МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный технический университет имени К.И.Сатпаева

Институт информационных и телекоммуникационных технологий
Кафедра вычислительной техники

Ж.К. Алимсеитова

ТЕОРИЯ ИНФОРМАЦИИ

Учебно-методический комплекс дисциплины

(для специальности 5В100200 - Системы информационной безопасности)

Алматы 2011

СОСТАВИТЕЛИ: Ж.К. Алимсеитова. Теория информации. Учебно-методический комплекс дисциплины (для специальности 5В100200 – Системы информационной безопасности). Алматы: КазНТУ имени К.И. Сатпаева, 2011. С.1-96

Аннотация УМК данной дисциплины позволяет ознакомить студентов с основными понятиями теории информации, дать знания о хранении, измерении, обработки и передачи информации, сжатии информации, информационном канале и его модели, кодировании. Полученные знания являются основой для изучения теории защиты информации. Учебно-методический комплекс дисциплины студента (УМК ДС) представляет собой документ, определяющий концепцию конкретного курса. УМК составлен на основе типовой программы, издается типографским способом и предназначается для студентов, обучающихся по кредитной системе. УМК содержит учебную программу дисциплины (Syllabus), тематический план курса, систему заданий для самостоятельной работы студентов, график выполнения отчетных работ по дисциплине, тестовые задания для самоконтроля, тематику письменных работ и перечень экзаменационных вопросов. Ценность данного УМК состоит в распределении учебного времени по темам и видам учебных занятий, организации самостоятельной работы студентов в аудиторное и внеаудиторное время, активизации познавательной и творческой деятельности студентов и обеспечения взаимосвязи учебного и исследовательского процессов.

Итоговая строка (табл.31., рис.18)

Рецензент, к.т.н., доцент Калижанова А.У.

Печатается по Типовой учебной программе, утвержденной Министерством образования и науки Республики Казахстан на 2009 год.

1 УЧЕБНАЯ ПРОГРАММА ДИСЦИПЛИНЫ – SYLLABUS

1.1 Данные о преподавателе:

Преподаватель, ведущий занятия: Алимсеитова Жулдыз Кенесхановна, старший преподаватель кафедры ВТ.

Контактная информация: 8(727)-257-71-60, zhuldyz_al@mail.ru
Время пребывания на кафедре 211 ГУК, 9.00-18.00

1.2 Данные о дисциплине:

Название: Теория информации
Количество кредитов: 3
Место проведения: компьютерные лаборатории кафедры Вычислительная техника

Таблица 1

Выписка из учебного плана

Курс	Семестр	Кредиты	Академических часов в неделю					Форма контроля
			Лекций	Практ. занятия	СРСП	СРС	Всего	
1	2	3	4	5	6	7	8	9
1	2	3	2	1	3	3	9	Экзамен

1.3 Пререквизиты: предшествующие дисциплины необходимые для изучения данной дисциплины: «Математика 2».

1.4 Постреквизиты: перечень дисциплин, в которых используются знания изучаемой дисциплины (по рабочему учебному плану специальности): «Теоретические основы защиты информации».

1.5 Краткое содержание дисциплины

Целью преподавания дисциплины «Теория информации» является изучение вопросов, связанных с основными понятиями теории информации, дать знания о хранении, измерении, обработки и передачи информации, сжатии информации, информационном канале е его модели, кодировании.

Задачи изучения дисциплины. В результате изучения курса студент должен приобрести систематизированные знания в вопросах: виды информации, основы измерения информации, энтропия, избыточность, кодирование информации, системы и каналы связи, информационные системы и их модели, операторы управления.

1.6 Перечень и виды заданий и график их выполнения

Таблица 2

Виды заданий и сроки их выполнения

Виды контроля	Вид работы	Тема работы	Ссылки на рекомендуемую литературу с указанием страниц	Сроки сдачи
1	**2**	**3**	**4**	**5**
Текущий контроль	СР1	История развития теории информации	3[4-6], 7	1 нед.
Текущий контроль	ПР2	Количественная оценка информации. Формула Шеннона.	1[31-40], 2[97-106], 3[12-20], 6[12-15]	2 нед.
Текущий контроль	СР2	Измерение семантической, геометрической информации	1[54-63], 3[20-21], 6[75-80]	3 нед.
Текущий контроль	ПР4	Способы измерения информации. Избыточность	1[41-44], 2[105-111], 3[12-20], 6[35-41]	4 нед.
Текущий контроль	К1	Контрольная работа по пройденному материалу		4 нед.
Текущий контроль	СР3	Эпсилон-энтропия. Дифференциальная энтропия.	1[40-44], 2[8-13], 4[40-50]	5 нед.
Текущий контроль	ПР6	Условная энтропия	1[31-40], 2[97-106], 3[12-20] 6[12-15]	6 нед.
Текущий контроль	СР4	Свойства условной энтропии. Избыточность информации.	3[12-20]	7 нед.
Текущий контроль	ПР8	Сжатие информации. Алгоритм Шеннона-Фэно. Алгоритм Хаффмена.	3[21-25, 28-33, 35-42], 7	8 нед.
Рубежный контроль	РК1	Контрольная работа по модулю 1		8 нед.
Текущий контроль	СР5	Формы представления сигналов. Преимущества цифровой формы представления сигналов. Программы-архиваторы.	3[7-10], 3[42-44], 6[23-29], 7	9 нед.
Текущий контроль	ПР10	Алгоритмы Лемпеля-Зива.	3[25-28, 33-35], 6[130-141]	10 нед.
Текущий контроль	СР6	Арифметическое кодирование. Матричное кодирование.	3[25-28, 33-35], 6[130-141]	11 нед.
Текущий контроль	ПР12	Оптимальное кодирование	1[97-119], 2[162-193], 6[23-29]	12 нед.
Текущий контроль	К2	Контрольная работа по пройденному материалу		12 нед.
Текущий контроль	СР7	Совершенные и квазисовершенные коды. Полиномиальные коды.	3[61-69]	13 нед.

		Коды Боуза-Чоудхури-Хоккенгема		
Текущий контроль	ПР15	Полиномиальные коды	3[61-69]	14 нед.
Рубежный контроль	РК2	Контрольная работа по модулю 2		15 нед.
Итоговый контроль	Экзамен			

1.7 Список литературы

Основная литература

1.Темников Ф.Е., Афонин В.А., Дмитриев В.И. Теоретические основы информационной техники. М.: Энергия, 1979.

2. Дмитриев В.И. Прикладная теория информации. М.: Высшая школа, 1989.

3. Лидовский В.В. Теория информации. Москва, 2003.

4. Акулинчев Ю.П., Дроздова В.И. Сборник задач по теории информации. Изд-во Томского Университета. Томск, 1976.

Дополнительная литература

5. Шеннон К. Работы по теории информации и кибернетике. Москва. Издательство иностранной литературы. 1963.

6. Вернер М. Основы кодирования. М.: Техносфера 2004, 288с.

7. www.google.ru

1.8 Контроль и оценка знаний

По кредитной технологии обучения для всех курсов и по всем дисциплинам Казахского национального технического университета имени К. И. Сатпаева применяется рейтинговый контроль знаний студентов. Сведения об оценке знаний осуществляются по балльной рейтинговой системе в виде шкалы с указанными всеми видами контроля.

Для каждой дисциплины устанавливаются следующие виды контроля: текущий контроль, рубежный контроль, итоговый контроль.

Видами текущего контроля являются контрольные работы, рефераты, семестровые задания, коллоквиумы, выполнение лабораторных работ и др. К итоговому контролю относятся курсовой проект или курсовая работа и экзамен. В зависимости от видов итогового контроля применяются различные виды контроля (таблица 3).

Таблица 3

Распределение рейтинговых процентов по видам контроля

Вид итогового контроля	Виды контроля	Проценты
Экзамен	Итоговый контроль	100
	Рубежный контроль	100
	Текущий контроль	100

Сроки сдачи результатов текущего контроля определяются календарным графиком учебного процесса по дисциплине (таблица 4). Количество текущих контролей определяется содержанием дисциплины и ее объемом, которое указывается в учебно-методическом комплексе дисциплины.

Таблица 4

Календарный график сдачи всех видов контроля по дисциплине «Теория информации»

Недели	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Недельное количество контроля	1	1	1	2	1	1	1	2	1	1	1	2	1	1	1
Вид контроля	СР1	ПР2	СР2	ПР4, К1	СР3	ПР6	СР4	ПР8 РК1	СР5	ПР 10	СР6	ПР 12, К2	СР7	ПР 15	РК2
Виды контроля: КП – курсовой проект; КР – курсовая работа; К – контрольная работа; Л – лабораторная работа; СР – самостоятельная работа; Кл – коллоквиум; РК – рубежный контроль; Р – рефераты и др.															

Итоговая оценка по дисциплине определяется по шкале (таблица 5).

Таблица 5

Оценка знаний студентов

Оценка	**Буквенный эквивалент**	**Рейтинговый балл (в процентах %)**	**В баллах**
Отлично	A	95-100	4
	A-	90-94	3,67
Хорошо	B+	85-89	3,33
	B	80-84	3,0
	B-	75-79	2,67
Удовлетворительно	C+	70-74	2,33
	C	65-69	2,0
	C-	60-64	1,67
	D+	55-59	1,33
	D	50-54	1,0
Неудовлетворительно	F	0-49	0

Перечень вопросов для проведения контроля по модулям и промежуточной аттестации

Вопросы для проведения контроля по 1 модулю:

1. На каком этапе обращения информации получают сигнал?
2. Для чего нужны информационные системы в теории информации?
3. Какие меры информации существуют?
4. Семантическая мера информации.
5. Что является основной характеристикой сообщения?
6. Что такое энтропия?

7. Когда энтропия максимальна?
8. Когда энтропия равна нулю?
9. Электрические каналы утечки информации.
10. В каких системах сигналы передаются в непрерывной форме?
11. Какова специфика оценки неопределенности выбора для непрерывного источника информации?
12. Виды каналов утечки информации при эксплуатации компьютера.
13. Какие свойства у функции плотности вероятности?
14. Что такое условное распределение?
15. Что такое избыточность?

Вопросы для проведения контроля по 2 модулю:
1. Как классифицируются методы дискретизации?
2. Как осуществляется передача информации в ИС?
3. Что такое техническая скорость передачи?
4. Что является единицей измерения технической скорости?
5. Кодирование часто используемых элементов.
6. Контекстное сжатие данных.
7. Кагда код является эффективным?
8. Что позволяет эффективное кодирование?
9. Теорема Шеннона о помехоустойчивом кодировании.
10. Методы помехоустойчивого кодирования.
11. Что такое линейный групповой код?
12. Как задается линейный групповой код?
13. Что является признаком ошибки в циклическом коде?
14. Что нужно для коррекции ошибки в циклическом коде?
15. Циклические коды исправляющие пакеты ошибок.

Вопросы для подготовки к промежуточной аттестации:
1. Что производится на этапе восприятия информации?
2. Аддитивная мера информации.
3. К какой мере относится мера Хартли.
4. Что такое 1 дит и чему он равен?
5. От чего зависит степень неопределенности?
6. Что такое дифференциальная энтропия?
7. Как определяется общая энтропия зависимых ансамблей?
8. Что оценивается коэффициентом избыточности?
9. Какие типы коэффициентов избыточности существуют?
10. В чем суть метода Шеннона-Фано?
11. На чем основаны корректирующие коды?
12. Как можно построить порождающую матрицу линейного группового кода?
13. Что такое сигнал?

14. Что такое помехоустойчивость?
15. Что нужно для увеличения скорости передачи информации?

1.9 Политика и процедура

Студент обязан посещать все занятия. Если по какой-либо причине студент не может посещать занятия, он будет нести ответственность за весь материал, изучаемый на пропущенных занятиях. Если без уважительной причины студент пропустил более половины всех занятий, преподаватель имеет право ставить «не аттестовано» и студент не допускается до экзамена.

Преподаватель имеет право удалить из учебной аудитории студентов, мешающих проведению занятия и нарушающих дисциплину, на одно занятие. При повторном нарушении порядка студент освобождается от занятий.

Домашняя работа обязательна для выполнения.

При проведении контрольных работ преподаватель предлагает задания, объем и уровень сложности которых соответствует фактически изученному материалу. Студент, замеченный преподавателем со шпаргалкой, либо нарушающий порядок проведения контрольной работы, удаляется из учебной аудитории без права пересдачи.

Повторное проведение контрольной работы исключается. В случае отсутствия студента на занятии по уважительной причине (подтвержденной документально) возможна сдача пропущенного вида контроля в более поздние сроки (максимально возможный балл в этом случае умножается на 0,8 – например, студент пропустил по уважительной причине контроль, максимальный балл за который равен – 5, при сдаче данного контроля в более поздние сроки максимальный балл, который он может получить будет равен 5 * 0,8 = 4 балла). При не сдаче очередного контроля по неуважительной причине, сдача контроля в более поздние сроки запрещается.

2 Содержание активного раздаточного материала

2.1 Тематический план курса

Таблица 6

Тематический план курса

Наименование темы	Количество академических часов			
	Лек-ция	Практ. Зан.	СРСП	СРС
1	2	1	4	5
1. Введение. Этапы обращения информации. Задачи и постулаты прикладной теории информации. Информационные системы.	2	1	3	3

2. Измерение информации. Виды информации.	2	1	3	3
3. Количественная оценка информации. Энтропия.	2	1	3	3
4. Свойства энтропии.	2	1	3	3
5. Энтропия при непрерывном сообщении.	2	1	3	3
6. Условная энтропия.	2	1	3	3
7. Взаимная энтропия. Избыточность сообщений.	2	1	3	3
8. Системы и каналы связи. Формы представления сигналов. Дискретизация информации. Теорема Котельникова. Передача информации в информационной системе.	2	1	3	3
9. Скорость передачи информации. Пропускная способность каналов.	2	1	3	3
10. Сжатие данных.	2	1	3	3
11. Кодирование. Эффективное кодирование.	2	1	3	3
12. Кодирование информации для канала с помехами. Разновидности помехоустойчивых кодов. Методы помехоустойчивого кодирования.	2	1	3	3
13. Линейные групповые коды (ЛГК).	2	1	3	3
14. Циклические коды.	2	1	3	3
15. Реализация схем кодирования и декодирования в ЦК.	2	1	3	3
Всего (часов)	**30**	**15**	**45**	**45**

2.2 Конспект лекционных занятий

Лекция 1. *Введение. Этапы обращения информации. Задачи и постулаты прикладной теории информации. Информационные системы.*

Теория информации является одним из курсов при подготовке инженеров, специализирующихся в области автоматизированных систем управления и обработки информации. Функционирование таких систем существенным образом связано с получением, подготовкой, передачей, хранением и обработкой информации, поскольку без осуществления этих этапов невозможно принять правильное решение и осуществить требуемое управляющее воздействие, которое является конечной целью функционирования любой системы.

Возникновение теории информации связывают обычно с появлением фундаментальной работы американского ученого К. Шеннона «Математическая теория связи» (1948). Однако в теорию информации органически вошли и результаты, полученные другими учеными. Например, Р. Хартли, впервые предложил количественную меру информации (1928), акад. В. А. Котельников, сформулировал важнейшую теорему о возможности представления непрерывной функции совокупностью ее значений в отдельных точках отсчета (1933) и разработал оптимальные методы приема сигналов на фоне помех (1946). Акад. А. Н. Колмогоров, внес огромный вклад в

статистическую теорию колебаний, являющуюся математической основой теории информации (1941). В последующие годы теория информации получила дальнейшее развитие в трудах советских ученых (А. Н. Колмогорова, А. Я. Хинчина, В. И. Сифорова, Р. Л. Добрушина, М. С. Пинскера, А. Н. Железнова, Л. М. Финка и др.), а также ряда зарубежных ученых (В. Макмиллана, А. Файнстейна, Д. Габора, Р. М. Фано, Ф. М. Вудворта, С. Гольдмана, Л. Бриллюэна и др.).

К теории информации, в ее узкой классической постановке, относят результаты решения ряда фундаментальных теоретических вопросов. Это в первую очередь: анализ вопросов оценки «количества информации»; анализ информационных характеристик источников сообщений и каналов связи и обоснование принципиальной возможности кодирования и декодирования сообщений, обеспечивающих предельно допустимую скорость передачи сообщений по каналу связи, как при отсутствии, так и при наличии помех.

Этапы обращения информации

Можно выделить следующие этапы обращения информации:

1) восприятие информации;
2) подготовка информации;
3) передача и хранение информации;
4) обработка информации;
5) отображение информации;
6) воздействие информации.

Рисунок 1 - Этапы обращения информации

На этапе восприятия информации осуществляется целенаправленное извлечение и анализ информации о каком-либо объекте (процессе), в результате чего формируется образ объекта, проводится его опознание и оценка. При этом отделяют интересующую информацию от шумов.

На этапе подготовки информации получают сигнал в форме, удобной для передачи или обработки (нормализация, аналого-цифровое преобразование и т.д.).

На этапе передачи и хранения информация пересылается либо из одного места в другое, либо от одного момента времени до другого.

На этапе обработки информации выделяются ее общие и существенные взаимозависимости для выбора управляющих воздействий (принятия решений).

На этапе отображения информации она представляется человеку в форме, способной воздействовать на его органы чувств.

На этапе воздействия информация используется для осуществления необходимых изменений в системе.

Задачи и постулаты прикладной теории информации

К теории информации относят результаты решения ряда фундаментальных теоретических вопросов:

- анализ сигналов как средства передачи сообщений, включающий вопросы оценки переносимого ими «количества информации»;
- анализ информационных характеристик источников сообщений и каналов связи и обоснование принципиальной возможности кодирования и декодирования сообщений, обеспечивающих предельно допустимую скорость передачи сообщений по каналу связи, как при отсутствии, так и при наличии помех.

В теории информации исследуются информационные системы при четко сформулированных условиях (постулатах):

1. Источник сообщения осуществляет выбор сообщения из некоторого множества с определенной вероятностью.
2. Сообщения могут передаваться по каналу связи в закодированном виде. Кодированные сообщения образуют множество, являющееся взаимно однозначным отображением множества сообщений. Правило декодирования известно декодеру (записано в его программе).
3. Сообщения следуют друг за другом, причем число сообщений может быть сколь угодно большим.
4. Сообщение считается принятым верно, если в результате декодирования оно может быть в точности восстановлено. При этом не учитывается, сколько времени прошло с момента передачи сообщения до момента окончания декодирования, и какова сложность операций кодирования и декодирования.
5. Количество информации не зависит от смыслового содержания сообщения, от его эмоционального воздействия, полезности и даже от его отношения к реальной действительности.

