолданылып, ол сигналдармен үздіксіз-сандық (АЦТ) және цифра-үздіксіз (ЦАТ) түрлендірулер жасайды.

Тізбекті интерфейс RS-232 микросұлбасында жіберу жылдамдығы – 9,6 Кбит/с болса, ал RS-432 жылдамдық 1000 Кбит/с шейін барады.

Дәл осы кезде деректерді жіберу жүйелеріндегі сигналдарды түрлендірушілерді зерттеуде көптеген сигналдарды өңдеу бағдаржолдары мен шарттары жаратылған [9,10,11,13,16,71].

Үздіксіз сигналдарды сандық арналармен жіберу үшін ең қолайлы кодтау түрі бұл циклдік кодтар. Мысалы, CCITT үлгіқалыбының

V.41 сериясында циклдік кодтар мен шешуші кері байланыс бірге қолданылады; мұнда "құраушы полином" мына түрде болады:

$$g(x) = x^{15} + x^{12} + x^5 + 1$$ [23,24].

Мұнда үздіксіз үздіксіз сигнал циклдік кодқа Уолш түрлендіруі жәрдемінде АЦТ да орындалады. Автоматиканың сандық құрылымдарында Грей коды кең қолданылады.

Циклдік кодтардың негізгі абзалдығы - қарапайымдығы (сұлбасы тек қана жарты қосындыторлардан ғана тұрады), сенімділігі мен жылдамдығы, өте жоғары анықтауыш қабілеті (амалда кез келген тақ және жұп қателерді табады).

1923 жылы Уолш Радемахердің толықсыз қатыстар (функциялар) жүйесін толықтыратын толық ортоқалыптыланған (ортонормалданған) қатыстар жүйесін құрды. Уолш қатыстар жиынын реті бойынша үш топқа бөлсе болады:

1) жиілігі бойынша тәртіптелуі (Уолш бойынша);

2) Пэли бойынша тәртіптелуі (диадикті);

3) Адамар бойынша тәртіптелуі.

Уолш теңдеуі келесідей көрсетіледі $Wal_w(i,t)$. $Wal_w(i,t)$ теңдеуінің S_i жиілігі келесідей анықталады:

$$S_i = \begin{cases} 0, i = 0, \\ i/2, i = жұп\ , \\ (i+1)/2, i = тақ\ . \end{cases}.$$

Грей кодын қолданғанда мына қатыс орынды болады:

$$Wal_w(j,\theta) = \prod_{\nu=1}^{n} [rad(\nu,\theta)]^{j_\nu}\ .$$

Мұнда Радемахердің тиісті қатыстары (функциялар) өзара көбейтіледі.

АЦТ және ЦАТ тарда циклдік кодтар істетіліп, олардағы бірінен кейін бірі тізілген код сөздері тек бір ғана цифрамен ерекшеленеді.

Осы циклдік кодтардың ішінде Грей кодын бөліп қараса болады; себебі оны тек жарты сумматорлар жәрдемімен де құрса болады .

Грей кодының циклдік түрлендіру бағдаржолын келесідей

көрсетсе болады. Грейдің n - орынды кодында код сөзі келесідей болсын: $g_{n-1}g_{n-2}\cdots g_2g_1g_0$.

Ол келесідей екілік $b_{n-1}b_{n-2}...b_2b_1b_0$ санға сәйкес келсін.

Онда Грей кодының g_i элементін мына бағдаржолмен алса болады:

$$g_i = b_i \oplus b_{i+1}, 0 \le i \le n-2;$$
$$g_{n-1} = b_{n-1,}$$

Мұнда $\oplus$ таңбасы екі модулімен қосуды көрсетеді.

Ал Грей кодын екілік кодқа кері түрлендіру үшін мыналарды істеу керек; түрлендіру сол жақтан басталады.

Мұнда ең солдағы бірінші дәреже Грей кодының сол жақтан бірінші дәрежесіне тең болады, яғни $b_n = g_n$.

Содан кейін, $b_i = \sum_{k=n}^{i} g_k$; мұнда екілік модулінде қосу амалы орындалады. Басқаша, бұл бағдаржолды былай көрсетсе болады; егерде g_i -ді сол жақтан санағанда, олардың саны жұп болса, онда $b_i = g_i$ болады.

Ал егерде тақ болса, онда $b_i = \overline{g_i}$ болады.

Радемахер қатыстары толықсыз ортоқалыптыланған қатыстар жиынын құрайды.

m жиіліктегі Радемахер теңдеуі $rad(m,t)$ әртүрлі полярлі және кезеңі 2^{m-1} болған тікбұрышты серпіндер тізбегінен тұрады.

Мұнда, m=0, $rad(0,t)$ бірлік серпін түрінде көрінеді.

Радемахер қатыстары кезең 1-ге тең болған кезеңді қатыстар болады, яғни $rad(m,t) = rad(m,t+1)$.

Осы қатыстарды төмендегі рекуррентті қатыстар жәрдемінде алса болады; $rad(m,t) = rad(1,2^{m-1}t)$, мұнда $rad(m,t) = \begin{cases} 1, t \in [0,1/2) \\ -1, t \in [1/2,1) \end{cases}$, яғни қатыстың элементтері тек оң және кері серпіндерден тұрады.

Радемахердің $\nu = \overline{1,3}$ үш элементті теңдеуі үшін жиілік бойынша тәртіптелген Уолш теңдеуінің мына мәндерін алса болады;

$$W(0,t) = + + + + + + + +$$
$$W(1,t) = r_1 = + + + + - - - -$$
$$W(2,t) = r_1 r_2 = + + - - - - + +$$
$$W(3,t) = r_2 = + + - - + + - -$$
$$W(4,t) = r_2 r_3 = + - - + + - - +$$
$$W(5,t) = r_1 r_2 r_3 = + - - + - + + -$$
$$W(6,t) = r_1 r_3 = + - + - - + - +$$
$$W(7,t) = r_3 = + - + - + - + -$$

Уолш жүйесі келесідей қасиеттерге ие болады:

1). ***Ортогоналдық қасиеті:***

Уолш теңдеуі [0,1] аралығында ортогонал болады:

$$\int_0^1 Wal_\alpha(t) Wal_\beta(t) dt = \begin{cases} 0, \alpha \neq \beta, \\ 1, \alpha = \beta \end{cases}.$$

2). Уолш теңдеуі 1 кезеңімен ***кезеңді қатыс (функция):***

$$Wal_\alpha(t) = Wal_\beta(t+1).$$

3). Уолш теңдеуі ***мультипликативті қатыс:***

$$Wal_\alpha(t) Wal_\beta(t) = Wal_\gamma(t) \text{ мұнда } \gamma = \alpha + \beta .$$

4). Уолш ***теңдеуінің модулі 1 ге тең,*** ал ***қатыстың орта мәні*** барлық $\alpha \neq 0$ үшін $\int_0^1 Wal_\alpha(t) dt = 0,$ мұнда $\alpha \neq 0$.

Түрлендіру бағдаржолын келесідей көрсетсе болады:

$$x(t) = \sum_{k=0}^{N-1} C_k Wal(k,t);$$
$$C_k = \frac{1}{N} \sum_{t=0}^{N-1} x(t) Wal(k,t)$$

.

Уолштың жылдам түрлендіру бағдаржолы матрица түрінде келесідей көрсетіледі: $C_x(\nu) = \frac{1}{W} H(\nu) X(\nu)$. Мұнда, Адамар ма-

трицаларын бөлшектеуді қолданса болады, яғни келесідей:

$$N = 2^n \quad H(n) = \begin{bmatrix} H(n-1)H(n-1) \\ H(n-1)H(n-1) \end{bmatrix} \qquad H(0) = 1.$$

Осыны қолданып, $H(3)$ді $H(2)$ арқылы өрнектесе болады және $W = \overline{1,7}$ үшін мынаны шығарса болады:

$$\begin{bmatrix} C_x(0) \\ C_x(1) \\ C_x(2) \\ C_x(3) \\ C_x(4) \\ C_x(5) \\ C_x(6) \\ C_x(7) \end{bmatrix} = \frac{1}{8} \begin{bmatrix} H(2)H(2) \\ H(2)-H(2) \end{bmatrix} \begin{bmatrix} x(0) \\ x(1) \\ x(2) \\ x(3) \\ x(4) \\ x(5) \\ x(6) \\ x(7) \end{bmatrix}.$$

Матрицаларды бөлшектеген соң мынаны алса болады:

$$\begin{bmatrix} C_x(0) \\ C_x(1) \\ C_x(2) \\ C_x(3) \end{bmatrix} = \frac{1}{8} [H(2)] \begin{bmatrix} x_l(0) \\ x_l(1) \\ x_l(2) \\ x_l(3) \end{bmatrix}$$

$$\begin{bmatrix} C_x(4) \\ C_x(5) \\ C_x(6) \\ C_x(7) \end{bmatrix} = \frac{1}{8} [H(2)] \begin{bmatrix} x_l(4) \\ x_l(5) \\ x_l(6) \\ x_l(7) \end{bmatrix}, \text{ мұнда } \begin{matrix} x_l(l) = x(l) + x(4+l); l = \overline{0,3}, \\ x_l(l) = x(l-4) - x(l); l = \overline{4,7} \end{matrix}.$$

Кейін, $H_2 = \begin{bmatrix} H(1)H(1) \\ H(1)-H(1) \end{bmatrix}$ орнына қойып, мынаны аламыз және

$$\begin{bmatrix} C_x(0) \\ C_x(1) \\ C_x(2) \\ C_x(3) \end{bmatrix} = \frac{1}{8}\begin{bmatrix} H(1)H(1) \\ H(1)-H(1) \end{bmatrix}\begin{bmatrix} x_l(0) \\ x_l(1) \\ x_l(2) \\ x_l(3) \end{bmatrix}$$ және

$$\begin{bmatrix} C_x(4) \\ C_x(5) \\ C_x(6) \\ C_x(7) \end{bmatrix} = \frac{1}{8}\begin{bmatrix} H(1)H(1) \\ H(1)-H(1) \end{bmatrix}\begin{bmatrix} x_l(4) \\ x_l(5) \\ x_l(6) \\ x_l(7) \end{bmatrix}.$$

Матрицаларды бөлшектеп және көбейтуден кейін мынаны аламыз:

$$\begin{bmatrix} C_x(0) \\ C_x(1) \end{bmatrix} = \frac{1}{8}[H(1)]\begin{bmatrix} x_l(0)+x_l(2) \\ x_l(1)+x_l(3) \end{bmatrix} = \frac{1}{8}[H(1)]\begin{bmatrix} x_2(0) \\ x_2(1) \end{bmatrix};$$

$$\begin{bmatrix} C_x(2) \\ C_x(3) \end{bmatrix} = \frac{1}{8}[H(1)]\begin{bmatrix} x_l(0)-x_l(2) \\ x_l(1)-x_l(3) \end{bmatrix} = \frac{1}{8}[H(1)]\begin{bmatrix} x_2(2) \\ x_2(3) \end{bmatrix};$$

$$\begin{bmatrix} C_x(4) \\ C_x(5) \end{bmatrix} = \frac{1}{8}[H(1)]\begin{bmatrix} x_l(4)+x_l(6) \\ x_l(5)+x_l(7) \end{bmatrix} = \frac{1}{8}[H(1)]\begin{bmatrix} x_2(4) \\ x_2(5) \end{bmatrix};$$

$$\begin{bmatrix} C_x(6) \\ C_x(7) \end{bmatrix} = \frac{1}{8}[H(1)]\begin{bmatrix} x_l(4)-x_l(6) \\ x_l(5)-x_l(7) \end{bmatrix} = \frac{1}{8}[H(1)]\begin{bmatrix} x_2(6) \\ x_2(7) \end{bmatrix};$$

Кейін, мынаны еске ала отырып $H(1) = \begin{bmatrix} H(0)H(0) \\ H(0)-H(0) \end{bmatrix} = \begin{bmatrix} 1 \\ 1-1 \end{bmatrix}$, теңдеулерді шығарамыз:

$$C_x(0) = x_2(0) + x_2(1) = \frac{1}{8} x_3(0);$$

$$C_x(1) = x_2(0) - x_2(1) = \frac{1}{8} x_3(1);$$

$$C_x(2) = x_2(2) + x_2(3) = \frac{1}{8} x_3(2);$$

$$C_x(3) = x_2(2) - x_2(3) = \frac{1}{8} x_3(3);$$

$$C_x(4) = x_2(4) + x_2(5) = \frac{1}{8} x_3(4);$$

$$C_x(5) = x_2(4) - x_2(5) = \frac{1}{8} x_3(5);$$

$$C_x(6) = x_2(6) + x_2(7) = \frac{1}{8} x_3(6);$$

$$C_x(7) = x_2(6) - x_2(7) = \frac{1}{8} x_3(7);$$

Мына $N = 2^n$ үшін жалпы итерациялар саны $n = \log_2 N$ болады. Барлық түрлендіру еселіктерін есептеу үшін қажетті арифметикалық амалдардың саны жуықтап алғанда келесідей $N \log_2 N$. r- итерациясында 2^{r-1} тобы қатысып, әрқайсысында $N / 2^{r-1}$ элементтен болады.

5.3 Бөгеуілсіз арна үшін Шеннонның негізгі кодтау теоремасы

Бөгеуілсіз арна үшін Шеннонның негізгі кодтау теоремасы хабарларды нәтижелі кодтау, олардың көлемін қысқарту және берілгендер қорына жазуға негізделген болып, былай баяндалады:

1. Арнаның өткізу қабілетінен кем болған хабар көзінің кез келген өнімділігінде, яғни келесідей шартта:

2. $I(Z) > C_Д$ ***,***

(мұнда ε кез келгене оң кіші сан) хабар көзі жаратқан барлық хабарларды жіберe алатын кодтау әдісін тапса болады.

3. Егер $I(Z) > C_Д$ ***болса, онда ешқандай кодтау әдісі шексіз жинақталған хабарларды жіберуі мүмкін емес.***

4. Осы теореманың математикалық дәлелдеуі өте қиын күрделі болғандықтан тек эвристикалық түсініктерге ғана сүйенеміз.

Кодталатын тізбектегі таңбалар саны N, ал хабар көзінің энтропиясы — $H(Z)$ болса, типтік тізбектердің саны $n_T \approx 2^{H(Z)N}$ болады.

Егер $N = T/\tau$, мұнда T- кодталатын тізбектің ұзындығы, τ — бір таңбаның ұзындығы, онда $n_T \approx 2^{\frac{H(Z)}{\tau}T} = 2^{\bar{I}(Z)T}$.

Манипуляция жылдамдығы V_T болғанда код қисындастыруындағы таңбалар саны TV_T, болып, n_k - код қисындастыруын құру мүмкіндігін береді:

$$n_k = m^{TV_T} = 2^{TV_T \log_2 m} = 2^{TC_Д} = 2^{T\left(\bar{I}(Z)+8\right)}. \qquad (5.1)$$

Осы теңдеулерден мынаны көрсе болады: $n_k > n_T$.

Содан, егер $C_Д > \bar{I}(Z)$ болса, онда арна өткізетін код қисындастыруылары барлық типтік тізбектерді кодтауға жетеді және де біршама артып та қалады.

Түрсіз тізбектерге таңбалар саны әжептеуір көп болған код қисындастыруыларын сәйкес қойса болады.

Алайда барлық түрсіз тізбектерге сол артықша болғандардың ішінен жалғыз бір қисындастыруыны алса болады.

Алайда $T \to \infty....(N \to \infty)$ болғанда түрсіз тізбектің ықтималдығы нөлге жақындайды; бірінші жағдайда, бұл ұзатудың нәтижелілігіне ешқандай әсер етпейді.

Ал екінші жағдайда, жіберу мен қабылдау арасындағы теңдестірудің сенімділік деңгейіне әсер етпейді.

Осында айтатын жай, типтік тізбектерді кодтаумен шектелсек олардың ықтималдығы тең болғандықтан, арнаның кіруіне түсетін таңбалар теңықтималды және өзара байланыссыз болады. Бұл жіберілетін хабарда артықшылықты толық жояды.

Теореманың екінші бөлімінде келесідей $\bar{I}(Z) > C_Д$ жағдайда хабар ұзату мүмкін болмайтынын көрсетеді. Сондықтан егер арнаның өткізу қабілеті хабар көзінің өнімділігінен кем болса, онда қабылдаушы жақта хабарлар жинақталуы анық. ***Шеннонның теоремасын*** басқа түрде де айтса болады;

H(Z) энтропиясымен берілген хабар көзін т әліпбилі көлемді таңбалар тізбегімен кодтау мүмкін болады; онда бір таңбаға тура келетін орташа $l_{ср}$ таңбалар саны мына шамаға $H(Z)/\log m$ ***кез келгенше жақын болады; бірақ кем болмайды.***

Егер хабарды ұзын жиынтықтармен кодтасақ, алдын көргеніміздей мұндай кодтау әдісін амалда құру мүмкін болады.

Егер кодтау жиынтықтарының (блоктарының) ұзындығын шексіз асимптоталық түрде арттырсақ, онда осы шекараға қол жеткізу мүмкін болады.

Таңбалардың корреляцияланбаған тізбегін нәтижелі кодтау әдістері.

Теорема айқын кодтау түрін көрсетпейді; бірақ ол код қисындастыруының әрбір таңбасын таңдағанда оның максимал ақпарат алуын көздеу керек екенін көрсетеді. Демек, әрбір таңба 0 және 1 мәндерін қабылдау ықтималдықтары өзара тең болуы керек және әрбір таңбалы таңдау алдыңғы таңбалы таңдауға байланысты болмауы керек.

Таңбалар арасындағы байланысты жою және нәтижелі кодтар құрудың құралымды әдістерін американ ғалымдары Шеннон және Фано ұсынған еді.

Сондықтан код аты ***Шеннон-Фано коды*** деп аталады.

Код келесідей құрылады. Хабар әліпбиінің әріптері баған бойынша олардың ықтималдығы кемейуі бойынша жазылады.

Кейін оларды ықтималдықтарының қосындысы жуықты түрде жақын болатындай етіп бағанды екіге бөлеміз. Жоғарыдағы таңбалардың тұсына мысалы, 1 деп, ал төменгі таңбалар тұсына – 0 деп таңбалаймыз.

Ал енді жоғарғы топты да, төменгі топты да көрсетілгендей етіп екіге бөлеміз және таңбалардың тұсына да 1,0 жазып шағымыз. Осыны жалғыз бір әріп қалғанша жалғастырамыз. Сонда әрбір әріптің тұсында 1,0 ден құрылған код қисындастыруылары пайда болады.

5.4 Энтропия қасиеттерін ақпаратты сығымдауда қолдану. Нәтижелі кодтар. Шеннон-Фано және Хафмен кодтарын құру қағидалары

Көбінесе ақпарат көзінің санақтық сипаттамалары анықталған болса, оған сәйкес түрде өте экономді қысқа кодтар құру мімкін болады. Мұнда әрине кедергі жоқ деп есептеледі. Амалда мұндай жағдайлар көп кездеседі; мысалы, үлкен мәтінді хабарларды мұрағатта сақтау және с.с. Мұнда қойылатын шарт – ақпаратты сығымдап, қысқарту ғана. Ал кедергіге шыдамдылық есепке алын-

байды. Бұл әдіс Шеннонның кедергісіз арнаға арналған теоремасына негізделеді. Теорияның мағынасы келесідей:

егер кейбір әліпбидің әріптерінен құрылған сөздер болса, онда ол сөздердің әріптерін екілік жүйеде кодтаудың ең тиімдіын тапса болады; онда әрбір әріпке тура келетін таңбалар саны сол әріптің энтропиясынан кем болмайды; немесе, ең жақсы жағдайда, әріптің энтропиясына тең болады.

Бұл теореманы шығарғанда кодтаудың анық әдісі көрсетілмеген; алайда осыдан ол әдісті былайша айтса да болады:

1). Әрбір екілік таңбалы (0 және 1) таңдағанда олардың ықтималдығы өзара тең немесе өте жақын болуы керек.

2). Әрбір таңбаның таңдауы алдынғыларына байланысты болмауы керек.

Егер әріптер өзара байланысты болмаса, онда Шеннон-Фано коды өте жақсы нәтиже береді.

Мұнда ең жоғары нәтиже алу үшін ***әрбір әріптің ықтималдығы екінің бүтін кері дәрежесіне тең болуы керек.***

Мұнда әрбір ***әріпке тура келетін таңбалар саны оның энтропиясына тең болады да ең нәтижелі код құрылған болады.***

Алайда амалда әрбір әріптің ықтималдығы өзара тең болмайды және айтылған шарт орындалмайды; сондықтан әріптердегі таңбалар саны оның энтропиясынан анағұрлым үлкен болады. Сондықтан ***абсолютті нәтижелі кодты амалда*** құрып болмайды. Нәтижелі кодтың энтропиясы келесідей болады:

$$H(Z) = -\sum_{i=1}^{8} p(z_i)\log\ p(z_i) = 1\frac{63}{64}.$$

Ал әрбір әріпке тура келетін таңбалар саны келесідей болады:

$$l_{cp} = \sum_{i=1}^{8} p(z_i)n(z_i) = 1\frac{63}{64}.$$ Мұндай код төменде келтірілген.

5.5 ***Зертханалық жұмыс*** Абсолютті нәтижелі код құру керек.

Шешімі: Жоғарыда келтірілген бағдаржолмен код құрамыз; әрбір әріптің ықтималдығы екінің бүтін кері дәрежесіне тең етіп 1-кестеде көрсетілгендей төмен қарай қоямыз.

1-кесте

Әріптер	Ықтималдықтар	Код қисындастыруы	Ажырату дәрежесі
z_1	½	1	
z_2	1/4	01	1
z_3	1/8	001	11
z_4	1/16	0001	111
z_5	1/32	00001	1V
z_6	1/64	000001	V
z_7	1/128	0000001	V1
z_8	1/128	0000000	V11

Әрбір таңбаның ықтималдығы екінің кері бүтін дәрежесі болғандықтан, артықшылық толығымен жойылады.

Мұндайда бір әріпке тура келетін таңбалардың орташа саны оның энтропиясына тепе тең болады.

Осыған сену үшін энтропияны есепейміз:

$$H(Z) = -\sum_{i=1}^{8} p(z_i)\log_2 p(z_i) = 1\frac{63}{64}.$$

Және әріптің орташа таңбалар санын есептейміз:

$$l_{cp} = -\sum_{i=1}^{8} p(z_i)n(z_i) = 1\frac{63}{64}.$$

Мұнда $n(z_i)$, z_i- әріне сәйкес келетін код қисындастыруындағы таңбалар саны. Жалпы жағдайда бір әріпке тура келетін таңбалар саны әліпби энтропиясынан көп болады.

Жалпы жағдайда әліпбидің санақтығына қарай код құрылса, онда тиімдіге жақын болғанымен, біраз айырмашылық болады; әрбір әріпке тура келетін таңбалар 3-тен кем, бірақ әліпбидің энтропиясынан көп болады.

5.6 ***Зертханалық жұмыс*** Төменгі кестеде келтірілген әріптер үшін Шеннон-Фано кодын құру керек.

Шешімі: Алдын ала есептеулерде ансамбл энтропиясы 2,76 тең.

Ал әріпке тура келетін таңбалар саны 2,84**.**

2-кесте

Әріптер	Ықтималдықтар	Код қисындастыруы	Ажырату дәрежесі
z_1	0,22	11	
z_2	0,20	101	1
z_3	0,16	100	11
z_4	0,16	01	111
z_5	0,10	001	1V
z_6	0,10	0001	V
z_7	0,04	00001	V1
z_8	0,02	00000	V11

Осы кестедегі әріптер энтропиясы 2,76 болып, ал әрбір әріпке тура келетін таңбалар саны 2,84.

Көрініп тұрғандай артықшылық сақталып отыр.

Мұны кемейту үшін әрбір екі әріп арасындағы байланысты да есепке ала отырып, код құрсақ, артықшылық біршама кемейеді.

5.7 ***Зертханалық жұмыс***

Әріптер арасындағы корреляцияны есепке ала отырып артықшылықты кемейту керек.

Шешімі:

Ал егер әріптер байланысты болмаса, онда Шеннонның теоремасының негізінде нәтижелі арттыру үшін **үлкенірек жиынтықтар** алсақ болады; мұнда нәтиженің артуы жиынтықтағы элементтердің арасындағы байланыстардың кемеуінен емес, ол байланыстар жоқ емес пе? Ал онда неден болады?

Код құру үдерісінде екі топқа ажыратуда әрбір топтың жиынды ықтималдықтары тең немесе өте жақын болуы керек еді; жиынтық ұзынырақ болған сайын сол шарт жақсырақ орындала береді.

Ақырында жиынтықтың ұзындығы шексіз өскенде, энтропия тиімдіге ұмтылады; яғни $\lim\limits_{n\to\infty} l_{ср} = H(Z) = 0{,}47$ болады.

Айталық $p(z_1) = 0{,}9;\ p(z_2) = 0{,}1$ болсын.

Сонда жиынтық ұзындығы екіге тең болғанда, әрбір жиынтыққа орташа 1,29 таңба, ал әріпке 0,645 таңба тура келеді.

Жиынтықтың ықтималдығы әрбір таңбаның ықтималдықтарының көбейтіндісіне тең болады, себебі олар байланыссыз.

Осы есептеулер 3-кестеде келтірілген.

3-кесте.

Жиынтықтар	Ықтималдықтар	Код	Бөлшектеу дәрежесі
$z_1 z_1$	0,81	1	1
$z_1 z_2$	0,09	01	11
$z_2 z_1$	0,09	001	111
$z_2\ z_2$	0,01	000	

4-кесте.

Жиынтықтар	Ықтималдықтар	Код қисындастыруылары	Бөлшектеу дәрежесі
$z_1 z_1\ z_1$	0,729	1	
$z_2\ z_1 z_1$	0,081	011	1
$z_1\ z_2\ z_1$	0,081	010	111
$z_1 z_1\ z_2$	0,081	001	11
$z_2\ z_2\ z_1$	0,009	00011	$1\vee$
$z_2\ z_1\ z_2$	0,009	00010	$\vee 1$
$z_1\ z_2\ z_2$	0,009	00001	$\vee$
$z_2\ z_2\ z_2$	0,001	00000	$\vee\mathbf{1}$

Үш әріпті жиынтықтарды кодтағанда бір жиынтыққа тура келетін таңбалар саны 1,59, ал әрбір әріпке тура келетін таңбалар саны 0,53; яғни энтропиядан 12%-ке ғана артады. Жиынтықтарда шексіз көп таңбалар болғанда ғана теориялық минимум H(Z) = 0,47 болады.

Шеннон Фано кодын құруда іртүрлі нәтиже шығуы мүмкін; екіге ажыратқанда бірде төменгі жақ үлкен болса, бірде жоғарғы жақ үлкен болуы мүмкін. Мысалы, 2-кесте мен 5-кестені салыстырсақ, 2-кестеде бір әріпке тура келетін таңбалар саны 2,84 болса, ал 5-кестеде бір әріпке тура келетін таңбалар саны 2,80. Мұндай кемшілік Хаффмен кодында жоқ.

5 - кесте.

Әріптер	Ықтималдықтар	Код қисындастыруы	Ажырату дәрежесі
z_1	0,22	11	
z_2	0,20	101	1
z_3	0,16	100	11
z_4	0,16	01	111
z_5	0,10	001	1V
z_6	0,10	0001	V
z_7	0,04	00001	V1
z_8	0,02	00000	V11

5.4.1 Шеннон-Фано және Хаффмен кодтарын құру әдістері

Айталық арнамен жіберілетін хабарды бірер $\{x_1; x_2; ...; x_m\}$ әліпбиінен алынған кездейсоқ таңбалар жиыны түрінде көрсетілетін болсын дейік. Мұнда осы хабардың кейбір таңбалары жиірек, ал кейбір таңбалары сирегірек ұшырайтын болады. Сонда әрбір таңбаға оның хабарда қайталану ықтималдығы сәйкес келеді.

Егерде хабар екілік сандар (цифралар) тізбегінен құралған болса (мұнда, мысалы үшін, бірлік таңбаның ықтималдығы берілген болып, ол *p*-ға тең болсын), ол хабарды ұзындығы өзгермейтін

(бекітілген) *n*-ге тең болған жиынтықтарға ажыратса болады. Мұнда әрбір жиынтық 2^n түрлі мәнге ие болуы мүмкін. Ондай болса әрбір жиынтықтың пайда болу ықтималдығын ықтималдықтарды көбейту теңдеуімен (егерде тізбектегі цифралар өзара байланысты болмаса) оңай анықтау мүмкін болады. Мысалы, ‘0101’ жиынтығы үшін ықтималдық келесідей анықталады *qpqp,* мұнда *q=1-p*.

Хабар таңбаларының ықтималдықтары әртүрлі болғанда бұларды кодтау үшін біркелкі болмаған екілік кодтарды қолданған жөн: жиі кездесетін таңбалар үшін қысқарақ код сөздерін, ал сирек кездесетін таңбалар үшін ұзынырақ код сөздерін қолдану керек болады.

Дәл осы қағидаға Шеннон-Фано и Хаффман кодтау әдістері негізделген. Екі әдісте де хабар таңбаларын алдын ала олардың ықтималдықтарының кему бойынша реттеп шығу керек.

Кейінгі іс-әрекеттер қарастырылатын әдіске байланысты болады.

Шеннона-Фано әдісі бойынша кодттауда алынған таңбалар кестесіндегі таңбалар бағанын жоғарыдан төмен қарай екіге ажыратамыз; мұнда жоғары жақтағы таңбалардың ықтималдықтарының қосындысы төмен жақтағы таңбалардың ықтималдықтарының қосындысына тең немесе жақын болуы керек. Сонда жоғары жақтағы таңбалардың тұсына бірлер жазамыз. Ал төмен жақтағы таңбалардың тұсына нөлдер (немесе керісінше) жазамыз.

Төмен және жоғары бөлімдерді дәл осындай екіге бөліп, жоғарыдағы аталған жұмыстарды атқарамыз.

Мысалы, егер *p=0,25* болғанда және хабар тізбегін 3 екілік жиынтықтарға ажрытқанда төмендегідей кесте аламыз

(сол жақтағы кесте).

Жиынтық	Ықтималдық
000	0.421875
001	0.140625
010	0.140625
100	0.140625
011	0.046875
101	0.046875
110	0.046875
111	0.015625

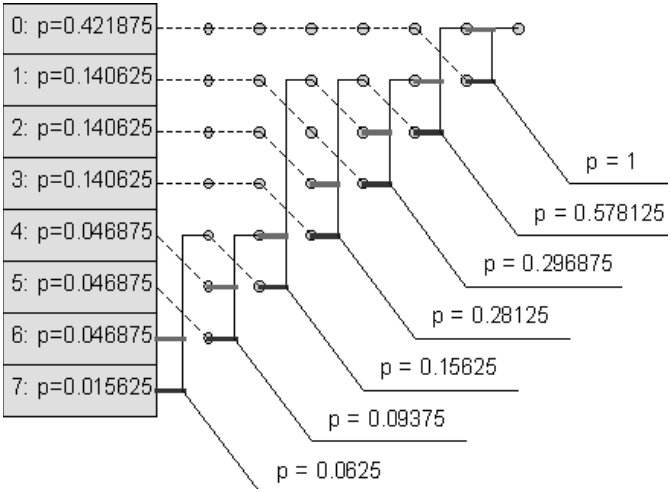
	Жиынтық	P	Код	Ұзындық
	000	0.421875	11	2
	001	0.14062	10	2
	010	0.140625	011	3
	100	0.140625	010	3
	011	0.046875	0011	4
	101	0.046875	0010	4
	110	0.046875	0001	4
	111	0.015625	0000	4

Дәл осындай түрде барлық X жиынтықтары үшін кодтар құрылады.

Хаффман әдісімен кодттау басқаша орындалады. Ықтималдықтары бойынша реттелген кестеден ең төмен ықтималдықты екі таңбалы алып, ықтималдықтарын қосамыз; алынған ықтималдықты сол кестедегі ықтималдықтар қатарына ***тәртіпті бұзбайтындай*** етіп орналастырамыз; әрине, бұл ықтималдық жоғарырақ орналасып, басқа ықтималдықтарды төмен қарай жылжытады. Алынған ықтималдықтан үлкендері өз орындарында қала береді. Нәтижеде барлық ықтималдықтар саны бірге кемейеді. Осындай тәртіпте жұмыстарды жалғастыра береміз. Сөйтіп, барлық таңбалардың ықтималдықтарын қосып шығамыз; ең ақырында барлық қосынды бірге тең болуы керек. Мұнда қандай таңбалар қалай біріктірілгендігін естен шығармау керек болады. Нәтижеде Хаффман ағашы келіп шығады.

Хаффман әдісі алдыңғыға қарағанда жақсырақ; себебі оның көмегімен әрқашанда ***префиксті код*** алынады.

Мысалы, $p=0.25$ үшін құрылған ағаш төмендегідей көрінеді (төменде біріктірілген элементтердің ықтималдықтары көрсетілген).



Таңбалардың кодтарын құру үшін ағаштың негізгі түбірінен төмен қарай сол таңбаға қарай жүріп отырамыз; жоғарыдағы жолмен жүргенде (суретте қызыл сызықты жол) бір деп таңбалап, ал төменгі (көк сызықты жол) сызықпен жүргенде – нөлмен таңбалаймыз.

Біздің жағдайда келесідей кесте шығады.

	Жиынтық	P	Код	Ұзындық
0	000	0.421875	0	1
1	001	0.140625	110	3
2	010	0.140625	101	3
3	100	0.140625	100	3
4	011	0.046875	11111	5
5	101	0.046875	11110	5
6	110	0.046875	11101	5
7	111	0.015625	11100	5

5.8 *Зетханалық жұмыстар*

Мысалы, тізбекте бірдің пайда болу ықтималдығы p=0.2 және жиынтық ұзындығы n=4 болсын; сонда Шеннона-Фано әдісі үшін келесідей мәндер аламыз:

Параметр	Мәні
Код сөзінің орташа ұзындығы *Lopm*	3.0656
Бір дәреженің орташа ұзындығы *Lopm/n*	0.7664
Код сөзінің теориялық орташа ұзындығы	3.6
Энтропия *H(x)*	0.721928
Мәні *H*(*x*)+1/*n*	0.971928

Мұнда: $L_{opm} = \bar{l} = \sum_{i=1}^{n} l_i p_i$, $H(x) = -plog(p)-qlog(q)$.

Осыдан мынаны көрсе болады: $H(x) < \frac{L_{opm}}{n} < H(x) + \frac{1}{n}$. .

Осындай болуы да керек; тиімді кодтаудың шекті мүмкіншіліктері осы теңсіздікпен анықталады.

Кодтар кестесі:

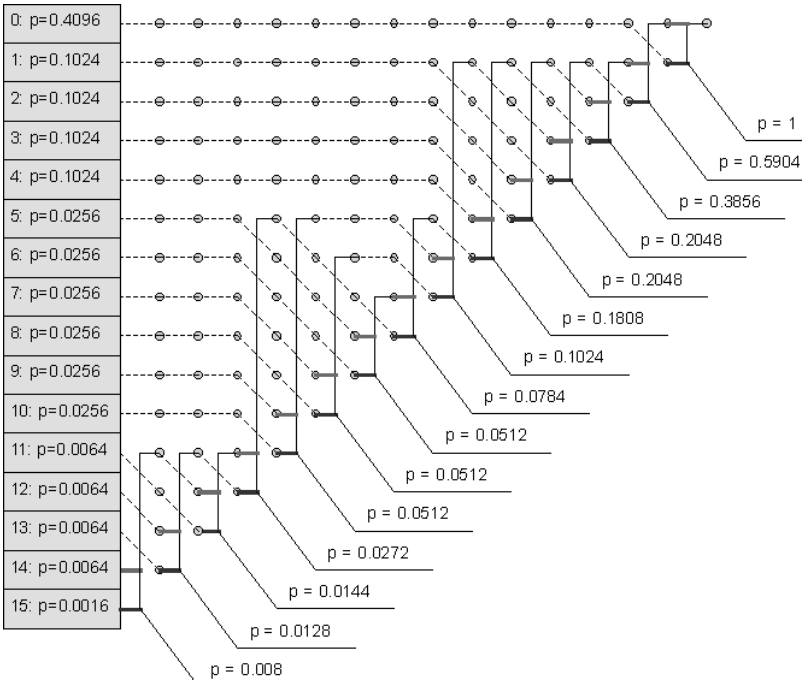
	Жиынтық	P	-log(P)	Код	Ұзындығы	Теор. ұзындығы
0	0000	0.4096	1.287	11	2	2
1	0001	0.1024	3.287	10	2	4
2	0010	0.1024	3.287	011	3	4
3	0100	0.1024	3.287	010	3	4
4	1000	0.1024	3.287	0011	4	4
5	0011	0.0256	5.287	00101	5	6
6	0101	0.0256	5.287	00100	5	6
7	0110	0.0256	5.287	00011	5	6
	1001	0.0256	5.287	000101	6	6
9	1010	0.0256	5.287	000100	6	6
10	1100	0.0256	5.287	00001	5	6
11	0111	0.0064	7.287	0000011	7	8
12	1011	0.0064	7.2877	0000010	7	8
	1101	0.0064	7.2877	0000001	7	8
14	1110	0.0064	7.2877	00000001	8	8
15	1111	0.0016	9.2877	00000000	8	10

Кестеде көрініп тұрғандай алынған код префиксті болады.

Шеннон кестесі:

	Жиынтық	Ықтималдық	7	6	5	4	3	2	1	0
0	0000	0.4096	1	1						
1	0001	0.1024	1	0						
2	0010	0.1024	0	1	1					
	0100	0.1024	0	1	0					
4	1000	0.1024	0	0	1	1				
5	0011	0.0256	0	0	1	0	1			
6	0101	0.0256	0	0	1	0	0			
7	0110	0.0256	0	0	0	1	1			
8	1001	0.0256	0	0	0	1	0	1		
9	1010	0.0256	0	0	0	1	0	0		
10	1100	0.0256	0	0	0	0	1			
11	0111	0.0064	0	0	0	0	0	1	1	
12	1011	0.0064	0	0	0	0	0	1	0	
13	1101	0.0064	0	0	0	0	0	0	1	
14	1110	0.0064	0	0	0	0	0	0	0	1
15	1111	0.0016	0	0	0	0	0	0	0	0

Хаффман әдісі үшін:
Хаффман ағашы:



Кодтар кестесі:

	Жиынтық	*P*	-*log*(*P*)	Код	Ұзындығы	Теор. ұзын дығы
0	0000	0.4096	1.28771	0	1	2
1	0001	0.1024	3.28771	100	3	4
2	0010	0.1024	3.28771	1111	4	4
3	0100	0.1024	3.28771	1110	4	4
4	1000	0.1024	3.28771	1101	4	4
5	0011	0.0256	5.28771	110011	6	6
6	0101	0.0256	5.28771	110010	6	6
7	0110	0.0256	5.28771	10101	5	6
8	1001	0.0256	5.28771	10100	5	6
9	1010	0.0256	5.28771	10111	5	6
10	1100	0.0256	5.28771	10110	5	6
11	0111	0.0064	7.28771	1100010	7	8
12	1011	0.0064	7.28771	1100001	7	8
13	1101	0.0064	7.28771	1100000	7	8
14	1110	0.0064	7.28771	11000111	8	8
15	1111	0.0016	9.28771	11000110	8	10

Параметр	Мәні
Код сөзінің орташа ұзындығы *Lopm*	2.9632
Бір таңбалық орташа ұзындығы *Lopm/n*	0.7408
Код сөзінің теориялық орташа ұзындығы	3.6
Энтропия $H(x)$	0.72193
Мәні $H(x)+1/n$	0.971928

5.5. Нәтижелі кодтардың префикстік талабы

Нәтижелі кодтарды құру әдістемесін жақсылап мән беріп қарасақ мынаны көрсе болады; ықтималдығы үлкен болған әріпке кемірек таңбалар, ал ықтималдығы кем болған әріптерге көбірек таңбалар беріледі. Сөйтіп, әрбір әріптің таңбалар саны әртүрлі болады. Бұл декодтауды қиындатады. Код қисындастыруын ажырату үшін ажыратушы белгілер таңдап алу керек болады. Алайда бұл орташа код қисындастыруының орташа ұзындығын арттырады. Мұндай белгілерді ендірмеу үшін еш қандай код қисындастыруы одан ұзынырақ болған қисындастыруымен бірдей болмауы керек.

Осы шартқа жауап беретін ***кодтар префиксті*** деп аталады.

Мысалы келесідей префиксті кодтың тізбегі берілген болсын: 100000110110110100. Келесідей код берілген: $\begin{matrix} z_1.....z_2.....z_3.....z_4 \\ 00...01..101..100 \end{matrix}$

болса, оның көмегімен декодтасақ мынаны аламыз:

$$\begin{matrix} 100...00...01..101..101..101..00 \\ ...z_4.....z_1.....z_2....z_3.....z_3.....z_3....z_1 \end{matrix}.$$

Ал префиксті болмаған 000101010101 қисындастыруы берілген болса, оны мына кодпен декодтасақ, $\begin{matrix} z_1.....z_2.....z_3.....z_4 \\ 00...01..101..010 \end{matrix}$ әртүрлі код қисындастыруын аламыз: $\begin{matrix} 00...01...01...01...010..101 \\ ..z_1....z_2....z_2.....z_2.....z_4.....z_3 \\ 00...010...101...010...101 \\ ..z_1.....z_4.....z_3.....z_4.....z_3 \end{matrix}$ немесе

00...01...010...101...01...01

..z_1....z_2.....z_4.....z_3.....z_2....z_2 аламыз.

Ал жоғарыда аталған Шеннон-Фано және Хаффмен кодтары префиксті екенін көреміз.

Нәтижелі кодтаудың кемшіліктері

Негізгі кемшілігінің бірі - кодтардың әртүрлі ұзындығы болып, арнаның кіруінде және шығуында да кодтарды жинақтаушы жинағыш керек болады.

Бұл жинағыш арнаның өткізу жылдамдығының біркелкі болуын қамтамасыз етеді.

Екінші кемшілік - жиынтық тиісті ұзындықта болуы үшін арнаның кіруінде және шығуында да оны (жиынтықты) жинақтау керек болады.

Тағы бір кемшілік - бірлік қателік жалғыз кателіке әкелмейді.

Бұдан кейінгі барлық таңбалар да қате болады; бұны ***қателер трекі*** деп атайды.

Әрине, арнайы әдістермен қателер трекін кемейтуге және минимумға жеткізуге әрекет етіледі.

Сондай ақ нәтижелі кодтаудың салыстырмалы күрделілігін де атап кету керек.

5.6. Криптогрфиялық ақпаратты жабу. “Электронды Үкімет” құруда компьютерлік ақпаратты қорғау және түпнұсқасын тексеру мәселелері.

Қазақстан Республикасының Президенті Нұрсұлтан Назарбаев Қазақстан халқына 2005-2006 ж.ж. “Жолдауларда” [1,2.] былай делінген:

“Электронды Үкімет” жобасын іске асыруды жеделдетсін. Ол үшін биылғы жылы “Біріздендірілген номерлердің ұлттық тізімі туралы” Заң қабылдануға және “Ақпараттандыру туралы” Заңға тиісті өзгерістер мен толықтырулар енгізілуге тиіс. Нақты іске асырылған жағдайда мұның өзі әрбір азаматтың енді қазіргі кезде жиі талап етіліп жүрген СТН, ӘЖҚ (РНН, СИК), төлқұжат нөмірі және де басқа да құжаттардың орнына өзінің әмбебеп дербес кодын иеленуіне мүмкіндік береді. Демек “Электронды Үкімет” құрылған кезде

адамдардың өзіне тән СТН, ӘЖҚ, төлқұжат нөмері және басқада құжаттар жүйеде сақталады және бұл берілгендер (құжаттар) өзге адамдардан, бұзғыншылардан сенімді түрде қорғалған болуы керек.

Осы "Жолдауларға" сәйкес Қазақстан Республикасында "Электрондық құжат және электронндық цифрлық қолтаңба туралы" Заң біраз алдынырақ қабылданды: 7.01.2003 жылы және іске қосылды [75]. Осы Заң электрондық цифрлық қолтаңбалар арқылы куәландырылған, құқықтық қатынастардың орнатылыуын, өзгертілуін немесе тоқтатылуын көздейтін электрондық құжаттарды жасау және пайдалану кезінде туындайтын қатынастарды, сондайақ азаматтық-құқықтық мәмілелер жасауды қоса алғанда, құқықтық қатынастарға қатысушылардың электрондық құжаттар айналымы саласында туындайтын құқықтары мен міндеттерін реттеуге бағытталған. Осы Заң мынадай бөлімдерден тұрады; I Тарау. Жалпы ережелер; II Тарау. Электронды құжат; III Тарау. Электронндық сандық қолтаңба.

Электрондық қолтаңба және электронды құжат (документ) жүйесін ендіру және жұмыс жасау үшін сол құжаттар сенімді түрде қорғалған болуы керек. Әрбір адам өзінің Біріздендірілген нөмерлеріне ие болып, сол нөмірде оған тиісті барлық құжаттар сақталады: төлқұжат, СТН, ӘЖҚ тағы сол сияқтылар.

Әрине бұл құжаттар өте сенімді түрде сақталуы тиіс. Мұның барлығы Ғаламтор жүйесі арқылы орындалады.

Банк жүйесінің құжаттары, фирмалардың құжаттары, өкіметтің басқару құжаттары, жеке адамдардың құжаттары атап өтілген жүйеде сақталады. Бұлардың сенімділік және құпиялық дәрежелері әртүрлі болғанымен барлығында да құжаттар "бөтен" адамдардан сенімді түрде қорғалған түрде болады. Ол құжаттар "өзгеріп" қалуынан да сенімді түрде сақталу керек. Құжаттардың көшірмесі керек болған жағдайда "Жүйе" сол көшірмені сенімді түрде бере алады. Электронды қолтаңба жәй қолданылып жүрген қолтаңбаға эквивалент болып, ол қолтаңбалы өзгертіп қою мүкіншілігі болмайды. Бұл құжаттарды ұрлап алуы, оны өзгертіп шығару мүмкіншілігі де болмайды. Бұл жұмыстарды атқарудағы негізгі мақсат - адамдардың құжаттар жасау немесе олармен жұмыс істеуде кеткен уақыты мен қаражатын үнемдеу. Сонымен адамдардың құжаттармен жұмыс істеуін автоматтандыру арқылы коррупцияны кемейтіп, адамдардың әлеуметтік жағдайын жақсарту болды.

“Электронды Үкіметті” құруда әртүрлі түрдегі мәліметтер электронды жүйеде сақталып, өңделеді және бір жерден басқа жерге жеткізіледі. Мұнда ақпаратты қорғау мәселесі негізгі мәселелердің бірі болып, ол көпдеңгейлі мәселенің ең жоғары деңгейінде **Үкіметтің Заңы** тұрады; бұл Заң Қазақстанда 2003 жылы қаңтарда қабылданған. Ақпаратты қорғаудың ең нәтижелі деңгейі бұл ***криптографиялық қорғау*** деңгейі болады.

5.6.1 “Электронды Үкімет” құруда ақпараттық желілердегі қауіпсіздік мәселелері

“Электронды Үкімет” құруда Үкімет шығарған заңдар мен нұсқаулар “Akorda.kz” сайтында сенімді түрде сақталады. Мұнда ақпараттарға электронды қолтаңба қойылып, шифрленіп сенімді түрде сақталады.

Сол берілгендерді ешқандай өзгерту мүмкіншілігі болмайды. Автордың өзі де сол құжаттарды өзгерте алмайды.

Автордың қолында “жабық кілт” болса да документ шифрленгенде сол күнгі дата қоса шифрленеді. Ал ашық кілттер сертификатталып, бұзғыншының қолына туссе де ол зиян келтіре алмайды.

Бұзғыншы басқа күнде құжатты бұзбақшы болғандығы себепті сол жабық кілтке қол жеткізгенде де құжаттарды өзгерте алмайды.

Сондықтан бұл құжаттар өте сенімді түрде сақталады. Олардың түпнұсқалылығын анықтау үшін аудит тексеру жүргізеді.

“Аутентификация” – түпнұсқаны тексеру үдерісі. Мұнда аудиттиісті кілттер жәрдемінде түпнұсқаны тексереді. Егер ол өзгерген болса, кілт өзгергендігін табады. Ал, егер өзгермеген болса, түпнұсқаның өзгермегендігін анықтайды. Бірақ аудиттің өзі де құжаттарды өзгерте алмайды. Қай жерде қандай өзгеріс болғандығын ол да анықтай алмайды.

Егерде құжат өзгерген болса, онда оны қайта орнату мүмкіншілігі бар. Басқа қорларда (базаларда) да құжаттардың көшірмелері шифрленген түрде сақталып, солардың жәрдемінде документ қайта орнатылады.

Ал енді бір құжаттарды арналармен басқа жерге жіберу үшін шифрлеу жүйесі қолданылады. Мұнда құжат шифрленіп және қысқартылып арналармен жіберіледі. Бұл жүйенің бірнеше түрі бар.

Симметриялы жүйелерде кілттер иерархиялы, яғни бірнешеу

болады. Мұнда бірінші кілт - жұмысшы кілт деп аталып, құжат сол кілтпен шифрленеді. Ал енді бұл кілттер негізінде сақталып, оны тарату үшін, екінші орынды кілтпен шифрленеді.

Екінші орынды кілттер ең жоғарғы кілтпен бірге бір жерде сақталады. Оны тек желі администраторы немесе қауіпсіздікке жауапты адам ғана білуі мүмкін. Бірақ бұл кілт уақытымен өзгертіліп отырады. Бұл жүйенің кемшілігі - кілттерді сақтау және қолданушыларға таратып беру өте қиынға соғады.

Қазіргі уақытта **ассиметриялы жүйелер**, яғни ***ашық кілтті*** жүйелер кең қолданылып келеді. Мұнда екі түрлі кілт болады: ашық және жабық кілттер.

Ашық кілттер сертификатталып, қолданушылардың бәріне таратылады. Таратуда жоғары орынды кілттер қолданылады. Хабарлар сол ашық кілтпен шифрленіп, тиісті абонентке жіберіледі. Сонда шифрды тек сол хабар алушы абонент қана аша алады. Басқа абоненттер және жіберуші автордың өзі де шифрды аша алмайды. Жабық кілттер ешқашан арналармен жіберілмейді. Бірақ та ашық кілт "дұшпанның " қолына түссе, ол біреудің атынан шифрлеп мәтін жіберуі мүмкін. Бұл - әрине жүйенің кемшілігі. Бірақта оңай және жылдам болғандығы себепті бұл жүйе кең қолданылады. Бұл жүйенің және бір кемшілігі – ашық кіліттерді генерациялау өте қиын болып, кей уақытта машинаның дәреже сеткасы жетпей қалуы да мүмкін. Себебі ассиметриялы жүйені (системаны) қолданған уақытта өте үлкен сандарды бөле отырып, олардан шыққан қалдықты анық табу керек. Мұнда машиналар үлкен сандармен істеген уақытта "жылжымалы үтір" тәртібінде істеп болмайды; себебі қалдықтар жуықталып кетеді. Ал бұл жүйеде тек қана "фиксацияланған (таңбаланған) үтір" тәртібінде істеу керек болады.

Қазіргі уақытта жалпы қолданудағы машиналардың дәрежесі 64 тен аспайды. Ал кіші сандарды қолдану жүйенің сапасын төмендетеді. Бұл - ашық кілтті жүйенің негізгі кемшілігі.

Электронды Үкіметте құжаттар құпия түрде сақталады. Мұнда көбінесе симметриялы жүйе қолданылып, кілттердің үшеуі де бір жерде сақталады. Ол кілттер арна арқылы шифрлеп жіберіледі. Симметриялы жүйені жергілікті деректер қорында қолданғанда сенімділігі өте жоғары болады.

Осы мәселелердің барлығы да қазіргі кезде Электронды Үкіметтің негізгі мәселелері болып табылады.

Осы бөлімде қауіпсіздік мәселелерінің ең негізгісі болған криптография әдістері мен бағдаржолдары қаралады. Соның ішінде қарапайым бағдаржолдар мен DES және ГОСТ-тың негізін құрушы алмастыру, орын ауыстыру, тізбектер және кешенді бағдаржолдар, гаммалау бағдаржолы, RSA бағдаржолымен шифрлеу және қолтаңба жасау бағдаржолдары қарастырылады.

Зертханалық жұмыстарда олар MS Excel- де үлгілеумен зерттелген.

Сонымен бірге Электрондық Үкіметте қолданылатын барлық бағдаржолдарға тиісті шолу жасалған: Эль-Гамаль, RSA, Диффи-Хельман және тағы басқа бағдаржолдарға талдау берілген.

Бұл бағдаржолдар мен бағдарламалар осы қолданбада MS EXCEL-де түзілген болып, ол нақты уақытта істеу мүмкіндігін береді. Бұл оқыту үдерісінде электрондық тақтада үдерістерді нақты уақытта көрсетуге және оқыту үдерісін өте нәтижелі жүргізуге мүмкіндік береді.

5.6.2 Мәліметтердің қауіпсіздігін қамтамасыз ету жүйелерінің құрылымы және ұйымдастыру қағидалары. Ақпараттық қорғаудағы криптожүйеге қойылатын талаптар

Ақпараттық қорғауда құпиялық дәрежелері

Мекемеге немесе фирмаға өзінің тұрақты қызметін қамтамасыз ету үшін әртүрлі қауіп-қатерлерден сенімді қорғанысты ұйымдастыруы қажет. «Қауіп-қатер» термині зиянға әкеліп соғатын, қандайда бір іс-әрекеттерді білдіреді. «Қауіпсіздік» дегенде «қауіп-қатер»-лерді болдырмау түсініледі.

Рұқсат етілмеген ақпаратқа рұқсат алу – ақпаратты техникалық құралдарда өңдеу кезінде рұқсатсыз техникалық құралдардың көмегімен алу.

Ақпаратты жою дегеніміз қандайда бір әрекеттердің нәтижесінде ақпарат техникалық өңдеу құралдарында өз жұмысын тоқтатуы.

Жалған ақпарат – техникалық өңдеу құралдарында әдейі шатастыратын жалған ақпарат жасау.

Келесідей әсерлердің нәтижесінде ақпараттардың қауіпсіздігі бұзылуы мүмкін:

1) қоршаған ортаның әсерлері (дауыл, жер сілкінуі, өрт, су басу және т.б.);

2) бұзушының қасақана әрекеттері (шпионаж, ақпараттық есептеу жүйелерінің құрамдас бөліктерінің бұзылуы және т.б.);

3) ішкі әсер, ықпаллар (аспап істен шығуы, математикалық және бағдарламалардағы қателіктер, жұмысшылардың жеткіліксіз кәсіби дайындығы).

Мәліметтер қауіпсіздігі дегеніміз – өңделетін, сақталатын, мәліметтерді кездейсоқ немесе қасақана алу, өзгерту, жою мүмкін болмаған жағдай.

Мәліметтерді қорғау – мәліметтердің қауіпсіздігін қамтамасыз етуге бағытталған әрекеттердің жиынтығы.

Мәліметтерді қорғау әдісі – мәліметтерді қорғау қатыстарын (мысалы, пароль қою әдістері, шифрлік әдістер және т.б.) іске асырушы әдістер жиыны.

Мәліметтерді қорғау әдістері негізінде қорғау құралдары жасалады (мысалы, шифрлеу (дешифрлеу) құрылғылары, пақызмет талдау бағдарламалары, қорғау сигналдарының көрсеткіштері, авторлық құқықтар туралы заңдар және т.б.). Қорғау механизмі – мәліметтерді қорғау құралдарының жиынтығы (мысалы, критографиялық протоколдер, операциялық жүйені қорғау механизмдері және т.б.).

Ақпараттық қауіпсіздікті қамтамасыз ету шаралары бес түрге бөлінеді:

1) заңды (заңдар, нормативті актілер, үлгіқалыптар);

2) моральдық-этикалық (жүріс-тұрыс қалыптыары, оларды орындамау адам мәртебесі жоғалуына алып келеді);

3) әкімшілік (ұйым басшыларының әрекеттері);

4) физикалық (бұзушылардың механикалық, электро-магниттік кедергі келтіруі);

5) аспаптық-бағдарламалық (электронды құрылғылар және ақпараттарды қорғау арнайы бағдарламалары).

Барлық ақпарттардың шығу арналары (утечка) жанама және түзу арналарға бөлінеді.

Жанама арналарда ақпараттық жүйелерге қосылу талап етілмейді. Жанама арналар бөлмелердің жеткіліксіз оқшаулаудан (изоляциялануынан) келіп шығуы мүмкін (тыңдаушы құрылғыларды қолдану, ұзақтан сүретке түсіру, электро-магниттік сәуленулердің ұстап қалынуы және т.б.)

Түзу арналар техникалық құралдарға жалғануды талап етеді. Түзу

арналардың болу себептері техникалық және бағдарламалық қорғау құралдарының жеткіліксіздігінен, операциялық жүйеден, деректер базасын басқару жүйелерінен болуы мүмкін.

Ақпарат құндылығы екі үлкен топ бойынша бағалануы тиіс:

- ақпараттың тағайындалуы бойынша;
- оны өңдеу шарттары бойынша.

Бірінші топта екі шартты көрсетуге болады:

- қауіпсіздікті қамтамасыз ету шараларының маңыздылығы;
- сәйкес шараларды орындау үшін ақпараттың маңыздылық деңгейі.

Екінші топта екі шартді көрсетуге болады:

ақпаратты өңдеу кезінде болатын жоғалтулар деңгейі;

- ақпаратты қайта қалпына келтіруге кететін шығындар.

5.6.2.а Ақпараттық қорғаудағы криптожүйенің құрылымы және ұйымдастыру қағидалары

Ақпараттарды өзгертуден және оны өзге адамдардың оқуынан қорғау бұрыннан келе жатқан мәселе.

Криптография тарихы - адам тілімен тетелес тарих. Сонымен қатар, алғашқы жазылған криптографиялық жүйені ескі қоғамда тек таңдалған адамдар басқарған.

Бірінші криптожүйе біздің эрамыздан әлдеқашан алдын кез-дескен. Юлий Цезарь патша өзінің жазбасында біршама жүйелік шифрды қолданған. Оның жаратқан бағдаржолы осы кезде оқыту бағдаржолы түрінде қолданылады.

Бірінші және екінші әлемдік соғыс жылдарында криптографиялық жүйелер қарқынды дамыды.

Осы кезде Электронды Үкімет құруда криптографиялық жүйелер негізгі жүйелерге айналды.

Не үшін криптографиялық әдістер қолданылған мәселе ақпараттық жүйеде қазіргі мезетте ерекше көкейкесті (актуалды) болды?

Бір жағынан компьютерлік желі және ғаламдықды желіге қосылған Ғаламторды қолдану кеңейтіліп, одан басқа адамдар үлкен көлемді мемлекеттік ақпараттарды, әскери және жеке құжаттарды алуға мүмкіндік көбейді.

Басқа жағынан алып қарағанда жүйелік және нейрондық

есептеулердің технологиясының дамуы, жаңа компьютерлердің пайда болуы, криптографиялық жүйе дискриптациясының ашу мүмкіндігін берді.

Ақпаратты қорғауды оны өзгерту жолымен амалға асыру мәселесімен **криптография айналысады (kryptos - құпия, logos-ғылым).**

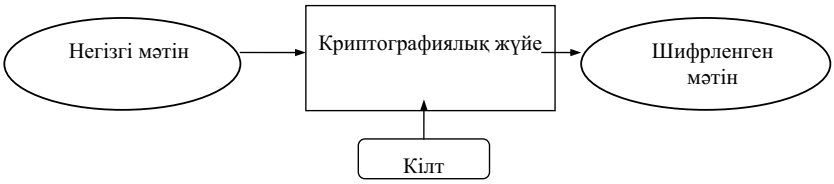
Криптология екі бағытқа бөлінеді: Криптография және Криптоталдау. Осы екі бағыттың мақсаты қарама-қарсы.

Криптография **–** берілген ақпаратты шифрлеу (кодтаудың бір түрі) арқылы жабық (адам түсінбейтін) түрге өзгертетін математикалық әдістер мен бағдаржолдарді іздеумен және құрумен айналысады.

Криптоталдау – шифрленген ақпаратты санақтық немесе басқа әдіспен талдау арқылы шифрлеу кілтін білмей тұрып, ақпаратты ашық түрге келтіру әдістерімен шұғылданады.

Қазіргі кезде криптография үлкен төрт бөлімге бөлінеді:

1. Симметриялы (жабық кілтті) криптография жүйелері.
2. Симметриялы емес (ашық кілтті) криптография жүйелері..
3. Электронды қолтаңба жасау жүйесі.
4. Кілттерді басқару жүйесі.



Криптографиялық әдістің негізгі бағыттары - байланыс арналары арқылы құпия ақпаратты жіберу және құпия түрде жеткізіп беру, ақпараттың түпнұсқасын тексеру (аутентификация) және өзгертулерді (подделка) анықтау, ақпаратты шифрленген түрде құпия сақтау.

Криптография ақпаратты құпия түрге өткізуде (шифрлеуде) тек кілтті қолданғанда ғана істей алады. Криптографияда мәтінтерді шифрлеу және шифрді кері талқылауда шифрленетін және дешифрленетін ақпарат көбінесе мәтін түрінде болып, ол кейбір әліпби негізінде құрылады.

Бұл терминдерді былай түсіндіреміз:

- Әліпби - ақпаратты кодтау үшін керек болған таңбалардың шекті жиыны.
- Мәтін - әліпбидің элементтерінің тәртіпті жиыны.

Қазіргі кездегі ақпараттық жүйеде қолданылатын әліпбилерге келесідей мысалдар келтіруге болады:

- Әліпби Z^{3} -32 орыс әліпбиінің әріптері және бос орын;
- Әліпби Z^{256} - ASCII және KOU-8 үлгіқалыпты кодтарының таңбалары.
- Екілік (бинарлы) әліпби- $Z^{2}=\{0,1\}$
- Сегіздік әліпби немесе он алтылық әліпби;

Шифрлеу – берілген ашық мәтінді шифрленген мәтінге айналдыру үдерісі.

Дешифрлеу - шифрлеу үдерісіне қарама-қарсы үдеріс болып, мұнда шифрленген мәтінді ашық мәтінге айналдырылады.

Негізгі мәтінді шифрлеу және дешифрлеу кілтпен амалға асырылады.

Кілт - мәтіндерді шифрлеу және дешифрлеу үшін қажетті ақпарат.

Криптографиялық жүйе - ашық мәтінді өзгертулермен жабық мәтінге айналдыру және керісінше амалдарды орындайтын жүйе.

Бұл жүйенің таңбасы k - деп таңбаланып, мұнда k - кілт болып табылады.

Кілттер кеңістігі К – бұл кілттердің шамаларының жиыны. Әдетте кілт әліпбидік таңбалардың тізбектелген қатары болады.

Криптожүйе симметриялық (жабық кілт) және ашық кілт (симметриялы емес) болып бөлінеді.

Симметриялық криптожүйеде шифрлеу және дешифрлеу үшін бір кілт және бір сұлба қолданылады.

Ашық жүйеде екі кілт қолданылады; олар бір-бірімен математикалық байланысқан ашық және жабық кілттер жүйесі. Барлық қолданушы адамдар ақпаратты ашық кілттің көмегімен шифрлей алады. Олардың қолында ашық кілт болады. Ал тек хабарламаны алған адам ғана өзінің жабық кілтімен шифрды аша алады.

Кілттерді тарату және басқару жүйесінде қолданушылар тобы арасында кілттерді құру және тарату мәселелері ақпаратты өңдеу жүйелерінде шешіледі. Мысалы, банк пен абонент арасында екі кілт болады; ашық кілт - банкте, ал жабық кілт - абоненттің өзінде болады. Платежканы абонент жабық кілтпен толтырып, банк оны ашық кілтпен оқиды. Бірақ ешкім оны өзгерте алмайды.

Автор жабық кілтпен мәтінді криптографиялық өзгерту жәрдемінде қолтаңба жаратады; мұнда ол **сигнатура** жаратып, қолданушыларға ашық кілтпен бірге сигнатура жібереді. Егер мәтіннің бірер әріпі өзгерсе, онда ашық кілт пен сигнатура мәтінді аша алмайды. Себебі ашық кілт екінші рет сигнатураны жаратқанда берілген сигнатурамен айырмашылығы болады. Сондықтан шифр ашылмайды.

Электронды қолтаңба мәтінді криптографиялық өзгертулермен оған қосылады; мұнда мәтінді басқа пайдаланушы алған кезде оның ***авторлығын*** және хабарламаның ***шындығын*** тексере алады.

Криптотұрақтылық - бұл шифрдың сипаттамасы болып, білім кілтісіз дешифрлеудің қиындығын анықтайтын көрсеткіш; бұның сипаттамасы - оны **кілтсіз дешифрлеуге кететін уақыттың** немесе **амалдардың мөлшерімен** анықталады. Криптотұрақтылықтың көптеген көрсеткіштері бар; олар мыналар:

- Барлық мүмкін болған кіліттердің мөлшері;
- Криптоталдау үшін қажет болған орташа уақыт мөлшері.

Криптографияның мақсаты - өзгертулерге тиісті бағдаржол және k параметрдің мәнін анықтау. Шифрлеудің ақпаратты қорғаудағы мақсаты криптотұрақтылық шифрімен шифрлеу және құпия кілтті сақтау болып табылады.

5.6.2. б Криптожүйеге қойылатын талаптар

Компьютер желілерінде қауіпсіздікті сақтау үшін шифрлеу әдістеріне әртүрлі үлгіқалыптар (стандарттар) ендірілген (мемлекеттік, ұлттық және халықаралық); мысалы үшін, АҚШ-та үлгіқалыптардың ұлттық бюросы 1977 жылы DES[77] (Data Encryption Standard) атты деректерді шифрлеу үлгіқалыбын қабылдап, ол 2001 ж. дейін қолданылып келді.

Осы үлгіқалыпты екі режим қолданылды: КАК (Key Auto Key) және СТАК (Cipher Text Auto Key). КАК тәртібінде деректер 64 биттік бөліктермен (порциялармен) шифрленеді. Кілт те ұзындығы 64 бит болады. СТАК (тәртібінде) жүйе стартстоп тәртібінде істеп, мұнда деректер 8 битпен шифрленеді; мұнда әріптер шифрленеді.

DES те алмастыру мен орын ауыстыру әдістері тізбектеп қолданылады. Осы кезде бұл бағдаржол өте күрделі болып, оның криптотұрақтылығы заман талаптарына сай емес.

Криптотұрақтылықты бағалау үшін **абсолютті крипотұрақтылық** түсінігі ендірілген болып, ол Шеннон бойынша былай анықталады: “ ... егер шифрді алу үшін ашық мәтінге біркелкі таралған кездейсоқ гамманы қосатын болсақ, онда алынған шифр абсолютті тұрақты болады...”. Мұнда кездейсоқ гамманың кезеңі (периоды) амалда шексіз болуы керек.

Криптографиялық қорғау үдерісі мәліметтерді әрі бағдарламалық, әрі ақпараттық түрде амалға асырылады. Аспаптық қорғауды жүзеге асыру - қымбат болғанымен оның абзалдықтары көп; жоғары жылдамдық, қарапайымдылық, қорғанудың жоғары деңгейі т.с.с.; сондықтан бағдарламалық қорғау кең қолданылады.

Қазіргі кездегі криптографиялық жүйе үшін ақпараттық қорғауды тұжырымдап айту келесі талаптардан тұрады:

- шифрленген хабар (мәтін) тек кілттің жәрдемінде ғана алынуы мүмкін болуы керек;
- шифрленген хабарға және ашық мәтінге қолданылған шифр кілтін анықтау үшін керек болған амалдар саны мүмкін болған кілттер санынан аз болмауы тиіс;
- барлық кілттерді орын ауыстыра отырып жасай отырып шифрлеу кілтін іздеудегі амалдар санының ең төменгі анық бағасы болуы керек және бұл көрсеткіш заманды есептеу технологиясының мүмкіндіктерінен жоғары болуы керек (желілік есептеулерді қоса есепке алғанда да);
- шифрлеу бағдаржолын білу қорғау тұрақтылығына әсер етпеуі керек;
- шамалы ғана өзгертілген кілт шифрленген хабардың өте үлкен өзгеруіне әкелуі керек;
- шифрлеу бағдаржолының құрылымдық элементтері өзгермеуі керек;
- шифрлеу үдерісінде қолданылатын қосымша биттер шифрленген мәтінде толығымен және сенімді түрде құпиялы болуы керек;
- шифрленген мәтіннің ұзындығы негізгі мәтіннің ұзындығымен бірдей болуы керек;
- шифрлеу үдерісінде тізбектеп қолданылатын кілттердің арасында қарапайым және оңай тәуелділік болмауы керек;
- әрбір кілт ақпараттардың сенімді қорғалуын қамтамасыз етуі керек;

- бағдаржол әрі бағдаржолдық, әрі бағдарламалық түрде орындалу мүмкіндігі болуы керек; мұнда кілт ұзындығының өзгеруі шифрлеу бағдаржолының сипатының өзгеруіне әкелмеуі керек.

5.6.2.в Ақпараттық қорғауда құпиялық дәрежелері.

Компьютерлі желілерде ақпаратты қорғаудың бірнеше дәрежесі бар.

Ең жоғарғы дәреже - Мемлекеттік Заң негізінде ақпараттарды қорғау.

Мұнда Мемлекттік Заңдар, баспада басылып шыққан құжаттар және т.б. құжаттар компьютер желілерінің тиісті сайттарында сақталып, ол құжаттар баспада шыққан құжаттар сияқты **сол дәрежеде** сақталады.

Егерде ол құжаттарды өзгертуге әрекет жасалса, мұндай әрекет жасаушылар **Заң алдында жауапқа тартылады;** демек, мемлекеттік Заңда компьютерлік ақпаратты (информацияны) ұрлау немесе бұзу әрекеттерін шектеп, бұзғындарға қарсы тиісті жаза қолдану мәселелері көрілген; мысалы, лицензиялы бағдарламаларды сатып алып, көбейту және сатуға тыйм салынады; Заң авторлардың құқұғын қорғайды.

Дәл сондай Ғаламтор желісіндегі сайттарға кіріп, олардағы информацияны өзгерту де мүмкін емес; оған да тиісті жаза шаралары қолданылады.

Хакерлер жабық, яғни құпия сайттарды ашып, ондағы ақпараттарды оқуына да тыйм салынады: ол ақпараттар шифрленген болып, хакерлер шифрдің кілтін бұзуы мүмкін. Әрине, мұндай жағдайда да бұзғыншыларға жаза қолданылады. Адамдар компьютерлік бұзғыншылық үшін Заң алдында жауап беретіндігін жақсы түсінуі керек.

Қорғанудың одан төменгі дәрежесі – административті бақылау; мұнда мекеме шығарған заңдар ақпаратты қорғауы тиісті. Мекемеде қолданылатын документтерге 3 түрлі құпиялық дәрежесі қойылуы мүмкін; ең төменгі дәреже - қызметте қолдану үшін (орысша - для служебного пользования – ДСП грифімен). Мұндай құжаттарды тек сол мекеменің сол жұмыспен айналысатын адамдары ғана жұмыс жүргізу мақсатында ғана қолданады. Бөтен адамдар қолдануы мүмкін емес.

Одан жоғарғы дәреже – Құпиялы (Секретно – С грифімен); мұндай құжаттар тек арнайы 1-бөлімде ғана сақталады да мекеме бастығы және сол бөлімнің бастығы мен сол құжатпеп жұмыс істейтін тізімде көрсетілген адамдар ғана қолданады.

Өте құпиялы құжаттар (Совершенно секретно – СС грифімен); мұндай құжаттармен Үкімет басы және сол құжатқа тиісті адамдар ғана таныс болады.

Физикалық қорғау орынында құжаттар темір сейфтарда, темір есіктермен және т.с.с. мен қорғалады. Бірақ көп жағдайда компьютер жүйелерде аталған әдістер қолайлы бола бермейді; сондықтан басқа әдістерді қарастырамыз.

Пақызметдік әдістерде әр қолданушы өзінің жеке пақызметін қойып, соны қолданады. Әрине, бұл әдісті тек компьютерге кірерде ғана қолданса болады; бірақ бұл әдісті ақпаратты желімен жіберуде қолданып болмайды.

Ақпаратты желімен жіберуде өте сенімді жақсы әдіс – **криптографиялық әдіс.** Бұл пәнде криптографиялық әдістердің кейбірін ғана қарастырамыз.

5.6.3 Қарапайым алмастыру шифрінің бағдаржолы

Мұнда хабардың әріптері сол әліпбидегі немесе басқа әліпбидегі әріптермен алмастырылады. Орын ауыстыру бағдаржолы алмастыру бағдаржолы мен бірге кешенді түрде **DES, ГОСТ** бағдаржолдарының негізін құрайды. Бұл бағдаржол, негізінен, моноәліпбилік криптографиялық жүйелерде қолданылады. Алайда көпәліпбилік жүйелерде де қолданса болады.

Алмастыру немесе Цезарь бағдаржолы.

Цезарь бағдаржолы алмастырудың (замена) бір түрі болып табылады. Ол моноәліпбилік алмастыру тобына жатады. Бұл бағдаржолды оңай түсіндіру үшін берілген әліпбидегі әріптерді бір қатарға жазып шығайық; екінші қатарда сол әріптерді солға қарай бір әріптік орынға (позицияға) жылжытып жазайық. Үшінші қатарға және бір қатарға солға қарай жылжытып жазайық және сол сияқты жолмен қатарларды толтырып шығамыз. Шифрлеу кілті бүтін санмен берілген болады. Мысалы үшін, кілт екіге тең болсын. Сонда бірінші қатардан берілген сөздің әріптерін нөмірлеп шығып, үшінші қатардан сол әріптерге сәйкес келетін әріптерді нөмірлейміз; соны-

мен берілген сөз шифрленді. Осы бағдаржол аналитикалық түрде былай жазылады:

$$c_j = i_j + b \bmod N,$$

c_j – j-ші әріптің шифрі; i_j – ашық мәтіннің j-ші әрібі; b - кіліттің сандық мәні; N – әліпбидің ұзындығы.

Осы шифрді дешифрлеу операциясы "+" таңбалы "–" таңбамен ауыстырумен орындалады; яғни шифрленген сөздің әріптерін төменгі үшінші қатардан нөмірлеп, ал сол әріптерге сәйкес келетін дешифрленген сөздің әріптерін бірінші қатардан оқимыз.

Алайда бұл бағдаржол тек қолда шифрлеуді түсіндіру үшін берілді. Ал компьютерлік жүйеде әрбір әріптің нөмірі (коды) екілік санақ жүйесінде жазылған болып, оларды шифрлеуде де, дешифрлеуде де "+", "-" орнына тек екілік модулде қосу $\oplus$ операциясы істетіледі; яғни бір кілт және бір сұлба істетіледі.

Ал амалда қолда шифрлеу үшін төмендегі Виженер кестенсін қолданған жөн. Осы кесте ағылшын әліпбиі үшін төменде келтірілген.

Мысалы: Кілт үшке тең болғанда, әріптер төменгі кестеде көрсетілгендей орын алмасады; мысалы, А әрпінің орнына г әрпі; Б әрпінің орнына д әрпі, В әрпінің орнына е әрпі және сол сияқты алмастырулар орындалады.

1-кесте.

А→г	Й→м	Т→х	Ы→ю
Б→д	К→н	У→ц	Ь→я
В→е	Л→о	Ф→ч	Э→_
Г→ж	М→п	Х→ш	Ю→а
Д→з	Н→р	Ц→щ	Я→б
Е→и	О→с	Ч→ъ	_→в
Ж→й	П→т	Ш→ы	
З→к	Р→у	Щ→ь	
И→л	С→ф	Ъ→э	

Таңбалардың орын алмасуы берілген шифр қадамына немесе кілт ұзындығына байланысты болады. Мысалы үшін, кілт ұзындығы бірге тең болса, А әрпінің орнына Б әрпі, Б әрпінің орнына В әрпі, т.с.с. лар жазылады. Өзінің қиын еместігі және өте қарапайымдығына қарамастан бұл бағдаржол осы кезде қолдану таппады; себебі кілтті компьютерсіз ақ жай әліпбиді жылжытумен оңай тауып алса болады.

Дегенмен оқыту мақсатында аталған шифрлерді қолданса болады. Төменде соларды қарастырамыз.

5.9 *Зертханалық жұмыс*

Цезарь немесе Алмастыру бағдаржолы мен шифрлеу бағдарламасы

Алмастыру бағдаржолы ең көне бағдаржолдардың бірі болып, оны Ерте Грекияда Гай Цезарь хаттарды құпия жазуда қолданған.

Бұл бағдаржолды MS Excel-де шифрлеу үшін, кітаптың бірінші бетін ашып, бірінші қатарға бағандардың аттарын қойып шығамыз; бірінші А бағанында ашық хат әріптері жоғарыдан төмен қарай баған бойынша жазылады.

Мысалы, хабар ретінде латын әліпбиінің әріптері қолданылған; *a,b,c,d,e,f,g,h,I,j,k,l,m,n,o, p,r, s, t,u,v,w, x,y,z, q*.

Кейінгі В бағанында әріптерге сәйкес келетін олардың кодтары жазылады; мысалда әріптер ондық натурал сандармен кодталған; 1,2,3,4,5,6,7,8,9,10,11,12, 13,14,15,16,17, 18, 19,20,….

Кейінгі С бағанында шифрлеу бағдаржолының кілті жазылады; мысалда, 7 жазылған. D бағанында шифрленген ақпарат жазылады; шифрлеу бағдаржолы келесідей: D2 =B2+C2.

Нақты жүйелерде шифрлеу бағдаржолында ондық қосу амалының орнына екілік модулде қосу амалы орындалады да, ал қосылғыштар екілік түрде болады.

Сонда шифрленген хабар келесідей болып: 8,9,10,11,12,13,14,15, 16,17,....., *g,h,i,j,k,l,m,n,o,p,...* әріптеріне сәйкес келеді.

Шифрленген хабар ақпараттар қоймасында сақталып, немесе арнамен жіберілуі мүмкін.

Шифрленген хабарды жіберу үшін оның көшірмесін алып, MS Wordқа тастаймыз; ол жерден көшірмесін алып MS Excel-дің басқа бағанына-F2 немесе басқа листке жазамыз. Мұның себебі, арнаның қабылдаушы ұшы жіберуші ұшымен ешқандай корреляцияланбаған болуы керек. G2 ге кілтті жазамыз. Ал H2 де келесідей түрде дешифрленген хабарды шығарып аламыз: H2= F2-G2.

Нақты жүйелерде шифрлеу бағдаржолында ондық айыру амалының орнына екілік модулде қосу амалы орындалады.

Сонда арнаның екі ұшында да екілік қосу орындалады да, біртүрлі электрондық сұлба қолданылады.

Сондықтан да мұндай шифрлеу жүйесі симметриялы жүйе деп аталады. Төмендегі суретте бағдаржолдың MS Excel-дегі көрінісі берілген.

	A	B	C	D	E	F	G	H	I
1	әріптері	коды	1-кілт	шифр1		шифр2	2-кілт	дешифр	әріптері
2	a	1	7	8		8	7	1	a
3	b	2	7	9		9	7	2	b
4	c	3	7	10		10	7	3	c
5	d	4	7	11		11	7	4	d
6	e	5	7	12		12	7	5	e
7	f	6	7	13		13	7	6	f
8	g	7	7	14		14	7	7	g
9	h	8	7	15		15	7	8	h
10	i	9	7	16		16	7	9	i
11	j	10	7	17		17	7	10	j
12	k	11	7	18		18	7	11	k
13	l	12	7	19		19	7	12	l
14	m	13	7	20		20	7	13	m
15	n	14	7	21		21	7	14	n
16	o	15	7	22		22	7	15	o
17	p	16	7	23		23	7	16	p
18	r	17	7	24		24	7	17	r

5.1-сурет Алмастыру бағдаржолының MS Excel-дегі бағдарламасының көрінісі

Көп әліпбилі жүйелер; бір рет пайдаланатын жүйелер.

Көп әліпбилі алмастыруладың әлсіз криптотұрақтылығы көп әліпбилі алмастыруларды қолдану арқылы шешіледі.

Көп әліпбилі алмастыру өзінде әртүрлі, кем дегенде екі алмастыруды қамтитын $\pi=(\pi_1, \pi_2, ...)$ кілтімен анықталады.

Алдымен көп әліпбилі жүйелер алмастырулардың нөлдік бастапқы қиылысуын қарап өтейік.

Мейлі $\{K_i: 0\le i<n\}$- бағынымсыз кездейсоқ ауыспалы бірдей мүмкіншіліктерінің орналасуы Zm көбейтіндісінің мәнін көрсетуші болсын.

$$P\text{кл}\{(K_0, K_1, ..., K_{n-1})=(k_0, k_1, ..., k_{n-1})\}=(1/m)^n$$

Бір рет қолданылатын жүйе шығу мәтінінін

$$X=(X_0, x_1, ..., x_{n-1})$$

шифрленген мәтінге былай өзгертеді.

$$Y=(Y_0, y_1, ..., y_{n-1})$$

ол үшін келесідей Цезарь алмастыруын қолданылады:

$$Y_i=C_{Ki}(x_i)=(K_i+X_i) \pmod m \; i=0...n-1 \quad (5.1)$$

Бұл алмастыру жүйесінде келесідей терминдер “бір реттілік лента” және “бір реттілік жиынтықнот” пайдаланады.

К кілттердің кеңістігі жүйесі бір реттілік алмастыруы (K_0, K_1, ..., K_{n-1}) рангты векторы болады да және де m^n нүктелерін ұстайды.

Шексіз кілттер шифрленуінің бір мысалын қарайық. Кілт ретінде келесідей мәтін қабылдайық: ”БЕСКОНЕЧНЫЙ КЛЮЧ”

Оның көмегімен келесідей мәтінді ”Шифр_нераскрываем” шифрлейміз.

Шифрлеуді кестеге жазамыз:

Ш	И	Ф	Р	У	Е	М	Ы	Й	_	МӘТ											
Б	Е	С	К	О	Н	Е	Ч	Н	Ы	Й	_	КЛ									

Шыққан мәтінді кілтсіз қалпына келтіру мүмкін емес.

Шексіз кілттер ретінде “ақ дыбысты” шығарып, мәтінге қосу тілдің санақтық сипаттамаларын өзгертеді.

Мұнда бір рет қолданылатын жүйелер теориялық жағынан дешифрлеуі шешілмейді десе болады; себебі мәтінді орнына келтіру үшін керекті мағлұматтар табылмайды.

Мағлұматтарды өңдеуде кезінде бұл құпиялылықты сақтау жүйесі қолданылуға жарамайтындығы неде? Жауабы оңай - олар икемсіз болып, әрбір әріп үшін шығу мәтінінде кілт мағынасында тәуелсіз таңдауды қажет етеді. Мұнда негізгі қиыншылық - кілтті жеткізіп беруде; себебі кілт –тәуелсіз кездейсоқ сандар тізбегі болады.

5.6.4 Виженер шифрлеуінің бағдаржолы.

Виженер шифрлеуін оңай түрде былай түсіндірсе болады; алмастыру шифрінде бір кілтті істеткен болсақ, енді оның орнына бірнеше кілттер алайық немесе кілттер тізбегін алайық; мысалы, 123 деген кілттер тізбегін.

Осы тізбекті ашық мәтін әріптерінің үстіне қайталап жазып кете береміз, мәтін таусылғанша.

Содан кейін әрбір әріптің үстінде жазылған санға қарай отырып, сол сан мәні бойынша төменгі қатарды табамыз және сәйкес әріпті табамыз.

Бұл бағдаржол алмастыру бағдаржолына ұқсас; бірақ кілт өзгеріп отырады.

Кілт ұзындығы шексіз артқанда бұл бағдаржол гаммалау бағдаржолына айналады.

Осыдан көрініп тұрғандай мұндай жүйенің криптотұрақтылығы кілт ұзындығына байланысты болады; яғни кілт қаншалықты ұзын болса, криптотұрақтылығы да арта береді.

Егер ашық мәтін таңбалары келесідей n таңбалардан $(i_0, i_1, ..., i_n)$ тұратын болып, ал кілт L санды $\boldsymbol{k} = (\boldsymbol{k_0}, \boldsymbol{k_1}, ..., \boldsymbol{k_n})$ таңбалардан тұратын болсын; онда Виженер криптожүйесінің бағдаржолы келесідей көрсетіледі:

$$y(t) = i_t + k_t \bmod n$$

Осында айта кететініміз, осындай кілттер тізбегін гамалау деп, ал кілттің өзін – гамма деп атайды.

Кілт ұзындығы мәтін ұзындығынан кем болғанда, кілтті бірнеше рет тізбектеп қайта қоса береді. Сонымен жұмыс кілтін келесідей көрсетсе болады:

$$\boldsymbol{k} = (\boldsymbol{k_0}, \boldsymbol{k_1}, ..., \boldsymbol{k_n}),\ \boldsymbol{k_j} = \boldsymbol{k_{(j \bmod r)}},\ \boldsymbol{0 \le j < \infty}.$$

Мысалы, $r = \infty$ кезінде және пайдаланушы кілті келесідей болғанда 15 8 2 10 11 4 18 жұмыс кілті кезеңді реттілігі былай болады.

15 8 2 10 11 4 18 15 8 2 10 11 4 18 15 8 2 10 11 4 18 ...

Келесідей болғанда m=2 тең Виженер алмастыру жүйесінің нұсқасы Вернама жүйесі деп аталады.(1917)

Ол кезде $k=(k_0, k_1, ..., k_{к-1})$ кілті қағаз лентада жазылады.

Шығу мәтініндегі әрбір әріп әліпбиде кейбір көмекші таңбалармен кеңейтілген.

Алғашында Бод кодын қолдану барысында бес битті таңбалары арқылы аударылды. Бод шығу мәтініне модуль екі бойынша кілт қосылды.

AT&T фирмасының көне телетайп жүйесінде, Вернама санау құрылымының және шифрлеу үшін қондырмалары АҚШ әскерінің байланыс жүйесінде қолданылды.

Құпиялылық көзқарастан жаман әдіс - сөзді немесе сөйлемді кілт негізінде қолдану тәжірибесі (кілт оңай есте сақталады); мұнда $k=(k_0, k_1, ..., k_{к-1})$ сөзі кілт ретінде қолданылады.

Ақпараттардың қауіпсіздігін сақтауда мұндай әдісті қолдану мүмкін емес. Кілттерді шығарып алу үшін бағдарламалы немесе аспапты құралдардың кілттерді кездейсоқтық генерацияларын қолдану арқылы табу қажет.

Ал бұл гаммалау әдісі деп аталады.

Анықтама: r- көп әліпбилі кілттің шифрленуі r-жиынының $\pi = (\pi_0, \pi_1, ..., \pi_{r-1})$ элементтері болып табылады.

Виженердің жинақталған жүйесі шығу мәтінін $(x_0, x_1, ..., x_{n-1})$ шифрленген мәтінге $(y_0, y_1, ..., y_{n-1})$ $\pi = (\pi_0, \pi_1, ..., \pi_{r-1})$ көмегімен мына ережеге сай орындалады:

$VIG_k : (x_0, x_1, ..., x_{n-1}) \rightarrow (y_0, y_1, ..., y_{n-1}) = (\pi_0(x_0), \pi_1(x_1), ..., \pi_{n-1}(x_{n-1}))$.

Көп әліпбилі жүйелердің криптотұрақтылығы кілттің ұзындығының қысқаруына байланысты бірден кемейеді.

Сондай болса да Виженер шифрінің осындай жүйесі кілттің жеткілікті ұзын болғанда, аспапты немесе бағдарлы жүйелерінің оншалықты қиын болмағандығы үшін осы күнгі автоматты жүйелерде (АЖ) қолданылу тапқан.

5.10 *Зертханалық жұмыс*

Виженер бағдаржолы мен шифрлеу бағдарламасы.

Виженер бағдаржолы мен шифрлеуде кіліттер орнына өзгеруші сандар тізбегі қолданылып, ол тізбек жіберуші мен қабылдаушының екі жағына да мәлім болуы керек.

Көбінесе адамдардың туылған күні, айы, жылы қолданылады.

Бірақта мәлім сандарды қолданғанның орнына беймәлім сандар тізбегін қолданған жөн.

Мұнда сандар тізбегі қаншалықты ұзын болса, соншалықты жүйенің криптошыдамдылығы жоғары болады.

Мысалда кілт орнына келесідей тізбек қолданылған: 2,4,1,9,8,5,0,8.

D2 бағанында шифрленген ақпарат мына бағдаржолмен алынады: D2 = B2+C2. Мысалда шифрленген ақпарат мына түрде болады: 3,6,4,13,13,11,7,16,11,14,12,21,21,19,22,20,29,29,27,23,32,27,30.

Шифрленген ақпарат сақталуы немесе арнамен жіберілуі мүмкін.

Шифрленген хабарды жіберу үшін оның көшірмесін алып, MS Wordқа тастаймыз; ол жерден көшірмесін алып MS Excel дің басқа бағанына- F2 немесе басқа листке жазамыз.

Мұның себебі, арнаның қабылдаушы ұшы жіберуші ұшымен ешқандай корреляцияланбаған болуы керек. G2- ге кілтті жазамыз.

Ал H2 де келесідей түрде дешифрленген хабарды шығарып аламыз: H2 =F2-G2. Шифрлеу дұрыс орындалған болса, онда H2 және B2 бағандары бірдей болуы керек.

	A	B	C	D	E	F	G	H	I
1	әріптері	коды	1-кілт	шифр1		шифр2	2-кілт	дешифр	әріптері
2	a	1	2	3		3	2	1	a
3	b	2	4	6		6	4	2	b
4	c	3	1	4		4	1	3	c
5	d	4	9	13		13	9	4	d
6	e	5	8	13		13	8	5	e
7	f	6	5	11		11	5	6	f
8	g	7	0	7		7	0	7	g
9	h	8	8	16		16	8	8	h
10	i	9	2	11		11	2	9	i
11	j	10	4	14		14	4	10	j
12	k	11	1	12		12	1	11	k
13	l	12	9	21		21	9	12	l
14	m	13	8	21		21	8	13	m
15	n	14	5	19		19	5	14	n
16	o	15	0	15		15	0	15	o
17	p	16	8	24		24	8	16	p
18	r	17	2	19		19	2	17	r
19	s	18	4	22		22	4	18	s
20	t	19	1	20		20	1	19	t
21	u	20	9	29		29	9	20	u
22	w	21	8	29		29	8	21	w
23	y	22	5	27		27	5	22	y

5.2 - сурет Виженер бағдаржолының MS Excel-дегі бағдарламасының көрінісі.

5.6.5 Гаммалау бағдаржолы

Егер Виженер бағдаржолында кілттің сандарын кездейсоқ сандармен алмастырса және кілттің ұзындығын жеткілікті дәрежеде ұзын етіп алсақ, бұл бағдаржол гаммалау бағдаржолына айналады.

Гаммалау криттографиялық жүйелерде кең қолдану тапқан.

Шын мәнісінде гаммалау мен шексіз кілттерді және Виженер шифрларын пайдалану арасындағы шекара шартты түрде десе болады.

Гаммалаумен шифрлау қағидасы гамманың шифр генерацияланған кездейсоқ сандардың тізбегін ашық мәтін тізбегіне екілік таңбаларымен екілік модулде қосу арқылы орындалады.

Дәл сол тізбекті екінші рет те дәл сондай етіп екілік модулде шифрге қосқанда ашық мәтін бұрынғы қалпына келеді.

Сондықтан мұндай жүйе **симметриялы** деп аталады.

Ал шифрлеу сұлбасы мен дешифрлеу сұлбасы бірдей болғандығы үшін бұл жүйе бастапқы кезде өте кең қолданылды.

Әсіресе жергілікті деректер қорында құпия ақпаратты сақтауда

өте қолайлы; себебі шифрлеуде де, дешифрлеуде де жалғыз кілт қолданылады.

Егер кілтті арнамен жіберу мәселесі болмаса, онда мұндай жүйеден абсолютті криптошыдамдылықты алса болады.

Егерде шифр гаммасы реттіліктердің (кезеңді) қайталануы жоқ болса, шифрленген қолдағы мәтіннің шешілуі (ашылуы) қиын болады, яғни абсолютті криптотұрақтылыққа жақын шифр алса болады.

Шифр гаммасы әрбір шифрленген сөз үшін кездейсоқ өзгерістерге еніп отыру керек.

Шындығында, егер гамма кезеңі бүкіл шифрланған мәтіннің ұзындығынан асып кетсе және шығу мәтіннің ешбір бөлігі таңбасыз болса, онда шифрды тек тікелей жинау арқылы шешуге болады.

Егерде қасқой адамға шығу мәтінінің бір үздігі мәлім болса және оған сәйкес шифрограммасы болса, гаммалау әдісі әлсіз болады.

Модул бойынша жай есептеу арқылы санақтық талдау жасаумен барлық мәтінді орнына келтірсе болады.

Қаскөй адамдар шығу мәтіннің мағынасын сезу арқылы табулары мүмкін. Сонымен, егерде барлық хабарламалардың көпшілігі «СОВ СЕКРЕТНО» сөздерінен басталатын болса, онда мәтін барысының криптоанализі едәуір оңайланады. Бұны ақпараттандыру жүйелерінің қауіпсіздігін құрған кезде есте сақтау керек.

5.11 ***Зертханалық жұмыс***

Гаммалау бағдаржолы мен шифрлеу бағдарламасы

Гаммалау бағдаржолы мен шифрлеу Виженер бағдаржолына өте ұқсас болып, айырмашылығы – кілттер тізбегі шексіз үлкен кезеңді кездейсоқ сандар тізбегінен тұрады. Гаммалау бағдаржолы DES және ГОСТ үлгіқалыптарында (стандарттарында) қолданылып, Шеннон бойынша **абсолюттік** немесе **өте жоғарғы криптотұрақтылықты** бере алатын бағдаржол.

Бірақта бұл бағдаржолдың кемшілігі - кілттерді абоненттерге таратып, жеткізіп беру мәселесі туындайды.

Сондықтан мұндай криптожүйені жергілікті **ақпараттар қоймасында** қолдану қолайлы болады.

Ал DES және ГОСТ үлгіқалыптарында бұл бағдаржол басқа да бағдаржолдармен **кешенді түрде бірге** қолданылған. Төменде сол бағдаржолды MS Excel-де құрылған бағдарламасы берілген.

Сонымен бағдаржол мына түрде болады;

- бірінші А бағанында ашық хат әріптері жоғарыдан төмен қарай баған бойынша жазылады. Мысалы, хабар ретінде латын әліпбиінің әріптері қолданылған: *a,b,c,d,e,f,g,h,i,j,k,l,m,n,o, p,r, s,t,u,v,w, x,y,z, q*.

Кейінгі В бағанында әріптерге сәйкес келетін олардың кодтары жазылады; мысалда әріптер ондық натурал сандармен кодталған;1,2,3,4,5,6,7,8,9,10,11,12, 13,14,15,16,17, 18, 19,20,….

Кейінгі Е бағанында шифрлеу бағдаржолының кілті жазылады;

мұнда кілтті жарату үшін кездейсоқ сандар қолданылған болып, С2 де random датчигі жәрдемінде кездейсоқ сандар жазылған; ал D2 де олар 10 ға көбейтілген.

Е2 де алынған кездейсоқ сандардың бүтін бөлігі ажыратылған болып, бұл кілтті құрайды.

Сонда кілт екі жайғасымды (позициялы) кездейсоқ сандар тізбегінен тұрады.

Ал шифрленген хабар F2 = B2+E2 бағдаржолымен алынады да, қарастырылып отырған мысалда келесідей тізбекті құрайды:

18,18,5,15,6,33,31,9,13,36,39,17,35,16,24,21,37,42,35,42,34,33,28,41,48,39.

Бұл шифрленген хабар мен кілт тізбегінің көшірмесі бірге алынып, басқа листке немесе бағанға жазылады. Мысалда Е және F бағандары Н және I бағандарына көшіріледі.

Дешифрлеу бағдаржолы алмастыру бағдаржолына ұқсас; яғни шифрден кілт коды айырылуы керек: J2 = I2 - H2.

Айта кететін жай, мұнда шифрлеу және дешифрлеуді біз ондық сандармен жүргізіп отырмыз; сондықтан шифрлеуде ақпаратқа кіліт қосылады, ал дешифрлеуде – шифрден кілт айырылады.

Бірақ нақты жүйеде ақпарат та, кілт де екілік санақ жүйесінде болып, олар шифрлеуде де, дешифрлеуде де тек екілік модулде қосу орындалады; мұнда екі операцияда да бір кілт және бір электрондық сұлба қолданылады. Сондықтан да мұндай жүйе симметриялы деп аталады.

Бағдаржол дұрыс істегенде J2 және B2 бағандары бірдей болуы керек.

	A	B	C	D	E	F	G	H	I	J	K
1	әріптері	коды	пкс	пкс2	кілт	шифр		кілт2	шифр2	дешифр	әріптері
2	a	1	0,24828	24,8281	24	25		24	25	1	a
3	b	2	0,06697	6,69749	6	8		6	8	2	b
4	c	3	0,90996	90,9959	90	93		90	93	3	c
5	d	4	0,16663	16,6634	16	20		16	20	4	d
6	e	5	0,22832	22,8322	22	27		22	27	5	e
7	f	6	0,75467	75,4671	75	81		75	81	6	f
8	g	7	0,15897	15,8973	15	22		15	22	7	g
9	h	8	0,58484	58,4841	58	66		58	66	8	h
10	i	9	0,39138	39,1377	39	48		39	48	9	i
11	j	10	0,13746	13,7464	13	23		13	23	10	j
12	k	11	0,8778	87,7803	87	98		87	98	11	k
13	l	12	0,40502	40,5021	40	52		40	52	12	l
14	m	13	0,13976	13,9756	13	26		13	26	13	m
15	n	14	0,14879	14,879	14	28		14	28	14	n
16	o	15	0,91283	91,2833	91	106		91	106	15	o
17	p	16	0,71109	71,1086	71	87		71	87	16	p
18	r	17	0,38712	38,7121	38	55		38	55	17	r
19	s	18	0,86212	86,2124	86	104		86	104	18	s
20	t	19	0,9454	94,54	94	113		94	113	19	t
21	u	20	0,47625	47,6246	47	67		47	67	20	u
22	w	21	0,0855	8,55005	8	29		8	29	21	w
23	y	22	0,65025	65,0249	65	87		65	87	22	y

5.3-сурет Гаммалау бағдаржолының MS Excel-дегі бағдарламасының көрінісі

5.6.6. Осы күндері қолданылатын деректерді шифрлеудің үлгіқалыпты жүйелері мен бағдаржолдары

Жоғарыда гаммалау бағдаржолы өте жоғары криптотұрақтылық беретінін көрдік.

Алайда мұндай шифрлеуді қолданудың шектелуі ондағы қолданылатын гамманы алудың қиындығы болса, екіншіден, жабық кілттерді сақтау мен оларды қолданушыларға тарату мәселесі болды.

Сондықтан амалда коминацияланған бағдаржолдар мен әдістер қолданылып келеді. Мысалы, Ресейде деректерді шифрлеудің үлгіқалыбы (үлгіқалып) ГОСТ 28147-89 [78] қабылданып, DES үлгіқалыбының кемшіліктерін халықаралық тәжірибе негізінде есепке алынды.

Бұл үлгіқалыбында бірнеше жұмыс тәртібі орындалып, барлық режимдерде кілттің жалпы ұзындығы 256 битке тең болған, әрқайсысының ұзындығы 32 бит болған 8 сандар жиынтығынен құрылған; жиынтық сандары: X(i) : W = X(7)X(6)X(5)…X(2)X(1) X(0);

Дешифрлеу үшін сол кілт қолданылады.

Алмастыру мен орын ауыстыру режимдерін бірге орындау үшін жеткілікті дәрежеде күрделі бағдаржолдар қолданылады.

Мұнда хабарлар 64 биттік жиынтықтерге ажратылып, әрбір Т жиынтығы және 32 орынды екі жиынтыққа ажыратылады: A(0), B(0).

Сонда шифрлеу бағдаржолы мына түрде болады:

- Для i =1,24, j = (i-1) mod8: A(i) = f (A(i-1)[+]X(j)) $\oplus$ B(i-1), B(i) = A(i-1).
- Для i =25,31, j = 32-I : A(i) = f (A(i-1)[+]X(j)) $\oplus$ B(i-1), B(i) = A(i-1).
- Для i =32 : A(32) = A(31) , B(32) = f (A(31)[+]X(0)) $\oplus$ B(31).

Шифрлеу жиынтығы мына түрде болады: T(64) = A(32)B(32).

Кері байланысты гаммалау бағдаржолы мына түрде болады:

Ш(1) = A(S) $\oplus$ T(1) = Г (1) $\oplus$ T(1), Ш(i) = A(Ш(i-1)) $\oplus$ T(i) = Г (i) $\oplus$ T(i), I = 1,m, мұнда A(S) – 64 биттік синхрожиынтық тізбегі, Г (i) - Гш = (Г (1), Г (2), Г (3), …, Г (m)) жиынынан құралған гаммалар тізбегі.