Информационные системы

В основе решения многих задач лежит обработка информации. Для облегчения обработки информации создаются ***информационные системы (ИС).*** Автоматизированными называют ИС, в которых применяют технические средства, в частности ЭВМ. Большинство существующих ИС являются автоматизированными, поэтому для краткости просто будем называть их ИС. В ***широком понимании*** под определение ИС подпадает любая система обработки информации. По ***области применения*** ИС можно разделить на системы, используемые в производстве, образовании, здравоохранении, науке, военном

деле, социальной сфере, торговле и других отраслях. По ***целевой функции*** ИС можно условно разделить на следующие основные категории: управляющие, информационно-справочные, поддержки принятия решений. Заметим, что иногда используется более ***узкая трактовка понятия ИС*** как совокупности аппаратно-программных средств, задействованных для решения некоторой прикладной задачи. В организации, например, могут существовать информационные системы, на которые возложены следующие задачи: учет кадров и материально-технических средств, расчет с поставщиками и заказчиками, бухгалтерский учет и т. п. Эффективность функционирования информационной системы (ИС) во многом зависит от ее архитектуры. В настоящее время перспективной является архитектура клиент-сервер. В распространенном варианте она предполагает наличие компьютерной сети и распределенной базы данных, включающей корпоративную базу данных (КБД) и персональные базы данных (ПБД). КБД размещается на компьютере-сервере, ПБД размещаются на компьютерах сотрудников подразделений, являющихся клиентами корпоративной БД. ***Сервером*** определенного ресурса в компьютерной сети называется компьютер (программа), управляющий этим ресурсом. ***Клиентом*** — компьютер (программа), использующий этот ресурс. В качестве ресурса компьютерной сети могут выступать, к примеру, базы данных, файловые системы, службы печати, почтовые службы. Тип сервера определяется видом ресурса, которым он управляет. Например, если управляемым ресурсом является база данных, то соответствующий сервер называется сервером базы данных. Достоинством организации информационной системы по архитектуре клиент-сервер является удачное сочетание централизованного хранения, обслуживания и коллективного доступа к общей корпоративной информации с индивидуальной работой пользователей над персональной информацией. Архитектура клиент-сервер допускает различные варианты реализации.

Основная литература: 1[31-44], 2 [97-111], 3 [4-6, 8-11].

Дополнительная литература: 6 [12-15, 35-41]

Контрольные вопросы

1. Какие этапы обращения информации существуют?
2. Задачи теории информации.
3. История развития теории информации.

Лекция 2. *Виды информации. Измерение информации.*

Измерение информации (меры информации)

Синтаксическая мера информации

Объем данных Vд. в сообщение измеряется количеством символов (разрядов) в этом сообщение. В различных системах счисления один разряд имеет различный вес и соответственно меняется единица измерения данных:

- в двоичной системе счисления единица измерения - бит (bit-binary digit-двоичный разряд);

- в десятичной системе счисления единица измерения – дит (десятичный разряд).

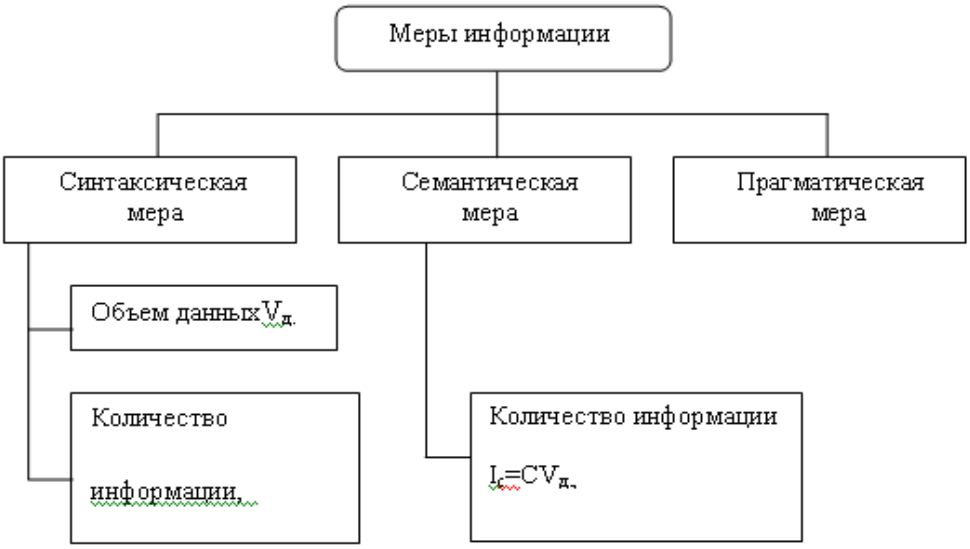


Рисунок 2 – Меры информации

Количество информации I на синтаксическом уровне невозможно определить без рассмотрения понятия неопределенности состояния системы (энтропии системы). Получение информации о какой–либо системе всегда связано с изменением степени неосведомленности получателя о состоянии этой системы. (Теория Шеннона).

Таблица 7

Характеристика мер информации

Мера информации	Единицы измерения	Примеры
Синтаксическая: шенноновский подход компьютерный подход	Степень уменьшения неопределенности Единицы представления информации	Вероятность события Бит, байт, Кбайт и т.д.
Семантическая	Тезаурус Экономически показатель	Пакет прикладных программ, ПК, компьютерные сети, Рентабельность, производительность и т.д.
Прагматическая	Ценность использования	Емкость памяти, производительность ПК, скорость передачи данных и т.д. Денежное выражение
Алгоритмическая	Минимальное число внутренних состояний машины	Машина Тьюринга

Семантическая мера информации.

Тезаурус- это совокупность сведений, которыми располагает пользователь или система.

В зависимости от соотношений между смысловым содержанием информации S и тезаурусом пользователя Sp. изменяется количество семантической информации Ic, воспринимаемой пользователем и включаемой им в дальнейшем в свой тезаурус.

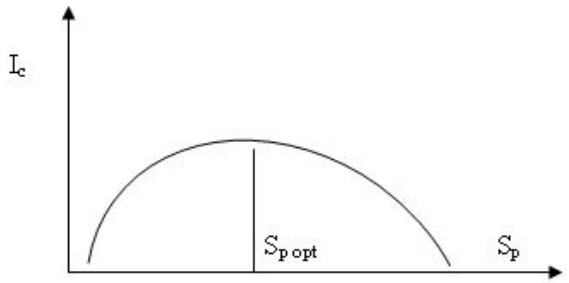


Рисунок 3 – Тезаурус

при $S_p \approx 0$ пользователь не воспринимает, не понимает поступающую информацию; при $S_p \rightarrow \infty$ пользователь все знает, и информация ему не нужна.

Максимальное количество информации I_c потребитель приобретает при согласовании ее смыслового содержания S со своим тезаурусом S_p ($S_p = S_{p\,opt}$) ,когда поступающая информация понятна пользователю и несет ему ранее не известные (отсутствующие в его тезаурусе) сведения.

Относительной мерой количества семантической информации может служить коэффициент содержательности C, который определяется как отношение количества семантической информации к ее объему:$C= I_c / V_{д.}$

Прагматическая мера информации. Эта мера определяет полезность информации (ценность) для достижения пользователем поставленной цели. Эта мера также величина относительная, обусловленная особенностями использования этой информации в той или иной системе. Ценность информации целесообразно измерять в тех же единицах (или близких к ним), в которых измеряется целевая функция.

Алгоритмическая мера информации. Каждый согласится, что слово 0101….01 сложнее слова 00….0, а слово, где 0 и 1 выбираются из эксперимента – бросания монеты (где 0-герб,1 –решка),сложнее обоих предыдущих .

Любому сообщению можно приписать количественную характеристику, отражающую сложность (размер) программы, которая позволяет ее произвести.

Так как имеется много разных вычислительных машин и разных языков программирования (разных способов задания алгоритма), то для определенности задаются некоторой конкретной вычислительной машиной, например машиной Тьюринга.

Сложность слова (сообщения) определяется как минимальное число внутренних состояний машины Тьюринга, требующиеся для его воспроизведения.

Структурные меры информации: структурная, геометрическая и др. меры информации.

Геометрическая (метрическая):

***Единица измерения* – метрон** (мера точности измеряемого параметра);

***Метронная мощность (плотность)*физической системы** – количество метронов в расчете на единичный объем координатного пространства;

Применяется и для оценки максимально возможного количества информации в заданных структурных габаритах - информационной емкости устройств.

Комбинаторная (структурная) возможное количество комбинаций информационных элементов

Перестановки – группы элементов, содержащие все имеющиеся в наличии элементы

Определение количества информации в комбинаторной мере - определение количества возможных или существующих комбинаций, т.е. оценка структурного разнообразия информационного устройства.

Аддитивная мера – мера Хартли – логарифм числа возможных размещений из h элементов по *l*

$$I = \log V_h^l = l * \log h$$

Позволяет производить суммирование количеств информации отдельных элементов информационного комплекса. **Всегда *положительна.***

Логарифм с основанием 2 - единица количества информации говорит о том, что произошло одно из двух равновероятных событий (***двоичная единица информации* или *бит).***

Логарифм с основанием 10 - количество информации в ***дитах*,** натуральный логарифм с основанием e=2,71828 – в ***нитах*.**

Таблица 8

Формулы измерения

$P_h = h!$	Количество перестановок из h элементов без повторений.
$P = \frac{\alpha + \beta + ...v\gamma}{\alpha!\beta!\gamma!}$	Количество *перестановок* из h элементов с *повторениями* при условии, что один из элементов повторяется α раз, другой β , последний γ раз.
Сочетания -	группы по l элементов, образуемые из h разных элементов, различающиеся между собой самими элементами.
$C_n = \frac{h!}{l!(h-l)!}$	Количество сочетаний из h элемен- тов по *l* (без повторений).
$C_n^{l(повт)} = \frac{(h+l-1)!}{l!(h-l)!}$	Количество сочетаний из h разных элементов по *l* элементов с повторениями, в которые элементы могут входить многократно (до группы по *l* элементов, образуемые из h разных элементов,

	различающиеся между собой либо самими элементами, либо порядком их следования.
$V_h^l = \frac{h}{(h-l)!}$	Количество размещений из h разных элементов по l элементов без повторений.
$v_h^{l(повт)} = h^l$	Количество размещений из h разных элементов по l элементов с повторениями.

Основная литература: 1[31-44], 2 [97-111], 2 [6-8, 11-12, 20-21]
Дополнительная литература: 6 [12-15, 35-41]
Контрольные вопросы:
1. Какие виды информации существуют?
2. Синтаксическая мера информации.
3. Прагматическая мера информации.
4. Алгоритмическая мера информации.
5. Геометрическая мера информации.

Лекция 3. *Количественная оценка информации.*

В качестве основной характеристики сообщения теория информации принимает величину, называемую **количеством информации**. Это понятие не затрагивает смысла и важности передаваемого сообщения, а связано со степенью его неопределенности.

Пусть алфавит источника сообщений состоит из **m** знаков, каждый из которых может служить элементом сообщения. Количество **N** возможных сообщений длины **n** равно числу перестановок с неограниченными повторениями:

$$N = m^n \qquad (1)$$

Если для получателя все **N** сообщений от источника являются равновероятными, то получение конкретного сообщения равносильно для него случайному выбору одного из **N** сообщений с вероятностью **1/N**.

Ясно, что чем больше **N***, тем большая степень неопределенности характеризует этот выбор и тем более информативным можно считать сообщение*.

Поэтому число **N** могло бы служить мерой информации. Однако, с позиции теории информации, естественно наделить эту меру свойствами *аддитивности*, т.е. определить ее так, чтобы она бала пропорциональна длине сообщения (например, при передаче и оплате сообщения - телеграммы, важно не ее содержание, а общее число знаков).

В качестве меры неопределенности выбора состояния источника с равновероятными состояниями принимают логарифм числа состояний:

$$I = \log N = \log m^n = n \log m \quad (2)$$

Эта логарифмическая функция характеризует **количество информации:**

Указанная мера была предложена американским ученым Р. Хартли в 1928г.

Количество информации, приходящееся на один элемент сообщения (знак, букву), называется **энтропией**:

$$H = \frac{I}{n} = \frac{n \log m}{n} = \log m \quad (3)$$

В принципе безразлично, какое основание логарифма использовать для определения количества информации и энтропии, т. к. в силу соотношения $\log_a m = \log_a b \log_b m$ переход от одного основания логарифма к другому сводится лишь к изменению единицы измерения.

Так как современная информационная техника базируется на элементах, имеющих два устойчивых состояния, то обычно выбирают основание логарифма равным двум, т.е. энтропию выражают как:

$H_0 = \log_2 m$.

Тогда **единицу количества информации** на один элемент сообщения называют **двоичной единицей** или **битом**. При этом единица неопределенности (двоичная единица или бит) представляет собой неопределенность выбора из двух равновероятных событий *(bit* — сокращение от англ. *binary digit* — двоичная единица)

Так как из $\log_2 m = 1$ следует $m = 2$, то ясно, что 1 бит - это количество информации, которым характеризуется один двоичный элемент при равновероятных состояниях 0 и 1.

Двоичное сообщение длины **n** содержит **n** бит информации.

Единица количества информации, равная 8 битам, называется **байтом**.

Если основание логарифма выбрать равным десяти, то энтропия выражается в десятичных единицах на элемент сообщения - **дитах**, причем 1 дит = $\log_{10}2$ бит = 3,32 бит.

Пример1. Определить количество информации, которое содержится в телевизионном сигнале, соответствующем одному кадру развертки. Пусть в кадре 625 строк, а сигнал, соответствующий одной строке, представляет собой последовательность из 600 случайных по амплитуде импульсов, причем амплитуда импульса может принять любое из 8 значений с шагом в 1 В.

Решение. В рассматриваемом случае длина сообщения, соответствующая одной строке, равна числу случайных по амплитуде импульсов в ней: **n = 600**.

Количество элементов сообщения (знаков) в одной строке равно числу значений, которое может принять амплитуда импульсов в строке,: **m = 8.**

Количество информации в одной строке: **I = n log m = 600 log 8,** а количество информации в кадре: **I′ = 625 I = 625 600 log 8 = 1,125 · 10^6 бит**

Пример2. Определить минимальное число взвешиваний, которое необходимо произвести на равноплечих весах, чтобы среди 27 внешне неотличимых монет найти одну фальшивую, более легкую.

Решение. Так как монеты внешне не отличимые, то они представляют источник с равновероятными состояниями, а общая неопределенность ансамбля, характеризующая его энтропию, поэтому составляет: H1= $Iog_2 27$ бит.

Одно взвешивание способно прояснить неопределенность ансамбля насчитывающего три возможных исхода (левая чаша весов легче, правая чаша весов легче, весы находятся в равновесии).Так как все исходы равновероятны (нельзя заранее отдать предпочтение одному из них), то результат одного взвешивания представляет источник с равновероятными состояниями, а его энтропия составляет: H2= $Iog_2 3$ бит.

Так как энтропия отвечает требованию аддитивности и при этом **H1=3H2= 3 $1og_2 3$**, то для определения фальшивой монеты достаточно произвести три взвешивания.

Алгоритм определения фальшивой монеты следующий. При первом взвешивании на каждую чашку весов кладется по девять монет. Фальшивая монета будет либо среди тех девяти монет, которые оказались легче, либо среди тех, которые не взвешивались, если имело место равновесие. Аналогично, после второго взвешивания число монет, среди которых находится фальшивая монета, сократится до трех. Последнее, третье, взвешивание дает возможность точно указать фальшивую монету.

Рассмотренная выше оценка информации основана на предположении о равновероятности всех знаков алфавита.

В общем случае каждый из знаков появляется в сообщении с различной вероятностью.

Пусть на основании статистического анализа известно, что в сообщении длины **n** знак $\mathbf{x_i}$ появляется $\mathbf{n_i}$ раз, т.е. вероятность появления знака:

$$Pi = \frac{ni}{n}, \text{ (i = 1, 2, 3, ... , m)} \qquad (4)$$

Все знаки алфавита составляют полную систему случайных событий, поэтому:

$$\sum_{i=1}^{m} Pi = 1 \qquad (5)$$

Число всех возможных сообщений длины **n**, в которых знак $\mathbf{x_i}$ входит $\mathbf{n_i}$ раз, где **i = 1, 2, 3 ... ,m,** определяется как число перестановок с повторениями из **n** элементов, спецификация которых $\mathbf{\{n_1, n_2, ..., n_m\}}$. Поэтому количество возможных сообщений определяют по формуле:

$$N = \frac{n!}{n1!n2!...nm!} \tag{6}$$

Например, план застройки улицы 10 домами, среди которых 3 дома одного типа, 5 другого и 2 третьего, можно представить

$$\frac{10!}{3!5!2!} = 2520 способами \tag{7}$$

Количество информации можно найти по формуле:

$I = \log N = \log n! - (\log n_1! + \log n_2! + ... + \log n_m!)$.

Для достаточно больших **n** это выражение можно преобразовать с помощью приближенной формулы Стирлинга:

$$\log n! \approx n(\ln n - 1) \tag{8}$$

Воспользовавшись формулой Стирлинга и соотношением $\sum_{i=1}^{m} ni = n$, получают:

$$\begin{aligned} I = \ln N = n(\ln n - 1) - \sum_{i=1}^{m} ni(\ln ni - 1) = n\ln n - \sum_{i=1}^{m} ni \ln ni = \\ = -n[-\ln n + \sum_{i=1}^{m} \frac{ni}{n}(\ln \frac{ni}{n} + \ln n)] = -n(-\ln n + \sum_{i=1}^{m} \frac{ni}{n} \ln \frac{ni}{n} + \\ + \ln n \sum_{i=1}^{m} \frac{ni}{n}) = -n \sum_{i=1}^{m} \frac{ni}{n} \ln \frac{ni}{n} \end{aligned} \tag{9}$$

Переходя к вероятностям и произвольным основаниям логарифмов, получают **формулы Шеннона для количества информации и энтропии*:***

$$\begin{aligned} I = -n \sum_{i=1}^{m} Pi \log Pi; \\ H = -\sum_{i=1}^{m} Pi \log Pi \end{aligned} \tag{10}$$

В дальнейшем в выражениях для количества информации I и энтропии H всегда используют логарифмы с основанием 2.

Основная литература: 1[44-46], 2[11-119, 125-128], 3 [12-19]
Дополнительная литература: 4[75-76]
Контрольные вопросы:

1. Что зависит от основания логарифма в формуле количества информации?
2. Формула Стирлинга.
3. Формулы Шеннона.

Лекция 4. *Свойства энтропии.*

При равновероятности знаков алфавита **Pi = 1/m** из формулы Шеннона получают:

$$H = -\sum_{i=1}^{m} Pi \log Pi = -\sum_{i=1}^{m} \frac{1}{m} \log \frac{1}{m} = -(m\frac{1}{m})(-\log m) = \log m \qquad (11)$$

Из этого следует, что при равновероятности знаков алфовита энтропия определяется исключительно числом знаков m алфавита и по существу является характеристикой только алфавита.