Осы бағдаржол өте жоғары криптотұрақтылыққа ие болады.

Алайда бұл жүйелер жергілікті деректер қорында істетіліп, желілерде істетілуі шектелген.

5.6.7 RSA типіндегі шифрлеу бағдаржолы мен бағдарламасы

Коммерциялық жүйелерде (мысалы, банк жүйелерінде) ақпаратты қорғау үшін ашық кілітті RSA типіндегі шифрлеу бағдаржолдары кең қолданылады; бағдаржолдың негізінде келесідей дәлел алынған; екі жай сандардың көбейтіндісін көбейткіштерге жіктеу (осы кездегі есептеу техникасының жылдамдығын есептегенде) амалда орындап болмайтын мәселеге айналады.

Осы бағдаржолдың математикалық негізі кітап соңында қосымшада берілген.

Әрине, көбейткіштер жетерлі дәрежеде үлкен болғанда осы мәселе өте қиын шешілетін мәселе қатарына жатады. Осындай жүйелердің криптотұрақтылығы осы шифрді ашуға кеткен амалдардың ең кем деген деңгейімен және осыған кеткен машина уақытымен өлшенеді.

Осындай жүйелер алыстағы клиенттердің кредиттік карточкаларымен жұмыс істеу үшін қолданылып келеді.

Сондықтан RSA бағдаржолы көптеген үлгіқалыптарда қолданылады; мысалы, SSL,S-HHTP,S-MIME,STT,PCT,S/WAN. RSA бағдаржолының жұмысы төменде келтірілген. RSA бағдаржолының құрылысы келесідей:

Айталық берілген $n = p \cdot q$, мұнда p, q -әртүрлі (жеткілікті дәрежеде үлкен) жай сандар болсын. $\varphi(n)$ – Эйлер теңдеуіне қарағанда e- жай саны болса, онда бірер d бүтін саны табылып, оған мына теңдік орынды болады: $e \times d = 1 \pmod{\varphi(n)}$; мұнда, егер p және q - жеткілікті дәрежеде үлкен жай сандар болса, онда n жіктелуі амалда мүмкін болмайды (осы заманға есептеу техникасы деңгейінде).

Амалда бағдаржол былай қолданылады; әрбір қолданушы екі үлкен жай (p, q) сандарды таңдап алады; олар жай сандардың генераторы жәрдемінде генерацияланады.

Содан кейін, жоғарыда көрсетілген бағдаржол бойынша екі жай сан e және d таңдалады; мұнда алынған (e , n) қос қисындастыруы ашық кілт, ал (d, n) қос қисындастыруы жабық кілт болады.

Мәтіндер ашық кілтпен шифрленіп, ал дешифрлеу жабық кілтпен амалға асырылады.

Мұнда криптотұрақтылық кілттің ұзындығымен өлшенеді.; мысалы, кілттің ұзындығы 50 болғанда, ширфді ашу операциясы $-1{,}4 \bullet 10^{10}$ болады.

Ал кілт ұзындығы 200 болса, ашу операциясы $\sim 1{,}2 \bullet 10^{23}$ болып, осы күндегі есептеу техникасының деңгейінде мүмкін болмайды.

Қолданушыларға келесідей модулдер қолдануға рұқсат етілген: n : - 768 bit – жеке меншіктік қолдануға; 1024 bit – коммерциялық ақпараттар үшін; 2024 bit - өте құпиялы ақпарат үшін ажыратылған.

5.12 *Зертханалық жұмыс*

Ашық кілтпен немесе RSA бағдаржолымен шифрлеу бағдарламасы.

Ашық кілт жарату бағдаржолы жоғарыда келтірілген. Төменде RSA бағдаржолы мен шифрлеуді мысалда MS Excel-де орындаймыз.

Мұнда ашық кілт ретінде {7,33}, ал жабық кілт ретінде {3,33} алынған.

А және В бағандары хабар мен оның кодтарымен толтырылады.

Ал С бағанында ашық кіліт жәрдемінде В-дағы сандар үстінен келесідей амалдар орындалады; В-дағы сандарды 7 дәрежеге көтеріп, шыққан сандарды 33-ке бөлеміз; $(B2)^7/3$ ден шыққан

қалдығы шифрленген хабар болып, оны D2-ге жазамыз. Шифрдің көшірмесін алып, MS Word-қа жазамыз.

MS Word-тан копия алып, MS Excel-дің басқа E2 бағанына жазамыз;

жабық кілт {3,33} жәрдемінде E2 бағанындағы шифрді ашамыз; мұның үшін E2 бағанындағы сандарды 3 дәрежеге көтереміз (F2), оны 33-ке бөліп, $(F2)^3/3$ қалдығын табамыз (G2). Сол қалдық ашық ақпараттың коды болады; оған сәйкес әріптер H2 бағанында берілген. Шыққан қалдықты G2 бағанына жазамыз. Шифрлеу дұрыс орындалған болса, онда G2 және B2 бағандары бірдей болуы керек.

	A	B	C	D	E	F	G	H
1	әріптері	коды	ашық кілт	шифр	шифр2	жаб кілт	дешифр	әріптері
2	a	1	1	1	1	1	1	a
3	b	2	128	29	29	24389	2	b
4	c	3	2187	9	9	729	3	c
5	d	4	16384	16	16	4096	4	d
6	e	5	78125	14	14	2744	5	e
7	f	6	279936	30	30	27000	6	f
8	g	7	823543	28	28	21952	7	g
9	h	8	2097152	2	2	8	8	h
10	i	9	4782969	15	15	3375	9	i
11	j	10	10000000	10	10	1000	10	j
12	k	11	19487171	11	11	1331	11	k
13	l	12	35831808	12	12	1728	12	l
14	m	13	62748517	7	7	343	13	m
15	n	14	1,05E+08	20	20	8000	14	n

5.4-сурет RSA бағдаржолының MS Excel-дегі бағдарламасының көрінісі

5.6.8 RSA бағдаржолы мен Электронды қолтаңбалы жасау және аутентификациялау бағдарламасы

5.13 ***Зертханалық жұмыс***

Электронды қолтаңбалы жаратудың қарапайым бағдаржолы RSA бағдаржолын қолданады. Мұнда қол қойылатын хабар бірнеше рет RSA бағдаржолымен шифрленіп, эталон түрінде қорда (базада) өте құпия түрде сақталады.

Ал желіде қолданылатын ақпарат осы құпия сақталған ақпаратты ашып, кейін қолданушыға жіберіледі.

Сонда қолданушыда еш қандай кілт жоқ болады. Кілт жүйенің өзінде болады. Қолданушыда ақпарат ешқандай да қорғалмаған екен деген ой туылады.

Ал егер Ғаламтордағы қолданушы мәтіннің бірер нүктесін өзгертпекші болса, онда жүйе оған рұқсат бермейді, әрине.

Мұнда жүйе уақыты-уақытымен сақталған хабарды арнайы бағдарлама-ревизормен оның түпнегізін тексеріп тұрады.

Мұндай амалдар ***аутентификация*** деп аталады.

Мұнда қолданылып жүрген және сақталып тұрған хабар дешифрленіп яғни ашылып, эталонды хабармен салыстырылады (***верификация***).

Егер салыстыру ешқандай айырмашылық бермесе, хабар дұрыс сақталған болып, қателік жоқ деп табылады.

Кері жағдайда, қателік бар деп, эталонды хабармен ауыстырылады.

Келтірілген мысалда RSA бағдаржолы қолданылған болып, төменде көрсетілген. A,B бағандары ақпарат және оның кодтарымен толтырылған.

C бағанында ақпаратты $(B2)^7 / 3$-тің қалдығы табылып, D2-ге жазылады.

Оның көшірмесі E2-ге көшіріледі. $(E2)^3 / 3$-нің қалдығы G2-ге жазылып, бұл ашылған хабарды білдіреді. Эталонды хабар H2-ге жазылады.

Аутентификация бағдаржолы G2- дегі хабарды H2-дегі хабармен салыстырады; салыстыру нәтижесі I2- ге жазылады; бұл операция екілік жүйеде екілік модулмен қосу арқылы амалға асырылады. I2 бағанның қосындысы нөлге тең болған жағдайда ешқандай өзгеріс болмады немесе “ТҮПНҰСҚА ӨЗГЕРМЕГЕН” деген хабар шығады.

Ал кері жағдайлардың барлығында “ТҮПНҰСҚА ӨЗГЕРГЕН” немесе хабар бұзылғандығы анықталады. Төменгі листте де осы бағдарламаның басқаша жағдайы берілген. Мысалда екі әріп өзгерген: I8, I17.

I2 бағандағылардың квадраттарының қосындысы I28 ұяшығында болып, ол нөлге тексетіледі; егер ондағы сан нөл болса, түпнұсқаның өзгермегені; ал кері жағдайда түпнұсқа өзгерген болып, оны қалпына келтіру үшін эталондық нұсқаны (ол G2- де) қайта көшіріп жазады.

Верификациялауда I2 бағанындағылардың квадраттарының қосындысы алынуының себебі ондағы шамалар оң (+) немесе (–) кері таңбалы болуы мүмкін.

	A	B	C	D	E	F	G	H	I	J	K	L
1	әріптері	аш текст	ашық кілт	шифр	шифр2	жаб кілт	дешифр	аш текст2	Верификация			
2	a	1	1	1	1	1	1	1	0			
3	b	2	128	29	29	24389	2	2	0			
4	c	3	2187	9	9	729	3	3	0	Электронды қолтаңбаны		
5	d	4	16384	16	16	4096	4	4	0	тексеру (аутентификациялау)		
6	e	5	78125	14	14	2744	5	5	0			
7	f	6	279936	30	30	27000	6	6	0			
8	g	7	823543	28	28	21952	6	7	-1			
9	h	8	2097152	2	2	8	8	8	0		түпнұсқа өзгерген	
10	i	9	4782969	15	15	3375	9	9	0			
11	j	10	10000000	10	10	1000	10	10	0		2	
12	k	11	19487171	11	11	1331	11	11	0			
13	l	12	35831808	12	12	1728	12	12	0			
14	m	13	62748517	7	7	343	13	13	0			
15	n	14	1,05E+08	20	20	8000	14	14	0			
16	o	15	1,71E+08	27	27	19683	15	15	0			
17	p	16	2,68E+08	25	25	15625	17	16	1			
18	r	17	4,1E+08	8	8	512	17	17	0			
19	s	18	6,12E+08	6	6	216	18	18	0			

5.5.а-сурет. Электронды қолтаңбалы тексеру бағдаржолының MS Excel-дегі бағдарламасының көрінісі

	A	B	C	D	E	F	G	H	I	J
15	n	14	1,05E+08	20	20	8000	14	14	0	
16	o	15	1,71E+08	27	27	19683	15	15	0	
17	p	16	2,68E+08	25	25	15625	17	16	1	
18	r	17	4,1E+08	8	8	512	17	17	0	
19	s	18	6,12E+08	6	6	216	18	18	0	
20	t	19	8,94E+08	13	13	2197	19	19	0	
21	u	20	1,28E+09	26	26	17576	20	20	0	
22	w	21	1,8E+09	21	21	9261	21	21	0	
23	v	22	2,49E+09	22	22	10648	22	22	0	
24	x	23	3,4E+09	23	23	12167	23	23	0	
25	y	24	4,59E+09	18	18	5832	24	24	0	
26	z	25	6,1E+09	31	31	29791	25	25	0	
27	q	26	8,03E+09	5	5	125	26	26	0	
28									2	
29			Электронды қолтаңбаны тексері -аутентификациялау						түпнұсқа өзгерген	
30			Верификация нәтижесі i28 де көрінеді;							
31			Егер (i28=0) болса, түпнұсқа өзгермеген;							
32			Егер (i28≠0)болса, түпнұсқа өзгерген.							
33										

5.5.б-сурет. Электронды қолтаңбалы тексеру бағдаржолының MS Excel дегі бағдарламасының көрінісі

Санды қолтаңба үшін Эль-Гамаля [77-79] бағдаржолы қолданылып, ол да осындай дәрежеде крипотұрақтылық көрсетеді. Бағдаржол негізінде **дискретті логарифмдеу** жатады. Осы бағдаржолдың математикалық негізі кітап соңында қосымшада берілген. Бағдаржол төмендегідей құрылған;

құпия ақпарат алушысы - *a* жабық кілтін генерациялап, *p* , *q* – параметрлерін таңдайды; онда *p* - жай сан, ал *q* - бүтін сан; мына бағдаржол бойынша ашық кілт $y = q^a \bmod p$ ті есептеп, оны адресатқа жібереді (құпия ақпаратты жіберуші адресатқа). Жіберуші *p*-дан кем болған кездейсоқ *к* санын таңдайды және *m* ашық хабары үшін мәлім болған *y* бойынша шифровка y_1, y_2 ні мына бағдаржолмен есептейді: $y_1 = q^k \bmod p$, және қабылдаушыға жібереді. Қабылдаушы *a* жабық кілті бойынша *m* хабарын тіктейді: $m = \left(y_1^a \bmod p\right) \oplus y_2$

NIST (National Institute of Sytandard and Technology) жаратқан DSA санды қолтаңбасында осы бағдаржол қолданылған [76,244].

Ресейде **электрондық қолтаңба** жаратуда осыған ұқсас бағдаржол **ГОСТ Р 34.10 – 94** [77,79] бойынша қабылданған.

Нақты криптжүйелерде эллипстік теңдеулер негізінде құрылған бағдаржолдар да қолданылады: $y^2 = x^3 + ax + b \bmod p$.

Диффи-Хелман бағдаржолы өте нәтижелі болып, қолданушыларға **кілттерді алмасу**ға мүмкіндік береді [77,79]. Бағдаржолда дискретті дәрежеге көтеру теңдеуі істетіледі. Бағдаржол қағидасы келесідей; Р элементтерден құралған Галуа өрісі берілген делік (Р – жай сан немесе кез келген орындағы жай сан); мұндай өрістерде логарифмдерді есептеп табу үдерісі қиын мәселе.

Егерде $y = \alpha^x, 1 \langle x \langle p-1,$ мұнда *p* - GF (*p*) өрісінің таңбаланған элементі болса және егер *p* дұрыс таңдалған болса, онда логарифм табу үшін мынаған $L(p) = \exp\{(\ell np \times \ell n \times \ell np)^{0,5}\}$ пропорционал есептеулер керек болады.

$K_{\text{р}}$ кілті екі абоненпен бірге есептеледі; олар бір-біріне мына түрдегі хабарды жібереді: $y_1 = \alpha^{x_1}, y_2 = \alpha^{x_2}$, соден соң оларды мына дәрежеге көтереді: олар арнамен келесідей мәндерді алады y_1, y_2, яғни $y_1^{x_2}, y_2^{x_1}$.

Сөйтіп екі абонентте екеуіне де ортақ болған келесідей кілтерді алады: $K_{12} = y_1^{x_2} = \alpha^{x_1 x_2}$, $k_{12} = y_2^{x_1} = \alpha^{x_2 x_1}$.

Галуа өрісінде 1000 биттік жай сандар есептеу үшін жорамалдап алғанда 10^{30} амалдар орындау керек болады.

DSS (Digital Signature Standard) сандық қолтаңба жарату

үлгіқалыпы қорғанудың хэштеу бағдаржолы SHA (Sekure Hash Algorithm) [77, 79] негізінде құрылған.

DSA сандық қолтаңба жарату бағдаржолы дискретті логарифмдерді есептеу қиындығы негізінде жаратылған; осы негізде жаратылған **Эль-Гамал** мен **Шнорр** [77,79] бағдаржолдары өте кең қолдану тапты.

Қолданушылар тобына ашық кілттің үш параметрі: *p, q, g* мәлім болады; 160 –биттік *q* (жай (*p*-1) бөлушісі) жай сан таңдалады. Кейін, *p* жай саны таңдалып, оның ұзындығы 512 мен 1024 бит аралығында 64 бит қадамымен алынған болсын; бүтін g саны мына теңдеуден таңдап алынады: $g = h^{\frac{(p-1)}{q}} \bmod p \rangle 1,1 \langle h \langle (p-1)$

Осы сандарды біле тұра қолданушы өзінің *x* кілтін (ол кездейсоқ немесе псевдокездейсоқ сан болып, $1 \langle x \langle (q-1)$) және ашық кілт *y* ті ($y = g^x \bmod p$) генерациялайды.

Әрбір қолтаңба жасау алдында кейбір бірегей бүтін кездейсоқ немесе псевдокездейсоқ сан *k* (0<*k* < *q*-1) генерацияланады;

осыдан кейін қолтаңбалы құратын *s* , *r* лер есептеледі; олардың мәндері мына теңдеулермен есептеледі: $r = (g^x \bmod p) \bmod q$,

$[s = [k^{-1}(H(M) + \boldsymbol{x}\ ]\ \bmod q.$

Тесттің өте аз өзгерісінде қолтаңба верификациясы өзгерісті (“подделка”) тауып алады.

Мұнда верификация бағдаржолы келесідей:

$w = (s^{/})^{-1} \bmod q$; $u_1 = [H(M^{/}) \times w] \bmod q$;

$v = [(g^{u_1} \times y^{u_2}) \bmod\ p] \bmod\ q$.

Егер $v = r^{'}$ болса, онда қолтаңба өзгермеген (подлинная), ал кері жағдайда қолтаңба өзгерген (подделка) болады.

СТБ-1176.02-99 сандық қолтаңба үлгіқалыпындағы бағдаржолда таңба ретінде құжаттарға қол қою уақыт мезгілі алынған болып, бұл қолтаңбаның имитотұрақтылығын әжептеуір арттырады; мұнда автордың өзі қолында барлық кілттер бола тұра, өзінің қолтаңбасын өзгерту (подделка жасау) мүмкіншілігіне ие болмайды [79]. Осының негізінде құрылған зертханалық жұмыстар Информатика және Телекоммуникациялар желілері мамандығындағы студенттерге оқыту үдерісінде қолданылып келеді.

Оқыту мақсатында **“Криптоцентр”** [78 жұмыстың қосымшасы]

бағдарламалар кешенін қолданса болады; мұнда құжаттарға электронды қолтаңба жасау, криптографиялық шифровка жасау, құжаттарды деректер қорында құпия сақтау, құжаттарды байланыс арнасымен жіберу алдында криптографиялық шифрлеу үшін жаратылған криптографиялық бағдарламалардың демоверсиялары бар. Олардың демоверсияларын осы саладағы мамандықтарға оқыту үдерісінде оқыту-әдістемелік материалдар ретінде қолданса болады.

II тараудың бақылау және емтихан сұрақтары.

1. Екілік кодтарды істетудің ақпаратты ұзату мен өңдеуде қолданудың абзалдықтары неде?
2. Грей коды не үшін қолданылады?
3. Ақпаратты криптографиялық жабу деп нені түсінеміз?
4. Заманауи криптографиялық жүйелерге қойылатын талаптар қандай?
5. Ақпараттық қауіпсіздікті қамтамасыз ету шараларының бес түрі.
6. Гаммалау шифрлеуінің негізгі кемшілігі неде?
7. Қарапайым криптографиялық алмастыру шифрінің бағдаржолы.
8. Гаммалау бағдаржолының қағидасы.
9. Алмастыру немесе Цезарь бағдаржолы.
10. Виженер бағдаржолы.
11. Орын ауыстыру және алмастыру бағдаржолдары бірге қолданатын криптографиялық жүйелер.
12. RSA крипографиялық жүйесі.
13. RSA бағдаржолымен қолтаңба жасау қағидасы.
14. Эль-Гамал бағдаржолының негізгі қағидасы.
15. Нәтижелі санақтық кодтаудың негізгі маңызы неде?
16. Шеннонның кедергісіз арна үшін теоремасының маңызы?
17. Таңбалардың ұзын тізбектерін кодтаудың нәтижелігі неде?
18. Ненің әсерінен нәтижелі кодттауда код қисындастыруының орташа ұзындығы кемейеді?
19. Нәтижелі кодттауда код қисындастыруыннң ұзындығы қай шекке дейін кемейеді?
20. Шеннон-Фано коды мен Хаффмен кодтарын құру методикасының абзалдығы неде?
21. Нәтижелі кодттар қай шартқа бойсынады?

22. Нәтижелі кодтарды қолданғанда қандай күрделіліктер мен қиындықтар болады?

Өзіндік жұмыстар (СӨЖ) тақырыптары.

1. Бөгеуілсіз арна үшін Шеннонның кодтау туралы негізгі теоремасы.
2. Үздіксіз-санды түрлендірушіде Грей, Уолш, Радемахер кодтарын (түрлендіру бағдаржолдарын) қолдану.
3. Бөгеуілсіз арна үшін Шеннонның негізгі кодтау теоремасы.
4. Энтропия қасиеттерін ақпаратты сығымдауда қолдану.
5. Нәтижелі кодтар; Шеннон-Фано коды.
6. Шеннон-Фано кодын құру қағидасы.
7. Хаффмен кодын құру қағидасы.
8. Нәтижелі кодтардың префикстік талабы.
9. Қарапайым кодтар (бөгеуілорнықсыз) кодтар.
10. Криптографиялық ақпаратты жабу қағидалары.
11. Қарапайым криптографиялық алмастыру шифрінің бағдаржолдары.
12. Осы кезде амалда қолданылатын криптографиялық бағдаржолдар.
13. Гаммалау бағдаржолының қағидасы.
14.Абсолютті криптотұрақтылық ұғымы.
15. Алмастыру бағдаржолы.
16. Цезарь бағдаржолы.
17. Виженер бағдаржолы.
18. Орын ауыстыру және алмастыру бағдаржолдары бірге қолданатын криптографиялық жүйелер.
19.Кіліттер алмасуында қолданылатын Диффи- Хелман бағдаржолының істеу қағидасы.
20. RSA крипографиялық жүйесі.
21. RSA бағдаржолымен қолтаңба жасау қағидасы.
22. Эль-Гамал бағдаржолының негізгі қағидасы.
23. Санды қолтаңба үшін Эль-Гамаль бағдаржолы.
24. Дискретті логарифмдеу негізінде құрылған криптографиялық бағдаржол.
25. DSA сандық қолтаңба жарату бағдаржолының істеу қағидасы.
26.“Криптоцентр” бағдарламалар кешенін не мақсатта қолданса болады?

VI ТАРАУ. БӨГЕУІЛДІ ДИСКРЕТ БАЙЛАНЫС АРНАСЫ БОЙЫНША ХАБАР ЖІБЕРУ КЕЗІНДЕГІ АҚПАРАТТАРДЫ КОДТАУ

6.1 Бөгеуілді байланыс арна үшін Шеннонның кодтау туралы негізгі теоремасы.

Кедергіге шыдамды кодтау теориясы Шеннонның зерттеу нәтижелеріне негізделген болып, мына теоремамен беріледі:

1. Егер хабар көзінің өнімділігі арнаның өткізу қабілетінен кем болса, онда осы хабар көзі құрған ақпараттың барлығын да кез келгенше қателіктің төмен ықтималдығымен ұзату мүмкіндігін беретін кодтау әдісін тапса болады.

2. Егер хабар көзінің өнімділігі арнаның өткізу қаблетінен артық болса, онда осы хабар көзі құрған ақпараттың барлығын да кез келгенше қателіктің төмен ықтималдығымен ұзату мүмкіндігін беретін кодтау әдісі болмайды.

Осы теорияның математикалық талқылаулар көп болғанымен оның ұғымы өзгермеді.

Теореманың дәлелін келтірмейміз. Алайда оны талқылайық.

Біріншіден оның орнықтылығын атап өтейік.

Теорема ақпаратты шындықпен ұзату кезінде жүйенің нәтижелілігінің мүмкін болған шегін көрсетеді.

Интуитивті түрде көз алдымызға келтірсек, кедергісі бар арнамен ақпаратты ұзатуда кез келгенше аз қателіктің ықтималдығын алу үшін шексіз көп артықшылық ендіру керек деп ойлаймыз; яғни жылдамдықты нөлге дейін кемейту керек деп ойлаймыз.

Теоремадан шығатыны, кедергілер ұзатудың анықтығына ешқандай шектеу қоймайды. Осы шектеу тек қана ұзату жылдамдығына қойылып, онда қалағанша шындыққа жетуге мүмкін болады.

Бірақ теорема құралымды емес; себебі мұнда кодтар құрудың жолдары көрсетілмейді. Алайда, осындай кодтау әдісі болуыныңтеориялық жағынан мүмкіндігі барлығын негіздеп, ғалымдарды айқын кодтар құруға жұмылдырады.

Айта кететін жай, ақпараттың өткізу қаблетіне шейін болған кез келген ұзату жылдамдықтарында қателіктің кез келгенше

кіші ықтималдығына жету үшін кодталатын таңбалар тізбегінің ұзындығын шексіз арттыру керек.

Сөйтіп, кедергі бар уақытта қатесіз ұзату тек теориялық түрде ғана болады. Ақпаратты ұзатуда өте кем қателік ықтималдығы және жетерлі дәрежеде жоғары нәтижелікке қол жеткізу тек өте үлкен әріптер тізбегін кодтағанда ғана болады.

Амалда шындық дәрежесі және нәтижелік екі себеппен шектеледі: кодттау және декодттау аспапсының өлшемдері мен бағасы және ұзатылатын хабардың іркілу уақытымен шектеледі.

Осы кезде салыстырмалы қарапайым кодтау әдістері қолданылып, олар аталған теорияның аталған мүмкіншіліктерін толық қолданбайды.

Алайда ұзату шындығына қойылатын талаптардың күннен күнге артуы және үлкен интегралдық сұлбаларды құрудағы үлкен табыстар осы мақсатта жаңа құрылымдар құруды талап етеді.

6.2 Бөгеуілді кодтау; жиынтықты кодтау; Кедергіге шыдамды кодтардың түрлері

Осы кезде құрылған Ғаламтор желісі, деректерді телеөңдеу құрылымдары, есептеу жүйелері мен желілері, аймақтық автоматтанған басқару жүйелері, ғылыми зерттеу жүйелерін автоматтандыру жүйелері, т.б. құрылуы кодтау теориясының дамуына және амалдық қолданылуына мүмкіндік жаратты. Жоғарыдағы жүйелерде шындыққа деген жоғары талап қателіктерді табатын және түзететін кодтар құруды талап етті.

Мұнда кодтауды сондай етіп құру керек болады, егерде кедергі әсерінен бұзылған сигналды қайта түзеткенде басқа таңбалар тізбегіне сай келетін сигналдан гөрі арнамен жіберіліп отырған таңбалар тізбегіне сай келетін сигналға жақын болуы керек. Жақындық дәрежесі сол кодтар тізбегінің бір-бірінен айырмашылығын көрсететін кодтың дәрежелер санымен өлшенеді.

Жоғарыда айтылғандарға қол жеткізу үшін кодтауда артықшылық ендіріледі. Мұнда қабылдаушы тарапта тексеру нәтижесінде қателіктерді табу және түзету мүмкін болатындай етіп кодтауда ұзатылатын таңбалар тізбегін құру керек болады.

Осындай қасиетке ие болған кодтарды ***кедергіге орнықты кодтар*** деп атайды.

Олар қателіктерді табуда да, сондай ақ түзетуде де түзетуші кодтар қолданылады.

Осындай кодтардың көпшілігінде айтылған шарттар олардың ***алгебралық құрылысынан*** келіп шығады. Сондықтан оларды ***алгебралық кодтар*** деп атайды.

Вагнер кодынан айырмашылығы Вагнер кодында түзетуші әрекеттер әрбір таңбаның ***бұзылу ықтималдығын бағалауға*** негізделген.

Алгебралық кодтарды екі үлкен кластарға бөлсе болады: ***жиынтықты*** және ***үздіксіз*** кодтар. Жиынтықты кодтауда кодталатын әрбір хабар әріпіне *к* таңбалар тізбегі сәйкес келсе, ол таңбалардың әрбіріне *n* таңбалар тізбегі сәйкес қойылады. Мұнда түрлендіру амалдарында тек қана *к* таңбалары қатысып, ал шығу тізбегі жіберілетін хабардағы басқа таңбаларға байланысты болмайды.

Егерде *n* барлық хабар әріптері үшін өзгермейтін болса, онда жиынтықтық код ***біртегіс*** деп аталады.

Жиынтықты кодтар ***ажыралатын*** және ***ажыралмайтын*** деп бөлінеді. Ажыралатын кодтарда ***ақпараттық*** **(*информациялық*)** ***таңбалар*** арна кодеріне келіп түсетін ақпараттың таңбалар тізбегі болып, ал ***артықша*** немесе ***тексеруші таңбаларды*** берілген тізбекке арна кодері құрып, ендіреді; бұл қателікті анықтау және түзету үшін қызмет етеді.

Ажыралмайтын кодтарда шығу тізбегіндегі таңбаларды ақпараттық және тексеруші деп ажыратып болмайды.

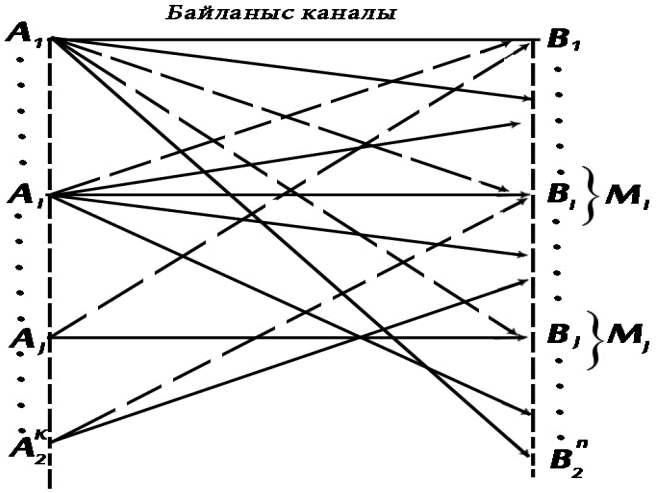
Үздіксіз **(*ағаш тәрізді*)** кодтарда кодталатын ақпараттық таңбалар тізбегіне артықша таңбаларды ендіру ***үздіксіз о***рындалады және олар тәуелсіз жиынтықтарға ажыратылмайды.

Үздіксіз кодтар да ***ажыралатын*** және ***ажыралмайтын*** деп бөлінеді. Осы кластағы кодтардың ішінде техникалық орындалуының ең қарапайымы ***жинақталатын*** **(*рекуррент*) *кодтар*** болады.

6.2.1 Жиынтықты кодтау

Артықшылықты қолданудың жалпы қағидалары

Кодтың қателіктерді анықтаушы және түзетуші қасиеті ондағы артықша таңбалардың барлығына байланысты болады. Кодтаушы құрылғының кіруіне *k* ақпараттың екілік таңбалар тізбегі келіп түседі. Ал оның шығуынан *n* екілік таңбалар тізбегі шығады; мұнда $n > k$.



6.1-сурет

Барлығы болып 2^k кіру және 2^n шығу таңбалар тізбектері болады. Осында барлық 2^n шығу таңбалар тізбектерінен 2^k ғана кіру тізбектеріне сай келеді. Оларды ***рұқсат етілген код қисындастыруылары*** деп атаймыз. Басқа мүмкін болған 2^n - 2^k шығу тізбектері ақпарат ұзатуда қолданылмайды.

Олар ***рұқсат етілмеген қисындастыруылар*** деп аталады. Ақпараттың бұзылуын былай түсіндірсе болады: кейбір жіберілген таңбалар шығуда басқа қате таңбалармен ауыстырылады.

Әрбір 2^k рұқсат етілген қисындастыруылар кедергілер әсерінен кез келген басқа қисындастыруыға ауысуы (транформация) мүмкін болып, барлығы $2^n \bullet 2^k$ мүмкін болған ұзатулар болады (6.1-сурет).

Осы суретте 2^k қатесіз ұзатулар қара толық сызықтармен көрсетілген.

Ал $2^k\left(2^k-1\right)$ оқиғалар басқа рұқсат етілген күйлерге өтуді және табылмайтын қателіктерді көрсетеді. Олар суретте үздік сызықтармен көрсетілген; $2^k\left(2^n-2^k\right)$ оқиғаларда рұқсат етілмеген қисындастыруыларға өту көрсетіліп, олар табылатын қателерге сай келеді. Суретте олар жіңішке үздіксіз сызықпен көрсетілген. Сондықтан, табылатын қате код қисындастыруылары жалпы мүмкін болған оқиғалар ішінде мынаған тең болады:

$$2^k\left(2^n - 2^k\right)/\left(2^k \bullet 2^n\right) = 1 - 2^k / 2^n \,. \quad (6.1)$$

6.2 *Зертханалық жұмыс*

Әрбір қисындастыруы бір ғана артық таңбасы ($n = k+1$) болған кодтың анықтау қаблетін табайық. Шығу тізбектерінің жалпы саны 2^{k+1}, яғни кодталатын кіру тізбектерінің жалпы санынан 2 есе көп болсын.

Шешімі:

Мұнда рұқсат етілген код қисындастыруыларының кіші жиыны деп бірліктердің (немесе нөлдер) жұп сандарынан құралған 2^k қисындастыруыларының кіші жиынын алса болады.

Кодтауда әрбір k информациялық таңбаларға бір ғана таңба (0 немесе 1) қосатын болып, онда әрбір код қисындастыруындағы бірлер саны жұп болсын.

Кез келген таңбаның транформациясы рұқсат етілген код қисындастыруын рұқсат етілмеген код қисындастыруыларының кіші жиынына өткізеді де, оны қабылдауда бірліктердің тақ санымен тауып алады.

Табылған қателер бөлігі келесідей болады:

$$1 - 2^k / 2^{k+1} = 1/2 \,. \quad (6.2)$$

Енді қателіктерді түзету жағдайын қарастырайық.

Кез келген декодтау әдісін келесідей ереже деп қараса болады;

Барлық рұқсат етілмеген код қисындастыруылар жиынын 2^k қиылыспайтын M_i кіші жиындарына ажыратса болады; мұнда олардың әрбірі бір ғана рұқсат етілген қисындастыруыға сәйкес келеді.

Қабылдауда егер рұқсат етілмеген қисындастыруы алынса және ол M_i кіші жиынына сәйкес келсе, онда A_i рұқсат етілген қисындастыруы жіберілген деп табылады. Егерде қабылданған қисындастыруы ақиқаттан да A_i дан құралған болса, яғни $2^n - 2^k$ болса, осындайда ғана қателік түзетіледі.

Мұнда рұқсат етілмеген қисындастыруыларға өту жағдайларының барлығының саны $2^k\left(2^n - 2^k\right)$ болады. Сөйтіп, артықшылық бар болған жағдайларда код қателіктерді түзете алады.

Сонымен, қателіктерді түзететін код қисындастыруылар санының қателікті табатын код қисындастыруылар санына қатысы келесідей болады:

$$\left(2^n - 2^k\right)/\left[2^k\left(2^n - 2^k\right)\right] = 1/2^k . \quad (6.3)$$

Кіші жиындарға бөлу әдісі осы кодпен қандай қателіктерді түзету керек екендігіне байланысты болады.

Осы кезде құрылған кодтар ***өзара байланысты болмаған қателіктердің*** анық бір ретілігін және қателіктің түйіншегін (түйіншегін) түзетуге арналған болады.

Кез келген бұзылған таңбалар қисындастыруының ықтималдығы тек бұзылған таңбалар r санына және бір таңбаның бұзылу p ықтималдығына байланысты болса, онда ***қателіктер өзара байланысты болмаған*** деп аталады.

Қателіктің реті деп код қисындастыруындағы бұзылған таңбалардың санына айтамыз. Өзара байланысты болмаған қателіктерде n-орынды код қисындастыруындағы кез келген r таңбаларының бұзылуының ықтималдығы Бернулли теңдеуімен табылады:

$$p_r = C_n^r p^r (1-p)^{n-r} . \quad (6.4)$$

Егерде кем ықтималды қателіктердің ықтималдығы көп болғандығы себепті бірінші кезекте соларды табу және түзету керек болады.

Таңбалар тізбегінде бұзылған таңбалардың кез келген қисындастыруының пайда болу ықтималдығы тек қана ***бұзылған таңбалар r саны*** мен ***бір таңбаның бұзылу p ықтималдығына*** ғана байланысты болса, онда жіберілетін таңбалар тізбегінің осындай бұзылуын ***өзара байланыссыз қателер*** дейміз.

Мұндай дискрет арнаның үлгісі ***биномиалдық*** деп аталады**.** Алайда амалда байланыс арналарында бір таңбаның бұзылу p ықтималдығы тұрақты болмайды; бұл шаманың өзгеруі қателіктердің топтасуына және қателіктер түйіншегінің пайда болуына әкеледі. Сондықтан нақты арналар үшін Бернулли теңдеуін жуықталған түрде қолданып болады. Мұндай арналардың үлгілері қателіктердің жинақталу заңына байланысты болады [автор].

6.2.2 Түзетуші кодтардың жалпы қағидалары; сапа көрсеткіштері

Кодтың түзетуші қаблетінің код қашықтығына байланысы

Алдын айтылғандардан мынаны байқаса болады; өзара байланысты болмаған қателіктер әсерінен жіберілген код қисындастыруының басқа код қисындастыруыларына өту кезінде жіберілген код

қисындастыруына ең жақын болған қисындастыруыға өту ықтималдығы жоғары болады.

Екі код қисындастыруының бірінен бірінің айырмашылығы Хэмминг мағынасындағы олардың ***арасындағы қашықтықпен*** немесе ***код қашықтығымен*** сипатталады. Ол код қисындастыруыларының бірінен бірінің айырмашылығы олардың ерекше таңбалар санымен өлшенеді және *d* белгіленеді.

Осыны табу үшін екі қисындастыруыны екілік модулі бойынша қосу керек.

Мысалы: $d = 7$ болғанда:

$$\begin{array}{r} 1001111101 \\ \oplus\ \underline{1100001010} \\ 0101110111 \end{array}$$

Барлық рұқсат етілген код қисындастыруыларының барлық жұп (пара) бойынша қосып шыққанда олардың ішінде ең кемі ***минимал код қашықтығы*** деп аталады.

Қабылдау кезінде декодтау келесідей өткізіледі; қабылданған код қисындастыруын оған ең жақын болған рұқсат етілген қисындастыруына ауыстырылады.

Осындай декодтау ***максимал шындыққа ұқсас әдісімен*** декодтау деп аталады. Осыдан шығатыны, $d = 1$ де барлық код қисындастыруылары рұқсат етілген болады. Мысалы, $n = 3$ те рұқсат етілген қисындастыруылар келесідей болады: 000, 001, 010, 011, 100, 101, 110, 111.

Кез келген бірлік қателік берілген қисындастыруын басқа қисындастыруыға айналдырады; яғни осы артықшылығы жоқ болған код түзетуші қабілеті болмайды.

$d = 2$ болғанда, бірлік қателік кез келген қисындастыруыны оның алдындағы рұқсат етілмеген қисындастыруыға өткізеді; мұндай жағдайда бірлік қателіктер анық түрде табылып, басқа рұқсат етілген қисындастыруға өте алмайды.

Рұқсат етілген код қисындастыруылары олардағы бірлік таңбалардың қосындысының жұптық қағидасы бойынша құрылуы мүмкін. Мысалы, $n = 3$ болғанда, рұқсат етілген қисындастыруылар: 000, 011, 101, 110 болады; ал рұқсат етілмеген қисындастыруылар мыналар: 001, 010, 100, 111.

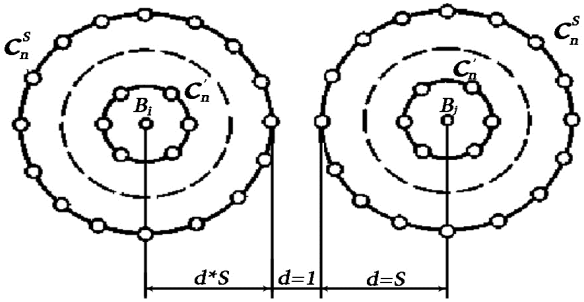
Осы код бірлік және басқа тақ қателіктерді табады.

Жалпы жағдайда r ретті қателіктерді табу үшін рұқсат етілген код қисындастырулар арасындағы минимал Хэмминг қашықтығы қателік ретінен, кем дегенде бірге артық болуы керек, яғни:

$$d_{0\min} \geq r+1 . \qquad (6.5)$$

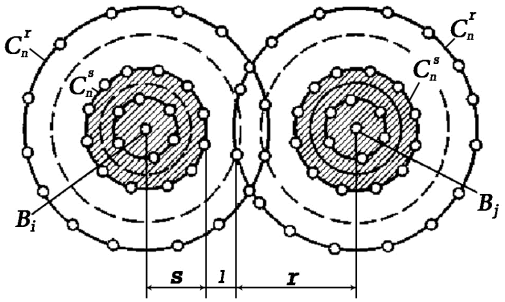
Осы жағдайда r реттіден аспайтын қателіктер рұқсат етілген бір қателікті екіншісіне өткізе алмайды.

Жалпы жағдайда декодтауда максимал шындыққа ұқсастық әдісі бойынша s ретті қателіктердің барлығын түзету үшін қателіктер өткізген рұқсат етілмеген қисындастыруы берілген код қисындастыруының кіші жиынының ішінде болуы керек.



6.2-сурет

Ал егер қателіктер әсерінен пайда болған рұқсат етілмеген қисындастыруы басқа таңбаның код қисындастыруының кіші жиынының ішінде болса, онда қателік



6.3-сурет

дұрыс түзетілмейді, яғни қателік өтіп кетеді. *n*-орынды рұқсат етілген қисындастыруылардың B_i (6.2-сурет) кіші жиыны рұқсат етілмеген қисындастыруылардан мына қателік әсерлерінен құрылады:

- Бірлік қателіктерден (олар өрістікте (сферада) орналасып, оның радиусы d=1 және олардың саны C^n);
- Екі ретті қателіктерден (олар өрістікте орналасып, оның радиусы d=2 және олардың саны C_n^2) және с.с. болады.

Кіші жиынның сыртқы өрістіктің радиусы $d = s$ болып, онда C_n^s рұқсат етілмеген код қисындастыруы болады. Аталған кіші жиындар өзара қиылыспауы керек болғандықтан, рұқсат етілген код қисындастыруылары арасындағы минималды Хэмминг қашықтығы мына талапқа жауап беруі керек:

$$d_{u\min} \geq 2s + 1 \tag{6.6}$$

Ал енді жалпы жағдайда барлық s ретті (6.3-сур.), қателіктерді түзету және барлық $r(r \geq s)$ ретті қателіктерді табу үшін минимал Хэмминг қашықтығын мына шарттан табу керек болады:

$$d_{u\min} \geq 2s + 1\,. \tag{6.7}$$

Мнимал код қашықтығын табуда қателіктердің байланысты болмаған жағдайына арналған минимал қашықтықты табу теңдеуі сигналға байланысты қателіктерге қарағанда артығырақ мәндер береді.

Нақты арналарда кедергі серпіндерінің ұзындығы көбінесе таңба ұзындығынан артық болады. Мұнда қисындастыруының жақын орналасқан таңбалары бірден бұзылады. Осындай қателіктер ***қателіктер дестесі (пачкасы)*** немесе ***қателіктер түйіншегі (түйіншегі)*** деп аталады. Қателіктер түйіншегі деп бірінші бұзылған таңбасы мен ақырғы бұзылған таңбасы арасында бұзылған таңбалар болып, ақырғы сиволдан соң кем дегенде ρ таңбалары бұзылмаған болады. ρ-ны таңдауда қателіктер санақтығы (статистикасы) анализ етіледі.

Мысалы, 00000000000000000 қисындастыруы мына қисындастыруға 01001000010101000 айналса және ρ ны үшке тең деп алсақ, онда осы қисындастыруыда екі түйіншек болып, ұзындықтары 5 және 4 таңба болады.

Көрсетілген декодтау әдісі осы жағдай үшін ең жақсы бола алмайды.

Асимметриялық арнада қателіктердің түйіншегі үшін тиісті түзетуші қаблетін алу үшін рұқсат етілген қисындастыруылар арасындағы минимал Хэмминг қашықтығы кемірек болуы да мүмкін.

Осы жерде айта кететін жай, әрбір түзетуші код кез келген қателіктер қисындастыруын түзету міндеттемесін бермейді. Кодтар, негізінен, берілген арнада көбінесе ықтималды болатын және қауіптірек болған қателіктер қисындастыруын түзетеді.

Егер кедергілер деңгейі мен сипаты күтілгеннен айырмашылығы көп болса, онда кодтың нәтижелігі күрт кемейеді.

Түзетуші кодты қолдану қатесіз қабылдаудың міндеттемесін бермейді; бірақ арнаның шығуында дұрыс нәтиже алудың ықтималдығын арттырады.

Түзетуші кодтардың сапа көрсеткіштері

Түзетуші кодтың негізгі сипаттамаларының бірі - ***код артықшылығы*** болып, ол тиісті түзетуші (түзетуші) қабілетке жету үшін керек болған код қисындастыруының ұзару дәрежесін көрсетеді.

Арна кодерінің шығу тізбегіндегі әрбір ***n*** *таңбалар*ына ***k*** информациялық және ***n-k*** тексеруші таңбалары тура келсе, онда кодтың ***салыстырмалы артықшылығы*** мына қатыстардың бірімен көрсетіледі:

$$R_n = (n-k)/n. \tag{6.8}$$

$$R_k = (n-k)/k. \tag{6.9}$$

R_k мәні мына аралықта өзгеруі мүмкін: 0-ден ∞ дейін.

Тиісті түзету қабілетіне ие болып, минимал артықшылыққа ие болған кодтар ***тиімді*** деп аталады.

Тиімді кодтарды табу мәселесінде, мысалы үшін, n - таңбалы екілік кодтың рұқсат етілген қисындастыруыларының максимал мүмкін болған Q санын табатын болайық; мұндай код өзара тәуелсіз қателердің s ретке дейінгісін түзететін болсын. Бұл дегені, кодтың ара қашықтығы $d = 2s+1$ нан кем болмайтын қисындастыруылар санын табу керек.

Әрбір рұқсат етілген код қисындастыруы үшін түзетілетін

қателердің жалпы саны $\sum_{i=1}^{s} C_n^i$ болады. Осындай қателердің әрбірі рұқсат етілмеген қисындастыруыға алып келеді; мұнда бұл қисындастыруы осы рұқсат етілген қисындастыруының кіші жиынына сәйкес келуі керек.

Осы қисындастыруымен бірге кіші жиын өз ішіне $1 + \sum_{i=0}^{s} C_n^i$ қисындастыруларды қосады.

Айтпақшыдай, осы кіші жиындар қиылыспаса, онда бірмәнді (анық) декодтау мүмкін болады. *n*-таңбалы екілік код қисындастыруының жалпы саны 2^n болса, онда **рұқсат етілген қисындастыруылар саны** мынадан аспауы керек:

$$2^n /(1 + \sum_{i=0}^{s} C_n^i) \qquad (6.10)$$

немесе $Q \leq 2^n / \sum_{i=0}^{s} C_n^i$. (6.11)

Осы **жоғарғы бағаны Хэмминг** тапқан.

Код қашықтығы *d* ның кейбір мәндері үшін сәйкес *Q* мына 6.1-кестеде көрсетілген.

6.1- кесте

d	*Q*	*d*	*Q*
1	2^n	5	$\leq \frac{2^n + 1}{n^2 + n + 2}$
2	$\leq 2^{n-1}$	…..	……
3	$\leq \frac{2^n}{n+1}$	…..	……
4	$\leq \frac{2^{n-1}}{n}$	$2k+1$	$\leq \frac{2^n}{1 + C_n^1 + C_n^2 + ... + C_n^k}$

Кейбір кодтарда осы қатыстар теңдікке айналса, онда ондай кодтар ***нығыз жайласқан кодтар*** деп аталады.

Алайда тиімдіге жақындау әрқашанда мақсатқа сай келе бермейді; одан кем түспейтін көрсеткіш - бұл кодтау және декодтау үдерісінің ***техникалық орындалуының күрделілігі*** болады.

Егер арна қымбат, сенімсіз және өте баяу болса, ал кодер, декодерлер жоғары сенімді және жылдам элементтерден құрылатын болса, онда осы құрылымдардың күрделілігі айтарлықтай қызмет ойнамайды.

Осындай жағдайда байланыс сызығын нәтижелі қолдану шешуші мәселеге айналады; сондықтан минимал артықшылығы бар түзетуші кодтарды қолдану керек болады.

Ал егер түзетуші код өте жоғары сенімділікті және жылдам элементтерден құралған жүйемен (мысалы, есептеу техникасымен) бірге істетілетін болса, онда кодтың сапа шарты жүйенің жалпы сенімділігі болады; мұнда кодер-декодерлердегі бұзылулар мен істен шығулар да есепке алынады. Мұндай жағдайда кодтардың артықшылығы үлкен болғаны және техникалық орындалуы оңай болғаны жөн.

Ал егерде байланыс жолдары өте алыс болса және арна нашар болса, онда код артықшылығы үлкен болуы керек.

6.3 Сызықты кодтар; топтық екілік код құру

Ажыратылатын кодтардың ішінде ең үлкен класты сызықты кодтар құрайды; мұнда тексеруші таңбалар мәлім бір ақпараттық таңбалар үстінде сызықтық амалдар орындаумен анықталады.

Екілік кодтарда әрбір тексеруші таңбалы анықталған ақпараттық таңбалармен қосқанда нөл шығуы керек болады.

Егер де тиісті тексеруші теңдеудің ақпараттық дәрежелеріндегі ***бірліктер саны тақ*** болса, осыған сәйкес тексеруші жайғасымның таңбасы 1-ге тең болады;

ал егерде сол ***бірліктер саны жұп*** болса, онда тексеруші жайғасымның таңбасы 0-ге тең болады.

Тексеруші теңдеулер (сондай-ақ тексеруші таңбалар) және осы әрбір теңдеуге кіретін айқын ақпараттық дәрежелер (разрядтар) қандай және қанша қателіктерді түзету керектігіне байланысты табылады.

Тексеруші таңбалар код қисындастыруының *кез келген жерінде* орналасуы мүмкін. Әдетте оларды код қисындастыруының соңына тіркейді.

Декодтауда сол тексеруші теңдеулердің ақиқаттығы тексеріледі; екілік кодтар жағдайында бұл осы тексеруші теңдеулердің әрбіріндегі ***таңбалар санын жұпқа тексеру*** арқылы орындалады. Мұнда тексеруші дәрежелер да есепке алынады. Тексерулер нәтижесінде қателіктің бар-жоқтығын анықтайтын немесе қате қай жайғасымда (жайғасымдарда) екенін анықтайтын ақпарат алынады.

Сызықты екілік код топтық болады, себебі оған қатысты код қисындастыруылары топ құрайды.

6.3.1 Сызықты кодтарға математикалық кіріспе

Сызықтық кодтардың математикалық сипаттамасының негізі ***сызықтық алгебра*** болып, оған ***векторлы кеңістіктер теориясы, матрицалар теориясы, топтар теориясы*** жатады. Кейбір анықтамаларды атап өтеміз.

Топ элементтер жиынынан құралған болып, онда бір негізгі операция анықталған болады және мына аксиомалар орындалады:

1. Топтың кез келген екі элементіне операция орындағанда осы топтың басқа элементі шығады ***(тұйықтық талабы).***
2. Топтың кез келген үш элементіне мына теңдіктер орынды болады; егер қосу операциясы болса, онда $(a+b)+c=a+(b+c)$, ал егер көбейту операциясы болса, онда $a(bc)=(ab)c$, немесе шартты түрде. $a \bullet 1 = 1 \bullet a = a$.
3. Кез келген G_n топта анық бір элемент бар болып, осы G_n топтағы бір a ның барлық мәндерінде мына шарт орындалады: $a+0=0+a=a$ (егер негізгі операция қосу болса); немесе, егер негізгі операция көбейту болса, онда мына шарт $a \bullet 1 = 1 \bullet a = a$ орындалады.

Бірінші жағдайда элемент ***нөл*** деп аталып, 0 таңбасымен таңбаланады, ал екінші жағдайда элемент ***бір*** деп аталып, 1 таңбасымен таңбаланады.

4. Топтың кез келген a элементі мына теңдеумен анықталатын элементке ие болады: $a+(-a) = -a + a = 0$ (егер негізгі операция қосу болса) немесе мына теңдеумен: $a^{-1} = a^{-1}a = 1$ (егер негізгі операция көбейту болса).

Бірінші жағдайда элемент ***қарсы элемент*** деп аталып, (-*a*) таңбаланады, ал екінші жағдайда – ***кері элемент*** деп аталып, келесідей таңбаланады: a^{-1}.

Топта анықталған операция коммутативті болса, онда топты ***коммутативті*** немесе ***абелдік*** деп атайды.

Егер топтағы элементтер саны шекті болса, ***топ шекті*** деп аталады.

Топтағы элементтер саны ***топ тәртібі*** деп аталады.

Топ шекті болуы үшін негізгі операция орындалғанда нәтиженің дәрежелер саны өзгермеуі керек. Осындай операцияға модул бойынша қосу операциясы жатады; екілік жүйеде бұл **екілік модул бойынша қосу операциясы:** $\oplus$ - mod 2. Мұндай операцияда қосынды нәтижесінде 1-лер саны тақ болса, 1; ал жұп болса, 0 жазылады. Мысалы:

$$\begin{array}{r} 1011101 \\ 0111101 \\ \oplus\ 0001110 \\ \hline 1101110 \end{array}$$

Біз таңдаған операция коммутативті болғаны үшін қаралып отырған топтар абелдік болады. Мұнда нөлдік элемент тек 0 дерден құралған болады.

Модул 2 бойынша айыру операциясы да қосу операциясына тең болады.

6.3 *Зертханалық жұмыс*

Төмендегі код қисындастыруылар жиыны топтарға жататынын анықтау керек:

1) 0001, 0110, 0111, 0011,
2) 0000, 1101, 1110, 0111,
3) 000, 011, 010, 011, 100, 101, 110, 111

Шешімі:

Бірінші жиын топқа жатпайды; себебі нөлдік элементі жоқ.

Екінші жиын да топқа жатпайды; себебі тұйықтық шарты орындалмайды; мысалы, 1101 және 1110 қисындастыруыларының модул 2 бойынша қосындысы 0011 қисындастыруын береді; ол берілген жиынға жатпайды.

Үшінші жиын барлық аталған шарттарға жауап береді және топқа жатады.

Топтың кіші жиындары кіші топтар деп аталып, топта анықталған амалдарға салыстырғанда топтар болады.

Мысалы, үш орынды код қисындастыруының кіші жиыны: 000, 001, 010, 011 мысалда көрсетілген үш орынды код қисындастыруының кіші тобын құрайды.

Айталық G_n Абель тобында A анықталған кіші тобы берілсін. Егерде B – кез келген A ға кірмейтін G_n нің элементі болса, онда B элементтерінің A кіші тобының әрбір элементімен екілік модул бойынша қосындысы A кіші тобы бойынша G_n тобының көршілес (смежный) класын құрады; бұл B элементімен туындайды.

Кез келген кіші топтың нөлдік элементі болғандықтан, әрине B элементі осы көршілес кластан табылатын болады.

Жаңа құрылған көршілес кластарға жатпайтын топтың кейбір B_j элементтерін тізбектеп алып, топтың барлығын A кіші тобы бойынша көршілес кластарға жіктеу мүмкін. Мұнда B_j элементтерін кіші топтың көршілес кластарының ***құрастырушы*** (***образующий - бейнелеуші***) элементтері деп атайды.

Жіктеу кестесінде құрастырушы элементтер әдетте сол жақ бағанда орналасқан болады; кейде мұндай кестені ***топтық кесте*** деп атайды.

Мұнда кіші топтың ең сол жақтағы элементі нөлдік элемент болады.

6.3 Зертханалық жұмыс

Үш орындық екілік код қисындастыруылар тобын екі орындық код қисындастыруыларының кіші топтарына жіктейміз. Мұндай жіктеуді 6.2-кестеге сәйкес орындаймыз.

6.2-кесте

$A_1 = 0$	A_2	A_3	A_4
000	**001**	**010**	
B_1	$A_2 + B_1$	$A_3 + B_1$	$A_4 + B_1$
100	**101**	**110**	

6.4 *Зертханалық жұмыс*

Төрт орынды (разрядтты) екілік код қисындастыруының тобын екі орынды код қисындастыруларының кіші топтарына жіктейміз. Көршілес кластарын құрастырушы ретінде қай элементтер таңдалғандығына байланысты жіктеудің әртүрлі нұсқалары бар. Төмендегі 6.3-кестесінде сол нұсқалардың бірі көрсетілген.

6.3-кесте

$A_1 = 0$ 0000	A_2 0001	A_3 0010	A_4 0011
B_1 0100	$A_2 \oplus B_1$ 0101	$A_3 \oplus B_1$ 0110	$A_4 \oplus B_1$ 0111
B_2 1010	$A_2 \oplus B_2$ 1011	$A_3 \oplus B_2$ 1000	$A_4 \oplus B_2$ 1001
B_3 1100	$A_2 \oplus B_3$ 1101	$A_3 \oplus B_3$ 1110	$A_4 \oplus B_3$ 1111

Сақина деп R элементтерінің жиыны айтылып, онда екі операция (қосу және көбейту) анықталған болады және мыналар орынды болады:

1) R жиыны қосу бойынша коммутативті болады;

2) $a \in R$ және $b \in R$ элементтерінің көбейтіндісі R элементі болады (қосу операциясына қарағанда тұйықтық);

3) R дің кез келген үш a, b және c элементтері үшін $a(bc) = (ab)c$ теңдігі орынды болады (көбейтудің ассоциативтік заңы);

4) R дің кез келген үш a, b және c элементтері үшін $a(b+c) = =ab+ac$ және $(b+c)a = ba+ca$ теңдіктері орынды болады (дистрибутивтік заңдар).

Егер сақинаның кез келген екі элементі үшін мына қатыс $ab = ba$ орынды болса, сақина ***коммутативтік*** деп аталады.

Сақинаның көбейту бойынша бірлік элементі және кері элементтері болмайды. Сақинаға мысал ретінде дәстүрлі көбейту және қосу амалдарына байланысты нақты жұп бүтін сандар жиынын алса болады.

F өрісі деп еш болмағанда екі элементтен құралған жиынға ай-

тылады; онда екі операция (қосу және көбейту) анықталған болады және мына аксиомалар орындалады:

1) элементтер жиыны қосу бойынша коммутативті топ құрады;

2) нөлсіз элементтер жиыны көбейту бойынша коммутативті топ құрады;

3) *a, b, c* жиынының кез келген үш элементі үшін мына қатыс орындалады (дистрибутивтік заң) $a(b+c)=ab+ac$ . .

Сондықтан *F* өрісі көбейту бойынша бірлік элементті коммутативті сақина болады; онда әрбір нөлсіз элемент өзінің кері элементіне ие болады. Өрістің, мысалы ретінде барлық нақты сандар жиынын алса болады.

GF(*P*) өрісі, *P* элементтерінің шекті санынан тұратын болса, оны шекті өріс немесе Галуа өрісі деп атайды. Кез келген *P* саны үшін, егер ол *q,* жай санының дәрежесі болса, онда оның *P* элементі бар болған өрісі болады. Мысалы, q модулді сандар жиыны, *q* – жай сан болғанда, өріс құрайды.

Өрісте екі элементтен кем болуы мүмкін емес; себебі онда кем дегенде қосу операциясына байланысты бірлік элемент (0) болуы керек және көбейту операциясына байланысты бірлік элемент (1) болуы керек.

Өрістің тек екі элементі 0 және 1 болса, оны *GF* (2) деп таңбалаймыз.

Екі элементті өрістегі қосу және көбейту ережелері төмендегідей:

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

Жалпы жағдайда, A_j және A_i кодтық қисындастыруларының қосындысы деп мына қисындастыруға айтамыз: $A_f = A_i + A_j$, мұнда кез келген A_k (k=1, 2, ..., n) таңбасы берілген қисындастыруылардың *к*- таңбаларының қосындысынан тұрады; мұнда қосу *GF*(*P*) өрісінің ережесі бойынша орындалады.

Мұнда барлық *n* – орынды (разрядты) код қисындастыруларының жиыны абелдік топ болады.

Жеке жағдайда, егер код негізі *q* жай саны болса, *GF*(*q*) өрісінде қосу ережесі берілген *q* модулімен қосу ережесімен тең болады.

Сызықтық код сызықтық векторлық кеңістіктің кіші кеңістігі ретінде

Жоғарыда көрілген алгебралық жүйелерде (топтар, сақина, өріс) амалдар математикалық нысандардың тек бір класына тиісті еді; мұндай амалдарды элементтер комжайғасымының ішкі заңдылықтары дейді.

Кодтау теориясында математикалық нысандардың (мысалы, L және Ω) екі класын өз ішіне алатын үлгілер кең қолданылады. Оларда комжайғасымдардың ішкі заңдарынан тыс элементтердің комжайғасымдарының сыртқы заңдылықтары да беріледі; онда кез келген $\omega \in \Omega$ және $a \in L$ элементтеріне $c \in L$ элементі сәйкес қойылады.

Егерде V элементтер (векторлар) жиынына төмендегі аксиомалар орынды болса, онда оған F элементтер өрісінің үстіндегі ***сызықтық векторлық кеңістік*** деп аталады:

1) V жиыны қосу операциясына байланысты коммутативтік топ болса;

2) V дағы кез келген вектор v және F-тегі кез келген скаляр c үшін *cv көбейтіндісі анықталған болса; ол V* да болады (скалярға көбейтудегі тұйықтық);

3) егер V-дегі u және v-лар векторлар болса және F тегі c және d лар скалярлар болса, онда мына қатыстар орында болады:

$$c(u+v) = cu + cv, (c+d)v = cv + dv$$ (дистрибутивтік заңдар);

4) егер v – вектор, ал c және d – скалярлар болса, онда $(cd)v = c(dv)$ және $1 \cdot v = v$ болады (скалярға көбейткендегі ассоциативтік заң).

Жоғарыда код қисындастыруларды дәрежелер (разрядттар) бойынша қосу ережесі анықталған еді; мұнда олардың барлық жиыны абелдік топ құрайтын.

Енді $GF(P)$ өрісінің n элементтерінің (код қисындастыруларының) тізбегін $GF(P)$ өрісінің a_i элементіне көбейту операциясын анықтайық.

Бұл векторды скалярға көбейтуге ұқсас орындалады: $a_i(a_1, a_2, ..., a_n) = (a_i a_1, a_i a_2, ..., a_i a_n)$.

[көбейту *GF(P)* өрісінің ережелері бойынша орындалады].

Таңдалған амалдарда дистрибутивтік заңдар мен ассоциативтік заң орындалғандықтан, барлық n - орындық кодтық қисындас-

тыруыларды $GF(P)$ өрісінің үстіндегі векторлық сызықтық кеңістік деп қарауға болады; ал ондағы кодтық қисындастыруыларды оның векторлары деп қараса болады.

Мысалы, екілік кодтауда векторлар $GF(2)$ өрісінің элементтерінен құралған (яғни 0 және 1) болады.

Қосу екілік модулде дәрежелер бойынша орындалады.

Векторды өрістің бір элементіне (1) көбейткенде ол өзгермейді; ал өрістің басқа элементіне (0) көбейткенде оны вектор кеңістігінің 0 = (0 0...0) таңбасымен белгіленген бірлік элементіне айналдырады.

Егер $GF(P)$ өрісінің n элементтік тізбегінің сызықтық кеңістігінде қосымша түрде векторларды көбейту операциясын берсек және олар анықталған шарттарға (ассоциативтік, тұйықтық, скалярға көбейтуде бисызықтық) қанағаттандыратын болса, онда n - орынды код қисындастыруыларының барлық жиыны $GF(P)$ еселіктері өрісінің үстіндегі сызықтық коммутативтік алгебраға айналады.

Егер векторлық кеңістіктің элементтерінің кіші жиыны вектор кеңістігінің аксиомаларына қанағаттандыратын болса, онда оны кіші кеңістік (подпространство) деп атайды.

Сызықтық код деп векторлардың жиынына айтылады және олар $GF(P)$ өрісінің үстіндегі барлық n-орынды код қисындастыруыларының векторлық кеңістігінде кіші кеңістік құрады.

Екілік кодтау жағдайында GF (2) өрісінің үстіндегі қисындастыруылардың кіші кеңістігін кез келген екілік код қисындастыруылары құрады; олар барлық n-орынды екілік код қисындастыруылар тобының кіші тобы болады. Сондықтан кез келген екілік сызықтық код ***топтық*** болады.

6.3.2 Топтық екілік код құру

Айқын түрдегі түзетуші кодты құру үшін сол кодтың көлемі Q анықталады; ол өлшенетін шаманың дискретті мәнінен және байланыс арнасындағы ең ықтималды қателік векторлары туралы санақтық деректерден тұрады. ***Қателік векторы (ажыратушы*** немесе ***табушы синдром)*** деп n-орынды (разрядты) екілік тізбекті айтып, онда қателік бар орындарға сәйкес 1-лер, ал басқа орындарға 0 дер сәйкес болған векторға айтады. Осыдан кейін кез келген қателері бар код қисындастыруын рұқсат етілген код қисындастыруы мен

қателік векторының модул 2 бойынша қосындысы немесе айырмасы деп қарау мүмкін болады.

Мына теңсіздіктен $2^k - 1 \geq Q$ (нөлдік қисындастыруы қаралмайды) екілік кодпен берілген командаларды жіберу үшін керек болған ақпараттық дәрежелер k санын табамыз. Әрбір 2^k-1 нөл емес k-орынды артықшылықсыз кодқа n таңбалық қисындастыруыны сәйкес қойуымыз керек болады.

Осындай қисындастыруының n — k тексеруші орындарындағы таңбаларының мәні мәлімбір ақпараттық орындардың таңбаларын модул 2 бойынша қосумен табылады.

Ақпараттық таңбалардың (нөлдік таңбаларды қоса) 2^k қисындастыруылар жиыны барлық n-орынды қисындастыруыларының кіші тобын құрып, онда аталған жолмен құрылған 2^k n- орынды қисындастыруылар жиыны да n-орынды код қисындастыруыларының кіші жиыны болады.

Бұл рұқсат етілген код қисындастыруы да топтық код болады. Осында тексеруші орындар разрядтар саны мен тексеруші орындағы таңбаларды анықтаушы теңдеулердегі ақпараттық орындардың нөмірлерін анықтау керек болады.

2^n тобындағы барлық n-орынды қисындастыруыларды іргелес кластарға кіші топтары бойынша 2^k рұқсат етілген n-орынды код қисындастыруыларына ажыратамыз; оларда тексеруші дәрежелер әлі толтырылмаған болады.

Кодтың өзінің кіші тобынан басқа жіктеуде $2^{n-k} - 1$ іргелес кластары саналады. Осында әрбір кластың элементтері код қисындастыруы мен осы кластың элементтерінің құраушыларының 2 модул бойынша қосындысына тең болады. Егерде әрбір кластың құрушы элементтері деп берілген байланыс арнасындағы өте ықтималды қателік векторларын қабылдасақ және олар түзетілуі керек болса, онда барлық рұқсат етілген қисындастыруыларға анықталған қателік векторы әсерінен пайда болған код қисындастыруылары іргелес кластарға топталады.

Кез келген байланыс арнасының шығуында пайда болған код қисындастыруын түзету үшін енді оның қайсы іргелес класта екенін анықтау керек болады.

Енді оны осы іргелес кластың құраушы элементімен 2 модуль бойынша қосып, кодтың шын қисындастыруын аламыз. Осыдан анықталатыны, барлық мүмкін болған қателіктер $2^n - 1$ санынан

топтық код іргелес кластардың ішінен тек қана $2^{n-k}-1$ қателік түрлерін түзете алады.

Алынған қисындастыруы қай іргелес класқа жататынын анықтау үшін әрбір іргелес класқа кейбір тексеруші таңбалар тізбегі сәйкес қойылуы керек болады; ол ***синдром*** немесе ***танушы*** деп аталады.

Осында қабылдау жеріндегі тексеру нәтижесінде синдромның әрбір таңбасы бір теңдіктің дұрыстығын анықтайды; ол теңдіктер кодтау уақытында тексеруші таңбалардың мәнін анықтау үшін құрылған болатын.

Жоғарыда айтылғандай сызықтық екілік кодта тексеруші таңбалардың мәнін таңдап алуда әр теңдеуге қатысты (тексеруші орындар да соның ішінде) таңбалардың модуль 2 бойынша қосындысы нөлге тең болуы керек еді.

Ондай болса осы таңбалардағы 1-лер саны жұп болуы керек.

Сондықтан синдромның таңбаларын анықтау операциясын ***жұпқа тексеру*** деп атайды. Егер қателік жоқ болса, онда жұпқа тексерудің барлығында нөлдер шығады және синдром тек нөлден құралады.

Егер тексеруші теңдік қанағатанбаса, онда синдромның тиісті орнында (орынында) 1 пайда болады. Қателікті анықтау осымен бітеді.

Қателіктер түзетілуі мүмкін болған жағдайды қарастырайық;

егер синдромдар жиыны мен іргелес кластар жиыны немесе түзетілуі керек болған қателік векторларының жиыны арасында қатал анық бір сәйкестік бар болса ғана қателік түзетілуі мүмкін болады.

Сондықтан, түзетілуі керек болған қателік саны артықша таңбалар саны $n - k$- ны табуда негіз болады. Олардың саны талап етілген симдромдар санын жабдықтауға жеткілікті болуы керек. Мысалы, егер барлық бірлік қателерді түзету керек болса, онда саны n болған түрлі қателерді түзету керек болады:

000 01
000..10
.....
010...00
100..00

Осында нөлден ерекше синдромдар саны n-нен кем болмауы керек.

Осыдан керек болған тексеруші орындар (дәрежелер) саны мына теңдеуден табылады:

$$2^{n-k} - 1 \geq n \qquad (6.12\ \text{a})$$

немесе

$$2^{n-k} - 1 \geq +C_n^1 \qquad (6.12\ \text{b})$$

Егер бірлік қателіктерден тыс екілік қателіктерді де түзету керек болса, онда теңдеулер мына түрге келеді: $2^{n-k} - 1 \geq C_n^1 + C_n^2$ (6.13)

Ал егер барлық өзара байланысты болмаған s ретті қателіктерді түзету керек болса, мына теңдікті қолданамыз:

$$2^{n-k} - 1 \geq C_n^1 + C_n^2 + \ldots + C_n^s. \qquad (6.14)$$

Алайда осы теңдіктер тек тексеруші орындардың (дәрежелердің) минималды шекті санын көрсетеді; ал амалда көп жағдайларда бұлар нақты болмайды.

Көбінесе тексеруші таңбалар саны теңдеулерден табылғанына қарағанда көбірек талап етіледі.

6.3.3 Синдром кестесін құрастыру

Бірлік қателіктерді табатын синдромды құрастырудан бастайық. Айталық 15 команданы кодттау керек болсын. Онда оған керек болған ақпараттық дәрежелер 4 болады. Мына теңдеуден

$$2^{n-k} - 1 = n$$

кодтың жалпы дәрежелер санын табамыз; түзетілетін қателіктер санын да табамыз (n = 7).

Үш артықша дәрежелер синдром ретінде үш орынды екілік түзбекті қолдану мүмкіндігін береді. Сонда синдром қателік бар дәреженің нөмірін екілік санақ жүйесінде көрсетеді. Қателік нөмірі ең кіші орыннан (дәрежеден) басталады (6.4-кесте).

6.4-кесте

Қателік векторы	Синдром	Қателік векторы	Синдром
0000001	001	0010000	101
0000010	010	0100000	110
0000100	011	1000000	111
0001000	100		

Осы түрде құрылған кодтар **Хэмминг кодтары** деп аталады**.**

Енді күрделірек болған бірлік және екілік тәуелсіз қателіктерді қарастырайық. Синдром ретінде бірінші және екінші орындардағы бірлік қателіктер үшін мына қисындастыруыларды алсақ болады: 0...001 және 0...010.

Үшінші орындағы қателік үшін мына қисындастыруыны 0...011 алып болмайды. Мұндай қисындастыруы бірдей екі қателіктерге: бірінші орындағы және екінші орындағы қателіктерге сәйкес келеді.

Алайда мұндай қателікке дәл сондай синдромды алса болады, яғни: 0...011.

Келесідей 0...0100 қателікке дәл сондай синдромды, ал 0...0101 қателігі екі қателік қосындысы (0...0100 және 0...0001) ретінде қаралып, олар үшін синдром 0...0101 алынса болады. Ал 0...0110 үшін синдром 0...0110 алса болады. Төртінші орындағы бірлік қателік 0...01000 үшін дәл сондай қисындастыруыны 0...01000 алған жөн. Онда мына қателік векторлары үшін

0...01001, 0...01010, 0...01100 сол векторлардың өздерін алған жөн болады.

Бесінші орында бірлік қате болса, оның синдромы ретінде төрт орынды қисындастыруы 01111 алынады. Ал қателік бесінші және одан төмен орындарда болса, алдын қолданылмаған синдромдарды табамыз:

Қателік векторы	Синдромдар
0 010001	0 0110
0 010010	0 01101
0 010100	0 01011
0 011000	0 00111

Осыдан шығатын қорытынды келесідей болады; бірнеше орындардағы жеке бірлік қателіктер векторының синдромын табу үшін сол жеке бірлік орындардағы қателікті табатын синдромдарды жеке жеке тауып, оларды модул 2 бойынша қосу керек болады. Сонымен, **код құру ережесін анықтау** және **тексеруші теңдеулерді құрастыру** үшін тек қана **әрбір орындағы бірлік қателікті табатын синдромды білу** жеткілікті болады.

Екі тәуелсіз қателікті түзететін кодтарды құру үшін оларға синдромды құру 29 орынға (дәрежеге) дейін ЭЕМ жәрдемінде орын-

далады. Ал бірінші 15 орынның синдромдары төмендегі кестеде берілген:

Дәреже нөмірі	Синдром	Дәреже нөмірі	Синдром	Дәреже нөмірі	Синдром
1	00000001	6		11	01101010
2	00000010	7		12	10000000
3	00000100	8		13	10010110
4	00001000	9		14	10110101
5	00001111	10		15	11011011

Осы қағида басқа түрдегі қателіктер үшін де анықталған, мысалы, үш тәуелсіз қателіктер үшін, екі және үш таңбалы қателіктер түйіншегі үшін де анықталған.

Тексеруші теңдеуді анықтау.

Сөйтіп, әрбір кодтың мақсаты берілген байланыс арнасы үшін ең ықтималды қателік векторын түзету (өзара тәуелсіз қателіктерді немесе қателік түйіншек) болса, әрбір жеке қателіктің дәрежесін табатын синдром кестесін құру мүмкін болады.

Осы кестені қолданып, қайсы таңбалық таңбалары жұпқа тексеруші теңдеуге қатысты екенін анықтау қиын емес.

Бірлік қателіктерді түзетуші кодтардың синдромдарын қарастырайық.

6.6-кесте

Дәреже нөмірі	Синдром	Дәреже нөмірі	Синдром	Дәреже нөмірі	Синдром
1	0001	7	0111	12	1100
2	0010	8	1000	13	1101
3	0011	9	1001	14	1110
4	0100	10	1010	15	1111
5	0101	11	1011	16	10000
6	0110				

Осы кестені кез келген деңгейде қырқу арқылы код құру мүмкін болады. Алайда кестеден көрініп тұрғанындай **тиімді кодтар** мыналар болады: (7, 4), (15, 11) және басқалар; мұнда бірінші сан *n,* ал

екінші сан k болып, басқа қодтардың ішінде тексеруші таңбалары бірдей болса да, ал информациялық таңбалары ең көп болады. Осы кестені жетінші орында кесеміз және барлық тексеруші теңдеулерге қатысты болатын таңбалардың нөмірлерін табамыз. Синдромның ең кіші орнын жұпқа тексерейік. Қате жоқ болғанда олардың қосындысы нөлге тең болады. Мысалы бірінші тексеруші теңдеу мына 1,3,5,7 орындардағы таңбаларды қамтуы керек:

$$a_1 \oplus a_3 \oplus a_5 \oplus a_7 = 0.$$

Ал енді екінші орында қате болса, оны мына теңдеумен тапса болады:

$$a_2 \oplus a_3 \oplus a_6 \oplus a_7 = 0.$$

Дәл осындай үшінші теңдеу табылады:

$$a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 0.$$

Кез келген ақпараттық орындарда қателікті табу үшін үш тексеруші дәреже болуы керек.

Осы орындардың нөмірлерін таңдағанда олардың әрбірі тек бір ғана теңдеуге қатысты болуы керек.

Осы талапқа жауап беретін орындардың әрбірінде олардың сәйкес синдромдарында бір бірліктен болуы керек.

Қарастырып отырған мысалда, ол бірінші, екінші және төртінші орындар болады. Осы айтылған талаптарға жауап беретін теңдеулер мыналар болады:

$$\begin{aligned} a_1 &= a_3 \oplus a_5 \oplus a_7, \\ a_2 &= a_3 \oplus a_6 \oplus a_7, \\ a_4 &= a_5 \oplus a_6 \oplus a_7. \end{aligned} \qquad (6.15)$$

Құрылған кодта минималды Хэмминг қашықтығы d_{min} = 3 болғандықтан ол бірлік және екілік қателіктерді табады.

6.6-кестеден көрініп тұрғандай бірлік қателіктердің кез келген синдромдарының қосындысы қателік болғанда нөлге тең болмайды.

6.4 *Зертханалық жұмыс*

15 сөзі болатын көлемді топтық код құрайық; ол екілік қателіктерді тауып, бірлік қателіктерді түзетсін.

(6.7) теңдеуіне сәйкес кодтың минимал Хэмминг қашықтығы 4 болуы керек. Осындай кодты екі этапта құрса болады.

Алдын берілген көлемдегі бірлік қателікті түзететін кодты құрамыз. Осы код Хэмминг (7, 4) коды болады.

Содан соң тағы бір орынды қосамыз. Ол рұқсат етілген қисындастыруылардағы бірліктердің жұптығын тексереді.

Сөйтіп, (8, 4) кодын аламыз.

$$a_1 = a_3 \oplus a_5 \oplus a_7,$$
$$a_2 = a_3 \oplus a_6 \oplus a_7,$$
$$a_4 = a_5 \oplus a_6 \oplus a_7,$$
$$a_8 = a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7.$$

(7,4) кодының синдромын S_i арқылы таңбалап, жұпқа тексерудің жалпы көрінісі келесідей болады:

$$S_2\left(S_2 = \sum_{i=1}^{8} a_i\right) \neq 1,$$

және 3-ке ретті қателіктерді жоқ деп, декодтау бағдаржолын келесідей жазамыз:

$S_1 = 0$ және $S_2 = 0$ болғанда қате жоқ;

$S_1=0$ және $S_2 = 1$ қате сегізінші орында болады;

$S_1=0$ және $S_2 = 0$ екілік қате (түзету жиынтықталады, қайта жіберуге сұрақ беріледі);

$S_1=0$ и $S_2=1$ бірлік қате (қателік түзетіледі).

6.5 *Зертханалық жұмыс*

6.6-кестесін қолданып, барлық бірлік және екілік қателіктерді түзететін (8,2) кодын құрамыз. 6.5-кестесін сегізінші орында кесіп, мына тексеруші теңдеулерді табамыз:

$$
\begin{aligned}
a_{11} &= \oplus a_5 \oplus a_6 = 0,\\
a_2 &\oplus a_5 \oplus a_8 = 0,\\
a_3 &\oplus a_5 = 0,\\
a_4 &\oplus a_5 = 0,\\
a_6 &\oplus a_8 = 0,\\
a_7 &\oplus a_\pi = 0.
\end{aligned}
\qquad (6.16)
$$

Ақырғы теңсіздіктен код құру теңдеулерін шығарамыз:

$$a_1 = a_5 \oplus a_8 \qquad (6.16\ \text{а})$$

$$a_2 = a_5 \oplus a_8 \qquad (6.16\ \text{б})$$

$$a_3 = a_5 \qquad (6.16\ \text{в})$$

$$a_4 = a_5 \qquad (6.16\ \text{г})$$

$$a_6 = a_8 \qquad (6.16\ \text{д})$$

$$a_7 = a_8 \qquad (6.16\ \text{е})$$

Осы кодта d_{min}= 5 болғандығы үшін оны 1-ден 4-ке дейінгі қателіктерді анықтауда қолданса болады. Екілік сызықтық кодттарды кодтау және декодтау үдерістерін көрсететін қатыстарды екілік модулдегі қосындыторлар жәрдемінде орындалуы болады. Алайда осы түрде құрылған декодерлер үлкен орынды қателіктерді түзетуші кодтарда өте күрделі болады. Мұндай жағдайда басқа декодтау қағидалары нәтижелі болады.

6.3.4. Қателіктерді анықтаушы және түзетуші кодтарды үлгілеу; Хэмминг кодтары және олардың желіде қолданылуы

Хэмминг кодтары кең қолданылуына негізгі себептер - кодер және декодерлердің қарапайымдығы және оның минимал артықшылығы.

ЭЕМ-нің шапшаң жадының сенімділігін арттыру үшін деректерді жадыда сақтауда Хэмминг коды қолданылады; ол жеке қателіктерді түзетіп, ал жоғары орынды қателіктерді анықтай алады.

Осы кездегі микропроцессорлар орны 64 биттен кем емес болғандықтан, олардың жадының да орындығы 64 биттен кем емес

болады. Осыған сәйкес Хэмминг коды (72, 64) болып, 64 ақпараттық және 8 тексеруші орындары болады. Осы кодты істеткенде болатын нәтижелікті есептеп тапса болады.

Айталық, бір орынды жадының модулі мәлімбір уақыт аралығында істен шығу ықтималдығы $P_1=10^{-5}$ болсын.

Дәл сол уақыт аралығында жадының 64 модулінің бірі істен шығу ықтималдығы $P_{жалпы} = 64*P_1=6.4*10^{-4}$ болады.

Ал Хэмминг кодын қолданғанда ақпаратты жоғалту үшін 72 орынның екі орынында екі қате болуы керек: $P_{жалпы} = (72*P_1)*(71*P_1)= 5.112*10^{-7}$.

Сөйтіп, 12.5% қымбаттығы артқанда сенімділік екі дәрежеге, яғни жүздеген есеге артады.

Мұндай есептеулер істен шығу ықтималдығы өте аз болғанда және кодер, декодерлердің бағасы жады модулінің бағасынан төмен болғанда ғана орынды болады. Сондықтан нақты жағдайда да осы есептеулерді қолданса болады.

6.3.5 Хэмминг кодтарының желіде қолданылуындағы нәтижелілігін арттыру әдістері

Компьютер желілерінде қолданылатын деректерді ұзату арналарының сенімділік немесе шындық дәрежесі үлгіқалып (стандарт) талабы бойынша әрбір екілік таңба үшін қателік ықтималдығы $10^{-6} \div 10^{-8}$ болуы керек [23].

Ал көпшілік нақты деректерді ұзату арналары, егерде оларда деректердің сенімділігін арттыру әдістерін қолданбаса, үлгіқалыптардың талабына жауап бермейді. Мұнда сенімділікті арттыру әдістері әртүрлі болады; олардың түрі деректерді ұзату желісінің типіне, қолданылатын арналардың түріне және жіберілетін ақпараттың түріне де байланысты болады.

Хэмминг кодтары ақпараттарды ұзату желілеріне арналған емес; алайда оны түрлендіріп ақпаратты ұзатудың радиожелісінде мәтінді хабарларды ұзатуда қолданса болады.

Жылжымалы нысандарды басқаруда кең қолданылатын декаметрлі, ультрақысқа толқынды ауқымдарда (ДКМ және УКВ) радиоарналардың сенімділік дәрежесі төмен болады (қателік ықтималдығы екілік таңбаға $\approx 10^{-2} \div 10^{-3}$); сондықтан оларды түйіншекті радиожелілерде қолдану нәтижелі емес. Алайда осын-

дай арналар жылдам істеуші автоматты әріпбасушы “Philips” фирмасының “Сокол -МР”, “СТР-114”, “STB-750” аспаптарында кең қолданылады.

Бұл аспаптар теңіздегі жылжымалы қызметтерде және соғыс-теңіз күштерінде кең қолданылады [80].

“Сокол -МР”, “СТР-114” аспаптарында ешқандай код артықшылығы жоқ болып, бұларда қателіктер сигналдардың сыртқы келбетіне қарай контролді серпіндер жәрдемінде анықталады.

Автордың ғылыми-зерттеу жұмыстары негізінен дискрет сигналдардың әрбір элементін жеке қабылдауда қабылдау сипатын бақылау нәтижесінде кедергіге орнықтылықты қамтамасыз ету әдістерін зерттеуге арналған [80]. Осы еңбекте код қисындастыруының 1 - элементінде шеткі бұзылу болмайтындығы көрсетілген; себебі код қисындастыруының басында сигналдар түзету етіледі.

Ал ионосфералық арналарда қателіктер негізінен сигналдардағы фединг үдерісі нәтижесінен болатын шеткі бұзылулардан болады. Ал сигналдардың майдалануынан (дробления) болатын қателіктер шеткі бұзылулардан болатын қателіктерге қарағанда өте кем болады. Мұнда жиынтықтағы қателіктерді түзету үшін қателік бар болған код қисындастыруын қайта жіберуді сұрау және оны қайта жіберумен амалға асырылады.

Ал арнайы деректерді жіберу жүйелерінде кері байланыс арналары мәлімбір себептермен істетілмейді; мысалы, автоматика жүйелерінде кері байланыс арналарының жоқтығынан немесе алыстағы абонентердің құпиялығынан. Мұндай жағдайларда қателіктерді анықтайтын және түзететін кодтарды қолдану мақсатқа сай келеді.

Автоматика және телемеханика жүйелерінде Хэмминг кодтары кең қолданылады; мысалы, Хэммингтің (7,4) коды. Бұл код небәрі 4 информациялық таңбаға ие. ISO-963 үлгіқалыбында 7 битті ISO 646 кестесінде 4 битті 16 код қисындастыруын немесе таңбаларын құрау ережелері берілген.

Осындай таңбалар көп терминалдық желілерде де кең қолданылады [81].

Алайда бұл кодты мәтіндерді ұзату жүйелерінде қолданып болмайды.

Хэммингтің коды өте тиімді кодтар қатарына жатып, келесідей керемет қасиеттерге ие;

- аспаптық орындалуының өте оңайлығы; тек қана кері байланысты жылжытушы регистрлерінен тұрады;

- тиімділеу мүмкіншілігі және тиімдіге жақын кодты табу мүмкіндігі;

- олар үшін өте қарапайым бағдаржолдар мен декодтау сұлбаларын құру мүмкіндігі және бұл сұлбаларды өте қарапайым құрылымдармен орындалу мүмкіндігі.

Осы абзалдықтардан тыс топты кодтар төмендегідей керемет қасиеттерге ие болады: тұйықтылығы, ассоциативтілігі, қайтарымдылығы және нөлдік сөздің барлығы.

Сол топты кодтардың ішінде (n,k) кодтар жиыны болады; егер оларда мына шарт орындалса: $\left(2^p - 1, 2^p - 1 - p\right)$, мұндағы $p=n-k$, онда ол кодтар **Хэмминг кодтары** (КХ) деп аталады.

Келесідей *КХ*-лар бар: (7,4),(15,11),(31,26),(63,57)….

КХ- лар келесідей керемет қасиеттерге ие:

1) Мына шарт орындалады: $2^{n-k} = 1 + n$;

2) Спектрі толық түрде анықталған және салмақты теңдеуі келесідей болады: $A(x) = \sum_{i=0}^{n} A_i x^i$, мұнда A_i - i салмақты код сөздерінің саны.

Осы жұмыста автор *КХ*- да келесідей өзгертулерді ұсынған;

1) *КХ* да код қашықтығы d = 3 деп алып, оны келесідей өзгертеміз: d = 4, яғни *КХ* (8,4):

2) Айталық, *КХ* (7,4) тексеруші матрица мына түрде берілсін

$$H = \begin{vmatrix} 1110 & 100 \\ 1101 & 010 \\ 1011 & 001 \\ 1111 & 111 \end{vmatrix}.$$

3) *КХ* ны d = 3 тен келесідей өзгертеміз: d = 4 болған *КХ* ға, яғни *КХ* (8,4):

Қатарлардың элементтерін *mod*2 бойынша қоса отырып, қосымша 8-элементтерді табамыз:

(*H*1 матрицаның 8- бағаны). $H1 = \begin{vmatrix} 1110 & 1000 \\ 1101 & 0100 \\ 1011 & 0010 \\ 1111 & 1111 \end{vmatrix}$

Кейін, ақырғы қатарды барлық қатарлар қосындысымен ауыстырамыз да, келесідей канондық түрге келеміз: *H*2:

$$H2 = \begin{vmatrix} 1110 & 1000 \\ 1101 & 0100 \\ 1011 & 0010 \\ 0111 & 0001 \end{vmatrix} .$$

Мұндай код барлық тақ қателіктерді анықтайды.

Код артықшылығы 100%.

Бұл кодтың қателіктерді анықтау және түзету қабілеті артқанымен ол мәтінттерді кодтауға жарамайды; себебі ақпараттық сөздері ең қысқа әліпби болған ағылшын әліпбиіне де жетпейді (ағылшын әліпбиінде 26 әріп бар).

2) Ағылшын және орыс әліпбиін кодтау үшін бес элементті стандарт МТК-2 қолдану да жеткілікті болады; ал егер 8-элементті МТК-5 немесе ASCII кодтарын істетсек, 128 таңбалы кодтай аламыз.

Бұлар қазіргі күнде ақпараттық технологияда толық қолданылады.

Бұларды қолданғанда $1 \div 5$ элементтерді ақпараттық деп, ал қалған 6 $\div 8$ элементтерін – тексеруші деп қолданса болады; ал *КХ*(7,4) те тексеруші элементтер 3 болғандықтан, ақпараттық элементтер саны 4 тен аспауы керек. Онда бір ақпараттық элемент кодталмай қалады; осы элемент ретінде автор код қисындастыруының (қисындастыруының) бірінші элементтін алуды ұсынған; мұның себебі онда шеткі бұзылу болмайды және ол элементтің қате болу ықтималдығы өте кем.

6.6 ***Зертханалық жұмыс*** Хэммингтің (7,4) кодын құру керек.

Шешімі:

Бағдаржол мына түрде болады; кодтауда мына екілік таңбалар істетіледі: $b_1, b_2, b_3, b_4, b_5, в_{6пр}, в_{7пр}, в_{8пр}$, мұнда b_1, b_2, b_3, b_4, b_5 - ақпараттық таңбалар, ал - тексеруші таңбалар. Ақырғылар былай та-

былады: $в_{6пр} = b_2 \oplus b_4 \oplus b_5$; $в_{7пр} = b_3 \oplus b_4 \oplus b_5$; $в_{8пр} = b_2 \oplus b_3 \oplus b_4$.
Қабылдаушы жақта осы элементтер штрихтармен таңбаланған:

$$b_1', b_2', b_3', b_4', b_5', в'_{6пр}, в'_{7пр}, в'_{8пр}.$$

Шығуда тексеруші элементтер жоғарыдағы бағдаржолдың өзімен табылады: $в'^{к}{}_{6пр} = b_2' \oplus b_4' \oplus b_5'$; $в'^{к}{}_{7пр} = b_3' \oplus b_4' \oplus b_5'$; $в'^{к}{}_{8пр} = b_2' \oplus b_3' \oplus b_4'$.

Қателіктер синдромы келесідей табылады:

$$C_2 = в_{7пр} \oplus в^{к}_{7пр} \quad ; \quad C_3 = в_{8пр} \oplus в^{к}_{8пр} .$$

Кейін, төмендегі 1-кестеден синдромның мәні мен қателіктердің орындарының нөмірі табылады. Кестенің 3-бағанында түзетілетін қателіктердің жайғасымдарының нөмірлері көрсетілген. Мұнда, бірінші орындағы қателіктер түзетілмейді, алайда олар анықталады.

Қателіктерді түзету бағдаржолдары төмендегідей; b_2' орнындағы $\hat{I}_2$ қателігі келесідей түзетіледі: $O_2 = b_2' \oplus (C_1 \cap C_3)$; басқа орындағы қателіктер де сол бағдаржолмен түзетіледі;

$O_3 = b_3' \oplus (C_2 \cap C_3)$; $O_4 = b_4' \oplus (C_1 \cap C_2 \cap C_3)$;

$O_5 = b_5' \oplus (C_1 \cap C_2)$.

Тексеруші орындағы қателіктер де сол сияқты түзетіледі;

$$O_6 = b_{6пр}' \oplus (\overline{C_2} \cap \overline{C_3}); \quad O_7 = b_{7пр}' \oplus (\overline{C_1} \cap \overline{C_3}); \quad O_8 = b_{8пр}' \oplus (\overline{C_1} \cap \overline{C_2}).$$

Ойлаужүйесі (логикалық) сұлбаларда келесідей амалдар қолданылады: $\cup$ - дизьюнкция, $\cap$ - коньюнкция, - керілеу және модул екі бойынша қосу - $\oplus$.

Кесте №1.

Кодтың дәрежелер нөмірлері	Синдромдар C_3 C_2 C_1	Қателік векторлары $O_i, i = 2 \div 8$
1	0 0 0	(1-дәрежеге сәйкес)
2	0 0 1	6 – дәреже
3	0 1 0	7- дәреже
4	0 1 1	5- дәреже
5	1 0 0	8 –дәреже
6	1 0 1	2 – дәреже
7	1 1 0	3- дәреже
8	1 1 1	4- дәреже

Қорытындылар:

Осы замандық сандық деректерді ұзату жүйелерінде қателіктерді түзетудің көптеген бағдаржолдары мен әдістері қолданылады.

Оларда тиімділікті максимал дәрежеде арттыру үшін бірнеше әдістер параллель түрде қолданылады.

а). Түйіншекті радиожелілерде, жергілікті желілерде *LLC*2, *LLC*3 протоколдары және ғаламдық желілерде *TCP/IP* протоколы қолданылып, циклдік полиномиалдық кодтар істетіледі; олар бұзылған түйіншектерді анықтайды; ал қателік бар болған жиынтық қайта жіберіледі, яғни қате жиынтықты түзету үшін оларды қайта жіберіледі.

Егерде түйіншектердің ұзындығын тиімді таңдап алсақ, деректерді ұзатуда ақпараттың максимал жылдамдығын қамтамасыз ету мүмкін болады.

б). Кері байланыс болмаған жағдайда түзетуші (түзетуші) кодтар істетіледі. Олардың ішінде ең "жетілгені" Хэмминг кодтары: *KX* (7,4), *KX*(15,11) және басқалар.

Алайда олар мәтін хабарларға арналған емес; *KX* (7,4) код таңбалары әліпбидің барлық әріптеріне жетпейді; ал *KX* (15,11) коды МТК-5 және ASCII үлгіқалыптарын қолданғанда өте үлкен артықшылыққа ие (~114%) болады.

Осы кодты оңтайландырып, өзгерткенде келесідей мүмкіндіктерге жетсе болады: *KX* (8,4) коды құрылғанда (мұнда $d = 3$ тен *KX* $d = 4$ ке өткенде) артықшылық 75% тен 100% ке артады.

Алайда бұл кодты да мәтінтерді кодтауға қолданып болмайды.

Автор ұсынған ***KX* (8,5) кодын МТК-2 үлгіқалыбын** қолданумен мәтінді хабарды жіберуге толық мүмкін болады; мұнда артықшылық ~60%.

6.3.6 Хэмминг кодтарын үлгілеудің қолданбалы бағдаржолдары

Хэмминг кодтарын MS Excel-де үлгілеу бағдаржолы жаратылған [автор].

Теңіздегі жылжымалы қызметтерде (ТЖҚ) және соғыс-теңіздік құрал күштерінде (ТҚК) «Philips» фирмасының «Сокол-МР», «СТР-114», «STB-750» [80] автоматты әріпбасу аспапсы кең қолданылады; мұнда аспап МТК-2 үлгіқалып негізінде істейді және артықшылықты кодтар істетілмейді.

Мұнда қателікті анықтау сигнал тегістеушісінің (огибающая) түрін бақылау арқылы жүргізіледі; ол ***жанама әдіс*** деп аталады. Жанама әдістерді зерттеуге автордың мына жұмысы арналған болып [80], онда нақты байланыс арналарынан өлшеп алынған сигналдардың бұзылған түрін аппроксимациялап, екілік сигналдардың бұзылу заңдылықтары табылған; олардың өңдеу арқылы тіркеуші (регистрирующий) контқызмет серпінтердің тиімді бейнесі (келбеті) мен параметрлері анықталған. Жанама әдістер аталған жүйелерде кең қолданылады.

Осы аспап ДКМ және УКВ ауқымдардағы радиоарналарға арналған болып, олардың шындық дәрежесі өте төмен (бір таңбаға қателік дәрежесі $10^{-2} \div 10^{-4}$) болады. Өткізу жылдамдығы төмен болғандығы себепті мұндай арналарды түйіншекті коммуникациялы желілерде қолданып болмайды.

Автоматика жүйелерінде және арнайы хабар жіберу желілерінде кейбір себепті кері байланыс арнасы істетілмейді; кері арнаны қолданып болмайтындығына себептің бірі қашықтағы абоненттің құпиялығы болуы да мүмкін [80]. Мұндай жағдайда қателікті анықтайтын және түзететін кодтар қолданылады.

Автоматика жүйелерінде *КХ*(7,4) Хэмминг коды істетіледі. Бұл кодтың $k = 4$ информациялық таңба және $p = 3$ түзетуші таңбасы бар.

Ақпараттық таңбаларды құрау үшін ISO-963 [23] үлгіқалыбының ережелері қолданылады; Хэмминг коды группалық кодтар қатарына жатып, олардың келесідей керемет қасиеттері бар: **тұйықтық, ассоциативтік, қайтарылымдық** және **нөл сөзінің барлығы**;

мұнда, Хемминг коды (*n, k*) кодттар тобын құрады: (2^p-1, 2^p-1-*p*), мұнда *p=n-k; n* – кодтың жалпы дәрежелер саны.

Сондықтан Хэммингтің келесідей кодтары бар: *КХ*(7,4), (15,11), (31,26), (63,57),…

Автордың жұмысында Хэммингтің (7,4) кодын *КХ*(8,5) кодына айналдыру әдісі көрсетілген болып, мұнда үлгіқалыпты ASCII и МТК-5 кодтарымен түйіншекті хабарларды жіберуге болады.

КХ(7,4*)* коды бірлік қателерді анықтап, түзете алады.

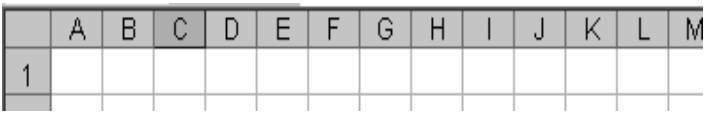
Кітаптың осы бөлімінде *КХ*(7,4) кодын MS Excel-де үлгілеу бағдаржолы құрылған. Бұл бағдаржолда қателіктер тек информациялық дәрежелерде деп есептелген. Жоғарыда зертханалық 6.6-жұмыста және кітаптың соңындағы 6-қосымшада берілген бағдаржолда қателіктер барлық дәрежелерге әсер етеді.

6.7 ***Зертханалық жұмыс***

Осы үлгілеу бағдаржолы бірнеше этаптан тұрады:

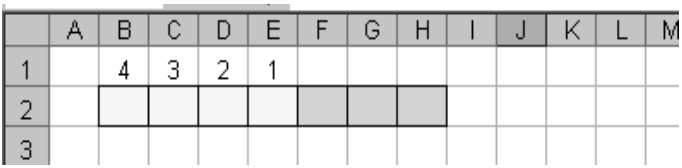
1. Жаңа документті құру: Пуск-Программы-MS Excel.

0 және 1 сандарын қолайлы орналастыру үшін барлық "ұяшықтар" біртүрлі етіп алынады (6.1-сурет).



6.1-сурет

2. Үлгілеу «скелетін» жарату. Мұның үшін 7 ұяшық (ячейка) керек: ақпарат үшін 4 дәреже, 3 – дәреже тексеру үшін. Қолайлы болу үшін ақпараттық және тексеруші дәрежелер әртүрлі түстерге боялады; мысалы, сары және жасыл түске (Сурет 6.2).



6.2-сурет

3. Кейін, әрбір дәреже кіші орыннан бастап нөмірленеді; мысалда, 1,2,3,4.

Егер осы орында 1 саны болса, онда осы таңбалық нөмірі екілік санақта үш дәрежеге жазылады; себебі артықша дәрежелер саны үшке тең. Ал орында 0 болса, онда дәрежелер үш нөлмен толтырылады.