Если же знаки алфавита неравновероятны, то алфавит можно рассматривать как дискретную случайную величину, заданную статистическим распределением частот $\mathbf{n_i}$ появления знаков $\mathbf{x_i}$ (или вероятностей $\mathbf{Pi = n_i / n}$) таблица 9:

Таблица 9

Пример распределения частот

Знаки x_i	x_1	x_2	. . .	x_m
Частоты n_i	n_1	n_2	. . .	n_m

Такие распределения получают обычно на основе статистического анализа конкретных типов сообщений (например, русских или английских текстов и т.п.).

Поэтому, если знаки алфавита неравновероятны и хотя формально в выражение для энтропии входят только характеристики алфавита (вероятности появления его знаков), энтропия отражает статистические свойства некоторой совокупности сообщений.

На основании выражения

$$H = -\sum_{i=1}^{m} Pi \log Pi = \sum_{i=1}^{m} Pi \log \frac{1}{Pi} \quad , \qquad (12)$$

величину **log 1/Pi** можно рассматривать как **частную энтропию**, характеризующую информативность знака $\mathbf{x_i}$, а **энтропию H -** как **среднее значение частных энтропий.**

Функция **(Pi · log Pi)** отражает вклад знака $\mathbf{x_i}$ в энтропию **H.** При вероятности появления знака **Pi=1** эта функция равна нулю, затем возрастает до своего максимума, а при дальнейшем уменьшении **Pi** стремится к нулю (функция имеет экстремум) рисунок 4 :

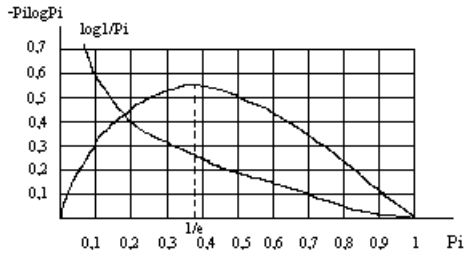


Рисунок 4 - Графики функций log 1/Pi и -Pi · log Pi

Для определения координат максимума этой функции нужно найти производную и приравнять ее к нулю.

Из условия $\frac{\partial}{\partial Pi}(-Pi\log Pi) = -\log Pi - \log e = -\log Pie = 0$ находят: **Pi e = 1**,где **e** - основание натурального логарифма.

Таким образом, функция: **(Pi log Pi)** при **Pi = 1/e = 0,37** имеет максимум: $\frac{1}{e}\log e = 0{,}531$, т.е. координаты максимума (0,37; 0,531)

Энтропия **H** - величина вещественная, неотрицательная и ограниченная, т.е. **H ≥ 0** (это свойство следует из того, что такими же качествами обладают все ее слагаемые **Pi log 1/Pi).**

Энтропия равна нулю, если сообщение известно заранее (в этом случае каждый элемент сообщения замещается некоторым знаком с вероятностью, равной единице, а вероятности остальных знаков равны нулю).

Энтропия максимальна, **если все знаки алфавита равновероятны**, т.е. $\mathbf{H_{max} = \log m}$.

Таким образом, степень неопределенности источника информации зависит не только от числа состояний, но и от вероятностей этих состояний. При неравновероятных состояниях свобода выбора источника ограничивается, что должно приводить к уменьшению неопределенности. Если источник информации имеет, например, два возможных состояния с вероятностями 0,99 и 0,01, то неопределенность выбора у него значительно меньше, чем у источника, имеющего два равновероятных состояния. Действительно, в первом случае результат практически предрешен (реализация состояния, вероятность которого равна 0,99), а во втором случае неопределенность максимальна, поскольку никакого обоснованного предположения о результате выбора

сделать нельзя. Ясно также, что весьма малое изменение вероятностей состояний вызывает соответственно незначительное изменение неопределенности выбора.

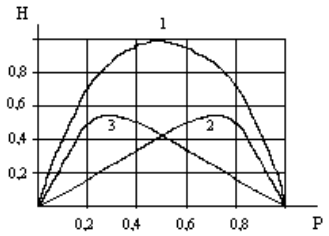
Пример 1. Распределение знаков алфавита имеет вид $\mathbf{p(x_1) = 0,1\ p(x_2) = 0,1\ p(x_3) = 0,1\ p(x_4) = 0,7.}$ Определить число знаков другого алфавита, у которого все знаки равновероятны, а энтропия такая же как и у заданного алфавита.

Особый интерес представляют ***бинарные сообщения***, использующие алфавит из двух знаков: **(0,1).** При **m = 2** сумма вероятностей знаков алфавита: $\mathbf{P_{1+}P_2 = 1}$. Можно положить $\mathbf{P_1 = P}$, тогда $\mathbf{P_2 = 1\text{-}P.}$

Энтропию можно определить по формуле:

$$H = -P1\log P1 - P2\log P2 = -P\log P - (1-P)\log(1-P), \qquad (13)$$

Энтропия бинарных сообщений достигает максимального значения, равного 1 биту, когда знаки алфавита сообщений равновероятны, т.е. при P = 0,5, и ее график симметричен относительно этого значения.(рисунок 5).



Рисисунок 5 - График зависимости энтропии **H** двоичных сообщений (1) и ее составляющих (2,3): - **(1 - P) log (1 - P)** и **- P log P** от **P**.

Пример 2. Сравнить неопределенность, приходящуюся на букву источника информации (алфавита русского языка), характеризуемого ансамблем, представленным в таблице 10, с неопределенностью, которая была бы у того же источника при равновероятном использовании букв.

Таблица 10

Ансамбль русского языка

Буква	Вероятность	Буква	Вероятность	Буква	Вероятность
А	0,064	л	0,036	ц	0,04
Б	0,015	м	0,026	ч	0,013
В	0,039	н	0,056	ш	0,006
Г	0,014	о	0,096	ш	0,003
Д	0,026	п	0,024	ъ,ь	0,015
е,ё	0,074	р	0,041	ы	0,016
Ж	0,008	с	0,047	э	0,003
З	0,015	т	0,056	ю	0,007

И	0,064	у	0,021	я	0,019
Й	0,010	ф	0,02	пробел	0,143
К	0,029	х	0,09		

Решение. 1. При одинаковых вероятностях появления любой из всех **m = 32** букв алфавита неопределенность, приходящуюся на одну букву, характеризует энтропия

H = log m = log 32 = 5 бит.

2. Энтропию источника, характеризуемого заданным табл. 2.2 ансамблем, находят по формуле:

$$H = -\sum_{i=1}^{m} p_i \log p_i = \text{ -0,064 log 0,064 -0,015log0,015 - 0,143log0,143} \approx 4{,}43$$

бит.

Таким образом, неравномерность распределения вероятностей использования букв снижает энтропию источника с 5 до 4,42 бит

Пример 3. Заданы ансамбли **X** (таблица 11) и **Y (**таблица 12**)** двух дискретных величин**:**

Таблица 11

Ансамбль X

Случайные величины x_i	0,5	0,7	0,9	0,3
Вероятности их появления	0,25	0,25	0,25	0,25

Таблица 12

Ансамбль У

Случайные величины y_j	5	10	15	8
Вероятности их появления	0,25	0,25	0,25	0,25

Сравнить их энтропии.

Решение. Энтропия не зависит от конкретных значений случайной величины. Так как вероятности их появления в обоих случаях одинаковы, то

$$H(X) = H(Y) = -\sum_{i=1}^{m} p_i \log p_i = \text{ - 4(0,25log0,25) = -4(1/4log1/4) =}$$

= log 4 = 2 бит

Основная литература: 1[44-46], 2[11-119, 125-128], 3 [12-19]

Дополнительная литература: 4[75-76]

Контрольные вопросы:

1. Что следует из равновероятности знаков алфавита?

2. Когда алфавит можно рассматривать как дискретную случайную величину?

3. Что такое частная энтропия?

Лекция 5. *Энтропия при непрерывном сообщении.*

В предыдущих лекциях была рассмотрена мера неопределенности выбора для дискретного источника информации. На практике в основном встречаются с источниками информации, множество возможных состояний которых составляет континуум. Такие источники называют *непрерывными* источниками информации.

Во многих случаях они преобразуются в дискретные посредством использования устройств дискретизации и квантования. Вместе с тем существует немало и таких систем, в которых информация передается и преобразуется непосредственно в форме непрерывных сигналов. Примерами могут служить системы телефонной связи и телевидения.

Оценка неопределенности выбора для непрерывного источника информации имеет определенную специфику. Во-первых, значения, реализуемые источником, математически отображаются случайной непрерывной величиной. Во-вторых, вероятности значений этой случайной величины не могут использоваться для оценки неопределенности, поскольку в данном случае вероятность любого конкретного значения равна нулю. Естественно, однако, связывать неопределенность выбора значения случайной непрерывной величины с плотностью распределения вероятностей этих значений. Учитывая, что для совокупности значений, относящихся к любому сколь угодно малому интервалу случайной непрерывной величины, вероятность конечна, попытаемся найти формулу для энтропии непрерывного источника информации, используя операции квантования и последующего предельного перехода при уменьшении кванта до нуля.

Для обобщения формулы **Шеннона** разобьем интервал возможных состояний случайной непрерывной величины **X** на равные непересекающиеся отрезки **Δx** и рассмотрим множество дискретных состояний $\mathbf{x_1, x_2, ... , x_m}$ с вероятностями $\mathbf{Pi = p(x_i)\Delta x\ (i = 1, 2, ... , m).}$ Тогда энтропию можно вычислить по формуле:

$$H = -\sum_{i=1}^{m} p(xi)\Delta x \log p(xi)\Delta x = -\sum_{i=1}^{m} p(xi)\Delta x \log p(xi) - -\sum_{i=1}^{m} p(xi)\Delta x \log \Delta x$$

В пределе при $\mathbf{\Delta x \to 0}$ с учетом соотношения:

$$\int_{-\infty}^{\infty} p(x)dx = 1, \qquad (14)$$

Получим $H(x) = -\int_{-\infty}^{\infty} p(x)\log p(x)dx - \log\Delta x$.

Первое слагаемое в правой части соотношения имеет конечное значение, которое зависит только от закона распределения непрерывной случайной величины X и не зависит от шага квантования. Оно имеет точно такую же структуру, как энтропия дискретного источника.

Поскольку для определения этой величины используется только функция плотности вероятности, т. е. дифференциальный закон распределения, она получила название относительной дифференциальной энтропии или просто **дифференциальной энтропии** непрерывного источника информации (непрерывного распределения случайной величины X).

Первое слагаемое в этой сумме, называемое также **приведенной энтропией**, целиком определяет информативность сообщений, обусловленных статистикой состояний их элементов.

Величина **logΔx** зависит только от выбранного интервала **Δx,** определяющего точность квантования состояний, и при **Δx =const** она постоянна.

Энтропия и количество информации зависят от распределения плотности вероятностей p(x).

В теории информации большое значение имеет решение вопроса о том, при каком распределении обеспечивается максимальная энтропия **H(x).**

Можно показать, что при заданной дисперсии:

$$\sigma^2 = \int_{-\infty}^{\infty} x^2 p(x)dx = const, \qquad (15)$$

наибольшей информативностью сообщение обладает только тогда, когда состояния его элементов распределены по нормальному закону:

$$p(x) = \frac{1}{\sigma\sqrt{\pi}} e^{-\frac{x^2}{2\sigma^2}}, \qquad (16)$$

Так как дисперсия определяет среднюю мощность сигнала, то отсюда следуют практически важные выводы.

Передача наибольшего количества информации при заданной мощности сигнала (или наиболее экономичная передача информации) достигается при такой обработке сигнала, которая приближает распределение плотности вероятности его элементов к нормальному распределению.

В то же время, обеспечивая нормальное распределение плотности вероятности элементам помехи, обеспечивают ее наибольшую “

информативность", т.е наибольшее пагубное воздействие на прохождение сигнала. Найдем значение энтропии, когда состояния элементов источника сообщений распределены по нормальному закону:

$$H = -\frac{1}{e\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{x^2}{2\sigma^2}} \log[\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}]dx - \log\Delta x =$$

$$= \log(\sigma\sqrt{2\pi}\frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{x^2}{2\sigma^2}} dx + \frac{\log e}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{x^2}{2\sigma^2}} dx - \log\Delta x) = \qquad (17)$$

$$= \log(\frac{\sigma}{\Delta x}\sqrt{2\pi e})$$

Найдем значение энтропии, когда состояния элементов распределены внутри интервала их существования **a ≤ x ≤ b** по равномерному закону, т.е.

$$\text{p(x)} = \begin{cases} \frac{1}{b-a} \bullet \text{p} \text{ЦИ} a \le x \le b \\ 0 \bullet \text{p} \text{ЦИ} x < a, x > b \end{cases}$$

$$H_p(x) = -\frac{1}{b-a}\int_a^b \log(\frac{1}{b-a} - \Delta x)dx = \log\frac{b-a}{\Delta x} \qquad (18)$$

Дисперсия равномерного распределения $\sigma_p^2 = \frac{(b-a)^2}{12}$, поэтому (b-a) = $2\sqrt{3}\sigma_p$. С учетом этого можно записать

$$H_p(x) = \log(\frac{\sigma_p}{\Delta x} 2\sqrt{3}). \qquad (19)$$

Сравнивая между собой сообщения с равномерным и нормальным распределением вероятностей при условии $H_н(x) = H_р(x)$, получаем:

$$\sigma_p^2 = \frac{e}{6}\sigma^2 \approx 1{,}42\sigma^2. \qquad (20)$$

Это значит, что при одинаковой информативности сообщений средняя мощность сигналов для **равномерного распределения** их амплитуд должна быть на 42% больше, чем при **нормальном распределении амплитуд.**

Пример 1. Найдите энтропию случайной величины, распределенной по закону с плотностью вероятности

$$p(x) = \begin{cases} 0, x \le 0 \\ x^2, 0 < x \le 1 \\ 1, x > 1 \end{cases}$$

Пример 2. При организации мешающего воздействия при передаче информации можно использовать источник шума с нормальным распределением плотности и источник, имеющий в некотором интервале равномерную плотность распределения. Определить, какой источник шума применять экономичнее, каков при этом выигрыш в мощности.

Решение. Сравнение источников следует проводить из условия обеспечения равенства энтропий, когда каждый источник вносит одинаковое мешающее воздействие при передаче информации, но, очевидно, затрачивая при этом не одинаковые мощности.

Как было показано выше, значение энтропии, когда состояния элементов распределены по нормальному закону, можно найти по формуле:

$$H(x) = \log(\frac{\sigma}{\Delta x}\sqrt{2\pi e}) = \log(\sigma_{\partial}\sqrt{2\pi e}) \qquad (21)$$

где $\Delta x = 1$ Ом, а $\frac{\sigma}{\Delta x} = \sigma_{\partial}$, т.е. $\sigma_г^2$ - дисперсия, характеризующая мощность, выделяемую на резистора с сопротивлением 1Ом.

Для равномерного распределения энтропию можно найти по формуле:

$$H_p(x) = \log\frac{b-a}{\Delta x}. \qquad (22)$$

Так как дисперсия равномерного распределения

$$\sigma_h^2 = \frac{(b-a)^2}{12}, \text{□ ”} b - a = 2\sqrt{3}\sigma_p, \textit{исследовательно}$$

$$H_p(x) = \log(\frac{\sigma_p}{\Delta x}2\sqrt{3}) = \log(\sigma_{p\partial}2\sqrt{3}), \textit{где}$$

$$\sigma_{p\partial} = \frac{\sigma_p}{\Delta x}, \Delta x = 1 \textit{м}“$$

$$H,(x) = H_{\text{р}}(x),\square'' \log(\sigma_{\partial}\sqrt{2\pi e}) = \log(\sigma_{\text{р}\partial} 2\sqrt{3}),$$

Так как $2\pi e\sigma_{\partial}^2 = 12\sigma_{\text{р}\partial}$,

$$\sigma_{\text{р}\partial}^2 = \frac{\pi Нь}{6}\sigma_{\partial}^2 \approx 1{,}42\sigma_{\partial}^2$$

Поэтому следует выбирать источник шума с нормальным распределением плотности распределения амплитуд, т.к. при той же неопределенности, вносимой им в канал связи, можно выиграть в мощности 42%.

Основная литература: 1[44-46], 2[11-119, 125-128], 3 [12-19]

Дополнительная литература: 4[75-76]

Контрольные вопросы:

1. Какие источники информации называются непрерывными?
2. Как непрерывные сигналы преобразуются в дискретные?
3. От чего зависит энтропия и количество информации?
4. Что определяет дисперсия?

Лекция 6. *Условная энтропия.*

До сих пор предполагалось, что все элементы сообщения независимы, т.е. появление каждого данного элемента никак не связано с предшествующими элементами.

Рассмотрим теперь два ансамбля

$X = (x_1, x_2, \ldots, x_r)$

$Y = (y_1, y_2, \ldots, y_s)$, (23)

которые определяются не только собственными вероятностями $p(x_i)$ и $p(y_j)$, но и условными вероятностями $p_{xi}(y_j)$, $p_{yj}(x_i)$, где i = 1, 2, ... , r ; j = 1, 2, ... , s.

Систему двух случайных величин (сообщений) X, Y можно изобразить случайной точкой на плоскости. Событие, состоящее в попадании случайной точки (X, Y) в область D, принято обозначать в виде $(X, Y) \subset D$.

Закон распределения системы двух случайных дискретных величин может быть задан с помощью таблицы 13.

Таблица 13

Закон распределения X и У

Y / X	y_1	y_2	. . .	y_s
x_1	P_{11}	P_{12}	. . .	P_{1s}
x_2	P_{21}	P_{22}	. . .	P_{2s}
:	:	:	:	:
x_r	P_{r1}	P_{r2}	. . .	P_{rs}

где P_{ij} - вероятность события, заключающегося в одновременном выполнении равенства $X = x_i$, $Y = y_j$. При этом

$$\sum_{i=1}^{r}\sum_{j=1}^{s} P_{ij} = 1. \qquad (24)$$

Закон распределения системы случайных непрерывных величин (X, Y) задают при помощи функции плотности вероятности p(x, y).

Вероятность попадания случайной точки (X,Y) в область D определяется равенством

$$P[(X,Y) \subset D] = \iint_D p(x,y)dxdy. \qquad (25)$$

Функция плотности вероятности обладает следующими свойствами:

1) $p(x,y) \geq 0$
2) $\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y)dxdy = 1$

Если все случайные точки (X,Y) принадлежат области D, то

$$\iint_D p(x,y)dxdy = 1.$$

Условным распределением составляющей X при $Y = y_j$ (yj сохраняет одно и то же значение при всех возможных значениях X) называют совокупность условных вероятностей $P_{yj}(x_1)$, $P_{yj}(x_2)$, ... , $P_{yj}(x_r)$

Аналогично определяется условное распределение составляющей Y.

Условные вероятности составляющих X и Y вычисляют соответственно по формулам:

$$P_{xi}(y_j) = \frac{P(x_i, y_j)}{P(x_i)}$$
$$P_{yj}(x_i) = \frac{P(x_i, y_j)}{P(y_j)} \qquad (26)$$

Для контроля вычислений целесообразно убедиться, что сумма вероятностей условного распределения равна единице.