4. Кейін, осы шыққан кодтардың әрбір дәрежесін бөлек түрде 2 модулінде қосу амалы орындалады; $1 \oplus 1 = 0; 1 \oplus 0 = 1; 1 \oplus 1 \oplus 1 = 1 \ldots$, мұнда бірлер саны жұп болса, нәтиже 0, ал тақ болса - 1 болады. Айталық, мысал үшін, ақпараттық таңбалар код қисындастыруы - 1|1|0|1| болып, жалпы таңбалар саны $n = 4 бит$ болсын; онда осыған сай келетін артықша таңбалар саны k - мына теңдеумен анықталады: $k > \log_2 n$; қаралған мысалда, $n = 4 бит$, $k = 3 бит$.

	A	B	C	D	E	F	G	H
1		4	3	2	1			
2		1	1	0	1			
3								
4		1	0	0	1			
5		2	0	0	0			
6		3	0	1	1			
7		4	1	0	0			

6.3-сурет

5. F,G,H дәрежелеріндегі тексеруші кодтарды есептеу үшін B2,C2,D2,E2 дәрежелеріндегі ақпараттық код нөмірленеді және 6.3-суретте көрсетілгендей B1,C1,D1,E1 дәрежелерге жазылады; кейін, ақпараттық дәрежелерде 1 болса, кодтың сол жайғасымының нөмірі екілік санақта 3 орында жазылады; мысалы, бірінші орында 1 бар; сондықтан оның нөмірі 1 болғандықтан - 0 0 1 жазылады; 3 орында бір бар, оның нөмірі 3 болғандықтан – 0 1 1 жазылады, т.с.с. Бұлар $C4 \div E4$ ұяшықтарына жазылады.

Сонан соң, әр дәреже 2 модулінде қосылады.

Осы амалдар MS Excelдің *fx* теңдеуі жәрдемінде келесідей кезекте орындалады: СУММ(), ОСТАТ(), ЕСЛИ().

6.4-суретте көрсетілгендей мына теңдеуде =ОСТАТ(СУММ(E4:E7)2) орындалады. Осы амалдарды әр орында орындаған соң (C8,D8,E8) ұяшықтарда 1|1|0 кодын аламыз.

6. Кейін, алынған қосынды кодтың әрбір дәрежесін инверсиялаймыз: $110 \rightarrow 001$ (C9,D9,E9);

осы операция мына қатыспен орындалады ЕСЛИ: =ЕСЛИ(E8=1;0;1). Алынған 001 коды 2 модулінде (F2,G2,H2) дәрежелеріндегі артықша кодтармен әрбір дәрежесі жеке қосылады. Артықша дәрежелер бос болғандықтан, қосынды нәтижесі 0 0 1 болады. Сонда шыққан код қисындастыруы **1101 001** құрылған Хэммингтің КХ(7,4) коды болады.

Сөйтіп, құрылған кодтың жалпы түрі келесідей болады: 1|1|0|1|0|0|1|.

	A	B	C	D	E	F	G	H	I	J
1		4	3	2	1					
2		1	1	0	1	0	0	=E9		
3										
4		1	0	0	1					
5		2	0	0	0					
6		3	0	1	1					
7		4	1	0	0					
8			1	1	=ОСТАТ(СУММ(E4:E7);2)					
9			0	0	=ЕСЛИ(E8=1;0;1)					

6.4.-сурет

Құрылған код қисындастыруы арнамен жіберілгенде кедергілердің әсерінен қателіктер пайда болады; мысалы, 3 орында қателік пайда болсын делік: 1|**0**|0|1|0|0|1|;

Декодтау операциясы кодтау амалдарына ұқсас болады; декодтау бағдаржолын құру үшін B,C,D,E,F,G,H бағандарындағыларды J,K,L,M,N,O,P бағандарына көшіреміз.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1		4	3	2	1					4	3	2	1			
2		1	1	0	1	0	0	1	ERROR	1	**0**	0	1	0	1	0
3																
4		1	0	0	1					1	0	0	1			
5		2	0	0	0					2	0	0	0			
6		3	0	1	1					3	0	0	0			
7		4	1	0	0					4	1	0	0			
8			1	1	0						1	0	1			
9			0	0	1						0	1	0			
10																

6.5-сурет

Кейін, кодтау үдерісіндегідей (K4÷M7) орындарын екілікте нөмірлеп шығамыз; алынған екілік сандардың әрбір дәрежесін екілік модулде баған бойынша тік түрде қосамыз, нәтижелер (K8,L8,M8)де; оларды әр дәрежесін екілікте инверсиялаймыз; нәтиже (K9,L9,M9). Алынған 010 кодты 2 модулінде артықша орындағылармен, яғни 001 мен қосамыз; осы операция мына теңдеумен орындалады: =ОСТАТ(СУММ(F11:F12); Бұл 6.6-суретте көрсетілген. Мұнда E9

және M9, D9 және L9, C9 және K9 ұяшықтарындағылар қосылады.

Нәтижеде 011 коды шығады. Осы код қателіктің жайғасымын көрсетеді, демек 3 позицияда қате бар. Осы үш орынды екілік кодпен қателіктің дәрежесін табатын дешифраторды келесідей құрса болады: ажаратылған төрт ұяшықтардың әрқайсысына бөлек түрде мына теңдеу жазылады: =ЕСЛИ($D$13*100+$E$13*10+$F$13=**100**;***4***;0).

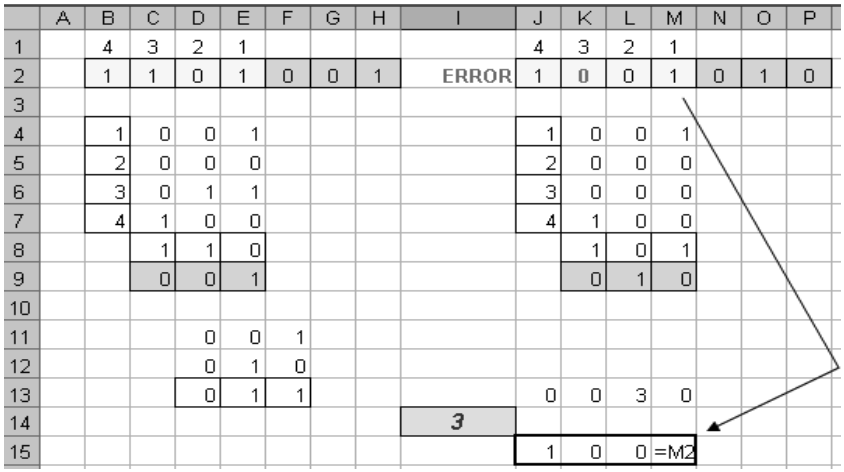
Осы мысалда қалың әріптермен ажыратылған 100 коды екілікте қателіктің жайғасымын көрсетеді; сонда 4 ұяшықтарға таралған сандар келесідей: |0|0|3|0|.

Осы сандарды қоса отырып, қателіктің дәрежесін тапса болады, яғни 3 ті. Қаралып отырған мысалда осы операция мына теңдеумен орындалады: I14: =СУММ(J13:M13).

Қателік табылғаннан соң оны түзету де сол 3-дәрежеге екілік түрдегі 1-ді екілік модулде қосумен орындалады; оны келесідей орындаса болады; қателік бар ұяшықтар 6.7-суретте көрсетілгендей бөлектеп көрсетіледі.

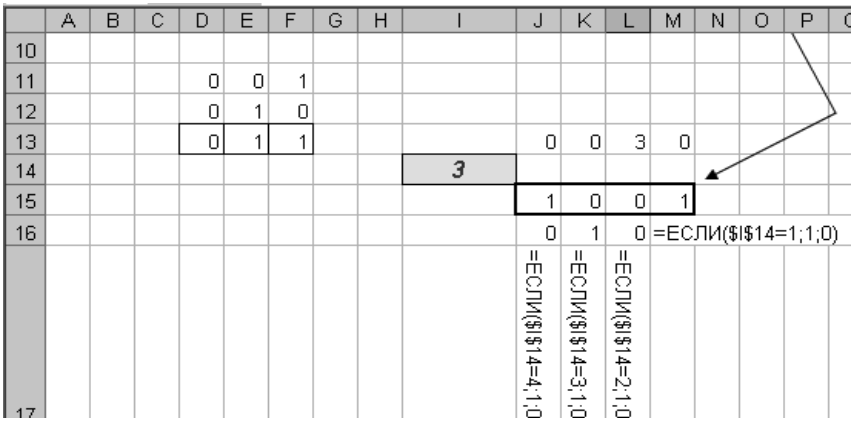
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1		4	3	2	1					4	3	2	1			
2		1	1	0	1	0	0	1	ERROR	1	0	0	1	0	1	0
3																
4		1	0	0	1					1	0	0	1			
5		2	0	0	0					2	0	0	0			
6		3	0	1	1					3	0	0	0			
7		4	1	0	0					4	1	0	0			
8			1	1	0						1	0	1			
9			0	0	1						0	1	0			
10																
11				0	0	=E9										
12				0	1	=M9										
13				0	1	=ОСТАТ(СУММ(F11:F12);2)										

6.6-сурет



6.7-сурет

Кейін, қателік нөмірі орналасқан I14 ұяшығы (көк түсте көрсетілген ұяшық) жәрдемінде қателіктің жайғасымын анықтаймыз, яғни 3-жайғасымды; мұның үшін M16-ға мына теңдеу жазылады: =ЕСЛИ($I$14=**1**;1;0), мұнда $ - абсолютті адрестеуді көрсетіп, ондағы сандар өзгермейді.



6.8-сурет

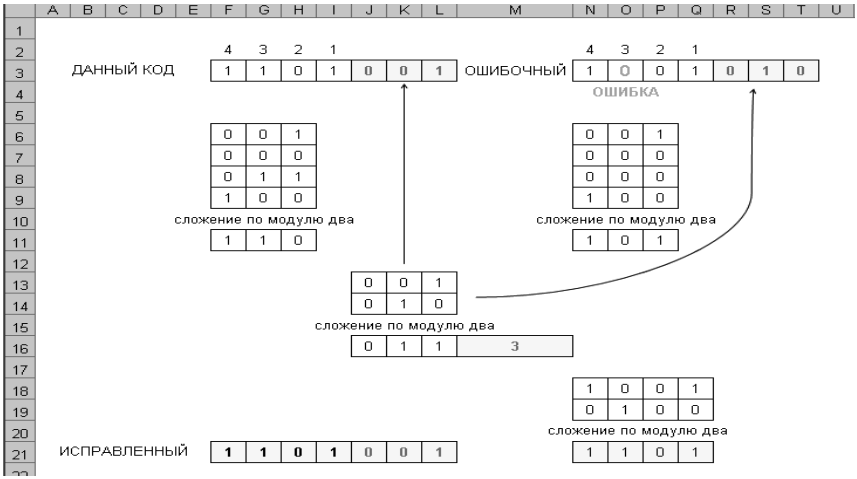
Ақырғыларды 2 модулімен қоса отырып, түзетілген кодты аламыз, яғни декодтау операциясы бітеді.

Бағдаржолдың ақырында келесідей қосымша амалдар орындалады: Сервис – Параметры – Вид.

Біткен түрде үлгілеу амалдары 6.8-суретте көрсетілгендей болады.

Хэмминг КХ(7,4) кодын үлгілеу бағдаржолының жалпы көрінісі 6.9-суретте көрсетілген.

Қарастырылған үлгіде қателіктер тек информациялық дәрежелерде болады; алайда нақты жағдайда қателіктер қосымша дәрежелерге де түсуі мүмкін. Мұндай код құру әдісі кітап соңындағы 6-қосымшада берілген.



6.9-сурет

Хэмминг КХ(7,4) кодын үлгілеу бағдаржолының жалпы көрінісі.

6.4 Топтық кодтарды мажоритарлық декодтау

Қателік дәрежесі жоғары болғанда оларды түзету үшін сызықты кодтарды қолдану тиімді болмайды; осындай болғанда ***мажоритар қағидада*** құрылған декодтау құрылымдары анағұрлым қарапайым болады. Бұл декодтау әдісін ***дауыс беру әдісі*** немесе ***тексерудің көптігі бойынша декодтау әдісі*** деп атайды.

Осы кезде мажоритарлық сұлбада декодтаушы көптеген кодтар бар, осындай кодтарды құрудың жаңа жолдары да жаратылған.

Мажоритарлық декодтау да тексеруші теңдеулер жүйесіне

негізделген болады. Мұнда жүйені әрбір тәуелсіз айнымалыға арнап бөлек түрде шешіледі және бұл жалғыз рет шешілмейді; себебі артықшылық жеткілікті болады.

Кез келген a_i таңбасы d (минимал код қашықтығы) мен әртүрлі тәуелсіз әдістермен басқа таңбалардың сызықтық қисындастыруыларымен көрсетіледі. Мұнда келесідей қарапайым (тривиал) тексеру $a_i = a_i$ қолданылады.

Есептеу нәтижелері осы таңбаға сәйкес мажоритар элементке беріледі.

Осы сұлба d кіруі және бір ғана шығуы бар болып, онда кірудің жартысынан көбіне сигнал түскенде шығуда ***бір*** болады, ал керісінше, кірудің жартысынан кеміне сигнал түскенде шығуда ***нөл*** болады.

Егер қателік болмаса, онда тексеруші теңдеулер бұзылмайды және шығуда сигналдың шын мәні шығады.

Егер тексерулер саны d^{2s+1} және қателіктер s ретті немесе одан кем болса, онда ол қателіктер s тексеруден көбін бұзбайды.

Сондықтан, бұзылмаған тексерулер көбірек болғандығы үшін олар арқылы дұрыс шешім қабылдануы мүмкін болады.

Осы шарт орындалуы үшін кез келген a_j (j тең емес i-ге) таңбасы тексеруші теңдеулердің біреуінен артығында қатыспауы керек.

Мұнда біз тексерулерді ажырата аламыз және тексерулерді ажырату жүйесін құра аламыз.

6.8 ***Зертханалық жұмыс*** (8,2) топтық кодының ақпараттық таңбаларын декодтау үшін ажыратылған тексеру жүйесін құрамыз.

Шешімі:

Код кез келген бірлік және екілік қателіктерді түзету үшін арналғандығы себепті әрбір таңбалы анықтау үшін тексеруші теңдеулер саны 5-тен кем болмауы керек. (6.16 а) және (6.16 б) теңдеулеріне a_8 мәндерін қойып, және (6.16д) және (6.16е) лерден алынған нәтижелерді a_5 қойып, (6.16 в) және (6.16г) және тривиал теңдеу болған $a_5 = a_5$ пен мына a_5 таңбасы үшін ажыралған теңдеулер жүйесін аламыз:

$$a_5 = a_6 \oplus a_1,$$
$$a_5 = a_\tau \oplus a_2,$$
$$a_5 = a_3,$$
$$a_5 = a_4,$$
$$a_5 = a_5.$$

Дәл осындай a_8 таңбасы үшін де ажыралған тексеру жүйесін құрамыз:

$$a_8 = a_3 \oplus a_1,$$
$$a_8 = a_4 \oplus a_2,$$
$$a_8 = a_6,$$
$$a_8 = a_7,$$
$$a_8 = a_8.$$

6.5 Сызықты кодтардың матрицалық көсетілуі

lxn өлшемді матрица деп *l* қатарда *n* бағаны (элементі) бар тік бұрышты кестені айтамыз:

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots\ldots & a_{1n} \\ a_{21} & a_{22} & \ldots\ldots & a_{2n} \\ \ldots\ldots & & \ldots\ldots & \\ \ldots\ldots & & \ldots\ldots & \\ a_{l1} & a_{l2} & \ldots\ldots & a_{ln} \end{bmatrix}$$

Матрицаны транспондау операциясында *A* матрицаның қатарлары екінші матрицаның бағандарымен, ал екіншінің бағандары біріншінің қатарларымен алмастырылады. Нәтижеде транспондалған келесідей матрица шығады:

$$A^T = \begin{bmatrix} a_{11}\ a_{21} \ldots\ldots\ a_{l1} \\ a_{12}\ a_{22} \ldots\ldots\ a_{l2} \\ \ldots\ldots\ldots\ \ldots\ldots\ldots \\ a_{1n}\ a_{2n} \ldots\ldots\ a_{\ln} \end{bmatrix}$$

Бірлік матрицаның бір диогоналы 1 ге, ал басқа элементтері нөлге тең болады.

Екі матрицаның $A = |a_{ij}|$ және $B = |b_{ij}|$ қосындысы ның өлшемдері өзгермейді *lxn:*

$$A + B \equiv \left|a_{ij}\right| + \left|b_{ij}\right| \equiv \left|a_{ij} + b_{ij}\right|.$$

Матрицаны $A = |a_{ij}|$ скаляр *c* санға көбейткенде де оның өлшемі өзгермейді:

$$cA \equiv c\left|a_{ij}\right| = \left|ca_{ij}\right|.$$

$A == |a_{ij}|$ өлшемі *lxn* және $B = |b_{ij}|$ өлшемі *nxm* болған матрицаларды көбейткенде пайда болған C_{ik} матрицасының өлшемдері *lxn* болып, онда

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk} \quad .$$

A матрицаның 1-қатарының элементтері *B* матрицаның *k* - бағанының элементтеріне көбейтіледі: .

Кодтау теориясында матрица элементтері ретінде *GF*(*P*) өрісінің элементтері көрінеді; ал матрицаның қатары мен бағандары векторлар деп қаралады. Матрицаларды қосу және көбейту *GF*(*P*) өрісінің ережелерімен орындалады.

6.9 ***Зертханалық жұмыс*** *GF*(*2*) өрісінің элементтерінен құралған матрицаның көбейтіндісін есептейміз:

$$M_1 = \begin{bmatrix} 011 \\ 100 \\ 001 \end{bmatrix},\ M_2 = \begin{bmatrix} 111 \\ 010 \\ 100 \end{bmatrix}.$$

Осында көбейтінді *Cik* матрицасы *M=M1M2*

$$c_{11} = (011)(101) = 0 + 0 + 1 = 1$$
$$c_{12} = (011)(110) = 0 + 1 + 0 = 1$$
$$c_{13} = (011)(100) = 0 + 0 + 0 = 1$$
$$c_{21} = (100)(101) = 1 + 0 + 0 = 1$$
$$c_{22} = (100)(110) = 1 + 0 + 0 = 1$$
$$c_{23} = (100)(100) = 1 + 0 + 0 = 1$$
$$c_{31} = (001)(101) = 0 + 0 + 1 = 1$$
$$c_{32} = (001)(110) = 0 + 0 + 0 = 0$$
$$c_{33} = (001)(100) = 0 + 0 + 0 = 0$$

Сөйтіп, болады. $M = \begin{bmatrix} 110 \\ 111 \\ 100 \end{bmatrix}$ болады.

Кодты құру заңдылығын біле тұрып, рұқсат етілген код қисындастыруыларының барлық жиынын анықтаймыз.

Оларды бірінің үстіне бірін қойып, матрицаны табамыз.

Матрицаның қатарлар жиыны *GF*(*P*) өрісінің элементтерінің *η*-орынды код қисындастыруыларының (векторларының) кіші кеңістігі болады.

Екілік (*n,k*)-кодында матрицаның *n* бағаны және 2*к*-1 қатары болады (нөлдік қатарды есептемегенде).

Мысалы, алдын қарастырған бірлік және екілік қателіктерді түзететін (8,2) кодында матрица мына түрінде болады:

$$\begin{bmatrix} a_5a_8a_1a_2a_3a_4a_6a_7 \\ 0.\ 1.1.1.0.0.\ 1.1 \\ 1.\ 0.1.1.1.1.\ 0.0 \\ 1.\ 1.0.0.1.1.\ 1.1 \end{bmatrix}$$

n және *k* үлкен болғанда кодтың барлық векторларын өз ішіне алатын матрица өте үлкен болады.

Алайда рұқсат етілген код қисындастыруыларының сызықтық кеңістігі де сызықты байланысты болады; себебі векторлардың бір бөлігі кеңстік базисі деп аталып, шектелген векторлар жиынының сызықты қисындастыруы түрінде көрсетіледі.

V_1, V_2, V_3, ..., V_n - векторлар жиыны сызықты байланысты деп аталады, егерде келесідей скалярлар $c_1 ... c_n$ (барлығы нөлге тең емес) жиыны бар болып, олар үшін мына теңдік орынды болса:

$$c_1 V_1 + c_2 V_2 + ... + c_n V_n = 0.$$

Осы келтірілген матрицада үшінші қатар бірінші және екінші қатарлардың екілік модул бойынша қосындысына тең болады.

Сызықты кодтың рұқсат етілген код қисындастыруыларының кеңістігін толық анықтау үшін сызықты байланысты болмаған векторлар жиынын матрица түрінде жазу жеткілікті болады.

Олардың санын векторлық кеңістіктің өлшемі деп атайды. $2k$ — 1 нөлге тең болмаған екілік код қисындастыруыларының ішінде тек k сы ғана векторлар болады.

Мысалы, (8,2) коды үшін $M_{8,2} = \begin{bmatrix} a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 \\ .1.1.\ 0.\ 0.0.\ 1.\ 1.\ 1 \\ .1.1.\ 1.\ 1.1.\ 0.\ 0.\ 0 \end{bmatrix}$.

Кеңістік базисін құрайтын және сызықты кодтың кез келген векторлар жиынынан тұратын матрицаны **кодты туындайтын** немесе **бейнелейтін немесе құраушы матрицасы** деп атайды.

Егер матрицаның k қатары болып, әр қатарда $GF(q)$ өрісінің n элементі болса, онда кодты (n, k) - код деп атайды.

Осы (n, k) - кодтың әрбір қисындастыруында k ақпараттық таңба және n-k – тексеруші таңбалар болады.

Рұқсат етілген код қисындастыруылар саны (нөлдікті есептемегенде)

$Q = qk$-1 болады.

Егерде кодтың құраушы (бейнелеуші) матрицасы берілген болса, онда $к$ ақпараттық таңбалардан тұратын кез келген A_{ki} тізбегіне сәйкес келетін рұқсат етілген код қисындастыруын оңай тапса болады:

$$A_{n,i} = A_{ki} \cdot M_{n,k} .$$

Мысал үшін, a_5=1, a_8=1 ақпараттық таңбаларына сәйкес келетін (8,2) кодының рұқсат етілген қисындастыруыларын келесідей тапса болады:

$$|11|M_{8,2} = [11]\begin{bmatrix}11000111\\11111000\end{bmatrix} = 00111111$$

Матрицаның қатарлар кеңістігі келесі амалдарды орындағанда өзгермей қала береді: 1) кез келген екі қатардың орын алмасуы;

2) кез келген қатарды өрістің нөл емес элементіне көбейтіндісі;

3) бір қатардың өрістің нөл емес элементіне көбейтіндісінің қандайдір бір қатармен қосындысы; сондай ақ бағандардың орын ауысуы.

Эквивалентті кодтардың қасиеттері өте жақын болады.

Осындай кодттардың түзетуші қасиеттері бірдей болады.

Сызықтық (*n, k*)-кодтың мүмкіншіліктерін талдау үшін және кодтау үдерісін оңайлату үшін бейнелеуші матрица ($M_{n,k}$) екі матрицадан құрылған болуы керек: *k*k* өлшемді бірлік матрицасынан және оң жаққа қосылып жазылатын *k**(*n-k*) - өлшемді қосымша матрица (тексеруші кіші матрица) дан болып, ол *n — k* тексеруші дәрежелерге сәйкес келеді:

$$M_{n,k} = [1_k\ P_{k,n-k}] = \begin{bmatrix} 10\ldots0\ p_{1,k+1}\ p_{1,k+2\ldots}\ p_{1,j\ldots}\ p_{1,n} \\ 01\ldots0\ p_{2,k+1}\ p_{2,k+2\ldots}\ p_{2,j\ldots}\ p_{2n} \\ \ldots\ldots\ \ldots\ldots\ \ldots\ldots\ \ldots\ldots\ .. \\ 0\ldots1\ldots0\ p_{i,k+t}\ p_{i,k+2\ldots}\ p_{i,j\ldots}\ p_{in} \\ \ldots\ldots\ \ldots\ldots\ \ldots\ldots\ \ldots\ldots\ .... \\ 00\ldots1\ p_{k,k+1}\ p_{k,k+2\ldots}\ p_{k,j\ldots}\ p_{k,n} \end{bmatrix}, \quad (6.17)$$

Осындай бейнелеуші матрицалы кодтың рұқсат етілген код қисындастыруының келесідей екекшеліктері бар:

- Бірінші *k* таңбалары берілген ақпараттық таңбалармен сәйкес келеді; ал ақырға (*n — k*) таңбалары тексеруші болады.
- Ақиқаттан да, егер $A_{ki} = (a_1\ a_2 \ldots a_i \ldots a_n)$ вектор-қатарды матрица $M_{n,k} = [1_k\ P_{k,n-k}]$ ге көбейтсек, мына векторды аламыз: $A_{ni} = (a_1 a_2 \ldots a_1 . a_k \ldots a_k + 1 \ldots a_j a_n)$;

мұнда $a_j\ (k + 1_k \le j \le n)$ тексеруші таңбалары мына ақпараттық $a_j = \sum_{i=1} a_i\ p_{ij}$ (6.18)

таңбалардың сызықтық қисындастыруылары болады.

Осы шарттарға жауап беретін кодтарды жүйелікті (**жүйелілік)** деп атайды.

Әрбір сызықтық кодқа өзіне сәйкес эквивалентті жүйелілік код сәйкес келеді. Осындай кодты құру туралы ақпарат матрица-қосымшада болады.

Егер код құру ережелері (кодтау теңдеулері) мәлім болса, онда матрица-қосымшаның кез келген қатарының таңбаларының мәндерін алу үшін бірлік матрицаның сәйкес қатарының таңбаларына сол ережелерді қолдану керек болады.

VI тараудың бақылау және емтихан сұрақтары.

1. Осы замандық сандық деректерді ұзату жүйелерінде қателіктерді түзетудің қандай әдістерін білесіз?
2. Оларда тиімділікті максимал дәрежеде арттыру үшін не істеу керек?
3. Түйіншекті радиожелілерде, жергілікті желілерде және ғаламдық желілерде қандай протоколдар қолданылады?
4. Деректерді ұзатуда ақпараттың максимал жылдамдығын қалай қамтамасыз етсе болады?
5. Түзетуші (түзетуші) кодтар қай жағдайларда істетіледі?
6. Хэмминг кодтары мәтінді хабарларды кодтауға арналған ба?

Қандай кемшілігі бар?

7. Хэмминг кодтары мәтінді хабарларды кодтауға арнап қалай өзгертсе болады?
8. Хэмминг кодының абзалдықтары қандай?
9. Хэмминг коды қандай қателіктерді түзете алады және қандай қателіктерді анықтай алады?
10. 64 дәрежелі кодтау үшін Хэмминг кодында неше қосымша дәреже керек болады?
11. Хэмминг кодын қай жағдайларда қолданған тиімді?

Өзіндік жұмыстар (СӨЖ) тақырыптары.

1. Бөгеуілді байланыс арна үшін Шеннонның кодтау туралы негізгі теоремасы.
2. Бөгеуілді кодтау; жиынтықты кодтау.

3. Түзетуші кодтардың жалпы қағидалары; сапа көрсеткіштері.
4.Сызықты кодтар; топтық екілік код құру.
5. Сызықты кодтраға математикалық кіріспе.
6. Топтық екілік код құру.
7. Синдром кестесін құрастыру.
8. Қателіктерді анықтаушы және түзетуші кодтарды үлгілеу.
9. Хэмминг кодтары және олардың желіде қолданылуы.
10. Хэмминг кодтарын үлгілеудің қолданбалы бағдаржолдары
11. Топтық кодтарды мажоритарлық декодтау.
12. Сызықты кодтардың матрицалық көрсетілуі.

.

VII ТАРАУ
ТҮЗЕТУШІ ТОПТЫҚ КОДТАР; ЦИКЛДІК КОДТАР

7.1.1 Хэмминг кодтары

Келесідей матрицаларды I_k, $P_{k,n-k}$ және $M_{n,k}$ (7,4) екілік кодына жазамыз. Төрт дәрежеге бірлік матрица былай жазылады:

$$I_4 = \begin{bmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}.$$

Қосымша матрицаның нұсқаларының бірін былай жазса болады:

$$P_{4,3} = \begin{bmatrix} 110 \\ 101 \\ 011 \\ 111 \end{bmatrix}.$$

Онда Хэммингтің екілік коды үшін матрица келесідей болады:

$$M_{7,4} = \begin{bmatrix} a_3a_5a_6a_7a_1a_2a_4 \\ 1.0.0.0.1.1.0 \\ 0.1.0.0.1.0.1 \\ 0.0.1.0.0.1.1. \\ 0.0.0.1.1.1.1. \end{bmatrix}.$$

Сондай-ақ жүйелілік код (7,4) үшін матрица келесідей болады:

$$M_{7,4} = \begin{bmatrix} a_1a_2a_3a_4a_5a_6a_7 \\ 1.0.0.0.1.1.0 \\ 0.1.0.0.1.0.1 \\ 0.0.1.0.0.1.1. \\ 0.0.0.1.1.1.1. \end{bmatrix}.$$

Өз алдында, берілген қосымша-матрица $P_{k,n-k}$ арқылы код құру ережелерін беретін теңдеулерді анықтаса болады.

Әр бағанның бірінші қатарындағы бірлік осы бағанды құрушы тексеруші орында бірінші ақпараттық дәреже қатысқандығын білдіреді.

Кез келген бағандағы кейінгі қатардағы бірлік осы бағанды құрушы тексеруші дәрежеде екінші ақпараттық дәреже қатысқандығын білдіреді және с.с.

Қосымша матрицада код құру ережелері туралы ақпараттың барлығы болғандығынан тиісті қасиеттерге ие болған жүйелілік (систематикалық) кодты синтездеу үшін соған сәйкес қосымша матрицаны құру керек болады.

Сызықты кодтың минимал код қашықтығы d оның нөл емес векторларының минимал ауырлығына тең болады; онда қосымша матрицаға келесідей шарттарды қанағаттандыратын k қатары қосылуы керек болады;

құраушы матрицаның вектор-қатары кез келген $l(1 \le l \le k)$ қатарларды қосумен құрылады да, ол d-1 ден кем болмаған нөл емес таңбалардан құралған болады.

Ақиқаттан да, аталған шарт орындалғанда кез келген рұқсат етілген код қисындастыруы құраушы матрицаның l қатарын қосындылаумен табылып, d-дан кем болмаған нөл емес таңбалардан тұрады; себебі бірлік матрицаның қатарларын қосқанда ол әрқашанда l нөлге тең емес таңбасы болады.

Осы жолмен минимал код қашықтығы $d = 3$ екілік (7,4) жүйелілік кодының құраушы матрицасын синтездейміз.

Осы үлгіленген шартқа ($l = 1$ болғанда) сәйкес қосымша матрицаның әрбір вектор-қатарында бірліктер екіден кем болмауы керек.

Үш дәрежетты векторлардың ішінде осындай векторлар төртеу болады: 011, 110, 101, 111.

Осы векторлар бірлік матрицаның қатарларымен кез келген тәртіпте сәйкестендіріледі. Осының нәтижесінде Хэмминг кодына эквивалент болған жүйелілік кодтың матрицасын аламыз, мысалы:

$$M_{7,4} = \begin{bmatrix} 1000...011 \\ 0100...111 \\ 0010...101 \\ 0001...110 \end{bmatrix}.$$

Осыдан мынаны көруге болады; осындай матрицаның бірнеше қатарын (l>1) қосқанда d = 3 кем болмаған нөлсіз таңбалары бар вектор-қатар аламыз. Келесідей $Mn,k = [I_k \; P_{k,n-k}]$ жүйелілік кодтың құраушы матрицасы болса, онда $(n-k)*n$ өлшемді H тексеруші матрицасын құруға болады:

$$H = \left[-P_{k,n-k}^{T} I_{n-k} \right] = \begin{bmatrix} p_{1,k+1}, p_{2,k+1} \ldots p_{k,k+1} - 1 ... 0 ... 0 \\ p_{1,k+2}, p_{2,k+2} \ldots p_{k,k+2} .. 0 - 1 ... 0 \\ ..... \\ p_{1,n}, ... p_{2,n} ..... p_{k,n} ..... 0 ... 0. - 1 \end{bmatrix}.$$

(7.1)

Бұзылмаған код векторы A_{ni} ді H матрицасына транспондалған матрицаға көбейткенде барлық құрамдас бөліктері нөлге тең векторды аламыз:

$$A_{ni} H^{T} = \left| a_1 a_2 , ..., a_k , a_{k+1} , ..., a_j , ..., a_n \right| \bullet \begin{bmatrix} p_{1,k+1} \cdots p_{1,j} \cdots p_{1,n} \\ p_{2,k+1} \cdots p_{2,j} \cdots p_{2,n} \\ ..... \; ..... \; ... \\ p_{k,k+1} \cdots p_{k,j} \cdots p_{k,n} \\ -1 ..... 0 ..... 0 \\ ..0 ..... -1 ..... 0 \\ ..0 ..... 0 ..... -1 \end{bmatrix} =$$

$$\left| S_{k+1}, S_{k+2} , ..., S_j , ..., S_n \right| = \left| 0,0 ... 0 ... 0 \right|.$$

Мұндағы әрбір S құрамдас бөлігі соған сәйкес декодттау теңдеуінің дұрыстығын тексеру нәтижесі болады: $S_j = \sum_{i=1}^{k} a_i P_{ij} - a_i = 0$ ..

Жалпы жағдайда, егер код векторы A_{ni} = (a_1, a_2,...ai,...,a_k, a_{k+1},...a_j,...,a_n) қателік векторымен

$\xi_{ni} = (\xi_1, \xi_2, ..., \xi_i, ..., \xi_k, ..., \xi_j, ..., \xi_n)$ бұзылғанда, онда оны табу үшін (A_{ni} + ξ_{ni}) векторын H^t матрицаға көбейткенде нөлсіз құрамдас бөліктер шығады:

$$S_i = \sum_{i=1}^{k} \xi_i P_j - \xi_j .$$

Осыдан: $S_j(k+1) \le j \le n$ таңбалары тек қана қателік векторларына ғана байланысты екені көрінеді, ал $S = (S_{k+1}, S_{k+2}, ..., S_j, ...S_n)$ векторы ***қателікті танушы немесе синдром*** болады.

Екілік кодтар үшін (қосу операциясы айыру операциясына тең) тексеруші матрица мына түрде болады:

$$H = \left[P^T_{k,n-k}, I_{n-k}\right] = \begin{bmatrix} p_{1,k+1}p_{2,k+1}...p_{k,k+1}.10...0 \\ p_{1,k+2}p_{2,k+2}..p_{k,k+2}01...0 \\ p_{1,n.....}p_{2,n}.....p_{k,n}...00...1 \end{bmatrix} . \qquad (7.1a)$$

7.1 ***Зертханалық жұмыс***

M құраушы матрицасы бар (7,4) коды үшін тексеруші матрица *H* табамыз:

$$M_{7,4} = \begin{bmatrix} 1000110 \\ 0100101 \\ 0010011 \\ 0001111 \end{bmatrix}.$$

1100011 код векторында қателік бар және жоқ болғандағы синдромдарды табамыз $P_{4,3}$. Матрица $P_{4,3}$ транспондаймыз:

$$P^T_{4,3} = \begin{bmatrix} 1101 \\ 1011 \\ 0111 \end{bmatrix}.$$

Тексеруші матрицаны жазамыз:

$$H = \begin{bmatrix} 1101100 \\ 1011010 \\ 0111001 \end{bmatrix}.$$

$$H = \begin{bmatrix} 1101100 \\ 1011010 \\ 0111001 \end{bmatrix}.$$

Бұзылмаған код 1100011 векторын H^t көбейткенде нөлдік синдром аламыз:

$$[1100011]\ldots\ldots\begin{bmatrix} 110 \\ 101 \\ 011 \\ 111 \\ 100 \\ 010 \\ 001 \end{bmatrix} = [000].$$

$$[1101011]\ldots\ldots\begin{bmatrix} 110 \\ 101 \\ 011 \\ 111 \\ 100 \\ 010 \\ 001 \end{bmatrix} = [111].$$

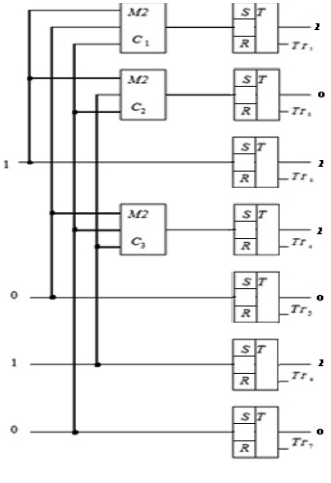
Код векторында қателік болсын, мысалы, 4 орында (1101011); сонымен 111 вектор-қатары осы кодта төртінші орында қателік барлығының синдромы болады.

Дәл осындай жолмен басқа қателіктердің де синдромдарын тапса болады. Барлық қателіктерді танушылары (синдромдары) Хэмминг (7,4) кодының танушыларына ұқсас; бірақ олар айқын қателік векторларына басқаша түрде сәйкестендіріледі; осы (эквивалентті) кодтың құраушы матрицасына сәйкес болады.

7.1.2 Топтық кодтарды кодтау және декодтаудың техникалық құралдары

Кодтау құрылғысы код құру ережелерінің теңдеулерінің негізінде құрылады. Кодтау құрылымының әрбір *n-k* тексеруші дәрежелеріндегі таңбалардың мәнін анықтау екілік модулді қосындыторлар негізінде анықталады. Қосындытордың әрбір орынында (бірінші орыннан тыс) төрт элемент ЖӘНЕ (вентил) және екі элемент НЕМЕСЕ қолданылады. Модуль екі бойынша қосындытор сұлбада М2 деп таңбаланған логикалық элемент.

Топтық кодтардың кодтаушы және декодтаушы құрылымдарын орындалуына мысалдар келтірейік.



7.1-сурет

7.2 Зертханалық жұмыс

Бірлік қателікті түзететін (7,4) кодының техникалық орындалуын қарастырайық. Код құру ережесі мына теңдеулермен анықталады:

$$a_1 = a_3 \oplus a_5 \oplus a_7,$$
$$a_2 = a_3 \oplus a_6 \oplus a_7,$$
$$a_4 = a_5 \oplus a_6 \oplus a_7.$$

Кодтаушы құрылымның сұлбасы 7.1-суретте келтірілген.

Арнадан қабылданған (қателігі бар болуы мүмкін) код қисындастыруы

n-орынды қабылдаушы регистрге түседі

(7.1- суретте Тг1-Тг7 триггерлері).

Триггерлердегі өткелді үдерістерден соң басқару жиынтығынен қосындыторлардың (*С*1- *С*3) әрбіріне сұрақ серпіні келіп түседі.

Басқару сұлбасынан синхроимпульс келгенде артықшылығы жоқ *к* орынды код қисындастыруы үздіксіз-кодты түрлендіргіштен *n* орынды регистрдің ақпараттық орындарына көшіріледі. Осыдан кейін, айталық регистрдің тригерлері 7.1-кестедегідей жағдайға көшеді.

7.1-кесте

Тг1	Тг2	Тг3	Тг4	Тг5	Тг6	Тг7
1	0	1	1	0	1	0

Біраз кешігуден соң $C1, C2, C_з$ қосындыторлардың шығуларындағы серпіндер тексеруші дәрежелердің триггерлерін жоғарыда берілген теңдеулерге сәйкес 0 немесе 1 жағдайларына өткізеді. Мысал үшін, C_1 қосындыторының кіруіне 3, 5 және 7 дәрежелеріндегі ақпараттар келіп түседі; сондықтан, Тг1 триггері 1 жағдайына, Тг2 триггері 0, Тг4 триггері – 1 жағдайына өткізіледі.

Регистрдегі рұқсат етілген қисындастыруы (7.2-кесте) басқару жиынтығынен келген серпіннен паралел немесе тізбекті түрде байланыс жолына оқып-жазылады. Кейінгі қисындастыруы кодталады.

7.2-кесте

Тг1	Тг2	Тг3	Тг4	Тг5	Тг6	Тг7
-	-	1	-	0	1	0

Енді декодтау және қателікті түзету сұлбасын қарастырамыз; олар тексеруші теңдеулер жиыны негізінде құрылған болады. (7 4) коды үшін олар мына түрде болады:

$$a_1 \oplus a_3 \oplus a_5 \oplus a_7 = 0,$$
$$a_2 \oplus a_3 \oplus a_6 \oplus a_7 = 0,$$
$$a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 0.$$

Қосындыторлардың шығу серпіндері синдром регистрінің триггерлерін 0 немесе 1 жағдайына өткізеді.

Егер тексеруші теңдеулер орындалса, онда синдром триггерлерінің барлығында 0 болады, яғни қателік жоқ дегені.

Егер қателік бар болса, онда синдром регистріне қателік векторы жазылады.

Қателік дешифраторы DC синдромдар жиынына қателік векторларының жиынын сәйкес қояды.

Дешифратордың шығу вентилдерін сұрақ еткенде түзету сигналдары қателік векторындағы **бірі** бар дәрежелерге ғана түседі.

Түзету сигналдары триггерлердің санақ кіруіне әсер етеді және олардың жағдайын өзгертеді, яғни осындай жолмен қателікті түзетеді.

Егерде ақпарат тек ақпараттық дәрежелерден ғана алынса, онда тексеруші дәрежелердің триггерлеріне түзету серпіндерін жібермесе де болады.

Хэммингтің (7,4) кодында синдром екілік үш орынды сан болып, онда қателік орынының нөмірі көрсетіледі.

Айталық жоғарыда құрылған код қисындастыруы арнада бұзылып, 7.3-кестедегі түрде қателіктермен қабылданған болсын.

7.3-кесте

Тг1	Тг2	Тг3	Тг4	Тг5	Тг6	Тг7
1	0	1	1	1	1	0

Қосындыторларды сұрақ еткенде C_1, C_2, C_3 шығуларында келесідей нәтижелер аламыз:

$$a_1 \oplus a_3 \oplus a_5 \oplus a_7 = 1+1+1+0 = 1,$$
$$a_2 \oplus a_3 \oplus a_6 \oplus a_7 = 0+1+1+0 = 0,$$
$$a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 1+1+1+0 = 1.$$

Сондықтан, қателік дәрежесінің нөмірі 101 немесе 5. Түзету серпіні Тг5 триггерінің кіруіне түсіп, қателікті түзетеді.

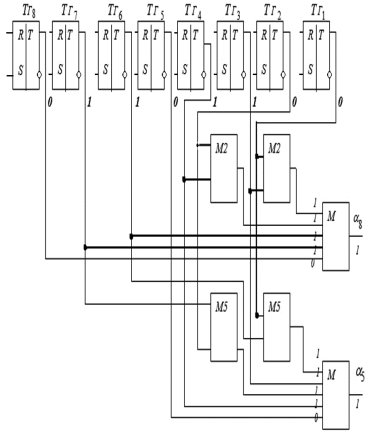
7.3 ***Зертханалық жұмыс***

Екі қателікті түзететін (8,2) топтық коды үшін мажоритарлық декодтау бағдаржолын орындаймыз.

Қабылдаушы регистрдің триггерлерінен сигналдар модуль екі бойынша қосудан соң ажратылған тексеру жүйесінің теңдеулеріне сәйкес *М* мажоритар элементтерге келіп түседі; олар түзетілген ақпараттық таңбаларды қалыптастырады.

Декодтау сұлбасы 7.2-суретте көрсетілген.

Мажоритар элементтердің кіруінде байланыс арнасынан бұзылған ақпарат (5- және 8 - ші) дәрежелерге келіп түседі. Көптік қағидамен шешім қабылдайтын мажоритарлық элементтер шығуда ақпараттық таңбалардың дұрыс мәндерін қайта тіктейтін болады.



7.2-сурет

7.2 Циклдік кодтар; жасаушы көпмүшеліктер, оларға қойылатын талаптар

7.2.1 Циклдік кодтарды құру. Жалпы түсініктер.

Кез келген топтық код (*n,k*) матрица түрінде жазылып, әрбірінде *n* таңбасы бар *k* сызықтық байланыссыз қатарлардан тұрады; және керісінше, кез келген *k* сызықты байланыссыз *n* - орынды код қисындастыруылар жиыны кейбір топтық кодттың құраушы матрицасы түрінде қаралуы мүмкін.

Осындай әртүрлі кодтардың арасынан төмендегідей қасиетке ие болғандарын ажыратып алайық; олардың құраушы матрицаларының қатарлары ***қосымша циклдік шартпен байланысқан*** болсын.

Осындай кодтың ***құраушы матрицаларының*** барлық ***қатарларын*** бір қисындастыруыны ***циклдік жылжытумен*** алуға мүмкін болады және ол осы ***кодтың құраушысы*** деп аталады. Осы шартқа жауап беруші кодтар ***циклдік кодтар*** деп аталады.

$$G = \begin{bmatrix} 001011 \\ 010110 \\ 101100 \\ 011001 \\ 110010 \\ 100101 \end{bmatrix}.$$

Жылжыту оңнан солға қарай жүргізіледі; сонда ең сол жақтағы шеткі таңба матрицаның оң жағына көшеді; яғни ***циклдік түрде айналады***.

Мысалы үшін 001011 код қисындастыруын циклдік жылжытумен алынатын қисындастыруылар жиынын жазайық.

Мүмкін болған циклдік (n, k)-кодтар саны әртүрлі (n, k) - топтық кодтар санынан әжептеуір кем болады.

Циклдік кодтарды көрсетуде n-орынды код қисындастыруылары жалған (фиктивті) айнымалы x-тің көпмүшеліктері түрінде көрсетіледі. Мұнда x-тің көрсеткіштері дәреже нөмірлеріне (нөлден бастап) сәйкес келіп, ал x-тің еселіктері жалпы жағдайда $GF(q)$ өрісінің элементтері болады.

Мұнда санның ең кіші дәрежесіне жалған айнымалы $x° = 1$ сәйкес келеді. $GF(q)$ өрісіндегі көпмүшелік $GF(q)$ өрісінің үстіндегі көпмүшелік деп аталады. Біз тек екілік кодтарды қарағандықтан x тің еселіктері тек 0 және 1 сандары болады.

Мысал үшін 01011 құраушы код қисындастыруын көпмүшелік түрінде көрсетейік:

$$G(x) = 0 \bullet x^4 + 1 \bullet x^3 + 0 \bullet x^2 + 1 \bullet x + 1.$$

Нөлдік еселіктері бар мүшелер қысқарғандықтан келесідей көпмүшелік қалады: $G(x) = x^3 + x + 1$. (7.2)

Нөл емес еселіктері бар мүшесіндегі x-тің ең үлкен дәрежесі ***көпмүшеліктің дәрежесі*** деп аталады.

Енді код қисындастыруылар үстіндегі амалдар көпмүшеліктер үстіндегі амалдарға алмастырылады. Көпмүшеліктерді қосу оның еселіктерін екілік модул бойынша келтірумен орындалады.

Аталған n — k орынды құраушы көпмүшеліктің циклдік жылжытуын орындағанда бірлікті код қисындастыруының соңына циклді түрде өткізбесек, бұл операция көпмүшелікті жай ғана x-ке көбейтуіне сәйкес келеді. Мысалы, егер матрицаның бірінші қатарын (001011) немесе оған сәйкес келетін $go(x) = x^3 + x + 1$ көпмүшелігін x ке көбейтсек, матрицаның екінші қатарын (010110) аламыз және ол мынаған сәйкес келеді: $x \cdot g0(x)$.

	0 0 1 0 1 1
⊕	0 1 0 1 1 0
	0 1 1 1 0 1

		x^3	+	0	+	x	+	1
	⊕					x	+	1
	⊕	x^3	+	0	+	x	+	1
x^4	+	0	+	x^2	+	x		
x^4	+	x^3	+	x^2	+	0	+	1

Осы екі қисындастыруының қосындысы болған қисындастыруы (0 1 1 1 0 1) мына екі көпмүшеліктің: $x^3 + x + 1$ және $x+1$ көбейтіндісіне тең болады $x^4 + x^3 + x^2 + 0 + 1$.

(n-m) - сол жақтағы үлкен орынында бірі бар матрицаның қатарын циклдікциклдік жылжыту деп осы қатарға сәйкес көпмүшелікті x ке көбейтіп, нәтижесінен x^{n+1} көпмүшелігін алып тасталғанына тең болады = x^{n-1}, яғни x^{n+1} модулі бойынша келтіруіне тең болады. Басқа сөзбен айтқанда, құраушы көпмүшелікті сәйкес түрде таңдап алынғанда, циклдік кодттың ***кез келген көпмүшелігі құраушы көпмүшелікке қалдықсыз бөлінеді.***

Рұқсат етілмеген код қисындастыруыларына сәйкес келетін бірде бір көпмүшелік құраушы көпмүшелікке қалдықсыз бөлінбейді.

Осы қасиет қателікті табуға мүмкіндік береді. Қалдықтың түріне қарап, қателік векторын да анықтаса болады.

Көпмүшеліктерді көбейту және бөлу кері байланысты жылжыту регистрлерінде ***оңай орындалады***; сондықтан да осы жай циклдік кодтардың кең қолдануына себеп болды.

7.2.2 Циклдік кодтар;

Циклдік кодтарға математикалық кіріспе

n-орынды циклдік кодтың әрбір рұқсат етілген қисындастыруы екі көпмүшеліктің көбейтіндісіне тең болады; олардың біреуі құраушы болып, онда осы қисындастыруыларды барлық *n*—1-ден үлкен болмаған орынды көпмүшелектердің барлық көбейтіндісінің кіші жиыны түрінде қарауға болады. Сондықтан осы кодтарды құру үшін ***алгебралық жүйелер теориясының*** бір тармағын - ***сақиналар теориясын*** қолдану керек болады.

Жоғарыдағы анықтамалардан *n*-орынды код қисындастырулар жиынынан сақина құру үшін екі операцияны беру керек: қосу және көбейту.

Екілік модул бойынша еселіктерге келтіруде көпмүшеліктерді қосу операциясын қолданған едік. Енді көбейту операциясын анықтайық.

Қарапайым әдістер бойынша көпмүшелікті көбейту операциясы және ұқсас мүшелерді екілік модул бойынша келтіру ***тұйықтық шарттарын*** бұзуы мүмкін. Ақиқаттан да көбейту нәтижесінде *n* — 1-ден де жоғары орынды көпмүшеліктер алынуы мүмкін, мысалы 2(*n*–1) ге дейін; ал оларға сәйкес код қисындастыруларының дәрежелер саны *n* артық болады және, сондықтан да қаралып отырған жиынға жатпайды.

Сондықтан таңбалық көбейту операциясы келесідей беріледі:

1) көпмүшеліктер қарапайым жай көбейту ережелерімен көбейтіледі, бірақ ұқсас мүшелер екілік модул бойынша келтіріледі.

2) егер де көбейтудің ең үлкен дәрежесі *n*—1-ден артпаса, онда ол таңбалық көбейтіндінің нәтижесі болады.

3) егер де көбейтудің ең үлкен дәрежесі *n* нен үлкен немесе тең болса, онда көбейтінді көпмүшелігі алдын ала анықталған *n* орынды көпмүшелікке бөлінеді және таңбалық көбейтудің нәтижесі болып бөліндінің қалдығы алынады.

Қалдық дәрежесі *n* — 1-ден артпайды; сондықтан осы көпмүшелік *n*-орынды код қисындастыруылар жиынына жатады.

Бірлікті код қисындастыруылар соңына өткізумен болатын циклдік жылжытуды талдаудан мынаған келеміз: осындай *n*-орынды көпмүшелік x^{n+1} болады. Ақиқаттан да, *n*-1 орынды көпмүшелікті *x* ке көбейткенде мынаны аламыз:

$$G(x) = \left(x^{n-1} + x^{n-2} + \ldots + x + 1\right) \bullet x = x^n + x^{n-1} + \ldots + x \quad . (7.3)$$

Сондықтан, осында да көбейту нәтижесі берілген код қисындастыруы циклдік жылжытумен құрылған код қисындастыруына сәйкес келуі үшін ондағы

x^n-ді 1 алмастыру керек болады.

Осындай алмастыру көбейтуден алынған көпмүшелікті x^{n+1}-ге бөлуге эквивалент болады; бөлуден қалған ***қалдықты айырым (вычет)*** деп немесе $\boldsymbol{x^{n+1}}$ ***модулге келтіру*** деп атайды.

Аталған сақинада $g(x)$ көпмүшелігіне ***реттік болған кіші жиынды*** барлық жиындардан ажыратып аламыз. Осындай кіші жиынды ***идеал*** деп, ал

$g(x)$- көпмүшелігін идеалдың ***құрушы көпмүшелігі*** деп атайды.

Идеалдағы әртүрлі элементтер саны оны құрушы көпмүшелік түрімен анықталады. Егер де құрушы көпмүшелікте 0 алсақ, онда барлық идеал тек осы көпмүшеліктен болады; себебі оны кез келген басқа көпмүшелікке көбейткенде 0 болады.

Егерде құрушы көпмүшелік деп 1 [$g(x) = 1$], онда идеалға сақинаның барлық көпмүшеліктері кіреді;

Жалпы жағдайда идеалдың элементтер саны 2^k болып, n — k орынды қарапайым көпмүшеліктен құралған болады.

Енді осыдан мынау түсінікті болады;

n-орынды екілік код қисындастыруларының сақинасында құрылған екілік циклдік код идеал болатыны көрінеді.

7.2.3 Құрушы көпмүшелікті таңдау; әртүрлі тәртіпті қателіктерді табу және түзету

Циклдік кодтардың анықтамасына сәйкес оның код қисындастыруына сәйкес келетін барлық көпмүшеліктер $g(x)$-ке қалдықсыз бөлінуі керек.

Мұның үшін кодтың құраушы матрицасының көпмүшеліктері $g(x)$-ке қалдықсыз бөлінуі керек. Ақырғылары циклдік жылжытумен алынады; бұл $g(x)$ ті x-ке тізбектеп көбейту және модул x^{n+1} бойынша келтірумен орындалады. Сондықтан, жалпы жағдайда $g_i(x)$ көпмүшелігі $g(x)\cdot x^i$ көбейтіндіні x^{n+1} көпмүшелігіне бөлуден қалған қалдық болып, мына түрде жазылады:

$$g_i(x) = g(x)x^i + c\left(x^n + 1\right). \qquad (7.4)$$

Мұнда егер $g(x)x^i$ дәрежесі n — 1- ден асса, $c = 1$ болады;

ал егер $g(x)x^i$ n—1- ден аспаса, $c = 0$ болады.

Осыдан шығатыны, матрицаның көпмүшеліктерінің барлығы да, сондай-ақ кодтың барлық көпмүшеліктері де $g(x)$ ке қалдықсыз бөлінеді; бұл тек x^{n+1} көпмүшелігі $g(x)$ ке қалдықсыз бөлінсе ғана орынды болады.

Сақина үшін топтың барлық қасиеттері орынды болғандықтан, ал идеал үшін кіші топтың барлық қасиеттері орынды болғандықтан, сақинаны жақын кластарға жіктесе болады; оларды ***идеал бойынша айырымды кластар*** деп атайды.

Жіктеудің бірінші қатары идеал болып, ондағы нөлдік элемент сол жақ шетінде орналасқан болады.

Бірінші айырымды кластың құраушысы ретінде идеалға жатпайтын кез келген көпмүшелікті алса болады.

Осы айырымды кластың басқа элементтерін идеалдың әрбір көпмүшелігін құрушы көпмүшелікпен қосу арқылы алса болады.

Егер $g(x)$ $m = n — k$ орынды көпмүшелігі x^{n+1} көпмүшеліктің бөлгіші болса, онда сақинаның кез келген элементі $g(x)$ ке қалдықсыз бөлінеді (онда ол идеалдың элементі болады); немесе бөлу нәтижесінде $r(x)$ қалдығы қалса, ол көпмүшелік болып, дәрежесі m-1-ден аспайды.

Сақина элементтері тек біртүрлі көпмүшелік $г_i(x)$ түріндегі қалдыққа ие болса, онда олар айырымдардың бір класына жатады.

г(x) көпмүшеліктерін айырымды кластардың элементтеріне жатқызсақ, сақинаның m орынды $g(x)$ құраушы көпмүшелігі болатын идеал бойынша жіктеуі 7.4-кестесінде көрсетілген; мұнда $f(x)$ — кез келген дәрежесі n — m — 1-ден аспайтын көпмүшелік.

7.4-кесте

0	$g(x)$	$x\,g(x)$	$(x+1)\,g(x)$	…	$f(x)g(x)$
$г_1(x)$	$g(x)+г_1(x)$	$x\,g(x)+г_1(x)$	$(x+1)g(x)+г_1(x)$	…	$f(x)g(x)+г_1(x)$
$г_2(x)$	$g(x)+г_2(x)$	$x\,g(x)+г_2(x)$	$(x+1)g(x)+г_2(x)$	…	$f(x)g(x)+г_2(x)$
…	…	…	…	…	…
…	…	…	…	…	…
$г_z(x)$	$g(x)+г_z(x)$	$x\,g(x)+г_z(x)$	$(x+1)g(x)+г_z(x)$	…	$f(x)g(x)+г_z(x)$

Сондықтан, циклдік кодтың ***түзетуші қабілетінің*** жоғары болуы көпмүшелікті бөлуде ***қалған қалдыққа байланысты*** болады;

қалдық үлкен болған сайын оның түзетуші қабілеті жоғары болады.

Ең үлкен қалдық, 2^{m-1} (нөлден басқа) тек келтірілмейтін қарапайым көпмүшелікте ғана болуы мүмкін болады; ол өзіне өзі бөлінеді де (1 -ден басқа) ешқандай басқа көпмүшелікке бөлінбейді.

7.2.4 Құраушы көпмүшелікті таңдау; әртүрлі тәртіпті қателіктерді табу және түзету

Берілген код көлемі бойынша ақпараттық орын саны k табылады. Содан соң берілген ретті қателікті табу және түзетуге жеткілікті болған ең кіші n ды табу керек болады.

Циклдік код құруда бұл мәселе тиісті болған көпмүшелік $g(x)$ ті табуға келеді. Барлық бірлік қателікті табатын циклдік кодтарды қарастырайық.

Байланыс арнасымен қабылданған кез келген, мүмкін қателігі бар, $h(x)$ код қисындастыруын кодтың бұзылмаған қисындастыруы $f(x)$ және қателік векторы $\xi(x)$- тің модуль екі бойынша қосындысына тең деп қарау мүмкін болады:

$$h(x) = f(x) \oplus \xi(x). \qquad (7.5)$$

$h(x)$ көпмүшелігін құраушы $g(x)$ көпмүшелігіне бөлгенде, егерде қателікке сәйкес көпмүшелік $g(x)$ ке бөлінбесе, онда қателік анықталады.

Ал $f(x)$ – кодтың бұзылмаған қисындастыруы болғандықтан, $g(x)$ -ке қалдықсыз бөлінеді.

Бірлік қателіктің векторы бұзылған орында ғана бірі бар болып, қалған орындарында тек нөлдері болады.

Оған келесідей көпмүшелік $\xi(x) = x^i$ сәйкес келеді.

Ақырғысы $g(x)$-ке бөлінбеуі керек. Мұнда x^{n+1} жіктеуіне қатысты келтірілмейтін көпмүшеліктер ішінде осы шартқа жауап беретін ең кіші орынды көпмүшелік $x+1$ болады; кез келген көпмүшелікті $x+1$-ге бөлгендегі қалдық нөлінші орындағы көпмүшелік болады және тек 0 және 1 мәніне ие болады.

Осындайда сақинаның барлығы тек идеалдан және жұп мүшелі көпмүшеліктен тұрады және мұнда айырымдықтардың жалғыз класы болып, ол жалғыз ғана қалдыққа ие болады; ол 1-ге тең болады.

Сөйтіп, ақпараттық орындардың кез келген санында тек жалғыз тексеруші орын керек болады.

Осы орынның таңбасының мәні кез келген рұқсат етілген код қисындастыруындағы бірліктердің жұптығын көрсетеді; сондықтан x+1 ге бөлінуін де көрсетеді.

Осы код тек бөлек орындардағы бірлік қателіктерді ғана анықтап қоймастан, сондай ақ кез келген тақ санды орындардағы қателіктерді де табады.

Бірлік қателіктерді түзету және екілік қателіктерді табу.

Циклдік кодтарда қателіктер синдромы қателіктер көпмүшелігін кодтың құраушы $g(x)$ көпмүшелігіне бөлуден қалған қалдықтар болғандықтан, $g(x)$ көпмүшелігінің бірліктері қателіктерге сәйкес келетін қалдықтардың тиісті санын табуға жеткілікті болуы керек.

Жоғарыда айтылғандай ең көп қалдықтарды келтірілмеген көпмүшеліктер береді.

Көпмүшеліктің дәрежесі $m = n - k$ болғанда, ол 2^{n-k}-1 нөлсіз қалдықтар береді (нөлдік қалдықтар қатесіз жіберулер синдромы болады).

Сондықтан, кез келген бірлік қателігінің түзету шарты мына теңсіздіктен шығады:

$$2^{n-k} - 1 \geq C_n^1 = n\,, \tag{7.6}$$

мұнда C_n n таңбалы код қисындастыруындағы әртүрлі бірлік қателіктердің жалпы саны; осыдан кодтың құраушы көпмүшелілігінің дәрежесін:

$$m = n - k \geq \log_2(n+1) \tag{7.7}$$

және код қисындастыруындағы таңбалар санын да табамыз.

Берілген 7.5 кестеден әртүрлі m үшін k және n-нің ең үлкен мәндерін табамыз.

Айтқанымыздай, құраушы көпмүшелік $g(x)$ екімүшелік x^{n+1} дің бөлгіші болуы керек. Кез келген мына түрдегі $x^{2m-1}+1 = x^n + 1$ екімүшелік барлық келтірілмейтін көпмүшеліктердің көбейтіндісі түрінде көрсетілуі мүмкіндігі дәлелденген; мұнда келтірілмейтін көпмүшеліктердің дәрежесі m санының бөлгіші болады (1 ден m - ге дейін қосып есептелгенде).

Сондықтан кез келген m үшін ең болмағанда бір m орынды келтірілмейтін көпмүшелік ұшырайды; ол x^{n+1} екімүшелік жіктелуінде көбейткіш болып қатысады.

Құраушы көпмүшелікті анықтаған соң, оның тиісті қалдықтар санын қамти алатынына көз жеткізу керек.

7.5-кесте

m	1	2	3	4	5	6	7	8	9	10
N	1	3	7	15	31	63	127	255	511	1023
k	0	1	4	11	26	57	120	247	502	1013

7.4 Зертханалық жұмыс Мына жағдай үшін құраушы көпмүшелік таңдаймыз: $n = 15$ және $m = 4$.

$x^{15}+1$ екімүшелігін басқа барлық келтірілмейтін көпмүшеліктер көбейтіндісі түрінде жазса болады; олардың дәрежесі 4 санының бөлушісі болады. Ол 1, 2, 4 ке бөлінеді.

Келтірілмейтін көпмүшеліктер кестесінде бір бірінші орынды көпмүшелік (x+1), бір екінші орынды көпмүшелік (x^2+ x+1), үш төртінші орынды көпмүшелік ($x^4 + x + 1$, $x^4 + x^3$+1, $x^4 + x^3$+x + 1) табылады.

Осы қатыстың дұрыстығына сену үшін барлық көпмүшеліктерді көбейтеміз: (x+1)($x^2 + x + 1$)($x^4 + x$+1)($x^4 + x^3$+ l)($x^4 + x^3 + +x^2$+x+1) = x^{12}+1.

Мысалы, төртінші орынды көбейткіштердің біреуін кодтың құраушы көпмүшелігі ретінде қабылдау мүмкін; мысал үшін, $x^4 + x^3 + 1$ көпмүшелігін, немесе екілік тізбек түріндегі 11001 қисындастыруын қабылдау мүмкін.

Төменгі орынды қателік векторлары мына түрде болады:

00...0001, 00...0010, 00...0100, 00...1000.

Оларға сәйкес көпмүшеліктердің дәрежелері $g(x)$ құраушы көпмүшелігінің дәрежесінен кем болады.

Сондықтан олардың өзі де нөлдік бүтін бөлімде қалдық болып есептеледі. Кейінгі жоғарғы орындағы (орындағы) қателік векторына сәйкес келетін қалдық 00...10000 ны 11001 ған бөлгенде шығады, яғни:

$$\begin{array}{r} 10000 \,|\, 11001 \\ \oplus\ 11001 \\ \hline 1001 \end{array}$$

Дәл осындай басқа қалдықтар да табылады.

Алайда оларды оңай жолмен де алса болады; бірлікті нөлдер қатарын $g(x)$ қисындастыруына бөліп және аралықтағы барлық қалдықтарды жазып аламыз:

1	0	0	0	0	0	0	0	0	0	0							
1	1	0	0	1	↓								Қалдықтар				
-	1	0	0	1	0												
	1	1	0	0	1	↓											
	-	1	0	1	1	0											
		1	1	0	0	1											
		-	1	1	1	1											
			1	1	0	0	1										
			-	0	1	1	1	0	0								
					1	1	0	0	1								
					-	0	1	0	1	0	→						
						-	1	1	0	0	1						
							-	1	1	0	1	→					
								1	1	0	0	1					
								-	0	0	1	1					
											1	1	0	0	1		
											-	0	0	0	1	→	1000

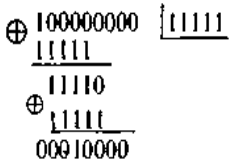
Кестеде бөлу операциясы көрсетілген; қалған қалдықтар оң жақта жазылған (оңға бағытталған нұсқағышпен көрсетілген). Жоғарыдан түсірілетін нөлдер төмен қараған нұсқағышпен көрсетілген. Бөлінгіш, бөлгіштер - көк және жасылмен таңбаланған; ал қалдықтар – қызылмен жазылған.

Кейінгі бөлуде қалдықтар қайталанады. Сонымен, берілген $g(x)$ке бөлгендегі әртүрлі қалдықтар саны $n = 15$ тең болады. Сондықтан, құрылған код кез келген бірлік қателікті түзете алады.

Дәл осындай көрсеткішті көрсететін құраушы көпмүшелік ретінде x^4+x+1 алса да болады. Мұнда құрылған код берілген кодқа эквивалент болар еді.

Алайда дәл осы мақсатта $x^4 + x^3 + x^2 + x + 1$ көпмүшелігін қолданып болмайды. Себебі мұнда қалдықтар саны 15 емес, бар жоғы 5 болады.

Қалдықтар:



Қалдықтар:

1111
0001
0010
0100
1000

Мұны былай түсіндірсе болады; $x^4 + x^3 + x^2 + x + 1$ көпмүшелігі $x^{15} + 1$ көпмүшелігінен тыс, мына $x^5 + 1$ көпмүшелігінің жіктелуіне де тиісті болады.

7.6 - кестеде барлық бірлік қателерді түзететін, барлық бірлік және екілік қателерді анықтайтын кейбір кодтардың негізгі сипаттамалары келтірілген.

7.6-кесте

Келтірілмейтін көпмүшелік дәрежесі	Құраушы көпмүшелік	Қалдықтар саны	Код ұзындығы
2	$x^2 + x + 1$	3	3
3	$x^3 + x + 1$	7	7
3	$x^3 + x^2 + 1$	7	7
4	$x^4 + x^3 + 1$	15	15
4	$x^4 + x + 1$	15	15
5	$x^5 + x^2 + 1$	31	31
5	$x^5 + x^3 + 1$	31	31

Бұл Хэммингтің бір қателікті түзететін циклдік коды болып, Хэммингтің топтық кодынан айырмашылығы - барлық тексеруші дәрежелер код қисындастыруының соңында орналасқан болады. $\xi(x) = x^j + x^i$.

Осы кодтарды кез келген екі қателіктерді табуға да қолданса болады.

Екі қателік векторына сәйкес көпмүшелік мына түрде болады: $\xi(x) = x^j + x^i$,

немесе $\xi(x) = x^i(x^{j-i} + 1)$, мұнда $j>i$. $j-i<n$, ал $g(x)$ x ке ретті болмағандықтан және n дәреже көрсеткішіне қатысты болғандықтан, $\xi(x)$ $g(x)$ ке бөлінбейді; сондықтан екі ретті қателіктерді таба алады.

Үш және төменгі реттік қателіктерді табу.

Бірлік, екілік, үштік қателіктерді табатын кодтардың құраушы көпмүшеліктерін Хэммингтің келесідей көрсетуімен анықтаса болады.

Егерде ұзындығы n болған $p(x^m)$ кодының құраушы көпмүшелігі анықталған болса және ол z ретті қателіктерді анықтайтын болса, онда $(z+1)$ реттік қателікті таба алатын кодтың құраушы $g(x)$ көпмүшелегін құру үшін $p(x^m)$ көпмүшелігін $x+1$ көпмүшелігіне көбейту керек болады; мұнда қосымша жұпқа тексеру ендіріледі. Мұнда кодтың қисындастыруындағы таңбалар саны тағы бір тексеруші таңбалы ендірумен n + 1- ге артады.

7.7 - кестесінде үш және одан төмен қателерді табатын кодтардың негізгі сипаттамалары берілген.

7.7 - кесте

Келтірілмейтін көпмүшелік дәрежесі	Құраушы көпмүшелік	Қалдықтар саны	Код ұзындығы
3	$(x+1)(x^3+x+1)$	4	8
4	$(x+1)(x^4+x+1)$	11	16
5	$(x+1)(x^5+x+1)$	26	32

$$n - k \geq 2b \qquad (7.8)$$

7.2.5 Циклдік кодтарды құру әдістері; матрицалық жазылуы; мажоритарлық декодтау

Циклдік кодтарды құру әдістері

Бірнеше кодтау әдістері мәлім. Былайша алғанда циклдік кодтарды құрудың ең оңай жолы - артықшылығы жоқ болған $a(x)$ код қисындастыруын (ақпараттық таңбалар) кодтың құраушы $g(x)$ көпмүшелігіне көбейту.

Мұндай әдіс оңай орындалады.

Алайда бұл әдісте көбейтуден кейінгі нәтижеден ақпараттық орындарды анық ажырату мүмкін болмайды.

Қателіктерді түзеткен соң мұндай қисындастыруылардан ақпараттық таңбаларды кодтың құраушы көпмүшелігінен ажыратып алу керек болады.

Әдетте циклдік кодтарда кодтың үлкен орынды орындарында ақпараттың k орны, ал төменгі n — k орындарында тексеруші таңбалары жазылады.

Мұндай жүйелілік код алу үшін келесідей кодтау шарасы қолданылады.

Артықшылығы жоқ кодтың k - орынды қисындастыруына сәйкес келетін $a(x)$ көпмүшелігін x^m - ге көбейтеміз; мұнда $m = n — k$..

Мұнда $a(x)$- ке жататын әрбір бірмүшеліктің дәрежесі өседі, сондықтан код қисындастыруының төменгі орындарына m қосылады, яғни $a(x)x^m$ болады. Ақырғы көбейтіндіні $g(x)$ көпмүшелігіне бөлеміз.

Жалпы жағдайда қандайда бір $q(x)$ бөліндіні аламыз; оның дәрежесі $a(x)$ және $r(x)$ қалдығының орынындай болады.

Ақырғы алынған қалдықты $a(x)x^m$ -ке қосамыз.

Нәтижеде келесідей көпмүшелікті аламыз:

$$f(x) = a(x)x^m + r(x) \ . \qquad (7.9)$$

$g(x)$- тің дәрежесі m болғандықтан, қалдық $r(x)$-тің дәрежесі m — 1- ден аспайды. Сондықтан, осы қосу операциясы $a(x)$- ке төменгі дәрежелер жағынан $r(x)$-ті тіркеуге сәйкес келеді.

Бұл жерде $f(x)$-тің $g(x)$-ке қалдықсыз бөлінуін дәлелдеу керек болады.

Мұның үшін $a(x)x^m$ көпмүшелігін келесідей жазамыз:

$$a(x)x^m = q(x)g(x) + r(x). \qquad (7.10)$$

Қосу және екілік модулде айыру амалдары бірдей болғандықтан, келесідей жаза аламыз:

$$a(x)x^m + r(x) = f(x) = q(x)g(x). \qquad (7.11)$$

Сонымен тиісті дәлелді алдық.

Сөйтіп, циклдік кодты құру үшін артықшылығы жоқ код қисындастыруын құраушы көпмүшелікке бөліп, қалған қалдықты артықшылығы жоқ код қисындастыруына тіркеу керек болады.

Мұндай әдіс ақпараттық дәрежелер құраушы дәрежелерден артық болғанда қолайлы болады. Және бір кодтау әдісін көрсетейік.

Циклдік кодтар топтық кодтардың бір түрі болғандықтан, оның тексеруші таңбалары кейбір ақпараттық таңбаларының екілік модулі бойынша қосындысына тең болады.

Тексеруші таңбаларды анықтаушы теңдік мына рекурренттік қатысты шешумен алынады:

$$a_{i+k} = \sum_{j=0}^{k-i} h_j a_{i+j} \quad , \qquad (7.12)$$

мұнда h – генераторлық көпмүшелік $h(x)$ тің екілік еселіктері болып, келесідей анықталады:

$$h(x) = \left(x^n + 1\right) / g(x) = h_0 + h_1 x + \ldots + h_k x^k . \qquad (7.13)$$

(7.13) қатысы a_0, a_1, ..., a_{k-1} ақпараттық таңбалар тізбегі бойынша $n - k$ тексеруші таңбаларды есептеуге мүмкіндік береді.

Тексеруші таңбалар, алдыңғыдай, төменгі дәрежелерде орналасады.

Алдыңғы кодтау әдісімен алынған қисындастыруылармен толық сәйкес келеді.

Осы әдіс тексеруші таңбалар саны ақпараттық таңбалар санынан асатын жағдайларда өте қолайлы болады; мысалы үшін, Боуза — Чоудхури — Хоквингем кодтарында.

Матрицалық жазылуы; мажоритарлық декодтау.

Mn,k циклдік кодының құраушы матрицасы екі матрицадан тұрады: бірлік I_k (k) (ақпараттық дәрежелерге сәйкес) және қосымша $C_{k,n-k}$ (тексеруші дәрежелерге сәйкес): $M_{n,k} = \left\| I_k C_{k,n-k} \right\|$. (7.14)

I_k матрицасын құру қиыншылық тұдырмайды. Егер циклдік кодтарды құру рекурренттік теңдеулерді шешумен амалға асырылатын болса, онда оның қосымша матрицасын анықтау үшін алдыңғы ережелерді қолдану мүмкін болады. Алайда әдетте циклдік кодтарда

$C_{k,n-k}$ нің қосымша матрицасының қатарлары $r(x)$ көпмүшелігін есептеумен анықталады.

$r(x)$- ке сәйкес келетін I_k матрицасының әрбір қатарын табу үшін $a(x)x^m$ ақпараттық көпмүшелігінің әрбір қатарын кодтың құраушы көпмүшелігіне бөлу керек.

Қосымша матрицаны I_k ны құрмастан ақ анықтауға болады.

Мұның үшін бір мен нөлден құрылған қисындастыруыны $g(x)$ ке бөлу және алынған қалдықтарды қосымша матрицаның қатарлары ретінде жазу жеткілікті болады. Егер қандай да бір $r(x)$-тің дәрежесі $n - k - 1$-ден кем болса, онда осы қалдықтан кейінгі матрица қатарларын табу үшін алдыңғы қатарды циклдік түрде солға қарай жылжыту операциясы $r(x)$- тің дәрежесі n — k—1- ге тең болғанша жалғастырылып отырылады. Мұнда бөлу амалы қосымша матрицаның k қатарларын шығарып алғанша жалғаса береді.

7.5 ***Зертханалық жұмыс***

$g(x) = x^4 + x^3 + 1$ көпмүшелікті (15,11) циклдік кодының құраушы матрицасын жазу керек. Алдыңғы бөлу нәтижелерін қолданып мынаны жазамыз:

$$M_{\text{б},1} = \begin{bmatrix} 00000000001.....1001. \\ 00000000010.....1011 \\ 00000000100.....1111 \\ 00000001000.....0111 \\ 00000010000.....1110 \\ 00000100000.....0101 \\ 00001000000.....1010 \\ 00010000000.....1101 \\ 00100000000.....0011 \\ 01000000000.....0110 \\ 1000000000.....1100 \end{bmatrix}.$$

Құраушы матрицаны құрудың басқа жолы да бар. Ол (n, k)-циклдік кодының негізгі ерекшеліктеріне байланысты болады. Ол алдыңғыдан қарапайымдау болғанымен матрица қолдануда қолайсыздау болады.

Кодтарды матрицалық түрде жазылуы жеткілікті дәрежеде кең таралған.

Қысқартылған циклдік кодтар

Циклдік кодтардың түзетуші мүкіндіктері құраушы көпмүшеліктің m дәрежесімен анықталады. Соның өзінде де қажетті

ақпараттық таңбалар саны кез келген бүтін сан болуы мүмкін болып, кодтың дәрежелер санын таңдап алу мүмкіндігі өте шектелген болады.

Егер, мысал үшін, $k = 5$ те бірлік қателіктерді түзету керек болса, онда үшінші орынды құраушы көпмүшелікті алу мүмкін болмайды. Себебі ол тек жеті қалдық береді; ал дәрежелердің жалпы саны 8 болады.

Сондықтан, төртінші орынды көпмүшелік алу керек болады және онда $n = 15$ болады. Мұндай код 11 ақпараттық дәрежелерге арналған болады.

Алайда минимал орынды код құру үшін (n, k) –кодта j бірінші ақпараттық таңбаларды нөлдермен алмастырып және оларды код қисындастыруынан шығарып тастау керек болады. Бірақ мұнда код циклдік болмайды; себебі мұнда бір рұқсат етілген код қисындастыруын циклдік жылжытқанда сол кодтың басқа рұқсат етілген код қисындастыруы келіп шыға бермейді.

Осындай жолмен алынған сызықтық $(n - j, k - j)$-код ***қысқартылған циклдік код*** деп аталады. Мұнда кодтың минимал қашықтығы осы код алынған (n, k)-кодтың минимал қашықтығынан кем емес болады.

Қысқартылған кодтың матрицасы (n, k)-кодтың құраушы матрицасынан жоғарғы дәрежелерге тура келетін j қатар мен бағандарын алып тастаумен құрылады. Мысал үшін, (9,5) кодының құраушы матрицасы (15,11) кодының матрицасынан алынып, мына түрде болады:

$$M_{9,5} = \begin{bmatrix} 00001.1001 \\ 00010.1011 \\ 00100.1111 \\ 01000.0111 \\ 10000.1110 \end{bmatrix}.$$

Қателікті анықтаушы циклдік кодтардың сандық желіде қолданылуы

Осы замандық сандық деректерді ұзату жүйелерінде қателіктерді түзетудің көптеген бағдаржолдары мен әдістері қолданылады. Оларда тиімділікті максимал дәрежеде арттыру үшін бірнеше әдістер параллел түрде қолданылады.

а). Түйіншекті радиожелілерде және жергілікті желілерде *LLC*2, *LLC*3 протоколдары және ғаламдық желілерде *TCP* прото-

колы қолданылып, циклдік полиномиалдық кодтар істетіледі; олар бұзылған түйіншектерді анықтап, ал қателіктерді түзету амалы түйіншектерді қайта жіберумен амалға асырылады.

Егерде түйіншектердің ұзындығын тиімді таңдап алсақ, деректерді ұзатуда информацияның максимал жылдамдығын қамтамасыз етуге болады.

б) Кері байланыс болмаған жағдайда түзетуші кодтар істетіледі. Олардың ішінде ең "жетілгені" Хэмминг кодтары: *КХ*(7,4), *КХ*(15,11) және басқалар. Алайда олар мәтін хабарларға арналған емес; *КХ*(7,4) кодының таңбалары толық әліпбиге жетпейді, ал *КХ*(15,11) *МТК*-5 и *ASCII* үлгіқалыптарын қолданғанда да өте үлкен артықшылығы бар (~114%) болады.

Циклдік кодтар сандық желілерде кең қолданылады; мұндай кодтың негізгі қасиеті: осы кодтың құрушы қисындастыруын циклді жылжытумен құрылады. Сондықтан да циклдік деп аталады.

Циклдік кодтардың ең негізгі қасиеті: жабық (рұқсат етілмеген) код қисындастыруылардан еш қайсысы құраушы қисындастыруыға қалдықсыз бөлінбейді.

Және бір қасиеті: **циклдік кодта ашық (рұқсат етілген) код қисындастыруылардың барлығы да құраушы полиномға қалдықсыз бөлінеді.**

Циклдік кодтардың абзалдығы: кез келген орындағы қателіктерді таба алады. Ал қателікті түзету - сол қате блокті қайталаумен орындалады.

Циклдік код құрудың бір әдісін келесідей мысалда қарастырайық.

7.6 *Зертханалық жұмыс*

Айталық хабар *n*=6 орынды код түрінде берілсін: $A = 100111$.

Сонда оның құраушы полиномы келесідей анықталады; $k = 2^6 - 1 = 63 = 7 * 9$.

Құрушы полином ретінде екі көбейткіштің модул бойынша кішісін аламыз: $g = 7_{10} = 111_2$.

Осы кодтың дәрежелер санын бірге кемейтіп, (яғни үшті бірге кемейтіп) сонша нөлдерді хабарға тіркейміз, яғни екі нөлді тіркейміз. $A(2^k) = 10011100$.

Алынған 10011**00** санды g=111ге бөлеміз.

$$
\begin{array}{l}
10011100\ !111 \\
\underline{111} \\
\quad 111 \\
\quad \underline{111} \\
\qquad 110 \\
\qquad \underline{111} \\
\qquad\quad \mathbf{10} \rightarrow CRC
\end{array}
$$

Алынған қалдықты хабар кодына екілік модул бойынша қосқанда ақырында келесідей түрде құрылған код аламыз: $A\left(2^k\right)' = 10011110$.

Құрылған кодтың дұрыстығын тексеру үшін және де сол 111 ге бөлеміз; егер бөлгенде қалдық болмаса, бұл кодтың дұрыс құрылғандығын көрсетеді. Айта кететін жай, құраушы көпмүшелікті таңдаудың әртүрлі әдістері бар болып, бұл жерде тек бір әдісті көрсеттік.

Мысалы: 1) 110011,101011, 110011,1010101,101101,...циклдік код құру керек.

2) 1010110, 1101101, 1011011, 1101010,1110011,1000110, 1100110, 1001001, 1010101, 1100011 кодтарына циклдік кодтар құру керек.

7.3 Қателік түйіншектерін табушы және түзетуші циклдік кодтар

Боуз-Чоудхури-Хоквингем, Рид-Соломон, Рид-Маллер кодтары

Кез келген орындағы байланыссыз қателерді анықтаушы және түзетуші кодтар.

Арнадағы байланыссыз қателіктерге арналған кодтар класы жаратылған болып, оған мысал Боуза — Чоудхури — Хоквингем кодтарын алса болады.

Кез келген оң бүтін сан m және $s<n/2$ үшін ұзындығы $n = 2^m–1$ және тексеруші дәрежесі ms тен аспайтын осы кластағы екілік код бар болып, ол 2s реттік қателіктерді табады, s реттік қателіктерді түзетеді.

Кез келген сызықтық жиынтықтық (n, k)-код үшін оның түзетуші қабілеті мен артықша таңбаларының арасындағы байланыс ***Рейджер шекарасы*** болады; мұнда код ұзындығы b- ға тең немесе кем болған қателік түйіншек түзуге арналған болады.

Сызықтық кодпен ұзындығы b тең немесе кем болған

түйіншектерді түзету және ұзындығы $l >= b$ немесе одан кем болған қателік түйіншек табу үшін ең болмағанда $b + 1$ тексеруші таңбалар керек болады.

Түйіншекті қателіктерді түзетуші циклдік кодтардың ішінде кең тараған Бартон, Файр и Рид — Соломон кодтары.

Бірінші екеуі – жиынтықтағы ***бір түйіншекті*** түзетсе, ал Рид — Соломон кодтары ***бірнеше пачкаларды*** түзетуге арналған.

Қателік түйіншектерін түзетуші циклдік кодтарды декодтау Файр коды мысалында көрілген.

Боуз-Чоудхури-Хоквингем кодтары

Минимал код қашықтығы берілген санға тең болған кодтарды құру мәселесі ашық қалған еді.

1960 ж. Боуз, Чоудхури, Хоккенгем өзара дербес түрде жоғарыда айтылған талаптарға жауап беретін полиномиал кодтарды құру жолын тапты.

Бұл кодтар авторлардың атымен ***БЧХ-кодтары*** деп аталды.

Бұл типті кодтар екілік болмауы да мүмкін; мысалы, амалда кең қолданылатын Рид-Соломон кодтары. Егерде $x^j + 1$ ($j = 2^k - 1$ болғанда) g(x) ке қалдықсыз бөлінсе және *j*-дің басқа ешқандай да кем мәндерінде бөлінбесе, *к* орынды g(x) көпмүшелігі ***қарапайым*** **(*анайы*)** деп аталады. Мысалы, $g(x) = 1 + x^2 + x^3$ көпмүшелігі анайы болады; себебі ол $x^7 + 1$ ді бөледі; ал $j < 7$ де $x^j + 1$ ді бөлмейді.

БЧХ-кодтары мен Файр кодтарын төменде толық қарастырамыз.

Рид-Соломон кодтары

БЧХ кодтары қалағанша ұзындықты және жылдамдықты кодтардың үлкен класын құрады. Бұл кодтардың абзалдығы - олардың параметрлерінің оңай және иілгіш түрде екендігінен ғана емес, сонымен бірге, жиынтықтың ұзындығы бірнеше жүзге жеткенде, сол параметрлердегі (жылдамдық пен ұзындық) кодтардың арасында көпшілігі тиімді болады.

Осы БЧХ кодтарының ішінде өте маңызды кіші класы $m = m_0 = 1$ болған кодтар бар; бұл кодтар Рид-Соломон кодтары.

Осы екілік болмаған кодтар $GF(q)$ өрісінің үстінде анықталған болып, оның жиынтығының ұзындығы $n=q-1$ болады; ал құраушы полиномы келесідей анықталады: $g(x) = (x - \alpha)(x - \alpha^2)..(x - \alpha^{2t})$.

Айта кететін жай, $g(x)$ дәрежесі $2t$ болып, *t* ретті қателігін түзету үшін, $2t$ тексеруші таңбалар керек болады.

Әдетте q=2m мәні алынады.

Мұнда код 2m-ші қателерді, яғни түйіншектерді түзетуге мүмкіндік береді. Мұндай кодтар екі орынды “каскадты кодттауда” қолданылады.

7.7. Зертханалық жұмыс

Ұзындығы 7 ге тең болған және екі таңбалы қатені түзететін Рид-Соломон кодының құраушы полиномын құрайық.

$GF(8)$ орындалуы кестеде берілген болады. Жоғарыдағы теңдеуді қолданып, құраушы полиномды мына түрде құрамыз:

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3 .$$

Сонымен, $g(x)$ (7,4) кодын құрады; ол барлық екілік қателерді түзетеді.

Айта кететін жай, құраушы полиномның еселіктері әдетте $GF(8)$ элементтері болады.

Рид-Соломон (n,k) кодының спектрі $1 \le j \le n-k$ болғанда $A_0 = 1, A_j = 0$ түрінде көрінеді:

$$A_j = C_n^j \sum_{h=0}^{j-1-(n-k)} (-1)^h C_j^h \left(q^{j-h-(n-k)} - 1\right),$$ мұнда n-k+1 ≤ j ≤ n.

Рид-Маллер кодтары.

Рид – Маллер кодтары екілік топтық кодтары болып, қосымша жұпқа тексерушісі бар циклдік кодтарға эквивалентті болады.

Анықтамасы.

Айталық v_0 - барлық құрамдас бөліктері 1-ге тең вектор.

Айталық $v_1, v_2, ..., v_m$ матрицаның қатарлары болып, оның бағандары ұзындығы m болған барлық екіліктер жиыны болсын.

***r* - дәрежелі Рид-Маллер коды** базис ретінде мыналарды қамтиды:

- барлық $v_0, v_1, v_2, ..., v_m$ векторларын;

- барлық құрамдас бөліктерінің r - орынды немесе одан кем векторларының көбейтіндісін қамтиды.

Осы анықтамада $a = (a_1, ..., a_n)$, $b = (b_1, ..., b_n)$ векторлардың компонентті көбейтіндісі келесідей көрсетіледі: $ab = (a_1 b_1, ..., a_n b_n)$.

r - орынды Рид-Маллер коды кез келген m – мәні үшін мына параметрлерге ие болады: $n = 2^m, k = \sum_{j=0}^{r} c_m^i, d = 2^{m-r}$.

Мұнда *r* - орынды код (*m*-*r*-1) орынды кодқа **дуалды** болады.

Бірінші орынды кодтар максимал ұзындықты кодтармен өте тығыз байланысты болады. Егерде максимал ұзындықты кодтан бастап оны жұпқа жалпы тексеруді қосып кеңейтсек, **ортогонал код** аламыз.

Осы кодтың ұзындығы $n = 2^m$ болады және әрбір нөл емес код сөзінің салмағы $d = 2^{m-1}$ болады. Сөйтіп, кез келген екі код сөзі 2^{m-1} жайғасымдарда сәйкес келіп, басқа қалған 2^{m-1} жайғасымдарда айырмашылығы болады.

Қарама-қарсы сигналдармен осы кодты қолдана отырып, 2^m код векторлары үшін 2^m ортогонал сигналдар жиынын аламыз. Осыдан **ортогонал код** деген ат қалған. Бірінші орынды Рид-Маллер коды ортогонал кодқа тек бірлерден құралған код сөзін қосумен алынады.

Егер жіберілетін сигналдарды қарастырсақ, бұл шара бастапқы ортогонал сигналдар жиынына қосымша сигналдарды қосқанға эквивалентті болады.

Осы себепті алынған кодқа **биортогоналды** деп атайды.

Ортогонал және биортогонал кодтардың сипаттары максимал ұзындықты кодтардың сипатына өте жақын болады.

Алайда когерентті жүйелерде биортогоналды кодтар жиірек қолданылады; себебі олар орындалуы кезінде кейбір абзалдықтарға ие болады.

Олардың негізгі кемшілігі - өте төмен жылдамдығы.

Төменгі кестеде ұзындығы 8 ге тең болған Рид-Маллер кодының базисті векторлары берілген.

Бірінші орынды кодты алу үшін құраушы матрицаның қатары ретінде v_0, v_1, v_2, v_3 алу керек.

Екінші орынды код алу үшін осы матрицаға v_1, v_2, v_1, v_3, v_2, v_3 қатарларды қосу керек болады. Ақыры, үшінші орынды кодты алу үшін матрицаға мына v_1, v_2, v_3 қатарды қосу керек.

Рид-Маллер кодының тағы бір абзалдығы, бұл кодтарда және жақын кодтарда (эвклидті-геометриялық және жобалық-геометриялық) табалдырықты декодтауды қолданып декодтауды орындау мүмкін болады.

$$\nu_0 = (11111111)$$
$$\nu_1 = (00001111)$$
$$\nu_2 = (00110011)$$
$$\nu_3 = (01010101)$$
$$\nu_1\nu_2 = (00000011)$$
$$\nu_1\nu_3 = (00000101)$$
$$\nu_2\nu_3 = (00010001)$$
$$\nu_1\nu_2\nu_3 = (00000001).$$

7.4 Файр кодтары

Бірлік және көршілес болған екі қателерді түзетуші кодтарды қарастыра отырып, екі қателік детекторының сұлбасы керек екенін көрдік. Мұндай сұлба екі ажыратылған синдромдарға қарай бапталған болады.

Ажыратылған синдромдар саны көп болғанда, мысал үшін әжептеуір ұзын қателік түйіншегі түзету кезінде, мұндай жол қабылданбайды; себебі декодтау сұлбасы өте күрделі болады.

Сондықтан да декодтау сұлбасында қателік детекторы керекті болған ажыратылған синдромға автоматты түрде бапталатын кодтар жаратылған.

Бұл бөлу сұлбасының жәрдемінде екінші таңдалған көпмүшелікте орындалады. Осындай кодтардың құраушы көпмүшелігі екі көпмүшелік көбейтіндісі түрінде көрсетіледі:

$$g(x) = g_1(x)g_2(x).$$

Мысал ретінде Файр кодтар класын қарастырамыз, оның құраушы көпмүшелігі:

$$g(x) = p(x)\left(x^{2b-1} + 1\right). \qquad (7.15)$$

Мұнда p(x) — келтірілмейтін көпмүшелік болып, оның дәрежесі $m >= b$ болады және мынаның дәрежесіне тиісті болады: $e = 2^{m-1}$; b — түзетілетін қателік түйіншегінің ұзындығы.

Арнадан келетін код $h(x)$ қисындастыруын бұзылмаған код қисындастыруы $f(x)$ және қателік түйіншегіне сәйкес вектор $B(x)$-тің модул екі бойынша қосындысы ретінде көрсетеміз, яғни:

$$h(x) = f(x) + x'B(x), \qquad (7.16)$$

мұнда x' қателік векторы $B(x)$ дағы қателік дестесін сипаттайды.

$f(x)$ векторы $g1(x)$ және $g2(x)$ көпмүшеліктердің әрбіріне қалдықсыз бөлінеді.

Сондықтан декодтау үдерісін талдауда $x'B(x)$ векторымен шектелеміз.

Айта кететін жай, қателік түйіншекдегі дәрежелер саны мен құраушы көпмүшелік $m = b$ дәрежесі арасындағы қатысты таңдап алғанымызда әртүрлі түзетілетін қателік түйіншектерінің **жиыны** өз кезегінде $p(x)$-ке бөлгенннен қалған қалдықтар жиынының өзі болады.

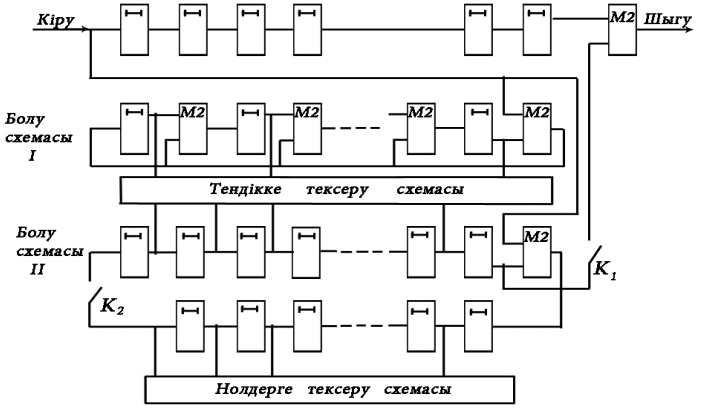
Қателік түйіншегінің n - тактындағы қалдығы ретінде (ажыратылған синдромның) $h(x)$-тің үлкен орындарында қателіктің көпмүшелігінің өзін алған жөн.

Сонда кейінгі тактарда оны түзету буынына буфер регистрінен $h(x)$ тізбегіне синхрон түрде шығарып, бұзылған таңбаларды оңай түзетсе болады.

Төмендегідей сұлбаны істетсек, n - тактағы қалдықты алу мүмкін болады; мұнда бөлу бірінші тактен басталып, $h(x)$ ті x^m ге көбейтумен аяқталады.

Келіп түсетін код қисындастыруылары уақыт аралығында таралған жағдай үшін Файр кодының декодтау сұлбасы 7.3 - суретінде көрсетілген.

$h(x)$ тің 1 - бөлу сұлбасына [$P(x)$ көпмүшелігіне] түсу кезінде ол сұлбада заңды түрде $B(x)$ қалдықтары тізбектеле бастайды; қалдықтардың бірі бірінші рет (2^{m-1}) - ші тактісінде көрінеді.



7.3-сурет

Сондықтан оның n-ші тактте көрінуі үшін барлық дәрежелер саны 2^{m-1}-ге ретті болуы керек.

$h(x)$ ті $(2b-1)$ көрсеткішіне тиісті болған $x^{2b-1}+1$ көпмүшелігіне бөлу үдерісінде $(2b-1)$ қалдықтар пайда болады.

Мына $B(x)x^{b-1}$ түрдегі вектор қалдықтың бірі болады.

Ол бірінші рет $(2b-1)$ - тактінде пайда болып, кейін ол циклді түрде $(2b-1)$ тактты кезеңімен қайталанып отырады.

Егеде біз осы қалдықты қателік детекторында қалдырғымыз келсе, яғни оны n-ші тактте алу керек болса, онда n саны $(2b-1)$-ге ретті болуы керек.

Қателік детекторы алдын ала істеп кетпеуі үшін 2^{m-1} және $2b-1$ сандары өзара жай сандар болуы керек; ал n саны олардың ең кіші ретті саны (бөлгіші) болуы керек. Екі бөлу сұлбаларындағы регистрлердегі $B(x)$ қалдықтарының теңдігі және 2 – бөлу ($x^{b2}+1$ көпмүшелігіне) сұлбасының басқада (b — 1) орындарының нөлге теңдігі табылған қателіктер түйіншегін түзету шартын көрсетеді және сұлба жолымен орнатылады.

Түйіншекті түзету мүмкіншілік шарты анықталған соң $K1$ кілті қосылады, ал $K2$-кілті ажыратылады.

Түзету сұлбасына (екілік модулі бойынша қосу) бір уақытта буфер регистрінен $B(x)$ таңбалары және 2-бөлу сұлбасының таңбалары шығарыла бастайды. Мұнда $h(x)$ векторындағы $B(x)$ қателік түйіншегі жойылады.

Жалпы жағдайда, $B(x)$ үлкен дәрежесіненорыннан емес, j - дәрежесінен бастална, n-ші тактте пайда болған қалдықтарды теңестіру үшін оларды тізбекті түрде x ке көбейтіп, бір сұлбада $p(x)$ модуліне келтіру керек; ал екінші сұлбада $(x^{2b-1}+1)$ модуліне келтіру керек болады.

Егер түйіншек j-ші орыннан бастална, онда регистрлердегі қалдықтар теңеспестен тұрып қосымша $(n-j)$ тактгерін істеу керек; мұнда $h(x)$ ті x^{m*j} көбейту есебінен оның мәні 1 ден n- ге дейін өзгереді.

$(n — j)$ қосымша жылжытудан соң буфер регистріндегілер жылжып, қате таңбалар және де түзету сұлбасының алдында болады.

Егерде $h(x)$ буфер регистрінен шығару уақытында түзетуді орындау шарттары орындалмаса, онда түзетілмейтін қателік анықталады.

7.8 Зертханалық жұмыс

Қателіктер түйіншегін келесідей құраушы көпмүшелікпен құрылған Файр кодымен түзету үдерісін қарастырайық: $g(x) = (x^3 + x^2 + 1)(x^5 + 1)$.

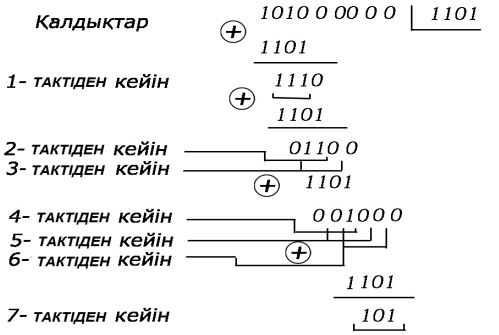
Код үш таңбадан тұратын қателігі бар (b = 3) түйіншекті түзете алады.

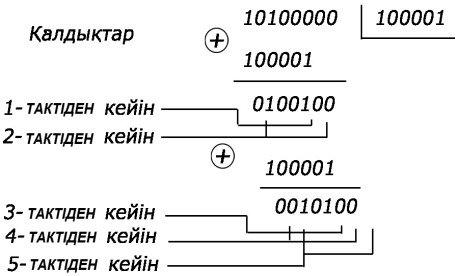
Код қисындастыруының ұзындығы $n = (2^3 — 1)(2 \cdot 3^{-1}) = 35$.

Айталық нөлдік код қисындастыруындағы үш жоғары дәрежелерде $B(x)$ = 101 қателік пайда болды делік. $B(x)$-ті $g1(x) = x^3 + x^2 + 1$-ке бөлгенде $B(x)$ қалдығы регистрде 7 тактілі кезеңмен пайда болады.

Ақиқаттан да, $B(x)$-ті $g2(x) = x^5 + 1$-ге бөлгенде $B(x)x^b$-1 қалдықтарының тізбектеліп алмасуы 5 такт кезеңімен өтеді.

Декодтау құрылғысының кіруіне нөлдік код қисындастыруы түсіп, оның жоғары орындарында 101 қателікті түйіншек болғанда 1-ші және 2-ші бөлу сұлбаларының регистрларындағы қалдықтарының өзгеру кезегін қарайық.





Бұл өзгерістер 7.8-кестесінде көрсетілген. Бөлу сұлбасының спецификациясына байланысты k тактта бірінші b — 1 қалдықтар бағандарды бөлгеннен ерекше болады.