Так как условная вероятность события y_j при условии выполнения события x_i принимается по определению

$$P_{x_i}(y_j) = \frac{P(x_i, y_j)}{P(x_i)}, \tag{27}$$

то вероятность совместного появления совокупности состояний

$$P(x_i,y_j) = P(x_i)\, P_{xi}(y_j). \tag{28}$$

Аналогично, условимся вероятность события x_i при условии выполнения события y_j:

$$P(x_i, y_j) = P(y_j) P_{yi}(x_i). \tag{29}$$

Поэтому общую энтропию зависимых ансамблей X и Y определяют по формуле Шеннона:

$$\begin{aligned} H(X,Y) &= -\sum_{i=1}^{r}\sum_{j=1}^{s} P(x_i, y_j)\log P(x_i, y_j) = \\ &= \sum_{i=1}^{r}\sum_{j=1}^{s} P(x_i) P_{x_i}(y_j)\log[P(x_i) P_{x_i}(y_j)] = \\ &= \sum_{i=1}^{r} P(x_i)\log P(x_i)\sum_{j=1}^{s} P_{x_i}(y_j) - \sum_{i=1}^{r} P(x_i)\sum_{j=1}^{s} P_{x_i}(y_j)\log P_{x_i}(y_j). \end{aligned} \tag{30}$$

С учетом соотношения $\sum_{j=1}^{s} P_{x_i}(y_j) = 1$ получают

$H(X,Y) = H(X) + H_X(Y)$, где $H(X)$ - энтропия ансамбля X;

$H_X(Y)$ - условная энтропия ансамбля Y при условии, что сообщение ансамбля X известны:

$$H_X(Y) = -\sum_{i=1}^{r} P(x_i)\sum_{j=1}^{s} P_{x_i}(y_j)\log P_{x_i}(y_j) \tag{31}$$

Для независимых событий X и Y: $P_{xi}(y_j) = P(y_j)$ и поэтому

$H_X(Y) = H(Y)$ и, следовательно, $H(X,Y) = H(X) + H(Y)$.

Если X и Y полностью зависимы, т.е. при появлении x_i неизбежно следует y_j, то $P(x_i,y_j)$ равна единице при $i = j$ и нулю при $i \neq j$. Поэтому $H_X(Y) = 0$, и , следовательно, $H(X,Y) = H(X)$, т.е. при полной зависимости двух ансамблей один из них не вносит никакой информации.

Полученное выражение для условной энтропии

$$H_X(Y) = -\sum_{i=1}^{r} P(x_i) \sum_{j=1}^{s} P_{x_i}(y_j) \log P_{x_i}(y_j) \qquad (32)$$

можно использовать и как информативную характеристику одного ансамбля X, элементы которого взаимно зависимы. Положив Y = X, получим

$$H = -\sum_{i=1}^{r} P(x_i) \sum_{j=1}^{s} P_{x_i}(x_j) \log P_{x_i}(x_j). \qquad (33)$$

Например, алфавит состоит из двух элементов 0 и 1. Если эти элементы равновероятны, то количество информации, приходящееся на один элемент сообщения: $H_0 = \log m = \log 2 = 1$ бит. Если же, например, P(0)=s, а P(1) = j, то

$$H = -\sum_{i=1}^{m} P_i \log P_i = -P(0)\log P(0) - P(1)\log P(1) =$$

$$= -(\frac{3}{4}\log\frac{3}{4} + \frac{1}{4}\log\frac{1}{4}) = 0{,}815$$

В случае же взаимной зависимости элементов, определяемой, например, условными вероятностями $P_0(0) = 2/3$; $P_0(1) = 1/3$; $P_1(0) = 1$; $P_1(1) = 0$, то условная энтропия

$$H = -P(0)[P_0(0)\log P_0(0) + P_0(1)\log P_0(1)] - P(1)[P_1(0)\log P_1(0) +$$

$$+ P_1(1)\log P_1(1)] = -\frac{3}{4}(\frac{2}{3}\log\frac{2}{3} + \frac{1}{3}\log\frac{1}{3}) = 0{,}685$$

Энтропия при взаимно зависимых элементах всегда меньше, чем при независимых, т.е. H'<H.

Пример 1: Задано распределение вероятностей случайной дискретной двумерной величины:

Таблица 14

Закон распределения X и У

Y / X	4	5
3	0,17	0,10
10	0,13	0,30
12	0,25	0,05

Найти законы распределения составляющих X и Y.

Решение: 1) Сложив вероятности “по строкам”, получим вероятности возможных значений X:

P(3) = 0,17 + 0,10 = 0,27
P(10) = 0,13 +0,30 = 0,43
P(12) = 0,25 + 0,05 = 0,30.

Запишем закон распределения составляющей X:

Таблица 15

Закон распределения составляющей X

X	3	10	12
$P(x_i)$	0,27	0,43	0,30

Контроль: 0,27 + 0,43 + 0,30 = 1

2) Сложив вероятности “по столбцам”, аналогично найдем распределение составляющей Y:

Таблица 16

Закон распределения составляющей У

Y	4	5
$P(y_j)$	0,55	0,45

Контроль: 0,55 + 0,45 = 1

Пример 2: Задана случайная дискретная двумерная величина (X,Y):

Таблица 17

Случайная дискретная двумерная величина (X,Y)

Y / X	$y_1 = 0,4$	$y_2 = 0,8$
$x_1 = 2$	0,15	0,05
$x_2 = 5$	0,30	0,12
$x_3 = 8$	0,35	0,03

Найти: безусловные законы распределения составляющих; условный закон распределения составляющей X при условии, что составляющая Y приняла значение $y_1 = 0,4$; условный закон распределения составляющей Y при условии, что составляющая X приняла значение $x_2 = 5$

Решение: 1) Сложив вероятности “по строкам”, напишем закон распределения X.

Таблица 18

Вероятность X

X	2	5	8
P(x)	0,20	0,42	0,38

2) Сложив вероятности “по столбцам”, найдем закон распределения Y.

Таблица 19

Вероятность У

Y	0,4	0,8
P(y)	0,80	0,20

3) Найдем условные вероятности возможных значений X при условии, что составляющая Y приняла значение $y_1 = 0,4$

$$P_{y1}(x_1) = \frac{P(x_1, y_1)}{P(y_1)} = \frac{0,15}{0,80} = \frac{3}{16},$$

$$P_{y1}(x_2) = \frac{P(x_2, y_1)}{P(y_1)} = \frac{0,30}{0,80} = \frac{3}{8},$$

$$P_{y1}(x_3) = \frac{P(x_3, y_1)}{P(y_1)} = \frac{0,35}{0,80} = \frac{7}{16}$$

Напишем искомый условный закон распределения X:

Таблица 20

Условный закон распределения X

X	2	5	8
$P_{y1}(x_i)$	3/16	3/8	7/16

Контроль: 3/16 + 3/8 + 7/16 = 1

Аналогично найдем условный закон распределения Y:

Таблица 21

Условный закон распределения У

Y	0,4	0,8
$P_{x2}(y_j)$	5/7	2/7

Контроль: 5/7 + 2/7 = 1.

Пример 3: Закон распределения вероятностей системы, объединяющей зависимые источники информации X и Y, задан с помощью таблицы:

Таблица 22

Закон распределения вероятностей системы

Y / X	y_1	y_2	y_3
x_1	0,4	0,1	0
x_2	0	0,2	0,1
x_3	0	0	0,2

Определить энтропии H(X), H(Y), $H_X(Y)$, H(X,Y).

Решение: 1. Вычислим безусловные вероятности $P(x_i)$ и $P(y_j)$ системы:

а) сложив вероятности “по строкам” , получим вероятности возможных значений X: $P(x_1) = 0,5$

$P(x_2) = 0,3$

$P(x_3) = 0,2$

б) сложив вероятности “по столбцам”, получим вероятности возможных значений Y:

$P(y_1) = 0,4$

$P(y_2) = 0,3$

$P(y_3) = 0,3$

2. Энтропия источника информации X:

$$H(X) = -\sum_{i=1}^{r} P(x_i)\log P(x_i) = -(0,5\log 0,5 + 0,3\log 0,3 +$$

$$+ 0,2\log 0,2) = 1,485, бит$$

3. Энтропия источника информации Y:

$$H(Y) = -\sum_{j=1}^{s} P(y_j)\log P(y_j) = -(0,4\log 0,4 + 0,3\log 0,3 +$$

$$+ 0,3\log 0,3) = 1,57 бит$$

4. Условная энтропия источника информации Y при условии, что сообщения источника X известны:

$$H(Y) = -\sum_{i=1}^{r} P(x_i) \sum_{j=1}^{s} P_{x_i}(y_j)\log P_{x_i}(y_j) \qquad (34)$$

Так как условная вероятность события y_j при условии выполнения события x_i принимается по определению

$$P_{x_i}(y_j) = \frac{P(x_i, y_j)}{P(x_i)}, \qquad (35)$$

поэтому найдем условные вероятности возможных значений Y при условии, что составляющая X приняла значение x_1:

$$P_{x_1}(y_1) = \frac{P(x_1, y_1)}{P(x_1)} = \frac{0,4}{0,5} = 0,8$$

$$P_{x_1}(y_2) = \frac{P(x_1, y_2)}{P(x_1)} = \frac{0,1}{0,5} = 0,2$$

$$P_{x_1}(y_3) = \frac{P(x_1, y_3)}{P(x_1)} = \frac{0}{0,5} = 0$$

Для x_2: $P_{x_2}(y_1) = \frac{P(x_2, y_1)}{P(x_2)} = \frac{0}{0,3} = 0$

$$P_{x_2}(y_2) = \frac{P(x_2, y_2)}{P(x_2)} = \frac{0,2}{0,3} = 0,67$$

$$P_{x_2}(y_3) = \frac{P(x_2, y_3)}{P(x_2)} = \frac{0,1}{0,3} = 0,33$$

Для x_3: $P_{x_3}(y_1) = \frac{P(x_3, y_1)}{P(x_3)} = \frac{0}{0,2} = 0$

$$P_{x_3}(y_2) = \frac{P(x_3, y_2)}{P(x_3)} = \frac{0}{0,2} = 0$$

$$P_{x_3}(y_3) = \frac{P(x_3, y_3)}{P(x_3)} = \frac{0,2}{0,2} = 1$$

Поэтому: $H_X(Y) = -$ [0,5 (0,8 log 0,8 + 0,2 log 0,2) +
+0,3 (0,67 log 0,67 + 0,33 log 0,33) + 0,2 (1 log 1)] = 0,635

5. Аналогично, условная энтропия источника информации X при условии, что сообщения источника Y известны:

$$H_Y(X) = -\sum_{j=1}^{s} P(y_j) \sum_{i=1}^{r} P_{y_j}(x_i) \log P_{y_j}(x_i). \qquad (36)$$

$$P_{y_j}(x_i) = \frac{P(x_i, y_j)}{P(y_j)};$$

(37)

Для y_1: $P_{y_1}(x_1) = \frac{P(x_1, y_1)}{P(y_1)} = \frac{0,4}{0,4} = 1$

$$P_{y_1}(x_2) = \frac{P(x_2, y_1)}{P(y_1)} = \frac{0}{0,4} = 0$$

$$P_{y_1}(x_3) = \frac{P(x_3, y_1)}{P(y_1)} = \frac{0}{0,4} = 0$$

Для y_2: $P_{y_2}(x_1) = \frac{P(x_1, y_2)}{P(y_2)} = \frac{0,1}{0,3} = 0,33$

$$P_{y_2}(x_2) = \frac{P(x_2, y_2)}{P(y_2)} = \frac{0,2}{0,3} = 0,67$$

$$P_{y_2}(x_3) = \frac{P(x_3, y_2)}{P(y_2)} = \frac{0}{0,3} = 0$$

Для y_3: $P_{y_3}(x_1) = \frac{P(x_1, y_3)}{P(y_3)} = \frac{0}{0,3} = 0$

$$P_{y_3}(x_2) = \frac{P(x_2, y_3)}{P(y_3)} = \frac{0,1}{0,3} = 0,33$$

$$P_{y_3}(x_3) = \frac{P(x_3, y_3)}{P(y_3)} = \frac{0,2}{0,3} = 0,67$$

$$H_Y(X) = -[0,4(1\log 1) + 0,3(0,33\log 0,33 + 0,67\log 0,67) +$$
$$+ 0,3(0,33\log 0,33 + 0,67\log 0,67)] \approx 0,55, \textit{бит}.$$

6. Общая энтропия зависимых источников информации X и Y:

$$H(X,Y) = -\sum_{i=1}^{r}\sum_{j=1}^{s} P(x_i, y_j)\log P(x_i, y_j) =$$
$$= -(0,4\log 0,4 + 0,1\log 0,1 + 0,2\log 0,2 + 0,1\log 0,1 + 0,2\log 0,2) =$$
$$= 0,529 + 0,332 + 0,464 + 0,332 + 0,464 = 2,12 \textit{ бит}.$$

Проверим результат по формуле:

$H(X,Y) = H(X) + H_X(Y) = 1,485 + 0,635 = 2,12$ бит

$H(X,Y) = H(Y) + H_Y(X) = 1,57 + 0,55 = 2,12$ бит

Пример 4: Известны энтропии двух зависимых источников H(X) = 5бит; H(Y) = 10бит. Определить, в каких пределах будет изменяться условная энтропия $H_X(Y)$ в максимально возможных пределах.

Решение: Уяснению соотношений между рассматриваемыми энтропиями источников информации способствует их графическое отображение.

При отсутствии взаимосвязи между источниками информации:

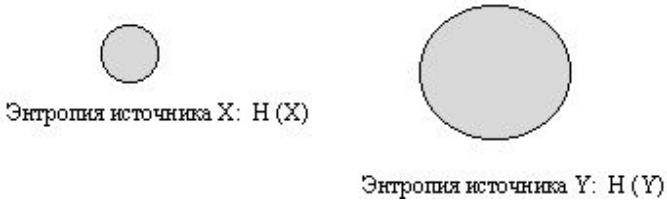


Рисунок 6 - Графическое отображение при отсутствии взаимосвязи между источниками информации

Если источники информации независимы, то $H_X(Y) = H(Y) = 10$ бит, а $H_Y(X) = H(X) = 5$ бит, и, следовательно, $H(X,Y) = H(X) + H(Y) = 5 + 10 = 15$ бит. Т.е., когда источники независимы $H_X(Y) = H(Y) = 10$ бит и поэтому принимают максимальное значение.

По мере увеличения взаимосвязи источников $H_X(Y)$ и $H_Y(X)$ будут уменьшаться:

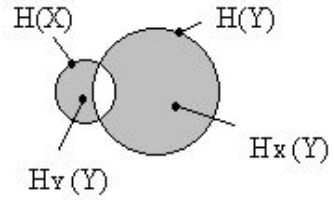


Рисунок 7 - Графическое отображение при взаимосвязи между источниками информации

При полной зависимости двух источников один из них не вносит никакой информации, т.к. при появлении x_i неизбежно следует y_j , т.е. $P(x_i, y_j)$ равно единице при $i = j$ и нулю при $i \neq j$. Поэтому

$H_Y(X) = 0$ и, следовательно, $H(X,Y) = H_X(Y)$.

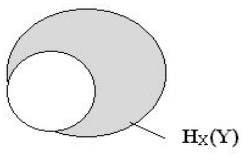


Рисунок 8 - Графическое отображение при взаимосвязи между источниками информации

При этом $H_X(Y) = H(Y) - H(X) = 10 - 5 = 5$ бит. Поэтому $H_X(Y)$ будет изменяться от 10 бит до 5 бит при максимально возможном изменении $H_y(X)$ от 5 бит до 0 бит.

Пример 5: Определите H(X) и $H_X(Y)$, если $P(x_1,y_1) = 0,3$; $P(x_1,y_2) = 0,2$; $P(x_3,y_2) = 0,25$; $P(x_3,y_3) = 0,1$

Пример 6: Определите H(X), H(Y), H(X,Y), если $P(x_1,y_1) = 0,2$; $P(x_2,y_1) = 0,4$;

$P(x_2,y_2) = 0,25$; $P(x_2,y_3) = 0,15$

Основная литература: 1[44-46], 2[11-119, 125-128], 3 [12-19]

Дополнительная литература: 4[75-76]

Контрольные вопросы:

1. Что такое ансамбль?
2. С помощью чего задается закон распределения системы случайных непрерывных величин?
3. Что является информативной характеристикой одного ансамбля элемены которого взаимно зависимы?

Лекция 7. *Взаимная энтропия. Избыточность сообщений.*

Взаимная энтропия

Пусть ансамбли X и Y относятся соответственно к передаваемому и принимаемому сообщениям. Различия между X и Y обуславливаются искажениями в процессе передачи сообщений под воздействием помех.

При отсутствии помех различий между ансамблями X и Y не будет, а энтропии передаваемого и принимаемого сообщений будут равны: H(X) = H(Y).

Воздействие помех оценивают условной энтропией $H_Y(X)$. Поэтому получаемое потребителем количество информации на один элемент сообщения равно: $E(X,Y) = H(X) – H_Y(X)$

Величину E(X,Y) называют **взаимной энтропией**.

Если ансамбли X и Y независимы, то это означает, что помехи в канале привели к полному искажению сообщения, т.е. $H_Y(X) = H(X)$, а получаемое потребителем количество информации на один элемент сообщения:E(X,Y)=0.

Если X и Y полностью зависимы, т.е. помехи в канале отсутствуют, то $H_Y(X) = 0$ и E(X,Y) = H(Y).

Так как $H_Y(X) = H(X,Y) – H(Y)$, то $E(X,Y) = H(X) + H(Y) – H(X,Y)$, или

$$E(X,Y) = \sum_{i=1}^{r} \sum_{j=1}^{s} P(x_i, y_j) \log \frac{P_{y_j}(x_i)}{P(x_i)}.$$

Пример15: Определите H(X) и E(X,Y), если $P(x_1,y_1) = 0,3$; $P(x_1,y_2) = 0,2$;

$P(x_2,y_3) = 0,1$; $P(x_3,y_2) = 0,1$; $P(x_3,y_3) = 0,25$.

Избыточность сообщений

Чем больше энтропия, тем большее количество информации содержит в среднем каждый элемент сообщения.

Пусть энтропии двух источников сообщений $H_1<H_2$, а количество информации, получаемое от них одинаковое, т.е. $I = n_1H_1 = n_2H_2$, где n_1 и n_2 - длина сообщения от первого и второго источников. Обозначим

$$\mu = \frac{n_2}{n_1} = \frac{H_1}{H_2}$$

При передаче одинакового количества информации сообщение тем длиннее, чем меньше его энтропия.

Величина μ, называемая **коэффициентом сжатия**, характеризует степень укорочения сообщения при переходе к кодированию состояний элементов, характеризующихся большей энтропией.

При этом доля излишних элементов оценивается **коэффициентом избыточности**:

$$r = \frac{H_2 - H_1}{H_2} = 1 - \frac{H_1}{H_2} = 1 - \mu \qquad (38)$$

Русский алфавит, включая пропуски между словами, содержит 32 элемента (см. Пример), следовательно, при одинаковых вероятностях появления всех 32 элементов алфавита, неопределенность , приходящаяся на один элемент, составляет $H_0 = \log 32 = 5$ бит

Анализ показывает, что с учетом неравномерного появления различных букв алфавита H = 4,42 бит, а с учетом зависимости двухбуквенных сочетаний H’ = 3,52 бит, т.е. $H' < H < H_0$

Обычно применяют три коэффициента избыточности:

1) частная избыточность, обусловленная взаимосвязью $r' = 1 - H'/H$;

2) частная избыточность, зависящая от распределения $r'' = 1 - H/ H_0$;

3) полная избыточность $r_0 = 1 - H'/ H_0$

Эти три величины связаны зависимостью $r_0 = r' + r'' - r'r''$

Вследствие зависимости между сочетаниями, содержащими две и больше букв, а также смысловой зависимости между словами, избыточность русского языка (как и других европейских языков) превышает 50% ($r_0 =1 - H'/ H_0 = 1 - 3,52/5 = 0,30$).

Избыточность играет положительную роль, т.к. благодаря ней сообщения защищены от помех. Это используют при помехоустойчивом кодировании.

Вполне нормальный на вид лазерный диск может содержать внутренние (процесс записи сопряжен с появлением различного рода ошибок) и внешние (наличие физических разрушений поверхности диска) дефекты. Однако даже при наличии физических разрушений поверхности лазерный диск может вполне нормально читаться за счет избыточности хранящихся на нем данных. Корректирующие коды С 1, С 2, Q - и Р - уровней восстанавливают все известные приводы, и их корректирующая способность может достигать двух ошибок на каждый из уровней С 1 и С 2 и до 86 и 52 ошибок на уровни Q и Р соответственно. Но затем, по мере разрастания дефектов, корректирующей способности кодов **Рида—Соломона** неожиданно перестает хватать, и диск без всяких видимых причин отказывает читаться, а то и вовсе не опознается приводом. Избыточность устраняют построением оптимальных кодов, которые укорачивают сообщения по сравнению с равномерными кодами. Это используют при архивации данных. Действие средств архивации основано на использовании алгоритмов сжатия, имеющих достаточно длинную историю развития, начавшуюся задолго до появления первого компьютера —/еще в 40-х гг. XX века. Группа ученых-математиков, работавших в области электротехники, заинтересовалась возможностью создания технологии хранения данных, обеспечивающей более экономное расходование пространства. Одним из них был **Клод Элвуд Шеннон**, основоположник современной теории информации. Из разработок того времени позже практическое применение нашли алгоритмы сжатия **Хаффмана** и **Шеннона-Фано**. А в 1977 г. математики **Якоб Зив** и **Абрахам Лемпел** придумали новый алгоритм сжатия, который позже доработал **Терри Велч**. Большинство методов данного преобразования имеют сложную теоретическую математическую основу. Суть работы архиваторов: они находят в файлах избыточную информацию (повторяющиеся участки и пробелы), кодируют их, а затем при распаковке восстанавливают исходные файлы по особым отметкам. Основой для архивации послужили алгоритмы сжатия **Я. Зива** и **А. Лемпела**. Первым широкое признание получил архиватор **Zip**. Со временем завоевали популярность и другие программы: **RAR, ARJ, ACE, TAR, LHA** и т. д.В операционной системе Windows достаточно четко обозначились два лидера: **WinZip** (домашняя страница этой утилиты находится в Internet по адресу **http://www.winzip.com)** и **WinRAR**, созданный российским программистом Евгением Рошалем (домашняя страница **http://www.rarlab.com). WinRAR** активно вытесняет **WinZip** так как имеет: удобный и интуитивно понятный интерфейс; мощную и гибкую систему архивации файлов; высокую скорость работы; более плотно сжимает файлы. Обе утилиты обеспечивают совместимость с большим числом архивных форматов. Помимо них к довольно распространенным архиваторам можно причислить **WinArj** (домашняя страница **http://www.lasoft-oz.com)**. Стоит назвать **Cabinet Manager** (поддерживает формат **CAB**, разработанный компанией Microsoft для хранения дистрибутивов своих программ) и **WinAce** (работает с файлами с расширением

ace и некоторыми другими). Необходимо упомянуть программы-оболочки **Norton Commander, Windows Commander или Far Manager.** Они позволяют путем настройки файлов конфигурации подключать внешние DOS-архиваторы командной строки и организовывать прозрачное манипулирование архивами, представляя их на экране в виде обычных каталогов. Благодаря этому с помощью комбинаций функциональных клавиш можно легко просматривать содержимое архивов, извлекать файлы из них и создавать новые архивы. Хотя программы архивации, предназначенные для MS-DOS, умеют работать и под управлением большинства версий Windows (в окне сеанса MS-DOS), применять их в этой операционной системе нецелесообразно. Дело в том, что при обработке файлов DOS-архиваторами их имена урезаются до 8 символов, что далеко не всегда удобно, а в некоторых случаях даже противопоказано.

Выбирая инструмент для работы с архивами, прежде всего, следует учитывать как минимум два фактора: эффективность, т. е. оптимальное соотношение между экономией дискового пространства и производительностью работы, и совместимость, т. е. возможность обмена данными с другими пользователями

Последняя, пожалуй, наиболее значима, так как по достигаемой степени сжатия, конкурирующие форматы и инструменты различаются на проценты, а высокая вычислительная мощность современных компьютеров делает время обработки архивов не столь существенным показателем. Поэтому при выборе программы-архиватора важнейшим критерием становится ее способность "понимать" наиболее распространенные архивные форматы.

При архивации надо иметь в виду, что качество сжатия файлов сильно зависит от степени избыточности хранящихся в них данных, которая определяется их типом. К примеру, степень избыточности у видеоданных обычно в несколько раз больше, чем у графических, а степень избыточности графических данных в несколько раз больше, чем текстовых. На практике это означает, что, скажем, изображения форматов **BMP** и **TIFF,** будучи помещенными в архив, как правило, уменьшаются в размере сильнее, чем документы **MS Word**. А вот рисунки **JPEG** уже заранее компрессированы, поэтому даже самый лучший архиватор для них будет мало эффективен. Также крайне незначительно сжимаются исполняемые файлы программ и архивы.

Программы-архиваторы можно разделить на три категории.

1. Программы, используемые для сжатия исполняемых файлов, причем все файлы, которые прошли сжатие, свободно запускаются, но изменение их содержимого, например русификация, возможны только после их разархивации.

2. Программы, используемые для сжатия мультимедийных файлов, причем можно после сжатия эти файлы свободно использовать, хотя, как правило, при сжатии изменяется их формат (внутренняя структура), а иногда и ассоциируемая с ними программа, что может привести к проблемам с запуском.

3. Программы, используемые для сжатия любых видов файлов и

каталогов, причем в основном использование сжатых файлов возможно только после разархивации. Хотя имеются программы, которые "видят" некоторые типы архивов как самые обычные каталоги, но они имеют ряд неприятных нюансов, например, сильно нагружают центральный процессор, что исключает их использование на "слабых машинах".

Принцип работы архиваторов основан на поиске в файле "избыточной" информации и последующем ее кодировании с целью получения минимального объема. Самым известным методом архивации файлов является *сжатие последовательностей одинаковых символов.* Например, внутри вашего файла находятся последовательности байтов, которые часто повторяются. Вместо того, чтобы хранить каждый байт, фиксируется количество повторяемых символов и их позиция. Например, архивируемый файл занимает 15 байт и состоит из следующих символов:

B B B B B L L L L L A A A A A

В шестнадцатеричной системе

42 42 42 42 42 4C 4C 4C 4C 4C 41 41 41 41 41

Архиватор может представить этот файл в следующем виде (шестнадцатеричном):

01 05 42 06 05 4C 0A 05 41

Это значит: с первой позиции пять раз повторяется символ "B", с позиции 6 пять раз повторяется символ "L" и с позиции 11 пять раз повторяется символ "A". Для хранения файла в такой форме потребуется всего 9 байт, что на 6 байт меньше исходного.

Описанный метод является простым и очень эффективным способом сжатия файлов. Однако он не обеспечивает большой экономии объема, если обрабатываемый текст содержит небольшое количество последовательностей повторяющихся символов.

Более изощренный метод сжатия данных, используемый в том или ином виде практически любым архиватором, — это так называемый оптимальный префиксный код и, в частности, кодирование символами переменной длины (алгоритм Хаффмана).

Код переменной длины позволяет записывать наиболее часто встречающиеся символы и группы символов всего лишь несколькими битами, в то время как редкие символы и фразы будут записаны более длинными битовыми строками. Например, в любом английском тексте буква E встречается чаще, чем Z, а X и Q относятся к наименее встречающимся. Таким образом, используя специальную таблицу соответствия, можно закодировать каждую букву E меньшим числом битов и использовать более длинный код для более редких букв.

Популярные архиваторы **ARJ, РАК, PKZIP** работают на основе ***алгоритма Лемпела-Зива.*** Эти архиваторы классифицируются как адаптивные словарные кодировщики, в которых текстовые строки заменяются указателями на идентичные им строки, встречающиеся ранее в тексте. Например, все слова

какой-нибудь книги могут быть представлены в виде номеров страниц и номеров строк некоторого словаря. Важнейшей отличительной чертой этого алгоритма является использование грамматического разбора предшествующего текста с расположением его на фразы, которые записываются в словарь. Указатели позволяют сделать ссылки на любую фразу в окне установленного размера, предшествующего текущей фразе. Если соответствие найдено, текущая фраза заменяется указателем на своего предыдущего двойника.

При архивации, как и при компрессировании, степень сжатия файлов сильно зависит от формата файла. Графические файлы, типа **TIF** и **GIF**, уже заранее компрессированы (хотя существует разновидность формата **TIFF** и без компрессии), и здесь даже самый лучший архиватор мало чего найдет для упаковки. Совсем другая картина наблюдается при архивации текстовых файлов, файлов **PostScript**, файлов **BMP** и им подобных.

Основная литература: 1[44-46], 2[11-119, 125-128], 3 [12-19]

Дополнительная литература: 4[75-76]

Контрольные вопросы:

1. Когда не будет различий между ансамблями?
2. Когда энтропии передаваемого и принимаемого сообщений будут равны?
3. Чем оценивают воздействие помех?
4. Что такое взаимная энтропия?
5. Что такое избыточность?

Лекция 8. *Формы представления сигналов. Дискретизация информации. Теорема Котельникова. Передача информации в информационной системе.*

Классификация сигналов по дискретно-непрерывному признаку.

Все сообщения по характеру изменяющиеся во времени можно разделить на **непрерывные и дискретные. Непрерывные по времени сообщения** отображаются непрерывной функцией времени. **Дискретные по времени сообщения характеризуются тем, что поступают в определенные моменты времени и описываются дискретной функцией t.**

Сообщения также можно разделить **на непрерывные и дискретные по множеству. Непрерывные множеству сообщения** характеризуются тем, что функция, их описывающая, может принимать непрерывное множество значений. **Дискретные по множеству сообщения –** это сообщения, которые могут быть описаны с помощью конечного набора чисел или дискретных значений некоторой функции.

Дискретности по множеству и времени не связаны друг с другом. Рассмотрим возможные типы сообщений подробнее.

Пусть сигнал описывается функцией X (t)

1) непрерывные по множеству и времени, или просто непрерывные; (рисунок 9.1)

2) непрерывные по множеству и дискретные по времени; (рисунок 9.2)

3) дискретные по множеству и непрерывные по времени; (рисунок 9.3)

4) дискретные по множеству и времени, или просто дискретные; (рисунок 9.4)

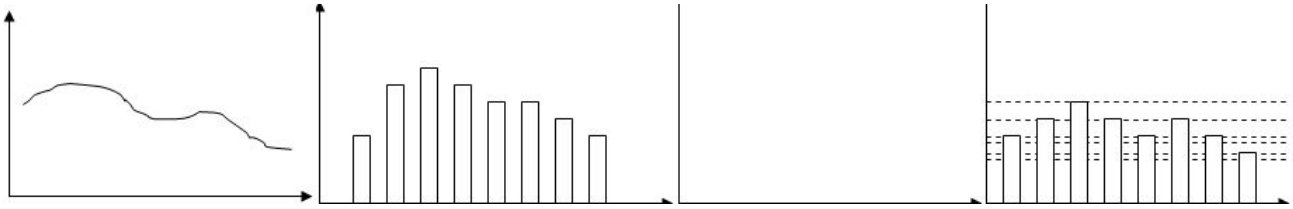


Рисунок 9 – Типы сообщений

Проблема дискретизации

Согласно строгому определению математического словаря, **"дискретность (от лат. discretus – разделенный, прерывистый) – прерывность;** противопоставляется непрерывности. Например, дискретное изменение количества величины во времени – это изменение, происходящее через определенные промежутки времени (скачками); система целых (в противоположность системе действительных чисел) является дискретной".

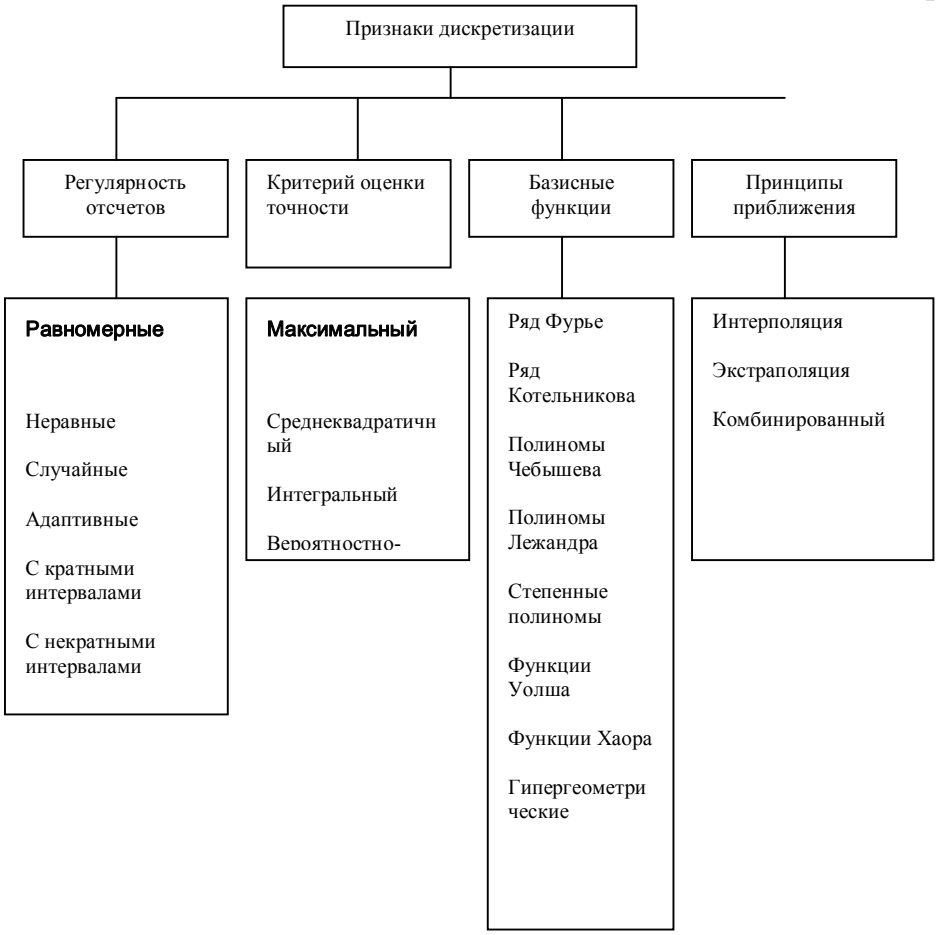
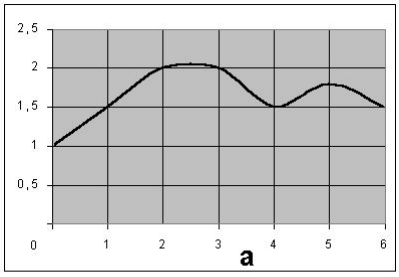


Рисунок 10 – Признаки дискретизации

Для большей наглядности дополним данное определение рядом примеров**. Дискретными являются показания цифровых измерительных приборов,** например, вольтметра (сравните со "старыми", стрелочными приборами). Очевидным образом дискретной является распечатка матричного принтера, а линия, проводимая графопостроителем, напротив, является непрерывной. **Дискретным является растровый способ представления изображений,** тогда как векторная графика по своей сути непрерывна. Дискретна таблица значений функции, но когда мы наносим точки из нее на миллиметровую бумагу и соединяем плавной линией, получается непрерывный график. Механический переключатель диапазонов в приемниках был сконструирован так, чтобы он принимал только фиксированные положения, а вот регулятор громкости вращался плавно, т.е. непрерывно.

Какое отношение приведенные выше рассуждения имеют к хранению информации в компьютере? Самое непосредственное! Компьютер по определению способен хранить только дискретную информацию. Его память, как бы велика она не была, состоит из отдельных битов, а значит дискретна. А из этого немедленно следует, что существует проблема преобразования естественной информации в пригодную для компьютера дискретную форму. В литературе ее называют проблемой дискретизации или квантования информации.



б

1	1,5	2	2	1,5	1,8	1,5
0	1	2	3	4	5	6

Рисунок 11 – Представление величин

Названная проблема всегда рассматривается при изложении принципов хранения звуковой информации, но обычно умалчивается во всех остальных случаях**. Непрерывная величина ассоциируется с графиком функции, а дискретная – с таблицей ее значений.** При рассмотрении этих двух объектов разной природы делается вывод о том, что с уменьшением интервала дискретизации (или, что то же самое, с увеличением количества точек в таблице) различия между ними существенно уменьшаются. Последнее означает, что при таких условиях дискретизированная величина хорошо описывает исходную (непрерывную).

Классификация методов дискретизации.

Формулировка теоремы Котельникова: Произвольный сигнал, спектр которого не содержат частот выше Fв, Гц, может быть полностью в

осстановлен, если известны отсчётные значения этого сигнала, взятые через равные промежутки времени1/(2Fв) с.