7.8-кесте

Такт нөмірі	Бөлу 2-сұлб. регистрдегі қалдық	Бөлу 1-сұлб. регистрдегі қалдық
1	01001	111
2	11010	011
3	00101	110
4	01010	001
5	$\underline{(10100)}\, B(x)x^{b-1}$	010
6	01001	100
7	10010	(101)
8	00101	111
9	01010	011
10	(10100)	110
11	01001	001
12	10010	010
13	00101	100
14	01010	(101)
15	(10100)	111
.	.	.
.	.	.
	.	.
28	00101	(101)
29	01010	111
30	(10100)	011
31	01001	110
32	10010	001
33	00101	010
34	01010	100
35	(10100)	(101)

Қателіктер түйіншегінің түзетілуінің мүмкіншілік шарттары 35-тактісінде орындалады. Одан кейінгі 3-тактісінде буфер регистрінен код қисындастыруын түзету сұлбасына шығаруда қателік түйіншегі жойылады.

7.4.1 Циклдік кодтарды мажоритарлық декодтау

Циклдік кодтың бір немесе бірнеше код қисындастыруына табылған бақылау жүйесі осы код қисындастыруының барлық таңбаларын декодтау үшін қолданылуы мүмкін. Себебі бақылау қатыстарына кез келген код қисындастыруы жауап береді; соның ішінде циклдік жылжумен алынған қисындастыруы да болады. Сонымен, a_{i+k} таңбасын декодтау үшін k жылжыту жеткілікті болады; және сол мажоритарлық бағдаржолмен «көпшілік бойынша» шешім қабылдау да жеткілікті болады. Мұнда негізгі қиындық бақылау жүйесін табу болады. Циклдік кодтарда тексеруші теңдеулер жиынын рекуррентті қатыстардан табу мүмкін болады. Бақылаушы теңдеулерді жазық түрде көрсетеміз:

$$\begin{aligned} &h_0 a_0 \oplus h_1 a_1 \oplus \ldots \oplus h_{k-1} a_{k-1} \oplus a_k = 0, \\ &h_0 a_1 \oplus h_1 a_2 \oplus \ldots \oplus h_{k-1} a_k \oplus a_{k+1} = 0, \\ &h_0 a_{n-k-1} \oplus h_1 a_{n-k} \oplus \ldots \oplus h_{k-1} a_{k+2} \oplus a_{n-1} = 0. \end{aligned} \qquad (7.17)$$

Осы жүйеден қандай да бір a таңбасын және кейбір таңбалардың жалғыз бір қосындысын таңдаймыз; сол теңдеулерді сол таңбаларға байланысты шешеміз. Мұнда келесідей жағдай болуы мүмкін:

1. Әрбір бақылаушы теңдеу кейбір a таңбасын басқа таңбалардың сызықты қисындастыруымен көрсетуі мүмкін болады және ол таңбалар еш қандай басқа теңдеулерге қатыспайды (ажыратылған тексерулер жүйесі).

2. Тек қандай да бір таңбалар қосындысы үшін ажыратылған тексерулер жүйесін құру мүмкін болады (квазиажыратылған тексерулер жүйесі).

3. Әрбір бақылаушы теңдеу қандай да бір ai таңбасын басқа a_j таңбаларының сызықты қисындастыруы арқылы көрсетуі мүмкін болады; алайда осы таңбаның басқа теңдеулерде қайталануын жою мүмкін болмайды.

Егерде еш болмағанда бір a таңбасы ($i \neq j$ болғанда) λ теңдеуіне қатысатын болса және ешқандай басқа a_j теңдеулеріне қатыспайтын болса, осындай жүйе λ - байланысты делінеді.

Жоғарыда қаралған жағдайларда мажоритар қағидасы қолданған декодтау құрылғыларының техникалық орындалуы мүмкін болады.

Ажыралған тексеру жүйесін қолданған кодтарда оның техникалық орындалуы ең оңай болады. Сондықтан тек соны қарастырамыз.

7.9 ***Зертханалық жұмыс***

Ажыратылған тексеру жүйесін құрайық және (7,3) циклдік кодының құраушы көпмүшелігі $g(x) = (x+1)(x^3 + x + 1)$ болса, оған декодтау құрылымының сұлбасын құрайық; бұл бірлік қателерді түзетіп, екілік қателерді табады ($d = 4$). Генераторлы көпмүшелікті табамыз:

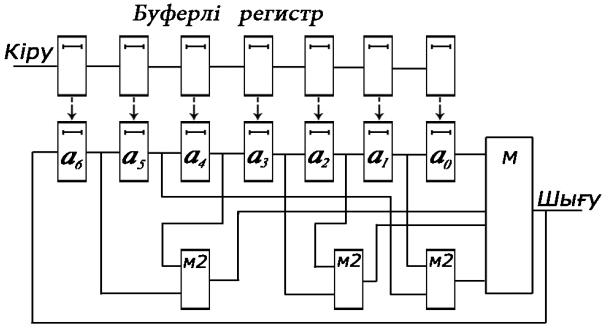
$$h(x) = \frac{x^7 + 1}{x^4 + x^3 + x^2 + 1} = x^3 + x^2 + 1.$$

Жоғары дәреже таңбасы $a0$ ді әртүрлі таңбалар арқылы көрсетіп және оған тривиал $a_0 = a_0$ тексеруді қосып, мына жүйені аламыз:

$$a_3 = h_0 a_0 \oplus h_1 a_1 \oplus h_2 a_2, a_3 = a_0 \oplus a_2;$$
$$a_4 = h_0 a_1 \oplus h_1 a_2 \oplus h_2 a_3, a_4 = a_1 \oplus a_3;$$
$$a_5 = h_0 a_2 \oplus h_1 a_3 \oplus h_2 a_4, a_5 = a_2 \oplus a_4;$$
$$a_6 = h_0 a_3 \oplus h_1 a_4 \oplus h_2 a_5, a_6 = a_3 \oplus a_5;$$

Келесідей тексеруші теңдеулерді жазамыз:

$$a_0 = a_4 \oplus a_6;\ a_0 = a_1 \oplus a_5;\ a_0 = a_4 \oplus a_6;\ a_0 = a_0. \quad (7.18)$$



7.4-сурет

Осыған сай декодтау құрылғысы төмендегі 7.4-суретте көрсетілген.

Буферлі регистрге келіп түсетін код қисындастыруы параллел түрде декодердің регистріне де түседі. Кейінгі әрбір n тактерінде мажоритар M элементінің кіруінде (7.18) теңдіктеріне сәйкес сигналдар қалыптасады.

Бірлік қателік бар болғанда бұзылған сигнал мажоритарлық элементтің төрт кірулерінің ішінде тек біреуінде ғана болады және мажоритарлық элемент кірудегі бұзылмаған сигналдардың көпшілігі бойынша шығудағы a_0 дұрыс шығу сигналын қалыптастырады.

Кезекті жылжытудан соң келесі таңбаның мәні жоғарыда айтылғандай табыла береді.

7.9 - кестесі мажоритар декодтау үдерісін көрсетеді; мұнда бірлік қателік төртінші орында болып, код қисындастыруы 1001110 болады.

7.9-кесте

Такт нөмірі	Регистр ұяшықтарының орны							Мажор. элем.кіруі	Шығу
	a_8	a_5	a_4	a_3	a_2	a_1	a_0		
1	0	1	1	0	0	0	1	0111	1
2	1	0	1	1	0	0	0	1000	01
3	0	1	0	1	1	0	0	0100	001
4	0	0	1	0	1	1	0	1110	1001
5	1	0	0	1	0	1	1	1111	11001
6	1	1	0	0	1	0	1	1111	111001
7	1	1	1	0	0	1	0	0000	0111001

Мына жағдайда, яғни мажоритар элементтің екі кіруінде сигнал «1», ал басқа екі кіруінде «0» болып, екілік қателікті таба алады.

7.5 Боуз –Чоудхури -Хоквингем кодтары.

Математикалық кіріспе.

Хэммингтің жалпыланған коды болып, ретті қателіктерді түзетеді**.** Мұндай кодтарды құраушы (жасаушы) көпмүшеліктердің түбірлері арқылы көрсетсе болады.

Анықтамасы.

т қателікті түзететін БЧХ анайы коды, бұл GF(q) өрісінің үстінде ұзындығы $n = q^m - 1$ ***тең болған жиынтықты код болып, оның үшін*** $\alpha^{m_0}, \alpha^{m_0+1}, ..., \alpha^{m_0+2t-1}$ ***(кез келген*** m_0 ***үшін) элементтері g(x) құраушы көпмүшеліктің түбірлері болады; мұнда*** α ***-*** $GF(q^m)$ ***өрісінің анайы элементі.***

Сондықтан БЧХ – кодтардың құраушы көпмүшеліктерін мына түрде жазса болады: $g(x) = HOK\left[m_{m_0}(x)\ m_{m_0+1}(x), ..., m_{m_0+2t-1}(x)\right]$.

Мұнда $m_0 = 1$ болғанда тар мағыналы БЧХ кодтары болады. БЧХ -ның анайы болмаған кодтары дәл осындай табылады; бірақ ***α***

α $GF(q^m)$ өрісінің анайы болмаған β – элементіне алмастырылады; ал жиынтықтың ұзындығы

β- ның дәрежесіне тең болады.

БЧХ – кодтар деп аталушы кодтар циклдік кодтардың кез келген s ретті байланыссыз қателіктерді түзететін үлкен класына жатады.

Олардың минималды код қашықтығы $d_{min} = 2s + 1$ кем болмайды.

Жалпы жағдайда осы түсініктер еселіктері $GF(q)$ (мұнда q –жай сан) өрісінде болған көпмүшеліктер жиыны үшін орынды болады. Бізді екілік кодтар қызықтырғаны үшін $q = 2$ мен шектелеміз.

Өткенде сақинаны айырымдар класына идеал бойынша жіктеу қарастырылған еді (7.4-кесте). Егер идеал $g(x)$тің құраушы көпмүшелігі ретінде m орынды келтірілмейтін көпмүшелікті алсақ және ол $n(n = 2^m—1)$ дәреже көрсеткішіне қарайтын болса, онда айырымдар класының жалпы саны, идеалды қосқанда, *2^m* болады. Алынған айырымдар класы үшін қосу және көбейту амалдарын көрсетеміз:

$$(r_i(x) + (r_j(x) = (r_i(x) + r_j(x) \bmod g(x)$$
$$(r_i(x) * (r_j(x) = (r_i(x) * r_j(x) \bmod g(x) \qquad (7.19)$$

мұнда $(r_j(x))$ - $g(x)$ көпмүшелік модулімен айырымдар класы болып, $r_i(x)$ элементін өз ішіне алады.

Мұнда айырымдар кластарының жиыны шекті өріс құрады.

Ол 2^m элементтерден құрылған болып, $GF(2^m)$ деп таңбаланады және $GF(2)$ ***үстінен өрістің т орынды кеңеюі*** деп аталады.

Өрістің бірлік және нөлдік элементері сәйкес (1) және (0) айырымдар кластары болады.

Өрістің кез келген нөл емес элементі (r_α (x)) үшін оған кері элемент $(r_b(x))$ табылып, ол мына теңдікті қанағаттандырады:

$$(r_\alpha(x) * (r_b(x) = (r_\alpha(x) * r_b(x) = (1)$$

7.10 ***Зертханалық жұмыс***

Қысқартылған БЧХ кодтың ұзындығы 7-ге тең болып, екілік қателерді түзететін болсын. Оның құраушы полиномын құру үшін оның түбірлерін табамыз: $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha -$ $GF(8)$- тің анайы элементі болсын.

$GF(8)$ орындалуы кестеде берілген болады.

Талап етілген түбірлердің минималды қатыстарын есептейміз:

$$m_1(x) = m_2(x) = m_4(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4) = x^3 + x + 1,$$
$$m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^5) = x^3 + x^2 + 1.$$

Сонымен құраушы полином мына түрде болады:

$$g(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Бұл полином тривиалды (7,1) - қайталанушы кодын құрады.

Ақиқаттан да бұл кодтың код қашықтығы d=7 болып, барлық үштік қателіктерді түзетеді.

Бұл таңқаларлық нәрсе емес; кейде БЧХ ның түзетуші қабілеті теориялықтан асып кетеді.

7.11 Зертханалық жұмыс

$g(x) = x^4 + x + 1$ келтірілмейтін көпмүшелігін қолданып, 24 орынды өріс құрамыз. Айырымдар класының толық жиыны кез келген көпмүшелікті $p(x)$ көпмүшелігіне бөлгенде қалған қалдықтар санына тең болады.

Берілген көпмүшелік үшін бұл 16 айырымдар класын құрады: (0), (1), (x), (x+1), (x^2), (x^2+1), (x^2+x), (x^2+x+1), (x^3), (x^3+1), (x^3+x), (x^3+x^2), (x^3+x+1), (x^3+x^2+1), (x^3+x^2+x), (x^3+x^2+x+1).

Өрістің элементтерін қосу кестесін құру оншалық қиын болмағандықтан, осы элементтердің көбейту кестесімен шектелеміз.

α арқылы (x) айырымдар класын таңбалайық; ол x көпмүшелігін қамтитын болсын; одан нөлдік элементті алып тастап, 7.10*а*-кестесін шығарамыз.

7.10*а*-кесте

	1	α	$\alpha+1$	⋯	$\alpha^3+\alpha^2+\alpha+1$
1	1	α	$\alpha+1$	⋯	$\alpha^3+\alpha^2+\alpha+1$
α	α	α^2	$\alpha^2+\alpha$	⋯	$\alpha^3+\alpha^2+1$
$\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	⋯	α
α^2	α^2	α^3	$\alpha^3+\alpha^2$	⋯	α^3+1
⋮	⋮	⋮	⋮	⋮	⋮
$\alpha^3+\alpha^2+1$	$\alpha^3+\alpha^2+1$	α^3+1	α^2		1
$\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	1		α^2
$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+1$	α		$\alpha^3+\alpha$

Осы мысалдан көрініп тұрғаны, көпмүшелік түрінде көрсетілген өріс элементтерін көбейтумен кесте құру әжептеуір қиын мәселе.

Алайда өріс элементтерін оның бір элементінің дәрежесі түрінде көрсетсек, мәселе оңайласады.

*Кез келген **шекті өрісте** ең болмағанда бір α элементі табылып, осы өрістің барлық нөлсіз элементтері осы элементтің әртүрлі дәрежесі α^i түрінде көрсетіледі; ал осы элемент **қарапайым** деп аталады.*

Өріс шекті болғандықтан ол $n=2^m-1$ нөлсіз элементтерден құралған болады; онда $\alpha^n = 1$ элементтерден бастап өріс қайталана бастайды.

Өріс элементтері α-ның кері дәрежесімен де көрсетіледі, себебі өріс әрбір нөлсіз элементтің мультипликативті кері элементін де қамтиды.

Базис ретінде α^{m-1}, α^{m-2}, ..., α, 1 элементтерін қолданып, өріс элементтерін екілік тізбектер түрінде де көрсету мүмкін (векторлы көрсету).

7.12 Зертханалық жұмыс

Келтірілмейтін көпмүшелік $g(x) = x^4 + x+1$ негізінде әртүрлі құрылған өріс элементтерін келтіреміз (кесте 7.10б).

7.10 б-кесте

Орынды көрсету		Көпмүшелікті көрсету				Векторлы көрсету
a^0	a^{-15}				1	0001
a^1	a^{-14}			α		0010
a^2	a^{-13}		α^2			0100
a^3	a^{-12}	α^3				1000
a^4	a^{-11}			α	+1	0011
a^5	a^{-10}		α^2	$+\alpha$		0110
a^6	a^{-9}	α^3	$+\alpha^2$			1100
a^7	a^{-8}	α^3		$+\alpha$	+1	1011
a^8	a^{-7}		α^2		+1	0101
a^9	a^{-6}	α^3	+	α		1010
a^{10}	a^{5-}		α^2	$+\alpha$	+1	0111
a^{11}	a^{-4}	α^3	$+\alpha^2$	$+\alpha$		1110
a^{12}	a^{-3}	α^3	$+\alpha^2$	$+\alpha$	+1	1111
a^{13}	a^{-2}	α^3	$+\alpha^2$		+1	1101
a^{14}	a^{-1}	α^3			+1	1001

Элементтерді α- нің кері дәрежесімен көрсету оны $\alpha^{15} = 1$-на бөлумен орындалады. Енді мынаны көрсетейік; шекті өрістің кез келген 2^m орынды элементі $x^{2^m} + x = 0$ теңдеуінің түбірі екенін көрсетейік.

Өрістің нөлсіз элементтері үшін мынаған ие боламыз:

$$x^{2^m-1} + 1 = x^n + 1 = 0 . \qquad (7.20)$$

Егер α - өрістің жай элементі болса, онда кез келген нөлсіз элемент α ның дәрежесі түрінде көрсетіледі, яғни $\beta = \alpha^i$.

Онда $\beta^{2m-1} = \alpha^{(2m-1)i} = 1$ және, сондықтан өрістің барлық нөлсіз элементтері $x^n + 1 = 0$ теңдеуінің түбірлері болады. Осы түбірлер $GF(2)$ өрісіндегі әртүрлі келтірілмейтін көпмүшеліктерге жатады; оларға $x^n + 1$ екімүшелігі жіктеледі. Осындай жіктеудің бағдаржолдары алдын келтірілген еді.

Мысалы, 7.13 зертханалық жұмыста көпмүшеліктер жиыны алынған болып, олардың түбірлері $GF(24)$ өрісінің элементтері болатын:

$$x^{15} + 1 = (x+1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x + 1) = (x^4 + x^3 + 1) *$$
$$*(x^4 + x^3 + x^2 + x + 1).$$

$x^n + 1$ екімүшеліктің түбірлері келтірілмейтін көпмүшеліктің құраушылары бойынша қалай таралған екендігі бізге қызық. Мына заңдылық дәлелденген;

- егер m орынды келтірілмейтін көпмүшеліктің түбірлерінің бірі β мәлім болса, онда осы көпмүшеліктің барлық басқа түбірлері β-ның анықталған дәрежелері болады, яғни: $\beta, \beta^2 \beta^4, ..., \beta^{2^{m-1}}$ **.**

Келтірілмейтін көпмүшеліктің түбірлерінің дәрежесі негізгі көрсеткіш болып, ол көпмүшелікке тән болады.

Ең кіші орынды $g(x)$ көпмүшелігі β элементі үшін минимал көпмүшелік деп аталып, мұнда $g(\beta)=0$ болады. Оны $g\beta(x)$ деп таңбалаймыз.

$GF(2)$ өрісі үстіндегі m орынды келтірілмейтін көпмүшелік жай деп аталады, егерде оның түбірі $GF(2^m)$ өрісінің жай элементі болса.

7.13 ***Зертханалық жұмыс***

Екімүшеліктің түбірлерінің таралуын табамыз:

$$x^{15}+1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)=(x^4+x^3+x^2+x+1).$$

Егер түбірлерді өріс элементтері деп қарасақ және өріс келтірілмейтін $g(x) = x^4 + x + 1$ көпмүшелікті қолданумен құрылған болса, онда көпмүшелік жай немесе қарапайым болады.

Ақиқатан да, $GF(2^4)$ өрісінің α анайы элементі $g(x)$ көпмүшелігінің түбірі болады. Оның басқа түбірлері сәйкес түрде мыналарға тең болады: α^2 , α^4 и α^8. Мына теңдеудің ақиқаттығына сенсе болады:

$$g_\alpha(x)=x^4+x\ +1=(x+\alpha\ )(x+\alpha^2)(x+\alpha^4)(x+\alpha^8).$$

Енді α^3 элементі үшін минималды көпмүшелік $g3(x)$ ті табамыз.

Оның түбірлері мына элементтер болады:

$$\beta=\alpha^3,\beta^2=\alpha^6,\beta^4=\alpha^{12},\beta^8=\alpha^{24}=\alpha^9,$$

$$g_{\alpha^3}(x)=(x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^9)=x^4+x^3+x^2+x+1.$$

осыдан .

Дәл осындай α^5 және α^7 элементтеріне минималды $g5(x)$ және $g7(x)$ көпмүшеліктерін анықтаймыз. $g5(x)$ тің түбірлер циклі α^5 және α^{10} қамтиды;

$g7(x)$ үшін сәйкес түрде α^7, α^{14}, α^{13}, α^{11}ларды аламыз.

Сондықтан:

$$g_{\alpha^7}(x)=(x+\alpha^7)(x+\alpha^{14})(x+\alpha^{13})(x+\alpha^{11})=x^4+x^3+1.$$

Сонымен, $x^{15} + 1$ көпмүшелігінің 14 түбірі таралды. Ақырғы түбір α^0 1-ге тең болып, $x + 1$ екімүшелігіне сәйкес келеді.

Кодтарды құру мен орындалуы ету

Боуз — Чоудхури — Хоквингем кодының құраушы көпмүшелігін таңдау үдерісі, егер ол бірлік қателікті түзетуге арналған болса, алдын жоғарыда көрсетілгеннен ешбір ерекшелігі жоқ болады.

Негізгі ерекшелігі - қателік синдромдарын интерпретация етуде.

Қаралып отырған жағдайда $GF(2^m)$ өрісінің примитив элементтерінің әртүрлі дәрежелері қателік синдромы ретінде қаралады.

Ол m орынды $g(x)$ таңдалған келтірілмейтін көпмүшелікті қолданумен құрылып, дәреженің $n = 2^m$—1 көрсеткішіне сәйкес келеді.

Примитив элементтің дәрежелерімен көрсетілген өрістің әртүрлі нөлсіз элементтерінің саны n-ге тең болғандықтан, әрбір бөлек орындағы қателік векторына өзінің синдромын

сәйкестендіру мүмкін болып, бұл қателікті түзету мүмкіндігін міндеттемелейді.

Екі қателік пайда болғанда құрылған код осы қателіктердің синдромдарының тек s қосындысын ғана анықтайды: $\xi_i + \xi_j = s_l$,

Мұнда ξ_i және ξ_j i және j дәрежелеріндегі қателік синдромдары.

Қателіктерді бірмәнді анық табу үшін және дербес бір теңдеу керек.

Осында ξ нен орынды қатысты қолданса болады.

Алайда синдромдардың квадраты мақсатқа сай нәтиже бермейді; себебі екінші теңдеу модуль екі бойынша қосуды есептегенде біріншінің квадраты болады екен.

Ақиқаттан да, $\xi_i^2 + \xi_j^2 = s_2 = (\xi_i + \xi_j)^2 = s_1^2$.

Егерде синдромдардың кубын қолдансақ, онда теңдеулер өзара байланыссыз болады: $\xi_i + \xi_j = s_1, \xi_i^3 + \xi_j^3 = s_3$.

Осындай қарастыру 3- және 4-еселік қателіктерді түзету жағдайына жалпылауға мүмкіндік береді және с.с. Мұнда алынған теңдеулерге сәйкес түрде бесінші, жетінші орынды синдромды теңдеулер қосылады және с.с.

Екеулік қателерді түзету мәселесін анығырақ қараймыз.

Екінші орынды түрлендіруді қарастырамыз:

$$s_3 = (\xi_i + \xi_j)(\xi_i^2 + \xi_i\xi_j + \xi_j^2) = s_1(s_1^2 + \xi_i\xi_j),$$

осыдан: $\xi_i\xi_j = s_1^2 + s_3 / s_1$.

Синдромдардың қосындысы мен көбейтіндісі мәлім болғандықтан, Виета теоремасының негізінде ξ_i және ξ_j синдромдары түбірлер болатын теңдеу құру мүмкін: $\xi^2 + s_1\xi + (s_1^2 + s_3 / s_1) = 0$.

Егер қателік біреу болса, онда $\xi_i = s_1, \xi_i^3 = s_3$ және оның синдромы мына теңдеуді қанағаттандырады: $\xi_i + s_1 = 0$.

Қателіктер жоқ болғанда, нөлдік синдромдар аламыз, себебі $s_1 = s_3 = 0$ болады. Амалда қолданылатын көпмүшелік түбірлері қателіктер синдромы болмастан, ал олардың мультипликативті кері $z = \xi^{-1}$ элементтері түбір болатын көпмүшеліктерді қолдану жөн болады.

Екеулік қателіктерді түзету үшін теңдеудің сол жағы мына түрге түрленеді:

$$\sigma(z) = 1 + s_1 z + (s_1^2 + s_3 / s_1) = 0. \qquad (7.21)$$

Бір қателік пайда болғанда $\sigma(z) = 1 + s_1 z$. 7.22)

Қателік жоқ болғанда: $\sigma(z) = 1$.

Қателік синдромдарының тақ дәрежелерінің қосындысы қалай табылады?

Аталған соманы анықтау үшін тізбекті түрде таңдалған анайы көпмүшелік *g(x)*ке минимал көпмүшеліктердің көбейткіштері ретінде α^3 элементтерін (екеулік қателер), α^5 (үшеулік қателер) және с.с. қосумен анықталады.

Қателік синдромдарының тақ дәрежелер қосындысы қабылданған код қисындастыруын соған сәйкес минимал көпмүшелікке бөлу нәтижесінде қалған қалдықтардан табылады.

Жалпы жағдайда БЧХ кодының құраушы көпмүшелігі анайы және минималды көпмүшеліктердің ең кіші ортақ бөлгіші (ЕОБ-НОК) түрінде көрінеді:

$$g(x) = ЕОБ[g_a(x)g_{a^j}(x)...g_{a^{71-1}}(x)]. \qquad (7.23)$$

Мысал үшін, екеулік байланыссыз қателерді түзетін және n =15 болған код үшін мынаны аламыз:

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$

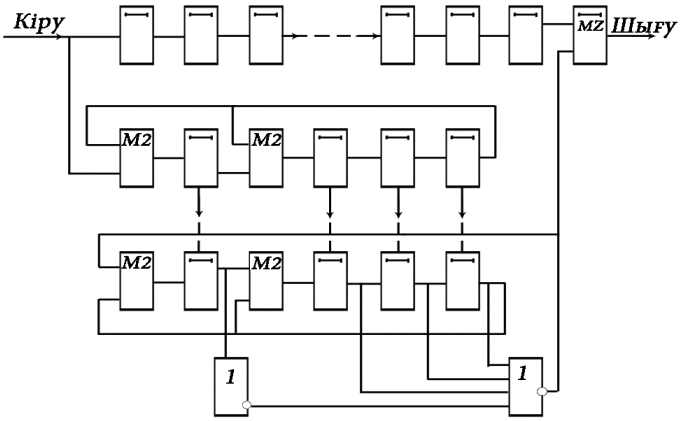
7.14 *Зертханалық жұмыс*

$g(x) = x^4 + x + 1$ құраушы көпмүшелігі бар Боуза - Чоудхури (15, 11) кодының бірлік қателікті түзету үдерісін қарастырайық.

7.10-кестесін қолданып, әрбір қателік векторына өзінің синдромын салыстырамыз; оның $GF(2^4)$ өрісінің анайы элементінің анық бір дәрежесі түрінде көрсетеміз. Нәтиже 7.11-кестесі түрінде көрсетілген.

7.11-кесте

Қателік векторлары	Қателік табушылар (синдромдар)	Синдромдардың $\alpha^3, \alpha^2, \alpha, 1$ базисіндегі векторлық көріністері
000000000000001	$\alpha^{-15} = \alpha^0$	0001
000000000000010	α^{-14}	0010
000000000000100	α^{-13}	0100
000000000001000	α^{-12}	1000
000000000010000	α^{-11}	0011
000000000100000	α^{-10}	0110
000000001000000	α^{-9}	1100
000000010000000	α^{-8}	1011
000000100000000	α^{-7}	0101
000001000000000	α^{-6}	1010
000010000000000	α^{-5}	0111
000100000000000	α^{-4}	1110
001000000000000	α^{-3}	1111
010000000000000	α^{-2}	1101
100000000000000	α^{-1}	1001



7.5-сурет

Декодтау сұлбасы 7.5-суретте көрсетілген. Қателік детекторы $1+s1z = 0$ теңдеуіне сәйкес құрылған.

Бірінші n = 15 тактінде байланыс арнасынан келетін $h(x)$ код қисындастыруын $g(x)$ ке бөлумен I регистрде қателік синдромы x^{-j} аламыз.

Содан соң ол сұлбаның II регистрінде синдромды α қосымша көбейтіп $g(x)$ модуліне келтіреді; яғни α^4 ті α + 1 ге келтіреді.

(n + 1)-ші такте $h(x)$ код қисындастыруының жоғары орынды таңбасы буфер регистрінен түзету қосындыторына келіп түседі.

Сонымен бір уақытта синдром α^{-j} ны α- ға қосымша көбейту орындалады және детектордың ИЛИ (НЕМЕСЕ) сұлбасына $1+si*\alpha$ векторы жіберіледі.

Егер $1 + s_1 \alpha$ нөлге (0) тең болмаса, онда $s_1 \alpha^{-1}$ -ге тең емес болады; сондықтан қателік жоғары орында болмағандығы анықталады.

Дәл осындай буфер регистрінен түзету түйініне тізбектеліп түсетін басқа таңбалар дұрыстығы талданады.

Түзету сұлбасында j-ші жайғасымындағы бұзылған таңба келіп түскенде (үлкен орыннан бастап), онда $1+s_1\alpha^j = 0$ және $s_1 = \alpha^{-j}$ болады. Мұнда детектордың ИЛИ (НЕМЕСЕ) сұлбасында шығу сигналы нөлге тең болады және НЕ (ЕМЕС) сұлбасының шығуындағы серпін қатені түзетеді.

7.15 ***Зертханалық жұмыс***

Келесідей құраушы көпмүшелігі $g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$ бар (15,7) кодының екілік қателікті түзету операциясының тізбегін қарастырамыз. Декодттау шарасында келесідей этаптарды ажыратамыз:

1) Байланыс арнасынан келген $h(x)$ код қисындастыруын $x^4 + x + 1$ көпмүшелігіне бөлумен қателік синдромдарының s_1 қосындысын табамыз;

2) $h(x)$ті $x^4 + x^3 + x^2 + x + 1$ көпмүшелігіне бөлумен $\alpha^9\ \alpha^6\ \alpha^1$ базисте синдромдардың $s3$ кубтарының қосындысын табамыз;

3) $\alpha^3\ \alpha^2\ \alpha 1$ базисінде s_3 өрнегін табамыз;

4) s_1^2, s_3/s_1 қатысын және $s_1^2 + s_3/s_1$ қосындысын есептеу;

$q(z) = 1+s_1z+(s_1^2 + s_3/s_1)z^2$ теңдеуінің түбірлерін анықтау сұлбасын құру; бұл $s1$- ны α- ға және $(s_1^2 + s_3/s_1)$- ны α^2 -ге қосымша көбейтумен орындалады.

Рид-Соломон кодтары.

БЧХ кодтары қалағанша ұзындықты және жылдамдықты кодтардың үлкен класын құрады. Бұл кодтардың абзалдығы олардың параметрлерін оңай және иілгіш түде екендігінде ғана емес, соны-

мен бірге, жиынтықтың ұзындығы бірнеше жүзге жеткенде, сол параметрлердегі (жылдамдық пен ұзындық) кодтардың арасында олардың көпшілігі тиімді болады.

Осы БЧХ кодтарының ішінде өте маңызды кіші класы $m = m_0 = 1$ болған кодтар бар; бұл кодтар Рид-Соломон кодтары. Осы екілік болмаған кодтар *GF(q)* өрісінің үстінде анықталған болып, оның жиынтығының ұзындығы n=q-1 болады; ал құраушы полиномы келесідей анықталады: $g(x) = (x-\alpha)(x-\alpha^2)..(x-\alpha^{2t})$.

Айта кететін жай, $g(x)$ дәрежесі 2t болып, t реті қателігін түзету үшін, 2t тексеруші таңбалар керек болады. Әдетте q=2m мәні алынады. Мұнда код 2m-ші қателерді, яғни түйіншектерді түзетуге мүмкіндік береді. Мұндай кодтар екі орынды "каскадты кодттауда" қолданылады.

7.16 *Зертханалық жұмыс*

Ұзындығы 7-ге тең болған және екі таңбалы қатені түзететін Рид-Соломон кодының құраушы полиномын құрайық.

GF(*8*) орындалуы кестеде берілген болады. Жоғарыдағы теңдеуді қолданып, құраушы полиномды мына түрде құрамыз:

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3 .$$

Сонымен, $g(x)$ (7,4) кодын құрады; ол барлық екілік қателерді түзетеді.

Айта кететін жай, құраушы полиномның еселіктері әдетте *GF*(8) элементтері болады.

Рид-Соломон (*n,k*) кодының спектрі $1 \le j \le n-k$ болғанда $A_0 = 1, A_j = 0$ түрінде көрінеді:

$$A_j = C_n^j \sum_{h=0}^{j-1-(n-k)} (-1)^h C_j^h \left(q^{j-h-(n-k)} - 1\right),$$ мұнда n-k+1$\le j \le n$.

VII тарудың бақылау және емтихан сұрақтары

1. Кедергілі арна үшін Шеннонның негізгі кодтау теоремасын түсіндіріңіз.
2. Ұзын таңбалар тізбегін кодтаудың абзалдығын түсіндіріңіз.
3. Қандай кодтарды кедергіге шыдамды деп атайды?
4. Неліктен кедергіге шыдамды кодтар қателіктерді анықтайды және түзетеді?
5. Жиынтықты және үздіксіз, ажыралатын және ажыралмайтын кедергіге шыдамды кодтарды сипаттаңыз.
6. Қателіктің дәрежесі деп нені түсінеміз?
7. Минималды код қашықтығы қалай табылады?
8. Анықталатын және түзетілетін қателіктер саны мен минималды код қашықтығы арасындағы қатысты жазыңыз.
9. Түзетуші кодтың негізгі сипатты көрсеткіштерін атаңыз.
10. Топтар, кіші топтар және жанасқан кластар түсініктерін анықтама беріңіз.
11. Сақина мен өріс түсініктерінің айырмашылығы неде?
12. Сызықты векторлі кеңістік қалай анықталады?
13. Қандай кедергіге шыдамды код сызықты делінеді?
14. Қателік векторы деп нені түсінеді?
15. Қателік синдромы деп нені айтамыз?
16. Берілген корректтелетін қателік векторларының жиыны үшін синдромдар кестесі қалай құрылады?
17. Тексеруші дәрежелер мәнін анықтайтын синдромдар теңдеуін синдромдар кестесінен қалай табады?
18. Мажоритарлық декодтаудың негізі неде?
19. Кодтың туындаушы матрицасының анықтамасын беріңіз.
20. Қандай код жүйелілік деп аталады?
21. Кодтың тексеруші матрицасы қалай құрылады?
22. Циклдік кодтың құраушы көпмүшелегі қандай талаптарға жауап беруі керек?
23. Сақинадағы идеал және идеал бойынша айырымдар класына анықтама беріңіз.
24. Циклдік кодтың құраушы көпмүшелігі қандай талаптарға жауап беруі керек?
25. Циклдік кодта қателік синдромдары қалай анықталады?
26. Ажыратылған синдром деп неге айтамыз?

27. Қандай құрылымдар циклдік кодтардың техникалық негізін құрады?

28. Циклдік кодтың декодтау үдерісін түсіндіріңіз. Боуз — Чоудхури – Хоквингем кодының құраушы көпмүшелігі қалай таңдалады?

29. Боуз – Чоудхури – Хоквингем кодының декодтау әдісі қандай?

30. Құраушы келтірілмейтін көпмүшеліктер бойынша xn+1 екімүшелік түбірлері қалай таралады?

Өзіндік жұмыстар (СӨЖ) тақырыптары.

1. Хэмминг кодтары.

2. Топтық кодттарды кодтау және декодтаудың техникалық құралдары.

3. Циклдік кодтар; Циклдік кодтарға математикалық кіріспе.

4. Құраушы көпмүшеліктер, оларға қойылатын талаптар.

5. Құраушы көпмүшелікті таңдау; әртүрлі тәртіпті қателіктерді табу және түзету.

6. Циклдік кодтарды құру әдістері; матрицалық жазылуы; мажоритарлық декодтау.

7. Қателікті анықтаушы циклдік кодтардың сандық желіде қолданылуы.

8. Қателік түйіншек табушы және түзетуші циклдік кодтар.

9. Боуз-Чоудхури-Хоккенгем, Рид-Соломон, Рид-Маллер кодтары.

10. Файр кодтары.

11. Циклдік кодтарды мажоритарлық декодтау.

12. Боуз-Чоудхури-Хоккенгем кодтары.

Қорытынды

Оқулық "Информатика", "Ақпараттық жүйелер", "Автоматтандыру және басқару", "Есептеу техникасы және бағдарламамен қамтамасыз ету" мамандықтарына арналған болып, Қазақстан Білім және ғылым министрлігі (2006 ж.) бекіткен оқу үлгіқалыбына толық жауап береді; оқулық жеті тараудан құрылған.

Кіріспеде "Ақпараттар теориясының" даму тарихы және қазіргі замандағы ақпараттар технологиясындағы орны көрсетілген.

Елімізде индустриялық-инновациялық бағдарламаның орындалуында, "Электронды Үкіметті" амалға асыруда заманауй ақпараттық технологияның өмірдің барлық салаларында (білім беру, медицина, бизнес, банк, және т.б.) кең нәтижелі қолдану негізгі мәселенің бірі болып отыр.

Ақпараттар теориясы заманауи ақпараттық технологияны жаратудың негізі болып, ақпаратты жинақтау, сенімді түрде (яғни ұрланудан, бұзылудан сақтау), сақтау, арналармен жіберу, бұзылған ақпаратты қайта тіктеу сияқты жұмыстарды орындауда негізгі теория болып қала береді.

Оқулықтың **бірінші тарауында** Ақпараттың философиялық тұжырымдамасы осы заманға сай келтірілген; осы кездегі қоғамдық ғылымдар мен жаратылыстану ғылымдарының арасындағы алшақтық қоғамда философиялық ғылымдардың нашарлауына және жастардың арасында әртүрлі келеңсіз жағдайлардың (діни және т.б. секталардың) көбеюіне себеп болғандығы айтылған.

Президент Н. Назарбаевтің "Жасампаз көшбасшылық философиясына" және осы кездегі озықты ғылыми философияларға негізделе отырып, ***ақпаратты тірі дүниедегі материяның түрі*** деп қаралады; жаратылыстану ғылымдарының тұжырымдамасына немесе осы кездегі биология, нейрофизиология, экстрасенсорика, парапсихология, информатика, кибернетика, экология және т.б. көптеген заманауй ғылымдарды зерттей отырып, осы кезге сай философиялық көзқарас жаратылған.

Бұл философия өткен ғасырдағы қарама-қарсылықтар философиясынан айырмашылығы: әлемді бір бүтін, ажыралмас дүние деп қаралып, материяның барлық келбетін (өлі, тірі, ескі көзқарастар болған – материялық, идеалдық, т.б.) жалғыз және үздіксіз шексіз дүние деп қаралады; мұнда тарихи ғалымдардың көзқарастарына анықтама бере отырып, дін мен ғылым арасындағы

қарама-қарсылықтарды адамдардың қолдан жасағандығы немесе олардың білімдерінің шектелгендігінен болатыны көрсетілген.

Қоғамның дамуында инфосфераның және ноосфераның негізгі қызметі көрсетілген.

Оқулықта "Ақпараттар теориясы" синтаксикалық өлшемдері негізінен Шеннон-Фано, Хартли теорияларына негізделген болса, шартты оқиғалардың энтропиясын зерттеуде Байесстің теориясы да қамтылған; осы теорияның негізінде болжау бағдаржолдары құрылған.

Үздіксіз ақпаратты өлшеуде дифференциалдық энтропия, кездейсоқ шаманың энтропиясын өлшеуде эпсилон-энтропияны есептеу әдістері берілген.

Оқулықтың екінші тарауында ақпараттар теориясында қолданылатын сигналдар мен үдерістердің үлгілері берілген; мұнда сигналдың уақыттық, жиілікті (корреляциялық, спектралдық) сипаттамалары берілген.

Спектралды талдау тарихы мен оны жаратқан ғалымдар туралы қысқаша ақпарат берілген. Детерминделген (периодты, периодсыз) сигнал қуатының спектр бойынша таралуы, қуатының спектралды тығыздығы, автокорреляциялық теңдеуі көрсетілген.

Стохастикалық және эргодикалық сигналдың ықтималдық сипаттамалары берілген.

Үшінші тарауда үздіксіз хабарларды дискреттеу мәселелері қаралған.

Сандық сигналдардың абзалдығы, осы кезде кең қолданылуының себептері көрсетілген.

Дискреттеу және кванттау теориясы Котельников, Найквист теоремаларының негізінде аталып, осы кездегі сандық техникадағы орны көрсетілген. Мұнда сигналдар мен хабарлардың артықшылығын есептеуде сапа шарттары толық жарытылған.

Дискреттеудің әртүрлі әдістері беріліп, олардың қолданылуы салыстырмалы бағаланған.

Тараудың соңында бақылау сұрақтары берілген.

Төртінші тарауда хабар көзінің және байланыс арнасының ақпараттық сипаттамалары берілген.

Дискрет хабар көзінің үлгілері, өнімділігі, артықшылық түсінігі анықталған. Сигнал мен хабар көзінің артықшылығын есептеу, сигналды энтропия бойынша оңтайландыру әдістері берілген.

Оңтайландыруда қысқарту еселіктерін қолдану көрсетілген.

Үздіксіз хабар көзінің энтропиясы бойынша оңтайландыру жолы, дискрет хабар көзінің өнімділігі көрсетілген.

Бөгеуілсіз және бөгеуілді байланыс арнасының өткізу қабілеті талданған.

Үздіксіз байланыс арнасының өткізу қабілеті, дифференциалды энтропия, сигналдың физикалық сипаттарының келісуі талданған; сигнал көлемі мен байланыс арнасының сиымдылығының ақпаратты жіберуге әсері көрсетілген.

Аспаптың сипаты ретінде хабар көзі мен байланыс арнасының санақтық келісуінің байланысқа әсері талданған.

Хабарлардың таралу заңын өзгертумен сигналдарды оңтайландыру әдістері көрсетілген.

Котельников теоремасының амалда қолданылуы берілген.

Бесінші тарауда бөгеулсіз дискрет байланыс арнасы бойынша хабар жіберуде ақпаратты кодтау мәселесі қаралған.

Мұнда бөгеуілсіз арна үшін Шеннонның кодтау туралы негізгі теоремасы берілген; энтропияның қасиеттерін ақпаратты сығымдауда қолданып, нәтижелі кодтарды жарату көрсетілген.

Шеннон-Фано, Хаффмен кодтарын құрудың әдістері көрсетілген. Ақпаратты криптографиялық жабуда шифрлеудің қарапайым бағдаржолдары, осы кезде қолданылып келе жатқан үлгіқалыпты бағдаржолдары және қолтаңба жасау қағидасы MS Excel- де жасалған бағдарлама негізінде көрсетілген.

Оларды үлгілеу бағдарламалары MS Excel-де зертханалық жұмыстар ретінде берілген.

Алтыншы тарауда бөгеулді дискрет байланыс арнасы бойынша хабар жіберуде ақпаратты кедергіге шыдамды кодтау мәселесі қаралған; мұнда жиынтықты түзетуші кодтардың жалпы қағидалары, сапа көрсеткіштері берілген. Топтық екілік код құруда синдром кестесін құрастыру, қателікті анықтаушы және түзетуші кодтарды талдау, үлгілеу қаралған.

Хэмминг кодтарының желіде қолданылу әдістері қарастырылған.

Топтық кодтардың мажоритарлық декодтау, сызықты кодтардың матрицалық көрсетілуі қаралған.

Жетінші тарау түзетуші топтық кодтарға, соның ішінде циклдік кодтарға арналған. Хэмминг кодтарын құру, циклдік кодтардың құраушы көпмүшелігін таңдау, әртүрлі қателіктерді табу мәселелері көрілген.

Циклдік кодтарды құрудың матрицалық жазылуы, мажоритарлық декодтау әдістері қаралған. Циклдік кодтардың осы кездегі байланыс арнасында қолданылуы көрсетілген.

Қателік түйіншегін табушы және түзетуші кодтар қатарында Боуз-Чоудхури-Хоквингем, Рид-Соломон, Рид-Маллер кодтарына анықтама берілген.

Файр кодтары толық қарастырылып, Файрдың декодтау әдісі де берілген.

Циклдік кодтарды мажоритарлық декодтау толық көрсетілген.

Боуз-Чоудхури-Хоквингем кодтарын құру әдістері берілген.

Әрбір тараудың соңында бақылау сұрақтары берілген.

Осы кезде Қазақстанда идустрияландыру және инновациялық бағдарламаны орындауда заманауи жаңа автоматтанған өндіріс орындарын құруда секундына жүздеген өлшемдерді анық өлшей алатын кибернетикалық автоматты ақпаратты өлшеуіш жүйелерінде теорияда өтілген Котельников-Найквист теоремасы кең қолданылса, ал ақпаратты сығымдап арнамен жіберуде, мұрағаттауда Шеннон-Фано, Хаффмен кодтары қолданылады.

Ал алыстағы жылжымалы нысандарды басқаруда радиоарналармен ақпараттарды ашық түрде жіберуде Боуз-Чоудхури-Хоквингем, Рид-Соломон, Рид-Маллердің каскадтты кодтары істетіледі.

Электронды Үкіметте ақпаратты құпия түрде сақтау немесе арнамен жіберуде жоғарыда аталған шифрлеу бағдаржолдары қолданылады.

Қысқасы, осы кезде сандық ақпараттық техника өмірдің барлық салаларын қамтыған кезде ақпараттар теориясы өте маңызды пәнге айналды.

Әдебиеттер

Негізгі:

1. Н. Назарбаев. Президент Н. Назарбаевтың Қазақстан халқына Жолдауы. 2005 ж. Астана қ.

(Н. Назарбаев. Послание Президента Н. Назарбаева народу Казахстана: «Казахстан на пути ускоренной экономической,социальной и политической модернизации», Астана, 18.02.2005.)

2. Н. Назарбаев. Президент Н. Назарбаевтың Қазақстан халқына Жолдауы. 2006 ж. Астана қ.

(Н. Назарбаев. Послание Президента Н. Назарбаева народу Казахстана: «Стратегия вхождения Казахстана в число 50 наиболее конкурентоспособных стран мира», Астана, 3.03.2006.)

3. Н. Назарбаев. Жас өскін демократиялардың әлеуеті. "Вашингтон таймс" газеті. 8 қыркүйек, 2009 ж.

4. Н. Назарбаев. Президент Н. Назарбаевтің Қазақстан халқына Жолдауы. 2012 ж. Астана қ.

5. М. Әшімбаев. Ғылымның тағдыры ғалымдардың қолында."Егемен Қазақстан", 2 қазан, 2009 ж.

6. Концепции современного естествознания, под ред. Д.с.н., проф. Самыгина С. И. Ростов н/Д: Феникс,2002 г. -352 с. 314-329

7. Аширов А. Экология сознания, курс лекции. Туркестан, 2007 г. -150с.

8. Тұрғынбаев Ә. Х. Философия. - Алматы: "Білім", 2005 ж., - 304 б.

9. Лидовский В. В., Теория информации. Уч. Пособие. –М., МВТУ, 2003. -105 с.

10. Скляр Б. Цифровая связь. – М.: С.-Питер., Киев: изд. дом Вильямс, 2003. -1104с.

11. Дитриев В. И. Прикладная теория информации. – М.: Высшая школа, 1989. -320с.

12. Введение в криптографию //Под ред. В. В. Ященко.-М.: МЦНМО: ЧеРо, 2000.

13. Темников Ф. Е. и др. Теоретические основы информационной техники. — М.: Энергия, 1979.

14. Дж. Кларк, Дж.Клейн. Кодирование с исправлением ошибок в системах цифровой связи. –М.: Радио и связь. 1989. -392с.

15. Злотник Б. М. Помехоустойчивые коды в системах связи. –М.: Радио и связь, 1989. 236 с.

16. Гоноровский И. С. Радиотехнические цепи и сигналы. – М.: Высшая школа, 1988. 675 с.

17. Клод Шеннон. Теория связи в секретных системах. В кн. «Работы по теории информации и кибернетике».- М.,ИИЛ,1963, -333-369с.

18. Цымбал В. П. Задачник по теории информации и кодированию. Киев. Высшая школа, 1976. -276с.

19. Орлов В. А.,Филипов Л. И. Теория информации в упражнениях и задачах. – М.: Высшая школа, 1976.-136с.

20. Хемминг Р. В. Теория кодирования и теория информации. — М.: Радио и связь, 1983.

21. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир.1976.

22. Новик А. А. Эффективное кодирование. — М: Энергия, 1965.

23. Стандарты в области телеобработки данных. Международн. центр НТИ, справочник, ч.1. – М. 1981 г.

24. Сети TCP/IP, Microsoft Windows 2000 Server / Пер. С англ. –М.: Изд.-торг.дом Русская Редакция , 2001. – 784 с.: ил.

Қосымша:

25. Глушков В. М. Мышление и кибернетика //Вопросы философии, 1963. № 1. с. 10—24.

26. Жаутиков О.А. Математиканың даму тарихы, Мектеп баспаханасы, Алматы,1968 ж.

27. Оразбаев Б. М. Сандар теориясы. Оқулық, Алматы қ., 1970 ж. -393 б.

28. Угаров В. А. Специальная теория относительности.“Наука“, 1969 г., 304 с.

29. Тело человека. Мозг человека. Документальные сериалы. Пр-во BBC FILMS,1998.

30. Атаулаханов Ф. Полчаса митоза. Интернет. 2008.

31. Тихоплав В. Ю. и др. Наше духовное исцеление. О чем предупреждают новые болезни. С.-Пб. ИД Весь, 2004 г.

32. Рустамов Н. Т. и др. Семантическая модель энергоинформационной медицины. “Вестник МКТУ”, №3, с. 123-131, Туркестан, 2008 г.

33. Энциклопедия кибернетики,т.1,2 //под ред. акад. Глушкова В.М., УСЭ, Киев, 1975 г.

34. Алиев Р. А. Гибридные зияткерлікьные системы. Ч. 3, Азербайджанская ГНА, Баку, 1998.

35. Блейхут Р. Теория и практика кодов, контролирующих ошибки.-М.: Мир, 1986.

36. Чичар И., Кернер Я. Теория информации. – М.: Мир, 1985.

37. Нечаев В. И. Элементы криптографии. – М.: Высшая школа, 1999.

38. Герасименко В. А., Мясников В. А. Защита информации от несанкционированного доступа. — М.: МЭИ, 1984.

39. Дмитриев В. И., Иванов А. В. Новые сверточные коды для исправления ошибок на магнитной ленте//Труды МЭИ. Вып. 495. 1980. С. 11 — 17.

40. Дэвис Д. и др. Вычислительные сети и сетевые протоколы. -М.: Мир, 1982.

41. Зиновьев А. Л., Филиппов Л. И. Введение в теорию сигналов и цепей. — М.: Высшая школа, 1975.

42. Игнатов В. А. Теория информации и передачи сигналов.—М.: Советское радио, 1979.