Передача информации в информационной системе

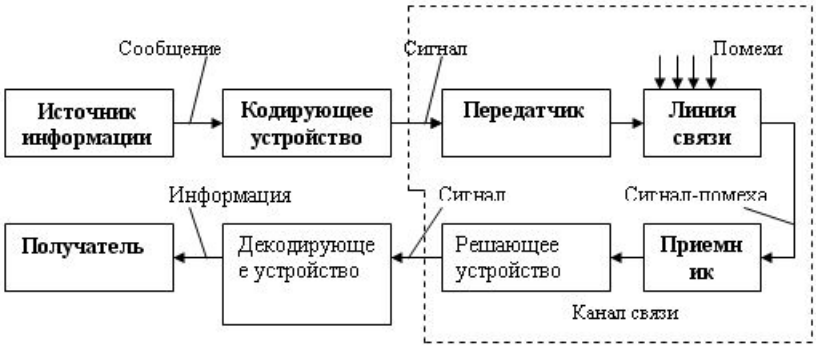


Рисунок 11 – Информационная система

Система состоит из отправителя информации, линии связи и получателя информации. Сообщение для передачи его в соответствующий адрес должно быть предварительно преобразовано в сигнал. **Под сигналом** понимается изменяющаяся физическая величина, отображающее сообщение. **Сигнал** – материальный переносчик сообщения, т.е. изменяющаяся физическая величина, обеспечивающая передачу информации по линии связи. Физическая среда, по которой происходит передача сигналов от передатчика к приемнику, называется ***линией связи***.

В современной технике нашли применение электрические, электромагнитные, световые, механические, звуковые, ультразвуковые сигналы. Для передачи сообщений необходимо принять тот переносчик, который способен эффективно распределяться по используемой в системе линии связи (FE: по радиолинии эффективно распределяется только электромагнитные колебания высоких частот – от сотен кГц до дес. тысяч МГц).

Преобразование сообщений в сигналы, удобные для прохождения по линии связи, осуществляется **передатчиком.**

В процессе преобразования дискретных сообщений в сигнал происходит кодирование сообщения**. В широком смысле кодированием** называется преобразование сообщений в сигнал. **В узком смысле кодирование** – это отображение дискретных сообщений сигналами в виде определенных сочетаний символов. Устройство, осуществляющее кодирование называется ***кодером***.

При передаче сигналы подвергаются воздействию помех. **Под помехами** подразумеваются любые мешающие внешние возмущения или воздействия (атмосферные помехи, влияние посторонних источников сигналов), а также искажения сигналов в самой аппаратуре (аппаратурные помехи), вызывающие случайное отклонение принятого сообщения (сигнала) от передаваемого.

На приемной стороне осуществляется обратная **операция декодирования**, т.е. восстановление по принятому сигналу переданного сообщения.

Решающее устройство*,* помещенное после приемника, осуществляет обработку принятого сигнала с целью наиболее полного извлечения из него информации.

Декодирующее устройство, (декодер) преобразует принятый сигнал к виду удобному для восприятия получателем.

Совокупность средств, предназначенных для передачи сигнала, называется каналом связи. Одна и та же линия связи может использоваться для передачи сигналов между многими источниками и приемниками, т.е. линия связи может обслуживать несколько каналов.

При синтезе систем передачи информации приходится решать **две основные проблемы, связанные с передачей сообщений:**

- обеспечение помехоустойчивости передачи сообщений
- обеспечение высокой эффективности передачи сообщений

Под **помехоустойчивостью** понимается способность информации противостоять вредному воздействию помех. При данных условиях, т.е. при заданной помехе, помехоустойчивость определяет верность передачи информации. Под **верностью** понимается мера соответствия принятого сообщения (сигнала) переданному сообщению (сигналу).

Под **эффективностью** системы передачи информации понимается способность системы обеспечивать передачу заданного количества информации наиболее экономичным способом. Эффективность характеризует способность системы обеспечить передачу данного количества информации с наименьшими затратами мощности сигнала, времени и полосы частот.

Теория информации устанавливает критерии оценки помехоустойчивости и эффективности информационных систем, а также указывает общие пути повышения помехоустойчивости и эффективности.

Повышение помехоустойчивости практически всегда сопровождается ухудшением эффективности и наоборот.

Основная литература: 2[18-39], 3 [45-57]

Дополнительная литература: 7

Контрольные вопросы:

1. Какие типы сообщений существуют?
2. Чем характеризуются дискретные по времени сообщения?
3. Какие существуют признаки дискретизации?
4. Какую информацию хранит компьютер?
5. Как классифицируются методы дискретизации?

Лекция 9. *Скорость передачи информации. Пропускная способность каналов.*

Скорость передачи информации по дискретному каналу.

Характеризуя дискретный канал связи, используют два понятия скорости передачи: технической и информационной.

Под *технической скоростью передачи* V_T, называемой также скоростью манипуляции, подразумевают число элементарных сигналов (символов), передаваемых по каналу в единицу времени. Она зависит от свойств линии связи и быстродействия аппаратуры канала.

С учетом возможных различий в длительностях символов скорость

$$V_\tau = 1/\tau_{ср}, \tag{39}$$

где $\tau_{ср}$ — среднее значение длительности символа.

При одинаковой продолжительности τ всех передаваемых символов $\tau_{ср} = \tau$.

Единицей измерения технической скорости служит бод — скорость, при которой за одну секунду передается один символ.

Информационная скорость, или скорость передачи информации, определяется средним количеством информации, которое передается по каналу в единицу времени. Она зависит как от характеристик данного канала связи, таких, как объем алфавита используемых символов, техническая скорость их передачи, статистические свойства помех в линии, так и от вероятностей поступающих на вход символов и их статистической взаимосвязи.

При известной скорости манипуляции V_T скорость передачи информации по каналу $\bar{I}(V,U)$ задается соотношением

$$\bar{I}(V,V) = V_\tau I(V,U), \tag{40}$$

где I(V,U) — среднее количество информации, переносимое одним символом.

Пропускная способность дискретного канала без помех. Для теории и практики важно выяснить, до какого предела и каким путем можно повысить скорость передачи информации по конкретному каналу связи. Предельные возможности канала по передаче информации характеризуются его пропускной способностью.

Пропускная способность канала $C_д$ равна той максимальной скорости передачи информации по данному каналу, которой можно достигнуть при самых совершенных способах передачи и приема:

$$C_Д = \max \bar{I}(V,U) = \max V_\tau I(V,U). \tag{41}$$

При заданном алфавите символов и фиксированных основных

характеристиках канала (например, полосе частот, средней и пиковой мощности передатчика) остальные характеристики должны быть выбраны такими, чтобы обеспечить наибольшую скорость передачи по нему элементарных сигналов, т. е. обеспечить максимальное значение V_T. Максимум среднего количества информации, приходящейся на один символ принятого сигнала I(V,U), определяется на множестве распределений вероятностей между символами $u_1 ... u_i ... u_m$.

Пропускная способность канала, как и скорость передачи информации по каналу, измеряется числом двоичных единиц информации в секунду (дв. ед./с).

Так как в отсутствие помех имеет место взаимно-однозначное соответствие между множеством символов {v} на выходе канала и {u} на его входе, то I(V,U)=I(U,V)=H(U). Максимум возможного количества информации на символ равен log m, где m — объем алфавита символов, откуда пропускная способность дискретного канала без помех

$$C_д = V_\tau \log m. \qquad (42)$$

Следовательно, для увеличения скорости передачи информации по дискретному каналу без помех и приближения ее к пропускной способности канала последовательность букв сообщения должна подвергнуться такому преобразованию в кодере, при котором различные символы в его выходной последовательности появлялись бы по возможности равновероятно, а статистические связи между ними отсутствовали бы. Доказано, что это выполнимо для любой эргодической последовательности букв, если кодирование осуществлять блоками такой длины, при которой справедлива теорема об их асимптотической равновероятности.

Расширение объема алфавита символов m приводит к повышению пропускной способности канала (рисунок 12), однако возрастает и сложность технической реализации.

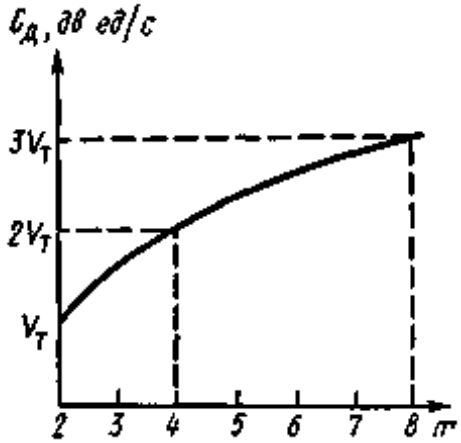


Рисунок 12 – График повышения пропускной способности канала

Пропускная способность дискретного канала с помехами. При

наличии помех соответствие между множествами символов на входе и выходе канала связи перестает быть однозначным. Среднее количество информации I(V,U), передаваемое по каналу одним символом, определяется в этом случае соотношением

$$I(VU) = H(V) - H_U(V) = H(U) - H_V(U). \qquad (43)$$

Если статистические связи между символами отсутствуют, энтропия сигнала на выходе линии связи равна

$$H(V) = -\sum_{j=1}^{m} p(v_j) \log p(v_j). \qquad (44)$$

При наличии статистической связи энтропию определяют с использованием цепей Маркова. Поскольку алгоритм такого определения ясен и нет необходимости усложнять изложение громоздкими формулами, ограничимся здесь только случаем отсутствия связей.

Апостериорная энтропия характеризует уменьшение количества переданной информации вследствие возникновения ошибок. Она зависит как от статистических свойств последовательностей символов, поступающих на вход канала связи, так и от совокупности переходных вероятностей, отражающих вредное действие помехи.

Если объем алфавита входных символов u равен m_1, а выходных символов υ — m_2, то

$$H_U(V) = -\sum_{i=1}^{m_1} \sum_{j=1}^{m_2} p(v_j u_i) \log p(v_j / u_i) \qquad (45)$$

Подставив выражения (44) и (45) в (43) и проведя несложные преобразования, получим

$$I(V,U) = \sum_{i=1}^{m_1} \sum_{j=1}^{m_2} p(v_j u_i) \log p \frac{p(v_j u_i)}{p(v_j) p(u_i)}. \qquad (46)$$

Скорость передачи информации по каналу с помехами

$$\bar{I}(V,U) = V_T \sum_{i=1}^{m_1} \sum_{j=1}^{m_2} p(v_j u_i) \log p \frac{p(v_j u_i)}{p(v_j) p(u_i)}. \qquad (47)$$

Считая скорость манипуляции V_T предельно допустимой при заданных технических характеристиках канала, величину I(V,U) можно максимизировать,

изменяя статистические свойства последовательностей символов на входе канала посредством преобразователя (кодера канала). Получаемое при этом предельное значение $C_Д$ скорости передачи информации по каналу называют *пропускной способностью* дискретного канала связи с помехами:

$$C_Д = \max_{p\{u\}} V_T \bar{I}(VU), \qquad (48)$$

где p{u} — множество возможных распределений вероятностей входных сигналов.

Важно подчеркнуть, что при наличии помех пропускная способность канала определяет наибольшее количество информации в единицу времени, которое может быть передано со сколь угодно малой вероятностью ошибки.

В гл. 6 показано, что к пропускной способности канала связи с помехами можно приблизиться, кодируя эргодическую последовательность букв источника сообщений блоками такой длины, при которой справедлива теорема об асимптотической равновероятности длинных последовательностей.

Произвольно малая вероятность ошибки оказывается достижимой только в пределе, когда длина блоков становится бесконечной.

При удлинении кодируемых блоков возрастает сложность технической реализации кодирующих и декодирующих устройств и задержка в передаче сообщений, обусловленная необходимостью накопления требуемого числа букв в блоке. В рамках допустимых усложнений на практике при кодировании могут преследоваться две цели: либо при заданной скорости передачи информации стремятся обеспечить минимальную ошибку, либо при заданной достоверности — скорость передачи, приближающуюся к пропускной способности канала.

Предельные возможности канала никогда не используются полностью. Степень его загрузки характеризуется **коэффициентом использования канала**

$$\lambda = \bar{I}(Z)/C_Д, \qquad (49)$$

где $\bar{I}(Z)$ — производительность источника сообщений; $C_Д$ — пропускная способность канала связи.

Поскольку нормальное функционирование канала возможно, как показано далее, при изменении производительности источника в пределах $0 \le \bar{I}(Z) \le C_Д$, λ теоретически может изменяться в пределах от 0 до 1.

Пример 1. Определить пропускную способность двоичного симметричного канала (ДСК) со скоростью манипуляции V_T в предположении независимости передаваемых символов.

Запишем соотношение (45) в следующем виде:

$$\mathrm{H}_{\mathrm{U}}(V) = -\sum_{i-1}^{2} p(u_i) \sum_{j=1}^{2} p(v_j / u_i) \log(v_j / u_i).$$

Воспользовавшись обозначениями на графе (рисунок 13.1), можем записать

$$H_U(V) = -p(0)[(1-p)\log_2(1-p) + p\log_2 p] - p(1)[p\log_2 p + (1-p)\log_2(1-p)] =$$
$$= -[p(0) + p(1)][p\log_2 p + (1-p)\log_2(1-p)].$$

Так как

$$p(0) + p(1) = 1,$$

то

$$H_U(V) = -p\log_2 p - (1-p)\log_2(1-p).$$

Величина $\mathrm{H_U(V)}$ не зависит от вероятностей входных символов, что является следствием симметрии канала.

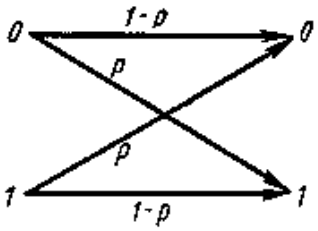
Следовательно, пропускная способность

$$C_Д = V_T[\max H(V) + p\log_2 p + (1-p)\log_2(1-p)].$$

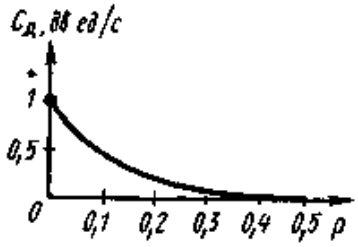
Максимум H(V) достигается при равенстве вероятностей появления символов, он равен 1. Отсюда

$$C_Д = \mathrm{V_T}[1 + p\log_2 p + (1-p)\log_2(1-p)]. \qquad (50)$$

График зависимости пропускной способности ДСК от ρ показан на рисунок 13.2. При увеличении вероятности трансформации символа с 0 до 1/2 $\mathrm{C_Д(p)}$ уменьшается от 1 до 0. Если ρ = 0, то шум в канале отсутствует и его пропускная способность равна 1. При p=1/2 канал бесполезен, так как значения символов на приемной стороне с равным успехом можно устанавливать по результатам подбрасывания монеты (герб—1, решетка — 0). Пропускная способность канала при этом равна нулю.



13.1



13.2

Рисунок 13 – График зависимости пропускной способности

Основная литература: 2[141-147]

Дополнительная литература: 7

Контрольные вопросы:

1. От чего зависит информационная скорость?
2. Что такое пропускная способность канала?
3. Что нужно для увеличения скорости передачи информации?
4. Как определяется пропускная способность канала с помехами?
5. Что такое апостериорная энтропия?

Лекция 10. *Сжатие данных.*

Закодированные сообщения передаются по каналам связи, хранятся в запоминающих устройствах, обрабатываются процессором. Объемы данных, циркулирующих в АСУ, велики, и поэтому во многих случаях важно обеспечить такое кодирование данных, которое характеризуется минимальной длиной получающихся сообщений. Эта проблема сжатия данных. Решение её обеспечивает увеличение скорости передачи информации и уменьшение требуемой памяти запоминающих устройств. В конечном итоге это ведет к повышению эффективности системы обработки данных.

Существует два подхода (или два этапа) сжатия данных:

- сжатие, основанное на анализе конкретной структуры и смыслового содержания данных;

- сжатие, основанное на анализе статистических свойств кодируемых сообщений. В отличие от первого второй подход носит универсальный характер и может использоваться во всех ситуациях, где есть основания полагать, что сообщения подчиняются вероятностным законам. Далее мы рассмотрим оба этих подхода.

Сжатие на основе смыслового содержания данных

Эти методы носят эвристический, уникальный характер, однако основную идею можно пояснить следующим образом. Пусть множество содержит $N = 2^k$ элементов. Тогда для кодирования элементов множества равномерным кодом потребуется $k = \log_2 N$ двоичных знаков. При этом будут использованы все двоичные кодовые комбинации. Если используются не все комбинации, код будет избыточным. Таким образом, для сокращения

избыточности следует попытаться очертить множество возможных значений элементов данных и с учетом этого произвести кодирование. В реальных условиях это не всегда просто, некоторые виды данных имеют очень большую мощность множества возможных значений. Посмотрим, как же поступают в конкретных случаях.

Переход от естественных обозначений к более компактным. Значения многих конкретных данных кодируются в виде, удобном для чтения человеком. При этом они содержат обычно больше символов, чем это необходимо. Например, дата записывается в виде «26 января 1982 г.» или в самой краткой форме: «26.01.82», при этом многие кодовые комбинации, например «33.18.53» или «95.00.11», никогда не используются. Для сжатия таких данных день можно закодировать пятью разрядами, месяц – четырьмя, год – семью, т.е. вся дата займет не более двух байтов. Другой способ записи даты, предложенный еще в средние века состоит в том, чтобы записывать общее число дней, прошедших к настоящему времени с некоторой точки отсчета. При этом часто ограничиваются четырьмя последними цифрами этого представления. Например, 24 мая 1967 года записывается в виде 0000 и отсчет дней от этой даты требует, очевидно, два байта в упакованном десятичном формате.

Аналогичным образом могут быть сжаты номера изделий, уличные адреса и т.п.

Подавление повторяющихся символов. Во многих данных часто присутствуют повторяющиеся подряд символы: в числовых – повторяющиеся старшие или младшие нули, в символьных – пробелы и т.п. Если воспользоваться специальным символом, указывающим на повторение, а после него помещать в закодированном виде число повторений, то тем самым можно уменьшить избыточность, обусловленную повторениями. Например, подавление повторений может быть произведено по следующей схеме. В коде ДКОИ-8 большая часть допустимых кодовых комбинаций не используется. Одну из таких комбинаций (например, с нулем во второй позиции) можно использовать как признак повторения. Тогда байт следующего вида с последующим байтом кода символа заменяют цепочку повторяющихся символов

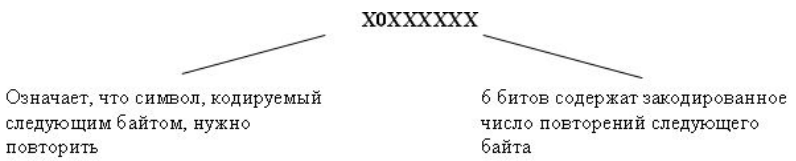


Рисунок 14 – Схема примера подавления повторяющихся символов

Эффективность такого метода определяется числом и размерами участков повторяющихся символов.

Кодирование часто используемых элементов. Некоторые данные, такие как имена и фамилии, принадлежат множеству возможных значений

очень большого размера. Однако в большинстве случаев используется лишь малая часть возможных значений (действует правило «90/10»-в девяноста процентах случаев используется 10 процентов возможных значений). Поэтому для сжатия данных можно определить множество наиболее часто используемых значений, экономно закодировать его элементы и использовать эти коды вместо обычного представления. В частности, имена людей можно кодировать одним байтом, что дает 256 возможных кодовых комбинаций. Если при этом использовать первый разряд как признак пола, то получится 128 женских и 128 мужских имен. Как обеспечить возможность записи имен, не входящих в закодированные? Для этого можно, например, условиться, что некоторая специальная кодовая комбинация длиной в один байт означает, что последующие байты содержат полное написание имени в обычном коде ДКОИ-8.

Аналогичным образом может быть произведено кодирование наиболее употребляемых фамилий (для этого могут понадобиться 2-байтовые коды). Многие сообщения и файлы содержат текстовые фрагменты из некоторых областей знаний. В таких текстах можно выделить множество наиболее употребительных слов, пронумеровать их и закодировать по вышеизложенному способу.

Контекстное сжатие данных. В упорядоченных наборах данных часто совпадают начальные символы или даже группы начальных символов записей. Поэтому можно закодировать данные, рассматривая их в контексте с предыдущими. В этом случае сжимаемым элементом данных может предшествовать специальная кодовая комбинация, характеризующая тип сжатия. **Например, возможны комбинации, указывающие на то, что:**

- элемент данных совпадает с предыдущим;
- элемент данных имеет следующее по порядку значение;
- элемент совпадает с предыдущим кроме последнего символа;
- элемент совпадает с предыдущим кроме двух (трех, четырех и т.д.) последних символов;
- элемент длиной *l* байтов не имеет связи с предыдущим.

При использовании подобных контекстных символов закодированные данные содержат только отличия текущих элементов от предыдущих.

Реализация сжатия данных требует специальных или (и) программных затрат, а также затрат памяти на предварительное кодирование с целью сжатия данных и последующее декодирование для восстановления первоначальной формы данных. Это означает, что сжатие данных – не всегда целесообразное мероприятие. Например, в базах данных обычно сжимаются архивные файлы с невысокой частотой использования. Сжатие применяется также для сокращения размеров индексных таблиц, используемых для организации поиска информации в индексно-последовательных файлах.

Рассмотрим сжатие на основе статистических свойств данных.

Этот подход называется также теорией экономного или эффективного кодирования. Он представляет собой универсальный метод, позволяющий сжимать данные, отвлекаясь от их смысла (семантики). А основываясь только на их статистических свойствах.

Вероятностная модель кодируемых сообщений.

Будем считать, что последовательность, которую нужно закодировать. Составлена из сообщений, принадлежащих некоторому конечному множеству с известным числом элементов *N*. Появление сообщений в последовательности носит вероятностный характер, т.е. каждому i-му сообщению (I=1,2…N) можно поставить в соответствие вероятность p_i его появления ($\sum_{i=1}^{N} p_i = 1$) – условие нормировки. Сообщения кодируются последовательности двоичных знаков (0 и 1). В качестве критерия экономности кода выступает средняя длина кодового слова, необходимая для кодирования одного сообщения.

Экономное кодирование основано на использовании кодов с переменной длиной кодового слова, которые мы и рассмотрим.

Коды с переменной длиной кодового слова.

До сих пор рассматривались равномерные коды, у которых кодовое слово всегда содержит одинаковое число знаков. Однако давно известны и коды, у которых длина кодового слова не постоянна, например код Морзе.

При использовании таких неравномерных кодов возникает задача выделения отдельных кодовых слов из закодированной последовательности для однозначного декодирования сообщений. В коде Морзе для этого предусмотрена специальная кодовая комбинация – разделитель (тройная пауза). Однако более экономным является использование при кодировании так называемого условия префиксности кода (условие Фано): никакое кодовое слово не должно являться началом другого кодового слова. Выполнение этого условия гарантирует однозначное расчленение последовательности на кодовые слова без применения разделителей**.** Очередное кодовое слово получается последовательным считыванием знаков до тех пор, пока получающаяся комбинация не совпадает с одним из кодовых слов.

Префиксный код называется примитивным, если его нельзя сократить, т.е. при вычеркивании любого знака хотя бы в одном кодовом слове код перестает быть префиксным. Нетрудно видеть, что если код префиксный и мы выбрали любой набор из нулей и единиц, не входящий в число кодовых слов, то возможно одно из двух: либо не существует кодового слова, начальный отрезок которого совпадает с нашим набором, либо (если такое кодовое слово существует), приписав к концу нашего набора нуль или единицу, мы получим какое-то кодовое слово или начальный отрезок кодового слова.

Двоичное кодирование как равномерным, так и неравномерным префиксным кодом удобно представлять в виде бинарного кодового дерева. Если мы всегда условимся сопоставлять левой ветви нуль, а правой – единицу, то каждой свободной вершине дерева будет однозначно

соответствовать некоторый набор двоичных знаков, показывающий, в какой последовательности нужно сворачивать направо и налево, добираясь до этой вершины из корня дерева. Таким образом, свободной вершине кодового дерева ставится в соответствие определенное кодовое слово. Например, рассмотренному коду соответствует дерево, приведенное на рисунке 15.

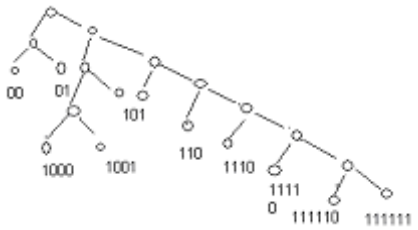


Рисунок 15 - Кодовое дерево примитивного префиксного кода.

Полезна следующая интерпретация процесса двоичного кодирования. На каждом шаге движения по кодовому дереву от корня к свободным вершинам происходит выбор одного из двух поддеревьев: правого и левого. Это соответствует разбиению множества сообщений на два подмножества (правое и левое) с присвоением им очередных двоичных знаков (единицы и нуля). Так, в рассмотренном примере исходное множество (0, 1,…,9) было разбито на два подмножества (0,1) и (2,3,…,9). При дальнейшем движении вправо множество (2,3,…,9) в свою очередь было разбито на два подмножества (2,3,4) и (5,6,…,9), а при движении влево множество (0,1) было разбито на два подмножества (0) и (1) и т.д. до тех пор, пока во всех подмножествах не осталось по одному элементу. Таким образом, кодовые комбинации характеризуют «историю» последовательного разбиения исходного множества сообщений на правые и левые подмножества.

Минимизация средней длины кодового слова.

Идея использования кодов переменной длины для сжатия данных состоит в том, чтобы сообщениям с большей вероятностью появления ставить в соответствие кодовые комбинации меньшей длины и, наоборот, сообщения с малой вероятностью появления кодировать словами большей длины. Средняя длина кодового слова определяется следующим образом:

$$L = \sum_{i=1}^{N} p_i l_i \,, \qquad (51)$$

где li – длина кодового слова для кодирования i-го сообщения

pi - вероятность появления i-го сообщения.

Возникает вопрос, как выбрать кодовые слова, чтобы для заданных вероятностей p1,p2,…..pN обеспечить по возможности меньшую среднюю длину кодового слова?

Для ответа на этот вопрос учтем тот очевидный факт, что равномерный код, всем кодовым комбинациям которого соответствуют равновероятные сообщения, является оптимальным, т.е. имеет минимальную длину кодового слова. На каждом шаге двоичного кодирования производится разбиение множества сообщений на два подмножества, причем одному из них приписывается единица, а другому – ноль. Таким образом, на каждом шаге производится кодирование подмножеств равномерным кодом длиной в I двоичный знак. Отсюда следует принцип: нужно стремиться так производить разбиение на два подмножества, чтобы суммарные вероятности подмножеств были одинаковыми (или как можно более близкими друг к другу).

Основная литература: 3 [21-45]

Дополнительная литература: 7

Контрольные вопросы:

1. Что обеспечивает применение сжатия данных?
2. Какие подходы к сжатию данных существуют?
3. В чем заключается сжатие на основе смыслового содержания данных?
4. В чем заключается подавление повторяющихся символов?
5. В чем заключается кодирование часто используемых элементов?

Лекция 11. *Эффективное кодирование.*

При кодировании каждая буква исходного алфавита представляется различными последовательностями, состоящими из кодовых букв (цифр).

Если исходный алфавит содержит m букв, то для построения равномерного кода с использованием k кодовых букв необходимо удовлетворить соотношение $m \le k_q$, где q - количество элементов в кодовой последовательности.

Поэтому

$$q \ge \frac{\log m}{\log k} = \log_k m . \qquad (51)$$

Для построения равномерного кода достаточно пронумеровать буквы исходного алфавита и записать их коды как q - разрядные числа в k-ичной системе счисления.

Например, при двоичном кодировании 32 букв русского алфавита используется $q = \log_2 32 = 5$ разрядов, на чем и основывается телетайпный код.

Кроме двоичных кодов, наибольшее распространение получили восьмеричные коды.

Пусть, например, необходимо закодировать алфавит, состоящий из 64 букв. Для этого потребуется $q = \log_2 64 = 6$ двоичных разрядов или $q = \log_8 64 = 2$ восьмеричных разрядов. При этом буква с номером 13 при двоичном кодировании получает код 001101, а при восьмеричном кодировании 15.

Обще признанным в настоящее время является позиционный принцип образования системы счисления. Значение каждого символа (цифры) зависит от его положения - позиции в ряду символов, представляющих число.

Единица каждого следующего разряда больше единицы предыдущего разряда в m раз, где m - основание системы счисления. Полное число получают, суммируя значения по разрядам:

$$Q = \sum_{i=1}^{l} a_i m^{i-1} = a_l m^{l-1} + a_{l-1} m^{l-2} + \ldots + a_2 m^1 + a_1 m^0, \qquad (52)$$

где i - номер разряда данного числа;

l - количество рядов;

a_i - множитель, принимающий любые целочисленные значения в пределах от 0 до m-1 и показывающий, сколько единиц i - ого ряда содержится в числе.

Часто используются двоично-десятичные коды, в которых цифры десятичного номера буквы представляются двоичными кодами. Так, например, для рассматриваемого примера буква с номером 13 кодируется как 0001 0011. Ясно, что при различной вероятности появления букв исходного алфавита равномерный код является избыточным, т.к. его энтропия (полученная при условии, что все буквы его алфавита равновероятны): $\log_k m = H_0$

всегда больше энтропии H = log m данного алфавита (полученной с учетом неравномерности появления различных букв алфавита, т.е. информационные возможности данного кода используются не полностью).

Например, для телетайпного кода $H0 = \log_k m = \log_2 32 = 5$ бит, а с учетом неравномерности появления различных букв исходного алфавита $H \approx 4{,}35$ бит. Устранение избыточности достигается применением неравномерных кодов, в которых буквы, имеющие наибольшую вероятность, кодируются наиболее короткими кодовыми последовательностями, а более длинные комбинации присваиваются редким буквам. Если i-я буква, вероятность которой P_i, получает кодовую комбинацию длины q_i, то средняя длина комбинации

$$q_{-\text{p}} = \sum_{i=1}^{m} p_i q_i \,. \qquad (53)$$

Считая кодовые буквы равномерными, определяем наибольшую энтропию закодированного алфавита как $q_{cp} \log m$, которая не может быть меньше энтропии исходного алфавита H, т.е. $q_{cp} \log m \geq H$.

Отсюда имеем

$$q_{-\mathrm{p}} \geq \frac{н}{\log m}. \qquad (54)$$

При двоичном кодировании (m=2) приходим к соотношению $q_{ср} \geq H$, или

$$\sum_{i=1}^{m} P_i q_i \geq -\sum_{i=1}^{m} P_i \log P_i . \qquad (55)$$

Чем ближе значение $q_{ср}$ к энтропии H, тем более эффективно кодирование. В идеальном случае, когда $q_{ср} \approx H$, код называют **эффективным**.

Эффективное кодирование устраняет избыточность, приводит к сокращению длины сообщений, а значит, позволяет уменьшить время передачи или объем памяти, необходимой для их хранения.

При построении неравномерных кодов необходимо обеспечить возможность их однозначной расшифровки. В равномерных кодах такая проблема не возникает, т.к. при расшифровке достаточно кодовую последовательность разделить на группы, каждая из которых состоит из q элементов. В неравномерных кодах можно использовать разделительный символ между буквами алфавита (так поступают, например, при передаче сообщений с помощью азбуки Морзе).

Если же отказаться от разделительных символов, то следует запретить такие кодовые комбинации, начальные части которых уже использованы в качестве самостоятельной комбинации. Например, если 101 означает код какой-то буквы, то нельзя использовать комбинации 1, 10 или 10101.

Практические методы оптимального кодирования просты и основаны на очевидных соображениях (метод Шеннона – Фано).

Прежде всего, буквы (или любые сообщения, подлежащие кодированию) исходного алфавита записывают в порядке убывающей вероятности. Упорядоченное таким образом множество букв разбивают так, чтобы суммарные вероятности этих подмножеств были примерно равны. Всем знакам (буквам) верхней половины в качестве первого символа присваивают кодовый элемент 1, а всем нижним 0. Затем каждое подмножество снова разбивается на два подмножества с соблюдением того же условия равенства вероятностей и с тем же условием присваивания кодовых элементов в качестве второго символа. Такое разбиение продолжается до тех пор, пока в подмножестве не окажется только по одной букве кодируемого алфавита. При каждом разбиении буквам верхнего подмножества присваивается кодовый элемент 1, а буквам нижнего подмножества - 0.

Пример 1: Провести эффективное кодирование ансамбля из восьми знаков:

Таблица 23

Эффективное кодирование ансамбля

Буква (знак) x_i	Вероят-ность Pi	Кодовые последовательности				Длина q_i	$p_i q_i$	$-p_i \log p_i$
		Номер разбиения						
		1	2	3	4			
x1	0,25	1	1			2	0,5	0,50
x2	0,25	1	0			2	0,5	0,50
x3	0,15	0	1	1		3	0,45	0,41
x4	0,15	0	1	0		3	0,45	0,41
x5	0,05	0	0	1	1	4	0,2	0,22
x6	0,05	0	0	1	0	4	0,2	0,22
x7	0,05	0	0	0	1	4	0,2	0,22
x8	0,05	0	0	0	0	4	0,2	0,22

$$q_{-\text{p}} = \sum_{i=1}^{m} p_i q_i = 2{,}7$$

$$H = -\sum_{i=1}^{m} Pi \log Pi = 2{,}7$$

Как видно, $q_{ср}$ = H, следовательно, полученный код является оптимальным.

Пример 2: Построить код Шеннона - Фано, если известны вероятности: $P(x_1) = 0{,}5$; $P(x_2) = 0{,}25$; $P(x_3) = 0{,}125$; $P(x_4) = 0{,}125$

Пример 3: Провести эффективное кодирование ансамбля из восьми знаков (m=8), используя метод Шеннона - Фано.

Решение: При обычном (не учитывающем статистических характеристик) двоичном кодировании с использованием k=2 знаков при построении равномерного кода количество элементов в кодовой последовательности будет $q \geq \log_k m = \log_2 8 = 3$, т.е. для представления каждого знака использованного алфавита потребуется три двоичных символа.

Метод Шеннона - Фано позволяет построить кодовые комбинации, в которых знаки исходного ансамбля, имеющие наибольшую вероятность, кодируются наиболее короткими кодовыми последовательностями. Таким образом, устраняется избыточность обычного двоичного кодирования, информационные возможности которого используются не полностью.

Так как вероятности знаков представляют собой отрицательные целочисленные степени двойки, то избыточность при кодировании устранена полностью.

Таблица 24

Эффективное кодирование ансамбля

Знаки (буквы) x_i	Вероятность Pi	Кодовые комбинации						
		Номер разбиения						
		1	2	3	4	5	6	7
x1	1/2	1						
x2	1/4	0	1					
x3	1/8	0	0	1				
x4	1/16	0	0	0	1			
x5	1/32	0	0	0	0	1		
x6	1/64	0	0	0	0	0	1	
x7	1/128	0	0	0	0	0	0	1
x8	1/128	0	0	0	0	0	0	0

Среднее число символов на знак в этом случае точно равно энтропии. В общем случае для алфавита из восьми знаков среднее число символов на знак будет меньше трех, но больше энтропии алфавита. Вычислим энтропию алфавита:

$$H = -\sum_{i=1}^{m=8} P(x_i)\log P(x_i) = 1\frac{63}{64}$$

Вычислим среднее число символов на знак:

$$q_{-\text{p}} = \sum_{i=1}^{m=8} P(x_i)q(x_i) = 1\frac{63}{64},$$

где $q(x_i)$ - число символов в кодовой комбинации, соответствующей знаку x_i.

Пример 4: Определить среднюю длину кодовой комбинации при эффективном кодировании по методу Шеннона - Фано ансамбля - из восьми знаков и энтропию алфавита.

Таблица 25

Ансамбль

Знаки (буквы) x_i	Вероятность Pi	Кодовые комбинации				
		номер разбиения				
		1	2	3	4	5
x1	0,22	1	1			
x2	0,20	1	0	1		
x3	0,16	1	0	0		
x4	0,16	0	1			
x5	0,10	0	0	1		
x6	0,10	0	0	0	1	
x7	0,04	0	0	0	0	1
x8	0,02	0	0	0	0	0

Решение: 1. Средняя длина кодовых комбинаций

$$q_{-\text{p}} = \sum_{i=1}^{m=8} P_i q_i = 2{,}84$$

2. Энтропия алфавита

$$H = -\sum_{i=1}^{m=8} P_i \log P_i = 2{,}76$$

При кодировании по методу Шеннона - Фано некоторая избыточность в последовательностях символов, как правило, остается ($q_{ср} > H$).

Эту избыточность можно устранить, если перейти к кодированию достаточно большими блоками.

Пример 5: Рассмотрим процедуру эффективного кодирования по методике Шеннона - Фано сообщений, образованных с помощью алфавита, состоящего всего из двух знаков x_1 и x_2 с вероятностями появления соответственно $P(x_1) = 0{,}9$; $P(x_2) = 0{,}1$.

Так как вероятности не равны, то последовательность из таких букв будет обладать избыточностью. Однако, при побуквенном кодировании мы никакого эффекта не получим. Действительно, на передачу каждой буквы требуется символ либо 1, либо 0, в то время как энтропия равна

$$H = -\sum_{i=1}^{m=2} P_i \log P_i = 0{,}47,$$

т.е. оказывается $q_{-\text{p}} = \sum_{i=1}^{m} P_i q_i = 1 \rangle H = 0{,}47.$

При кодировании блоков, содержащих по две буквы, получим коды:

Таблица 26

Кодирование блоков

Блоки	Вероятности	Кодовые комбинации		
		номер разбиения		
		1	2	3
x1x1	0,81	1		
x1x2	0,09	0	1	
x2x1	0,09	0	0	1
x2x2	0,01	0	0	0

Так как знаки статистически не связаны, вероятности блоков определяют как произведение вероятностей составляющих знаков.

Среднее число символов на блок

$$q_{-\text{р}} = \sum_{i=1}^{m=4} P_i q_i = 1{,}29,$$

а на букву 1,29/2 = 0,645, т.е. приблизилось к H = 0,47 и таким образом удалось повысить эффективность кодирования.