43. Колесников В. Д , Мирончиков Е. Т. Декодирование циклических кодов. — М.: Связь, 1968.

44. Колмогоров А. Н. Три подхода к определению понятия «количество информации»// Проблемы передачи информации. 1965. Т. 1. Вып. 1. с. 25-38.

45. Коган И. М. Прикладная теория информации. — М.: Радио и связь, 1981.

46. Кузьмин И. В., Кедрус В. А. Основы теории информации и кодирования. — Киев: Высшая школа, 1977.

47. Кузьмин И. В., Явна А А., Ключко В. И. Элементы вероятностных моделей АСУ,- М.: Советское радио, 1975.

48. Липкин И. А. Основы статистической радиотехники, теории информации и кодирования, - М.: Советское радио, 1978.

49. Логинов В. М. и др. Экономичное кодирование, - Киев.: Техника, 1976.

50. Мамиконов А. Г. Управление и информация, - М.: Наука, 1975.

51. Мельников Ю. Н. Достоверность информации в сложных системах. — М.: Советское радио, 1973.

52. Пенин П. И. Системы передачи цифровой информации. — М: Советское радио, 1976.

53. Пугачев В. С. Теория случайных функций и ее применение к задачам автоматического управления. — М.: Изд-во технико-теоретической литературы, 1957.

54. Основы кибернетики. Теория кибернетических систем /Под ред. К. А. Пупкова. — М.: Высшая школа, 1976.

55. Дмитриев В. И. Учебное пособие по курсу «Теория информации и кодирования». — М.: МЭИ, 1977.

56. Советов Б. Я. Теория информации. — Л.: Изд. ЛГУ, 1977.

57. Солодов А. В. Теория информации и ее применение к задачам автоматического управления и контроля. — М.: Наука, 1967.

58. Тарасенко Ф. П. Введение в курс теории информации. — Томск: Изд. ТГУ, 1963.

59. Фельдбаум А. А. и др. Теоретические основы связи и управления. — М.: Физматгиз, 1963.

60. Финк Л. М. Теория передачи дискретных сообщений. — М.: Советское радио, 1970.

61. Харкевич А. А. Борьба с помехами. — М.: Физматгиз, 1965.

62. Харкевич А. А.Теория информации и опознование образов. В 3-х томах, Наука, 1973г.-525с.

63. Хартли Р. Передача информации. Теория информации и ее приложения //Под ред. А. А. Харкевича. — М.: Физматгиз, 1959.

64. Хетагуров Я. А., Руднев Ю. П. Повышение надежности цифровых устройств методами избыточного кодирования. — М.: Энергия, 1974.

65. Хинчин А. Я. Об основных теоремах теории информации// //УМН. 1956. № 1 (67). С. 17—75.

66. Четвериков В. Н. Преобразование и передача информации в АСУ. — М.: Высшая школа, 1974.

67. Тукубаев З. Б. Результаты моделирования разнесенного приема сигналов в условиях общей гауссовской модели замирания, НТС Техника средств связи, сер. ТПС, вып. 7,-М., 1989 г.

68. Тукубаев З. Б. Моделирование разнесенного приема сигналов и вопросы прогнозирования в условиях общих гауссовских замираний, НТС Техника средств связи, сер. СС, вып. 6, -М.,1990 г.

69. Тукубаев З. Б. Обобщенный алгоритм измерения, аппроксимации, моделирования и прогнозирования в управлении пространственно-временными каналами. Журнал “Проблемы информатики и энергетики”, изд. Фан, вып.5, Ташкент,1998 г.

70. Тукубаев З. Б. и др. Обобщенный алгоритм измерения, аппроксимации, моделирования и прогнозирования в пространственно-временных каналах. Материалы международной конф. “Вычис-

лительные технологии и матем. моделиров. в науке,технике и образовании", ВТММ-2002,ч.5, Новосибирск-Алматы, 2002.

71. Тукубаев З. Б.,Тукубаева Г. З. Методы оценки адекватности имитационного моделирования, ХҚТУ Хабаршысы, Түркістан, №3,2007

72. Тукубаев З. Б. и др. Некоторые вопросы внедрения новой имитационной технологии. Международн. НТК "Казахстан за 10 лет: проблемы экономики», МКТУ, Туркестан, 2001.

73. Тукубаев З. Б. ж.т.б. Информация және информатиканың қәзіргі замандық философиялық тұжырымдамасы. ХҚТУ Хабаршысы, №3, 2007 ж., 244-252 б.

74. Тукубаев З. Б. және т.б. Кибернетика және үлгілеу, ХҚТУ Хабаршысы, №3, 2008 ж., 21-31б.

75. Тукубаев З. Б. Моделирование СПДИ с поблочной передачей с накоплением в условиях преднамеренных помех. Тезисы докл. ОНТК «По мәселем распространения радиоволн», НИИССУ. - М.: 1986 г.

76. «Об электронных документах и об электронной подписи», Закон Республики Казахстан, №371 11 ЗРК, Астана, 3.01.2003.

77. Мартин Дж. Вычислительные сети и распределенная обработка данных, - М., Финансы и статистика,1986.

78. Вильям Столлингс. Криптография и защита сетей. Изд. Дом «Вильямс», - М. -Л.-Киев, 2001, -672 с.

79. Масленников М. Практическая криптография, С.-Петербург», БХВ-Петербург», 2003.- 464 с.

80. Голиков В. Ф. и др. Криптографическое кодирование информации; Метод.указания по дисциплине"Криптографическая защита информации в телекоммуникациях". Ч.3 : Электронная цифровая подпись. –Мн.: БГУИР, 2003 г.

81. Тукубаев З. Б. Исследование и анализ поэлементных способов контроля качества сигналов на ЭВМ. Кандидатск. диссертация. – Ташкент, 1977 г. – 350 с.

82. Арипов М. Н. Передача дискретной информации по низкоскоростным арнаам связи.-М.: Связь,1980.- 128с.

1 Қосымша.

ТЕСТ СҰРАҚТАРЫ МЕН ЖАУАПТАРЫ

1. Хабар мен ақпараттың (информацияның) айырмашылығы бар ма? Ж: Бар.

2. Хабар мен ақпараттың қайсысы қабылдаушыға субьектив байланысты болады? Ж: Ақпарат қабылдаушыға субьектив байланысты болады.

3. Ақпараттың анықтамасы қандай? Ж. Ақпарат тірі биологиялық мүшеге әсер етіп, оның ойлау жүйесінде (жүйке жүйесі де ойлау жүйесінің бір бөлімі деп қаралады) түйсік немесе өзгеріс тудыратын хабардың бір бөлігіне жатады.

Жансыз жүйелерде ақпарат (информация) хабарға айланады; оның еш қандай да семанитикасы болмайды.

4. Хабардың (сигналдың) қандай түрлері болады? Ж: Детерминделген, стохастикалық, үздіксіз, дискрет ж.с.с.

5. Ақпараттың түрлері? Ж: Синтаксикалық, мағыналық, құндылықты, сигматикалы.

6. Шеннонның ақпараттық теориясында ақпараттың қай түрі жүйенің қай құрылымына тиісті қаралады? Ж: Ақпараттың синтаксикалық түрі қаралып, жүйенің хабар жіберуші арнаға тиісті қаралады.

7. Синтаксикалық ақпарат (информация) немен өлшенеді? Ж: Энтропиямен.

8. Энтропия екілік, үштік, ондық, натурал санақ жүйелеріндегі өлшем бірліктері қандай? Ж: bit, tit, det, nat.

9. Энтропияның логарифмдік өлшемі қандай және оны кім ұсынған? Ж: $H(X) = \log_2 N$. 1928 ж. Хартли ұсынған.

10. Энтропияның ықтималдық өлшемі қандай және оны кім ұсынған? Ж: $H(X) = -\sum_{i=1}^{N} P_i \log_2 P_i$, К. Э. Шеннон ұсынған.

11. Котельников немесе санақтар теоремасы. Ж: Дискреттеу қадамы сигналдың спектрінің жоғары жиілігінің /частотасының/ екі еселенгеніне кері пропорционал болады; яғни: $\Delta t = \frac{1}{2F_a}$.

12. Найквист теоремасы. Ж: Дискреттеу жиілігі (частотасы) сигналдың спектрінің жоғарғы жиілігінің екі еселенгеніне тең болады; яғни: $f_д = 2F_д$.

13. Котельников теоремасының салдары немесе квадраттық

нәтиже. Ж: $[0,T]$ аралығындағы $x(t)$ сигналының қуаты сол сигналдың Котельников қадамдарымен алынған өлшемдеріндегі сигнал амплитудаларының квадраттарының қосындысына тең болады; яғни:

$$.\sigma^2(x) = \int_0^T x^2 dt \approx \sum_{i=1}^{N} x^2\left(\frac{1}{2W}\right).$$

14. Котельников қатарымен дискретті өлшемдерді интерполяциялау. Ж: Котельников қатары мен теңдеуі:

$$x(t) = \sum_{i=1}^{N} x(k\Delta t) \bullet \varphi(k\Delta t);\ \ \varphi(k\Delta t) = \frac{Sin(k\Delta t)}{k\Delta t}.$$

15. Үздіксіз хабарларды кванттауда қайсы теңдеу "келтірілген энтропия" деп аталады? Ж: $H^{\bullet}(X) = -\int_{-\infty}^{\infty} \omega(x)\log\omega(x)dx.$

16. Мына теңдеуде энтропияның кемейуі неге байланысты болады? $H(X) = H^{\bullet}(X) - \log_2 \Delta x$. Ж: Кванттау қадамына байланысты болады.

17. Егер де Х,У хабарлар ансамблі берілген болып, олар толық немесе жартылай байланысты болса, онда энтропия қалай анықталады? Ж: $H(XY) \le H(X) + H(Y)$

18. Егер де Х,У хабарлар ансамблі берілген болып, олар байланыссыз болса, онда энтропия қалай анықталады? Ж: $H(XY) = H(X) + H(Y)$

19. Бинар ансамблде энтропия қандай жағдайда максимал болады және неге тең болады? Ж: $p = q = \frac{1}{2}$.

20. Энтропия қандай қатыс? Ж: Дөңес қатыс.

21. Егер $X = \{x_1, x_2, ..., x_n\}$ оқиғалар ансамблі берілген болса, оның энтропиясы қандай жағдайда нөлге тең болады? Ж: оқиғалардың біреуі алдын-ала мәлім болса.

22. Егер $X = \{x_1, x_2, ..., x_n\}$ оқиғалар ансамблі берілген болса, оның энтропиясы қандай жағдайда максимал болады? Ж: Барлық элементтердің ықтималдықтары өзара тең және $\frac{1}{n}$ болса.

23. Х,У өзара статистикалы байланысты оқиғалар ансамблі болса, онда олардың элементтері болған x_i, y_j нің бір уақытта орындалу ықтималдығы $P(x_i, y_j)$ қандай анықталады? Ж: $P(x_i, y_j) = P(x_i)P(y_j / x_i)$.

24. X ансамблінің x_i оқиғасы орындалғанда У ансамблінің жеке шартты энтропиясы қандай анықталады? Ж: $H(Y/x_i) = -\sum_{j=1}^{m} P(y_j/x_i)\log P(y_j/x_i)\cdot$

25. X оқиғалар ансамблі орындалғанда У ансамблінің орташа шартты энтропиясы $H(Y/X)$ қандай анықталады? Ж:

$$H(Y/X) = -\sum_{i=1}^{n} P(x_i)\sum_{j=1}^{m} P(y_j/x_i)\log P(y_j/x_i).$$

26. X,У ансамблдері санақтық байланысты болса, мына теңдеу $H(X,Y) = H(X) + H(Y/X)$ орынды ма? Ж: Ия, орынды.

27. X,У ансамблдері санақтық байланысты болса, мына теңдеу $H(X,Y) = H(X) + H(Y/X)$ қате ме? Ж: жоқ, қате емес.

28. X,У ансамблдері санақтық байланысты болса, мына теңдеу $H(X,Y) = H(X) + H(Y)$ қате ме? Ж: Ия, қате.

29. X,У ансамблдері санақтық байланыссыз болса, мына теңдеу $H(X,Y) = H(X) + H(Y)$ қате ме? Ж: Жоқ, дұрыс.

30. X,У ансамблдері санақтық байланыссыз болса, мына теңдеу $H(X,Y) = H(X) + H(Y/X)$ қате ме? Ж: Ия, қате.

31. X,У ансамблдері санақтық байланысты болса, мына теңдеу $H(Y) \geq H(Y/X)$ қате ме? Ж: Жоқ, дұрыс.

32. X,У ансамбльдері санақтық байланыссыз болса, мына теңдеу $H(X) \neq H(X/Y)$ қате ме? Ж: Ия, қате.

33. X,У ансамбльдері санақтық байланысты болса, мына теңдеу $I(YX) = H(X) + H(Y) - H(XY)$ дұрыс па? Ж: Ия, дұрыс.

34. Толық информацияның қасиеттерінен төмендегідейі дұрыс па?

Ж: $I(YX) = I(XY)$ Ия, дұрыс.

35. X,У ансамбльдері санақтық байланыссыз болса, мына теңдеу $I(XY) = H(X) - H(Y/X)$ дұрыс па? Ж: Ия, дұрыс.

36. X,У ансамбльдері біріккен болса, онда біріккен ансамблдердің энтропиясы $H(XY)$ қалай табылады? Ж: $H(XY) = \sum_{j=1}^{m}\sum_{i=1}^{n} P(x_i y_j)\log P(x_i y_j).$

37. Ұшаққа оқ атылды. Оқтың тию ықтималдығы 7/8 болса, онда “оқ тиді” деген хабар келсе, ол қанша бит ақпарат (информация) әкеледі? Ж: Атқанда оқтың тимеу ықтималдығын табамыз: ол

1/8 болады. Сонда меншікті ақпарат: $I_0 = -\log_2 q = -\log_2 \frac{1}{8} = 3$ бит. Ал толық ақпарат:

$$I(XY) = -P\log_2 P - q\log q = -\frac{1}{8}\log\frac{1}{8} - \frac{7}{8}\log\frac{7}{8} \approx 0{,}5213.$$

38. Ұшаққа 3 рет оқ атылды. Оқтың тию ықтималдығы 0,5 болса, онда "оқ тиді" деген хабар келсе, ол қанша бит ақпарат (информация) әкеледі? Ж: Үш рет тимеді ықтималдығын табамыз. 0,5*0,5*0,5 =0,125. Еш болмағанда бір рет тиу ықтималдығы: 1-0,125=0,875 болады. Толық ықтималдық:

$$I(X) = -\sum_{i=1}^{2} P_i \log P_i = -0{,}125\log 0{,}125 - 0{,}875\log 0{,}875 \approx 0{,}52$$

39. Үздіксіз хабардың энтропиясын есептегенде келтірілген энтропия қай теңдеумен көрсетіледі? Ж: $H^{\bullet}(X) = -\int_{-\infty}^{\infty} \omega(x)\log\omega(x)dx.$

40. Үздіксіз хабардың қуаты шектелген болса, яғни ($D_x = \sigma_x = const$), бұл хабардың энтропиясы максимал болуы үшін оның амплитудасы қандай заңмен таралған болуы керек? Ж: $\omega(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}$ болуы керек.

41. Үздіксіз кедергінің орташа қуаты шектелген болса, яғни ($D_x = \sigma_x = const$), онда оның амплитудасы қандай заңмен таралғанда кедергі нәтижелі болады? Ж: $\omega(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}$ заңмен таралғанда кедергі нәтижелі болады.

42. Үздіксіз хабардың қуаты шектелмеген болса, яғни ($D_x = \sigma_x \to \infty$), бұл хабардың энтропиясы максимал болуы үшін оның амплитудасы қандай заңмен таралған болуы керек? Ж: $\omega(x) = \frac{1}{b-a}x$, яғни амплитудасы біртегіс заңмен таралған болуы керек.

43. Үздіксіз кедергінің орташа қуаты шектелмеген болса, яғни ($D_x = \sigma_x \to \infty$), онда оның амплитудасы қандай заңмен таралғанда кедергі нәтижелі болады? Ж: $\omega(x) = \frac{1}{b-a}x$, яғни амплитудасы біртегіс заңмен таралған болуы керек.

44. Үздіксіз хабардың амплитудасы қалыпты заңмен таралған болса, онда оның энтропиясы неге тең? Ж: $H(X) = \log\left(\frac{\sigma}{\Delta x}\sqrt{2\pi e}\right)$.

45. Үздіксіз хабардың амплитудасы біркелкі (біртегіс) заңмен таралған болса, онда оның энтропиясы неге тең? Ж: $H(X) = \log\left(\frac{b-a}{\Delta x}\right)$.

46. Егер үздіксіз хабарлардың амплитудалары қалыпты және біркелкі таралған болса және олардың энтропиялары өзара тең болса, олардың қуаттары немесе дисперсиялары қандай қатыста болады? Ж: $\sigma_б^2 = 1{,}42\sigma_и^2$, мұнда $\sigma_а^2, \sigma_i^2$ – амплитудалары біркелкі және қалыпты таралған хабарлардың дисперсиялары.

47. үздіксіз хабарлардың амплитудалары қалыпты және біркелкі таралған болса және олардың энтропиялары немесе информативтігі өзара тең болса, олардың қайсысының қуаты немесе дисперсиясы кем болады? Ж: амплитудасы қалыпты заңмен таралған сигналдың қуаты кем болады.

48. Үздіксіз хабардың қысқарту еселігі қандай көрсетіледі? Ж: $\mu = \frac{n_{\min}}{n_{real}} = \frac{H_{real}}{H_{\max}}$.

49. Үздіксіз хабардың артықшылық еселігі қандай көрсетіледі? Ж: $r = \frac{H_{\max} - H_{real}}{H_{\max}}$

50. Сигналдар мен арналарды қәйтіп санақтық келістіруге болады? Ж: Олардың амплитудаларының таралу заңын қисық сызықты түрлендіргішпен түрлендіріп, қалыпты заңға немесе қалыптыға жақын заңға жақындатумен орындалады.

51. Үздіксіз сигналдың дискретті шамалары Котельников теоремасында қалай көрсетіледі? Ж: Котельников қатарымен көрсетіледі:

$$x(t) = \sum_{i=1}^{N} x(k\Delta t) \bullet \varphi(k\Delta t);$$

$$\varphi(k\Delta t) = \frac{Sin\,\omega_m(k\Delta t)}{\omega_m(k\Delta t)} = \frac{Sin\,\omega_m(t - k\Delta t)}{\omega_m(t - k\Delta t)}$$. Бұл Котельников теңдеуі.

52. Котельников теоремасын қолдану үшін қандай шарт орындалуы керек? Ж: Сигнал спектрінің ең жоғары жиілігі шектелген болуы керек, яғни $F_в$ шектелген болуы керек.

53. Котельников теоремасының негізгі маңызы неде? Ж: Үздіксіз сигналды анағұрлым кем нүктелер жәрдемінде дискрет түрге келтіру және бұлжытпай қайта тіктеу мүмкін.

54. Нақты жағдайда сигнал спектрі анық шектелмеген болса, Котельников теоремасын қандай шартпен істетсе болады? Ж: Сигнал спектрінің жоғары жиілігі шартты түрде белгілеп алынады; одан

жоғары жиіліктердегі сигнал гармоникаларының жиынды энергиясы сигналдың жалпы энергиясының оннан бірінен аспауы керек.

55. Үздіксіз сигналды дискреттегенде дискрет (строб) серпіндер ұзындығына қандай шарт қойылады? Ж: серпін ұзындығы $\tau_n < \frac{1}{2F_в}$, яғни спектрдің жоғарғы жиілігімен анықталады.

56. Котельников немесе санақ теңдеуінің негізгі қасиеті қандай? Ж: $t = k\Delta t$ уақыт мезгілдерінде $\varphi_{\max}(t) = 1$ болады.

57. Котельников теоремасымен сигналдарды өңдегенде оларды қайта тіктеу (интерполяция) қалай амалға асырылады? Ж: Интерполяциялауда Котельников қатары қолданылады: $x(t) = \sum_{i=1}^{N} x(k\Delta t) \bullet \varphi(k\Delta t)$;

$$\varphi(k\Delta t) = \frac{Sin\,\omega_m(k\Delta t)}{\omega_m(k\Delta t)} = \frac{Sin\,\omega_m(t - k\Delta t)}{\omega_m(t - k\Delta t)}.$$

58. Котельников теоремасының 2-салдарында квадраттық нәтиже деп неге айтамыз? Ж: 1 Ом кедергілі резистордан *x(t)* тоғы өткенде ажыралып шығатын қуатқа айтамыз.

$$\sigma^2(x) = \int_0^T x^2 dt \approx \sum_{i=1}^{N} x^2\left(\frac{1}{2W}\right) = \frac{1}{2F_m}\sum_{k=1}^{2F_m T} x^2\left(\frac{k}{2F_m}\right).$$

59. Арнаның өткізгіштік қабілеті қандай анықталады? Ж: $C = W\log\left(1 + \frac{P}{N}\right)$, *P,N*-сигнал мен кедергінің қуаттары.

60. Хабарлардың энтропиясын есептегенде әріптер арасындағы корреляция есепке алынбаса, онда табылған энтропия ақиқатты шамасынан кем болады ма? Ж: жоқ, ақиқатты шамадан табылған шамасы көбірек болады.

61. Кедергі жоқ болғанда кодтау үшін Шеннонның 1-теоремасы қандай түрде жазылады? Ж: $\frac{H(X)}{\log D} \le \overline{L} \le \frac{H(X)}{\log D} + \varepsilon$.

62. Код сөзінің орташа ұзындығы қалай табылады? Ж: $\overline{L} = \sum_{i=1}^{n} l_i P_i, P_i, L_i$ – сол сөздің ықтималдығы мен сөздегі таңбалар саны.

63. Кодтың нәтижелігі қалай табылады және нені білдіреді? Ж: $\lambda = \frac{H(X)}{\overline{L}}$, код сөзіндегі әрбір екілік таңбаның меншікті энтропиясын көрсетеді.

64. Екі әріп арасындағы корреляция есептелгендегі энтропия қалай табылады?

Ж: Орыс тілінде 32 әріп болса, энтропия келесідей табылады: $H_2(X) = -\frac{1}{2}\sum_{i=1}^{\mathfrak{Z}}\sum_{j=1}^{\mathfrak{Z}} P(x_i x_j)\log P(x_i x_j)$.

65. Нәтижелі кодтарға қойылатын негізгі талап қандай? Ж: Негізгі талап, кодтың әрбір екілік таңбасының информативтігі максимал болуы керек, яғни: $\lambda = \frac{H(X)}{\bar{L}} \to \max$.

66. Шеннон-Фано кодын құруда қандай талаптар қойылған?Ж: әр орындағы таңбаларды таңдағанда, олар алдыңғысына байланысты болмауы керек; 0,1 таңбаларының ықтималдықтары өзара тең немесе өте жақын болуы керек. Барлық таңбалардың ықтималдықтарының қосындысы 1 ге тең болуы керек.

67. Кедергісіз арнаның өткізгіштік қабілеті қандай табылады? Ж: $B = V\bar{L}\log D[bit/c]$.

68. Кедергісіз арнада өткізгіштік туралы Шеннонның 1-теоремасы қалай көрсетіледі? Ж: $\frac{B}{H} - \varepsilon \le V \le \frac{B}{H}$.

69. Кедергілі арнаның екілік үлгісі матрицада қалай көрсетіледі? Ж: $\begin{Vmatrix} p & q \\ q & p \end{Vmatrix}$.

70. Кедергілі арнаның екілік симметриялы үлгісі қалай көрсетіледі?

Ж: Y p: 1 $\longrightarrow$ 1 Z

q: 0 $\longrightarrow$ 0

71. Кедергілі арна үшін Шеннонның 2-теоремасы қандай жазылады? Ж:

Егер $\overline{H}(X) = B - \varepsilon$ болса, онда $P_{ош} < \eta$ орындалатын кодтау әдісін тапса болады.

72. Кедергілі арна үшін Шеннонның 2-кері теоремасы қандай жазылады? Ж:

Егер $\overline{H}(X) > B$ болса, онда $P_{ош} < \eta$ орындалатын ешқандай кодтау әдісі табылмайды.

2-қосымша.

Криптологияның математикалық негіздері.
Салыстырулар теориясы. Қалындылар теориясы

Кез келген *n* оң бүтін сан үшін және кез келген бүтін *a* үшін *a* ны *n* ге бөлгенде, *q* бүтін бөлінді және *r* қалдық шығады; ол мына теңдеуді қанағаттандырады: $a=qn+r;\ 0 \le r < n; q = \lfloor a/n \rfloor$, мұнда $\lfloor x \rfloor$ таңбасы x тен аспайтын ең үлкен бүтін сан.

Модуль бойынша салыстыру операциясы келесідей қасиеттерге ие:

1. $a \equiv b \bmod n$ болады, егер де $a-b$ айырмасы n ге толық бөлінсе.

2. Егерде $(a \bmod n) = (b \bmod n)$ болса, онда $a \equiv b \bmod n$ болады.

3. Келесідей теңдеуден: $a \equiv b \bmod n$ келесідей теңдеу $b \equiv a \bmod n$ шығады.

4. Егерде $a \equiv b \bmod n, b \equiv c \bmod n$ болса, онда $a \equiv c \bmod n$ болады.

Айырымдар класының арифметикасы

Модуль n бойынша салыстыруда анықтамадан мәлім болғанындай барлық бүтін сандар жиыны келесідей жиында $\{0,1,...,(n-1)\}$ өз бейнесін табады.

Осы жерде келесідей сұрақ туындайды: осы жиынның шеңберінде арифметикалық амалдар анықтау мүмкін бе?

Ия, мүмкін екен және соған тиісті амалдар жиынын айырымдар класының арифметикасы деп аталады екен. Осы арифметиканың қасиеттерін қарастырайық.

Айырымдар класының арифметикасының амалдары келесідей қасиеттерге ие:

$$1.\left[(a \bmod n) + b \bmod n\right] \bmod n = (a+b) \bmod n.$$
$$2.\left[(a \bmod n) - b \bmod n\right] \bmod n = (a-b) \bmod n.$$
$$3.\left[(a \bmod n) \times b \bmod n\right] \bmod n = (a \times b) \bmod n.$$

8 модуліндегі арифметика.

8 модулімен қосу.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

8 модулімен көбейту.

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Айырымдар класының арифметикасының қасиеттері.

n нен кем болған және кері емес бүтін сандар жиыны берілген дейік:

$$Z_n = \{0,1,...,(n-1)\}.$$

Бұл жиынды басқаша айтқанда n модулі бойынша **қалындылар жиыны** деп те атайды. Осы жиында n модулі бойынша арифметикалық амалдар үшін төмендегідей қасиеттер орынды болады.

Қасиеттері	Теңдеулер көрінісі
Коммутативті заң	$(\omega + x) \bmod n = (x + \omega) \bmod n,$ $(\omega \times x) \bmod n = (x \times \omega) \bmod n.$
Ассоциативті заң	$[(\omega + x) + y] \bmod n = [\omega + (x + \omega)] \bmod n,$ $[(\omega \times x) \times y] \bmod n = [\omega \times (x \times \omega)] \bmod n.$
Дистрибутивті заң	$[(\omega \times x) \times y] \bmod n = [\omega \times x) \times (x \times y)] \bmod n.$
Теңдіктер	$(0 + \omega) \bmod n = \omega \bmod n,$ $(1 \times x) \bmod n = \omega \bmod n.$
Аддитивтік кері $(-\omega)$	Кез келген $\omega \in Z_n$ үшін келесідей z табылып, мынау орынды болады: $\omega + z \equiv 0 \bmod n$.

Қалындылар туралы қытай теоремасы.

Бұл теореманы қытай математигі Сунь-Цзе біздің дәуірімізге дейінгі 100 жылдары дәлелдеген. Осы теорема қазіргі кезде криптографияда кең қолданылып келеді. Теореманың негізіне тоқтайық. Анық ауқымдағы сандар жиынынан алынған бүтін сан берілген болсын және екі өзара жай (қарапайым) сандар да берілген болсын. Сонда егер берілген санды жай санның біріншісіне бөлгенде қалған қалдық санды екінші жай санмен өңдеп, бастапқы берілген санды қайта тіктесе болады.

Мысалы, бүтін сандардан құралған $Z_{10}(0,1,...,9)$ жиыны берілген болсын. Осы жиын ішіндегі санның кез келгенін 2 және 5 модулінен қалған қалдықтар арқылы қайта тіктесе болады. Осы екі сан 10 ның жай бөлгіштері. Мысалы, ондық сан x берілген болып, осы екі санға бөлгендегі қалған қалдықтар: $r_2 = 0, r_5 = 3$ болсын, яғни $x \bmod 2 = 0, x \bmod 5 = 3$. Онда ізделінген сан жұп болып, жалғыз шешім $x = 8$ болады.

Қытай теоремасын келесідей қалыптастырса болады. Өзары жай m_i қос сандар жиыны берілген болып, олар келесідей $M = \prod_{i=1}^{k} m_i$ түрде берілсін, яғни $\gcd(m_i, m_j) = 1, 1 \le i, j \le k, i \ne j$.

Егерде мына шарттар: $A \leftrightarrow (a_1, a_2, ..., a_k)$ болып, мұнда $A \in Z_M, a_i = Z_{m_i}, a_i = A \bmod m_i, 1 \le i \le k$ болса, Z_M жиынынан кез келген **бүтін мәнді** *к* сандар тобымен көрсетсе болады.

Қытай теоремасын былайша түсіндірсе болады.

1. Z_M мен оның декарт көбейтіндісі $Z_{m_1} \times Z_{m_2} \times ... \times Z_{m_k}$ арасында тек қана бірмәнді байланыс бар болып, мұны **биекция** деп атайды. Басқаша айтқанда әрқандай $A, 0 \le A < M$ бүтін саны үшін жалғыз ғана $k, (a_1, a_2, ..., a_k)$ сандар тобы сәйкес келеді де (мұнда $0 \le a_i < m_i$);

керісінше, әрқандай $k, (a_1, a_2, ..., a_k)$ сандар тобы үшін Z_M жиынынан жалғыз ғана А табылады.

2. Z_M жиынының элементтерімен өткізілетін амалдар *к* сандар тобында сәйкес элементтері болады; мұнда осы амалдар мәлімбір жүйеде әрбір кеңстік өлшемдері бойынша тәуелсіз өткізіледі.

3-қосымша.

Эйлер және Ферма теоремалары.

Эйлер және Ферма теоремалары криптографияда ашық кілт жаратуда кең қолданылады.

Ферма теоремасы.

Егерде p ***жай саны және*** a ***оң бүтін саны беріліп, ол*** p ***ға бөлінбейтін болсын.***

Сонда әрқашанда мына салыстыру орынды болады: $a^{p-1} \equiv 1 \bmod p$**.**

Осы теореманың альтернативасы өте керек болуы мүмкін. Ол былай: $a^p \equiv a \bmod p$. Бұл теңдеу кез келген бүтін a үшін дұрыс.

7 модулі бойынша қосу

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

7 модулі бойынша көбейту

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	3	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

7 модулі бойынша аддитивті және мультипликативті керілері

w	$-w$	w^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Эйлер функциясы.

Эйлер теңдеуі келесідей таңбамен таңбаланады $\phi(n)$; ол оң бүтін мәндерге ие болған сан болып, *n*- нен кем және онымен өзара жай сан болады.

Төменде Эйлер теңдеуінің кейбір мәндері берілген.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8
n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\phi(n)$	8	16	6	18	8	12	10	22	4	20	12	18	12	28	8

P жай саны үшін $\phi(n) = p - 1$ болатыны түсінікті. Айталық екі жай *p,q* сандары берілсін және *n=pq* болсын. Онда келесідей жазса болады:

$$\phi(n) = \phi(np) = \phi(p) \times \phi(q) = (p-1) \times (q-1).$$

Эйлер теоремасы.

Модуль n- мен өзара жай кез келген a сандары үшін келесідей салыстыру орынды болады: $a^{\phi(n)} \equiv 1 \bmod n$ **.**

Осы теореманың келесідей альтернативасы болады:

$a^{\phi(n)+1} \equiv a \bmod n$.

Осы теореманың салдары RSA криптографиялық бағдаржолында қолданылады.

Кез келген екі жай *p,q* сандары және *n,m* бүтін сандары берілген болсын;

мұнда *0<m<n* болсын.

Онда келесідей жазса болады: $m^{\phi(n)+1} \equiv m^{(p-1)(q-1)+1} \equiv m \bmod n$.

Бұл жерде *n, m* өзара жай сандар болғандықтан Эйлер теоремасының шарттары орындалады.

Сондай-ақ мына альтернативалар да пайдалы болады:

$$\left[m^{\phi(k)}\right]^k \equiv 1 \bmod n,$$
$$m^{k\phi(n)} \equiv 1 \bmod n,$$
$$m^{k\phi(n)+1} \equiv m^{k(p-1)(q-1)+1} \equiv m \bmod n.$$

4-қосымша.

Модулярлық арифметика. Дискретті логарифмдер.

Дискретті логарифмдеу ашық кілтпен шифрлеудің бірталай криптографиялық бағдаржолдарының негізін құраған; мысалы, Диффи-Хэльман бағдаржолында кілттерді алмасуда және сандық қолтаңбаның DSA бағдаржолында де қолданылады.

Эйлер теоремасының негізінде өзара жай *a,n* сандары үшін мына қатынас орындалады: $a^{\phi(n)} \equiv 1 \bmod n$; мұнда $\phi(n)$ Эйлер теңдеуі;

ол оң бүтін мәнді сандардан болып, *n* нен кіші және онымен өзара жай болады. Енді одан жалпы болған келесідей қатысты қарастырамыз:

$$a^m \equiv 1 \bmod n .$$

Егер *a* және *n* өзара жай сандар болса, осы теңдеуді қанағаттандыр^тын ең кем дегенде бір бүтін сан *m* табылады. Мұндағы сан $m = \emptyset(n)$ болады.

Осы оң *m* сандарының ішіндегі ең кемі үшін келесідей аттар қолданылады:

- *n* модулі бойынша a санының дәрежесі;
- *n* модулі бойынша a санына сәйкес келетін көрсеткіш;
- a дәрежелерімен генерацияланатын тізбек кезеңкезеңінің ұзындығы.
- Осы a санынының ең үлкен дәрежесі – $\emptyset(n)$ болады.

Мысалы үшін 19 модулімен 7 санының *n* модулі бойынша дәрежелерін қарастырайық.

Осы *Ø(n)* дәреже сәйкес келген сандар модул *n* бойынша бастапқы түбірлері деп аталады. Мысалы, *P* - жай сан үшін, егер a - *P*- ның бастапқы түбірі болса, онда: $a, a^2, ..., a^{p-1}$ - олар әртүрлі болады;

n модулі бойынша 19 жай саны үшін оның бастапқы түбірлері 2,3,10,13,14,15 болады. Барлық сандардың бастапқы түбірлері бола бермейді. Бастапқы түбірлері бар сандар тек мына бүтін сандар*:* 2,4, $p^a, 2p^2$.

Мұнда *p* - кез келген тақ және жай сан.

Индекстер.

Жай нақты оң сандар үшін логарифм дәрежеге келтірудің негізгі теңдеуі болады. Осы сиякты қатыс айырымдар класының ариф-метикасында да болады. Жай логарифмдеудің қасиеттерін еске түсірейік; берілген санның логарифмі деп, берілген оң (және 1-ге тең болмаған) негізді дәрежеге келтіріп, сол дәрежені табамыз. Яғни

берілген негізгі *x* және кез келген *y* үшін $y = x^{\log_x y}$ болады. Оның келесідей қасиеттері бар.

$\log_x(1) = 0;$ $\log_x(yz) = \log_x(y) + \log_x(z);$

$\log_x(x) = 1;$ $\log_x(y^z) = z\log_x(y);$

Кейбір p – жай сандарының бастапқы түбірлерін қарастырамыз (осы сияқты аргументтерді жай болмаған сандар жағдайында да қолданса болады).

Мұндай жағдайда, a санының дәрежелері 1 - ден (p-1) - ге дейін өзгерсе, олар 1 - ден (p-1) дейін әрбір бүтін санды тек 1 реттен жаратады.

Онда әрқандай оң *в* санын айырымдар класында мына түрде көрсетсе болады*: в* ≡ *r mod p,* мұнда $1 \le r \le (p-1)$.

Осыдан мыналар шығады, кез келген бүтін *в* және *p*- жай санының кез-келген бастапқы a түбір үшін тек бір ғана *i* дәреже көрсеткішін тапса болады да оның үшін $в \equiv a^i \bmod p$, болады; мұнда $1 \le i \le (p-1)$.

Осы дәрежені *в* санының *p* модуліндегі және a негізіндегі индексі деп аталады. Бұл келесідей жазылады: $ind_{a,p}(в)$.

Мына мысалды қарастырайық*: mod 9* берілген болып, жай сан болмасын. Мұнда *Ø(n)*=6 және a =2 бастапқы түбірі болсын. a -ның дәрежелерін табайық:

$$2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 7(16); 2^5 = 5(32); 2^6 = 1(64); \bmod 9;$$

Енді қалдықтарды тәртіпке келтірейік*:*

Сонда олар 1,2,4,5,7,8,1,... болып, оған сәйкес дәрежелері*:* 0,1,2,5,4,3,...

Кез келген өзара жай сандар үшін Эйлер теоремасын қолданып, мына теңдеуді жазса болады: $a^{\theta(n)} \equiv 1 \bmod n$.

Осылардан төмендегідей қорытынды жасаймыз.

Кез келген *Z* бүтін санын мына түрде көрсетсе болады: *Z=q+kØ(n).*

Эйлер теоремасы бойынша*:. Егер де Z=qmodØ(n) болса, онда Z=q+kØ(n. болады.*

Алдынғыларды есепке ала отырып мына теңдеулерді аламыз:

$$ind_{a,p}(xy) = \left[ind_{a,p}(x) + ind_{a,p}(y)\right] \bmod Ø(p),$$

Сондай-ақ: $ind_{a,p}(y^2) = \left[rxind_{a,p}(y)\right] \bmod Ø(p).$

Логарифмдер мен индекстер арасында ұқсастық болғандықтан, индекстерді ***дискретті логарифмдер*** деп атаймыз. Мұнда еске алатын жай, егерде a m - нің бастапқы түбірі болса, онда a негізде m модулімен дискрет логарифмдері бір мәнді түрде анықталады.

Дискретті логарифмді есептеу

$y \equiv g^x \bmod p$ теңдеулерін қарастырамыз. g және p берілгенде y - ті табу оңай іс. Ең қиын болғанда x рет қайта көбейту керек болып, оған нәтижелі бағдаржол бар. Алайда егер y,g және p берілген болса, олардан x - ті табу (дискретті логарифмдеу), жалпылап айтқанда, оңай мәселе емес. Бұл мәселені күрделілік жағынан үлкен сандарды жай көбейткіштерге жіктеу мәселесімен салыстыруға болады; сондықтан ол *RSA* – криптографиялық бағдаржолында қолданылады.

Ақырғы кезде, жай сандар модулімен дискретті логарифмдерді есептеудің ассимтоталық ең жылдам мәнін бағдаржолдармен есептегенде мына тәртіпте бағаланады:

$$e^{(\ln p)^{1/3} \ln(\ln p)^{2/3}}.$$

Үлкен жай сандар үшін бұл есептеулер қазіргі есептеу технологияларының амалдағы мүмкіндіктерінен сыртта болады.

Осы қасиетті криптографияда **ашық кілттерді жаратуда** қолданса болады.

5-*қосымша.*

GF(2) – өрісінің үстінен келтірілмейтін көпмүшеліктер кестесі.

№ п/п	Дәреже	Көпмүшелік	Екілік тізбек
1	1	x+1	11
2	2	$x^2 + x + 1$	111
2 3	3	$x^3 + x + 1$	1011 1101
5 6 7	4	$x^3 + x^2 + 1$ $x^4 + x + 1$ $x^4 + x^3 + 1$	10011 11001 11111
8 9 10 11 12 13	5	$x^5 + x^3 + 1$ $x^5 + x^2 + x + 1$ $x^5 + x^3 + x^2 + x + 1$ $x^5 + x^4 + x^2 + x + 1$ $x^5 + x^4 + x^3 + x + 1$ $x^5 + x^4 + x^3 + x^2 + 1$	100101 101001 101111 110111 111011 111101
14 15 16 17 18 19 20 21 22	6	$x^6 + x + 1$ $x^6 + x^3 + 1$ $x^6 + x^4 + x^2 + x + 1$ $x^6 + x^4 + x^3 + x + 1$ $x^6 + x^5 + 1$ $x^6 + x^5 + x^2 + x + 1$ $x^6 + x^5 + x^3 + x^2 + 1$ $x^6 + x^5 + x^4 + x + 1$ $x^6 + x^5 + x^4 + x^2 + 1$	1000011 1001001 1010111 1011011 1100001 1100111 1101101 1110011 1110101

23 24 25 26 27 28 29 30 31 32 33 34 35 36 37	7	x^7+x+1 x^7+x^3+1 $x^7+x^3+x^2+x+1$ x^7+x^4+1 $x^7+x^4+x^3+x^2+1$ $x^7+x^5+x^2+x+1$ $x^7+x^5+x^3+x+1$ $x^7+x^5+x^4+x^3+1$ $x^7+x^5+x^4+x^3+x^2+x+1$ x^7+x^6+1 $x^7+x^6+x^3+x+1$ $x^7+x^6+x^4+x+1$ $x^7+x^6+x^5+x^2+1$ $x^7+x^6+x^5+x^3+x^2+x+1$	10000011 10001001 10001111 10010001 10011101 10100111 10101011 10111001 10111111 11000001 11001011 11010011 11010101 11100101 11101111
38 39 40		$x^7+x^6+x^5+x^4+1$ $x^7+x^6+x^5+x^4+x^2+x+1$ $x^7+x^6+x^5+x^4+x^3+x^2+1$	11110001 11110111 11111101
41 42		$x^8+x^4+x^3+x+1$ $x^8+x^4+x^3+x^2+1$	100011011 100011101
43 44 45 46		$x^8+x^5+x^3+x+1$ $x^8+x^5+x^3+x^2+1$ $x^8+x^5+x^4+x^3+1$ $x^8+x^5+x^4+x^3+x^2+x+1$	100101011 100101101 100111001 100111111

47 48 49 50 51 52 53 54	8	$x^8+x^6+x^3+x^2+1$ $x^8+x^6+x^4+x^3+x^2+x+1$ $x^8+x^6+x^5+x\ \ +1$ $x^8+x^6+x^5+x^2+1$ $x^8+x^6+x^5+x^3+1$ $x^8+x^6+x^5+x^4+1$ $x^8+x^6+x^5+x^4+x^2+x+1$ $x^8+x^6+x^5+x^4+x^3+x+1$	101001101 101011111 101100011 101100101 101101001 101110001 101110111 101111011
55 56 57 58		$x^8+x^7+x^2+x+1$ $x^8+x^7+x^3+x+1$ $x^8+x^7+x^3+x^2+1$ $x^8+x^7+x^4+x^3+x^2+x+1$	110000111 110001011 110001101 110011111
59 60 61 62		$x^8+x^7+x^5+x+1$ $x^8+x^7+x^5+x^3+1$ $x^8+x^7+x^5+x^4+1$ $x^8+x^7+x^5+x^4+x^3+x^2+1$	110100011 110101001 110110001 110111101
63 64 65 66 67 68 69 70		$x^8+x^7+x^6+x+1$ $x^8+x^7+x^6+x^3+x^2+1$ $x^8+x^7+x^6+x^4+x^2+x+1$ $x^8+x^7+x^6+x^4+x^3+x^2+1$ $x^8+x^7+x^6+x^5+x^2+x+1$ $x^8+x^7+x^6+x^5+x^4+x+1$ $x^8+x^7+x^6+x^5+x^4+x^2+1$ $x^8+x^7+x^6+x^5+x^4+x^3+1$	111000011 111001101 111010111 111011101 111100111 111110011 111110101 111111001

6-***қосымша***

Хэмминг кодын құруға мысалдар

Хэммингтің (n,k) кодтар жиынынан (7,4) коды берілген болып, хабар коды келесідей болсын: 1001; осыған Хэмминг кодын құрайық.

4 орын информациялық болғанда, 3 орын қосымша (тексеруші) болатыны анықтау Хэммингтің $\left(2^p-1,2^p-1-p\right), p=n-k$ теңдеуінен табылады; демек берілген хабар кодына 3 нөлді тіркейміз де келесідей код қисындастыруын аламыз: 1001 000.

Осы қисындастыруындағы әрбір таңбаны оңнан солға қарай нөмірлеп шығайық. Нөмірлерді таңбалардың үстіне жазамыз.

7 6 5 4 3 2 1

1 0 0 1 **0 0 0**

Кодтың бірлері бар орындардың нөмірлерін баған бойынша жазып шығайық; мысалда, 7 және 4-тің нөмірлерін жазамыз:

7 - 111

4 - 100

Нөмірлердің тұсына олардың екілік санақтағы кодын жазайық, яғни 7- нің тұсына 111 -ді, ал 4- тің тұсына 100- ді жазамыз.

Жазылған кодттың әрбір орнын жеке екілік модулде қосып шығамыз; сонда мынаны аламыз:

$$\begin{array}{r} 111 \\ \oplus \\ \underline{100} \\ 011 \end{array}$$

Алынған код қисындастыруын қосымша орындарға әрбір орнын жекелеп екілік модулде қосамыз; ол орындарда нөлдер болғандықтан құрылған Хэмминг код келесідей болады: 1 0 0 1 **0 1 1**.

Кодтың дұрыстығы былай тексеріледі;

Алдыңғыдай бірлері бар орындардың нөмірлерін жазып шығып, олардың әрбір орнын екілік модулде қосамыз.

Сонда қосындының нәтижесі нөл болуы керек.

$$\begin{array}{r} 001 \\ 010 \\ 100 \\ \underline{111} \\ 000 \end{array}$$

Бұл құрылған код байланыс арнасымен жіберілгенде, айталық бірінші орында қателік болды, яғни бірінші дәреже транформацияланды: 1 →0.

Кез келген орында қателік болса, ол таңбалық құрамы кері таңбаға транформацияланады.

Арнаның шығуында алынған қисындастыруы мына түрде болады: 1 0 0 1 0 1 **0** .

Таңбаларды нөмірлеп, екілік модулде қосып шықсақ нәтиже келесідей болады:

$$\begin{array}{l} 010 \\ 100 \\ \underline{\underline{111}} \\ 001_2 \rightarrow 1_{10} - орын \end{array}$$

Алынған код қисындастыруы екілік-сегіздік жүйеде қате бар болған орынды көрсетеді; яғни 1-орында қате бар.

Қателікті түзету үшін келесідей код қисындастыруы 0 0 0 0 0 0 1 әр орын бойынша екілік модулде қосылады; нәтижеде табылған қателік түзетілді:

1 0 0 1 0 1 **1 .**

Егер қателік екінші дәрежеге түскен болса, онда келесідей қисындастыруы арна шығуында болады: 1 0 0 1 0 **0** 1; онда қосынды келесідей болады:

$$\begin{array}{l} 001 \\ 100 \\ \underline{111} \\ 010_2 \rightarrow 2_{10} орын \end{array}$$

Қателіктің түзету жолы көрсетілгендей; яғни келесідей код қисындастыруы 0 0 0 0 0 1 0 әр орын бойынша екілік модульде қосылады.

Егер қателік үшінші орынға түскен болса, онда келесідей қисындастыруы арна шығуында болады: 1 0 0 1 **1** 1 1; онда қателікті табу операциясы келесідей болады:

001

010

011

100

111

$011_2 \rightarrow 3_{10}$ *орын*

Қателікті түзету үшін келесідей код қисындастыруы 0 0 0 0 **1** 0 0 әр дәреже бойынша екілік модулде қосылады; нәтижеде табылған қателік түзетілді:

1 0 0 1 **0** 1 1 **.**

Егер қателік төртінші орынға түскен болса, онда келесідей қисындастыруы арна шығуында болады: 1 0 0 **0** 0 1 1; онда қателікті табу операциясы келесідей болады:

001

010

111

$100_2 \rightarrow 4_{10}$ *орында*

Қателікті түзету үшін келесідей код қисындастыруы 0 0 0 **1** 0 0 0 әр орын бойынша екілік модулде қосылады; нәтижеде табылған қателік түзетілді:

1 0 0 **1** 0 1 1 **.**

Егер қателік бесінші орынға түскен болса, онда келесідей қисындастыруы арна шығуында болады: 1 0 **1** 1 0 1 1; онда қателікті табу операциясы келесідей болады:

001

010

100

101

111

$101_2 \rightarrow 5_{10}$ *орын*

Қателікті түзету үшін келесідей код қисындастыруы 0 0 **1** 0 0 0 0 әр орын бойынша екілік модульде қосылады; нәтижеде табылған қателік түзетілді:

1 0 **0** 1 0 1 1 .

Егер қателік алтыншы дәрежеге түскен болса, онда келесідей қисындастыруы арна шығуында болады: 1 **0** 0 1 0 1 1; онда қателікті табу операциясы келесідей болады:

$$\begin{array}{l} 001 \\ 010 \\ 100 \\ 110 \\ \underline{111} \\ 110_2 \rightarrow 6_{10} орын \end{array}$$

Қателікті түзету үшін келесідей код қисындастыруы 0 **1** 0 0 0 0 0 әр дәреже бойынша екілік модулде қосылады; нәтижеде табылған қателік түзетілді:

1 **0** 0 1 0 1 1 .

Егер қателік жетінші орынға түскен болса, ондакелесідей қисындастыруы арна шығуында болады: **0** 0 0 1 0 1 1; онда қателікті табу операциясы келесідей болады:

$$\begin{array}{l} 001 \\ 010 \\ \underline{100} \\ 111_2 \rightarrow 7_{10} орын \end{array}$$

Қателікті түзету үшін келесідей код қисындастыруы **1** 0 0 0 0 0 0 әр орын бойынша екілік модулде қосылады; нәтижеде табылған қателік түзетілді:

1 0 0 1 0 1 1 .

Тукубаев Зухирхан Бейсекович

ҚОЛДАНБАЛЫ АҚПАРАТТАР ТЕОРИЯСЫ

Басуға 28.12.2012 ж. қол қойылды.
Қағазы офсеттік. Қаріп түрі «Times».
Пішіні 60х901/16. Офсеттік басылым. Баспа табағы 27.
Таралымы 1000 дана. Тапсырыс № 216.

Тапсырыс берушінің дайын файлдарынан
басылып шықты.

ЖШС РПБК «Дәуір», 050009,
Алматы қаласы, Гагарин д-лы, 93а.
E-mail: rpik-dauir81@mail.ru