Кодирование блоков, содержащих по три знака, дает еще больший эффект:

Таблица 27

Кодирование блоков

Блоки	Вероятность Pi	кодовые комбинации				
		номер разбиения				
		1	2	3	4	5
x1x1x1	0,729	1				
x2x1x1	0,081	0	1	1		
x1x2x1	0,081	0	1	0		
x1x1x2	0,081	0	0	1		
x2x2x1	0,009	0	0	1	1	
x2x1x2	0,009	0	0	0	1	0
x1x2x2	0,009	0	0	0	0	1
x2x2x2	0,001	0	0	0	0	0

Среднее число символов на блок равно 1,59, а на знак - 0,53, что всего на 12% больше энтропии.

Следует подчеркнуть, что увеличение эффективности кодирования при укрупнении блоков не связано с учетом все более далеких статистических связей, т.к. нами рассматривались алфавиты с независимыми знаками.

Повышение эффективности определяется лишь тем, что набор вероятностей получившихся при укрупнении блоков можно делить на более близкие по суммарным вероятностям подгруппы.

Рассмотренная методика **Шеннона - Фано** не всегда приводит к однозначному построению кода, т.к. при разбиении на подгруппы можно сделать большей по вероятности как верхнюю, так и нижнюю подгруппы:

Таблица 28

Кодирование подгрупп

Знаки (буквы) x_i	Вероятность Pi	1-е кодовые комбинации					2-е кодовые комбинации				
		номер разбиения					номер разбиения				
		1	2	3	4	5	1	2	3	4	5
x1	0,22	1	1				1	1			

x2	0,20	1	0	1			1	0			
x3	0,16	1	0	0			0	1	1		
x4	0,16	0	1				0	1	0		
x5	0,10	0	0	1			0	0	1		
x6	0,10	0	0	0	1		0	0	0	1	
x7	0,04	0	0	0	0	1	0	0	0	0	1
x8	0,02	0	0	0	0	0	0	0	0	0	0

Основная литература: 1[97-119, 150-169, 172-204], 2[162-193, 197-211, 219-236, 239-245], 3[45-50]

Дополнительная литература: 4[23-29, 130-133, 141-152, 161-215]

Контрольные вопросы:

1. Что такое кодирование?
2. Что такое кодовая последовательность?
3. Как для телетайпного кода достигается устранение избыточности?
4. В чем разница между равномерными и неравномерными кодами?
5. Присутствует ли избыточность в методе Шеннона-Фано?

Лекция 12. *Кодирование информации для канала с помехами. Разновидности помехоустойчивых кодов. Методы помехоустойчивого кодирования.*

Ошибка в кодовой комбинации появляется при ее передаче по каналу связи вследствие замены одних элементов другими под воздействием помех. Например, 2-кратная ошибка возникает при замене (искажении) двух элементов. Например, если кодовая комбинация 0110111 принята как 0100110, то имеет место двукратная ошибка.

Теория помехоустойчивого кодирования базируется на результатах исследований, проведенных **Шенноном** и сформулированных в виде теоремы:

1. При любой производительности источника сообщений, меньшей, чем пропускная способность канала, существует такой способ кодирования, который позволяет обеспечить передачу всей информации, создаваемой источником сообщений, со сколь угодно малой вероятностью ошибки.

2. Не существует способа кодирования, позволяющего вести передачу информации со сколь угодно малой вероятностью ошибки, если производительность источника сообщений больше пропускной способности канала.

Из теоремы следует, что помехи в канале не накладывают ограничений на точность передачи. Ограничение накладывается только на скорость передачи, при которой может быть достигнута сколь угодно высокая точность передачи.

Теорема не затрагивает вопроса о путях построения кодов, обеспечивающих идеальную передачу информации, но, обосновав принципиальную возможность такого кодирования, позволяет вести разработку конкретных кодов.

При любой конечной скорости передачи информации вплоть до пропускной способности канала, сколь угодно малая вероятность ошибки

достигается лишь при безграничном увеличении длительности кодируемых последовательностей знаков. Таким образом, безошибочная передача при наличии помех возможна лишь теоретически.

Обеспечение передачи информации с весьма малой вероятностью ошибки и достаточно высокой эффективностью возможно при кодировании чрезвычайно длинными последовательностями знаков.

На практике точность передачи информации и эффективность каналов связи ограничивается двумя факторами:

1) размером и стоимостью аппаратуры кодирования/декодирования;
2) временем задержки передаваемого сообщения.

Разновидности помехоустойчивых кодов

Коды, которые обеспечивают возможность обнаружения и исправления ошибки, называют **помехоустойчивыми**.

Эти коды используют для:

1) исправления ошибок – **корректирующие коды**;
2) обнаружения ошибок.

Корректирующие коды основаны на введении избыточности.

У подавляющего большинства помехоустойчивых кодов помехоустойчивость обеспечивается их алгебраической структурой. Поэтому их называют **алгебраическими кодами**.

Алгебраические коды подразделяются на два класса:

1) блоковые;
2) непрерывные.

В случае блоковых кодов процедура кодирования заключается в сопоставлении каждой букве сообщения (или последовательности из k символов, соответствующей этой букве) блока из n символов. В операциях по преобразованию принимают участие только указанные k символов, и выходная последовательность не зависит от других символов в передаваемом сообщении.

Блоковый код называют **равномерным**, если n остается постоянным для всех букв сообщения.

Различают разделимые и неразделимые блоковые коды. При кодировании разделимыми кодами выходные последовательности состоят из символов, роль которых может быть отчетливо разграничена. Это информационные символы, совпадающие с символами последовательности, поступающей на вход кодера канала, и избыточные (проверочные) символы, вводимые в исходную последовательность кодером канала и служащие для обнаружения и исправления ошибок.

При кодировании неразделимыми кодами разделить символы входной последовательности на информационные и проверочные невозможно.

Непрерывными (древовидными) называют такие коды, в которых введение избыточных символов в кодируемую последовательность информационных символов осуществляется непрерывно, без разделения ее на

независимые блоки. Непрерывные коды также могут быть разделимыми и неразделимыми.

Методы помехоустойчивого кодирования.

Рассмотрим простые практические способы построения кодов, способных обнаруживать и исправлять ошибки. Ограничимся рассмотрением двоичных каналов и равномерных кодов.

Метод контроля четности. Это простой способ обнаружения некоторых из возможных ошибок. Будем использовать в качестве разрешенных половину возможных кодовых комбинаций, а именно те из них, которые имеют четное число единиц (или нулей). Однократная ошибка при передаче через канал неизбежно приведет к нарушению четности, что и будет обнаружено на выходе канала. Очевидно, что трехкратные, пятикратные и вообще ошибки нечетной кратности ведут к нарушению четности и обнаруживаются этим методом, в то время как двукратные, четырехкратные и вообще ошибки четной кратности – нет.

Практическая техника кодирования методом контроля четности следующая. Из последовательности символов, подлежащих передаче через канал, выбирается очередной блок из *k-1*символов, называемых **информационными, и к нему добавляется k-й символ, называемый контрольным.** Значение контрольного символа выбирается так, чтобы обеспечить четность получаемого кодового слова, т.е. чтобы сделать его разрешенным.

Метод контроля четности представляет значительную ценность и широко применяется в тех случаях, в которых вероятность появления более одной ошибки пренебрежимо мала (во многих случаях, если наверняка знать, что кодовое слово принято с ошибкой, имеется возможность запросить повторную передачу). В то же время избыточность кода увеличивается минимально и незначительно при больших *k*(в *k/(k-1)*раз).

Метод контрольных сумм. Рассмотренный выше метод контроля четности может быть применен многократно для различных комбинаций разрядов передаваемых кодовых слов – и это позволит не только обнаруживать, но и исправлять определенные ошибки.

Пример:

Будем из входной последовательности символов брать по четыре информационных символа $a_1a_2a_3a_4$, дополнять их тремя контрольными символами $a_5a_6a_7$ и получившееся семисимвольное слово посылать в канал. Контрольные символы будем подбирать так, чтобы были четными следующие суммы:

$s_1 = a_1 + a_2 + a_3 + a_5$,

$s_2 = a_1 + a_2 + a_4 + a_6$,

$s_3 = a_1 + a_3 + a_4 + a_7$.

В каждую сумму входит по оному контрольному символу, поэтому данное требование всегда выполнимо.

Благодаря «маленьким хитростям», предусмотренным при формировании контрольных сумм, проверка их четности на выходе канала позволяет однозначно установить, была ли допущена при передаче однократная ошибка и какой из разрядов был при этом искажен (ошибками большей кратности пренебрегаем). Действительно, если один из семи символов был искажен, то, по крайней мере, одна из сумм обязательно окажется нечетной, т.е. четность всех контрольных сумм s_1, s_2, s_3 свидетельствует об отсутствии однократных ошибок. Далее, лишь одна сумма будет нечетной в том, (и только в том) случае, если искажен входящий в эту сумму один из трех контрольных символов (a_5, a_6 или a_7). Нечетность двух или трех сумм означает, что искажен тот из информационных символов a_2, a_3 или a_4, который входи в обе эти суммы. Наконец, нечетность всех трех сумм означает, что неверно принят входящий во все суммы символ a_1.

Итак, в данном примере метод контрольных сумм, увеличивая длину кода в 7/4=1,75 раза за счет введения избыточности, позволяет исправить любую однократную ошибку (но не ошибку большей кратности). Основываясь на этой идее, в принципе, можно построить коды, исправляющие все ошибки большей (но всегда ограниченной) кратности.

Основная литература: 3 [50-57], 1[97-119, 150-169, 172-204], 2[162-193, 197-211, 219-236, 239-245], 3[45-50]

Дополнительная литература: 4[23-29, 130-133, 141-152, 161-215]

Контрольные вопросы:

1. Когда появляется ошибка в кодовой комбинации?
2. Чем ограничивается точность передачи информации и эффективность каналов связи?
3. Какие коды называют помехоустойчивыми?
4. Где используют помехоустойчивые коды?
5. Какие коды называют алгебраическими?

Лекция 13. *Линейные групповые коды (ЛГК).*

Наиболее простыми кодами, относящимися к классу помехоустойчивых кодов, являются коды ЛГК. Теория этих кодов базируется на понятии группы.

Группой G называется совокупность элементов, для которых определена некоторая бинарная операция (*) и выполняются следующие аксиомы: 1) замкнутость - выбранная бинарная операция может быть применена к любым 2 элементам группы. Результат операции должен принадлежать группе. 2) ассоциативность a*b*c=a*(b*c), 3) наличие единичного элемента. В группе обязательно существует единичный элемент, причем единственный. Если выбранная операция – сложение, то единичный элемент обозначается “0”: a+0=a, 0+a=a, где a – любой элемент группы. Если умножение, то – “1”: a*1=a, 1*a=a, 4) наличие обратного элемента. Каждый элемент группы кроме единичного обладает обратным элементом. Для сложения: a+(-a)=0, если умножение: $a*a^{-1}=1$.

Определение: группа называется аддитивной, если в качестве операции над ней используется сложение.

Определение: Группа называется абелевой, если она коммутативна: a+b=b+a, ab=ba.

Определение: группа, состоящая из конечного множества элементов, называется конечной группой.

В помехоустойчивом кодировании используют конечные, коммутативные и аддитивные группы. Элементами групп являются 0 и 1, а операция (+) - сложение по модулю 2.

Пример 1: M={0,1} (+). Является ли это множество группой?

0(+)1=1; (0+1)+1=0+(1+1). Наличае единичного элемента: им является “0”, а обратным элементом для “0” является “0”, а для “1” - “1”. Т.о., данное множество М с операцией $\oplus$ является группой.

Определение: ЛГК – это конечная, аддитивная, коммутативная группа G, элементами которой является двоичные векторы, а в качестве операций в группе используется $\oplus$. Двоичным вектором является последовательность 0 и 1: 10110001. Его длина равна 8. ЛГК задаётся двумя способами: 1) либо перечислением векторов 2) либо матричным представлением. Максимальный набор линейнонезависимых двоичных векторов образуют порождающую матрицу некоторого кода. Любой вектор кода ,не принадлежащий матрице, может быть получен путём линейной комбинации некоторого количества строк к этой матрице.

Рассмотрим матрицу G:

100	1
010	2
001	3

Полученная кодовая комбинация принадлежит двоичному трёхразрядному коду, все векторы этого кода, полученные из порождающей матрицы G путём всех возможных комбинаций над строками матриц. Нулевой вектор принадлежит любому коду.

1	100
2	010
3	001
1+2	110
1+3	101
2+3	011
1+2+3	111
	000

всегда добавляется 0-й вектор (как начало координат)

Определение: 1) расстояние по Хеммингу между двумя векторами a и b является количество несовпадающих позиций.

Пример 2: A=1011001, B=1101001, $\rho(a,b)=2$.

2) Вес слова – количество единиц в слове, ω(A)=4, ω(B)=4.

Обнаруживающая способность b – способность кода обнаруживать b и менее ошибок.

Корректирующая способность кода t – способность кода исправлять t и менее ошибок.

d_{min}-кодовое расстояние. (минимальное расстояние по Хеммингу между любой парой векторов называется *кодовым расстоянием*). Поскольку 0 также является вектором, то расстояние между произвольным вектором a и нулевым вектором будет равно ρ(A,0)=ω(A).

$d_{min}= \omega_{min}$.

Определение: $d_{min}\geq b+1$(*), $d_{min}\geq 2t+1$(**).

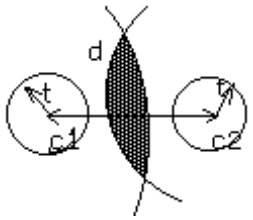


Рисунок 16 – Графическое представление кода

Доказываем (**): Если $d\geq 2t+1$, то сферы не соприкасаются, иначе возникает неопределённость c_1 и c_2 – центры сфер в n-мерном пространстве, представляющие кодовые слова. Радиусы сфер t – корректирующая способность кода.

Если $d\geq 2t+1$, то сферы не соприкасаются и каждое некодовое слово, имеющее не более t ошибок может быть заменено кодовым, которое не является центром соответствующей сферы. Если d=2t, то сферы касаются. И если ошибочное слово находится в области касания, то неизвестно на что его заменить. Если $d\leq 2t$, то сферы имеют общий объем, внутри которого некодовые слова не могут быть исправлены.

Так как в качестве слова, например c_1 может быть началом коорд., то расстояние d должно быть равно весу кодового слова. (**) доказано.

Т.о., задачи построения помехоустойчивых кодов состоит в том, чтобы обеспечить расстояние между словами не менее d. Для этого порождающая матрица G строится по следующему правилу:

$$G_{k\times n}=\left\|\begin{array}{l} 10\ldots0\ \ P11\ P12\ldots P1(n-k) \\ 01\ldots0\ \ P21\ P22\ldots P2(n-k) \\ \\ 00\ldots1\ \ Pk1\ Pk2\ldots Pk(n-k) \end{array}\right\| = |P$$

Определение: мощность кода N – это количество слов принадлежащих коду и $N=2^k$.

Всего можно построить 2^n слов, кодовых же только 2^k.

Пример 3: k=3, n=6, 2^6=64, 2^3=8.

Такое представление кодов называется каноническим, левосторонним, систематическим. Код матрицы I – это матрица информационных разрядов, в них полезная информация. Разряды P – содержат обнаруживающую и корректирующую способность данного кода. Чем больше размер (n-k), тем больше b,t, при этом экономичность кода падает. Скорость кода: R=k/n.

Пример 4: k=3, n=6

	p1	p2	p3
	1	0	0
	0	1	0
	0	0	1

$\omega_{min}=3$, $d_{min}=3=2t+1 \Rightarrow t=1$, $b+1=3 \Rightarrow b=1$

1	100110	3
2	010101	3
3	001011	3
1+2	110011	4
1+3	101101	4
2+3	011110	4
1+2+3	111000	3
	000000	

Вывод: данная порождающая матрица порождает код, характеризующийся следующими свойствами: $N=2^k=8$, скорость кода R=k/n=1/2, обнаруживающая способность b=2, корректирующая способность t=1.

Порождающую матрицу ЛГК длины n с k информационными разрядами можно построить по следующим правилам: 1) все векторы порождающей матрицы должны быть различны и линейнонезависимы. 2) нулевой вектор не входит в множество векторов порождающей матрицы, но является обязательным кодовым словом. 3) каждый вектор порождающей матрицы V_i должен иметь вес $\omega_{Vi} \geq d_{min}$. 4) расстояние по Хеммингу между любыми двумя векторами порождающей матрицы $\rho(V_i,V_j) \geq d_{min}$.

Порождающая матрица ЛГК построенная по этим правилам должна быть проверена на соответствие требуемым значениям b и t. Для этого по построенной матрице строятся все векторы кода и выписывается из вес. Если вес $\geq d_{min}$, то построение кода закончено. Поставим задачу построить ЛГК заданной мощности и заданной корректирующей способностью.

Основная литература: 1[97-119, 150-169, 172-204], 2[162-193, 197-211, 219-236, 239-245], 3[45-50]

Дополнительная литература: 4[23-29, 130-133, 141-152, 161-215]

Контрольные вопросы:

1. На чем базируется линейные групповые коды?
2. Что такое группа?
3. Какая группа называется адитивной?
4. Какая группа называется абелевой?
5. Какая группа называется конечной?

Лекция 14. *Циклические коды.*

ЦК – это разновидность линейно группового кода относящийся к систематическому коду. Циклический вектор двоичного кода удобно задавать в

виде многочлена (а не комбинации 0,1). F(x)=an-1xn-1(+)an-2an-2(+)…(+)a1x(+)a0 (*)

x – основание системы счисления, в которой строится код. ai, где i=0,(n-1) – это цифры данной системы счисления. Например: x=3, ai=0,1,2. Мы рассм. X=2, ai=0,1.

Пример: представить числовую последовательность в виде многочлена F(x)=1x3(+)0x2(+)0x(+)1, F(x)=x3(+)1. Представление двоичных векторов в виде многочлена позволяет перейти от действий над векторами к действию над многочленами. При этом сложение векторов предполагает сложение многочленов, которое осуществляется как сумма по модулю x одноименных коэффициентов. Умножение векторов соответствует умножению по правилу умножения многочленов, деление векторов – это деление многочленов, причем операция "-" преобразуется в операцию "+" по модулю. F1(x)=x3+x2+1, F2(x)=x+1.

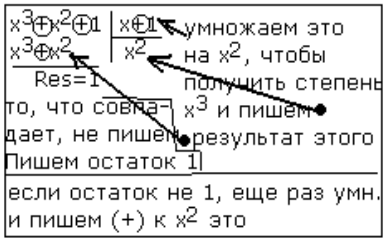


Рисунок 17 – Схема кодирования

1) F1(x)+F2(x)=x3+x2+x (в двоичной системе 1+1=0),
2) F1(x)*F2(x)=(x3+x2+1)(x+1)=x3+x3+x3+x2+x+1=x4+x2+x+1,
3) F1(x)/F2(x)=x2.

Основным свойством циклического кода является: если некоторый вектор принадлежит циклическому коду, то любой другой вектор, полученный из данного путем произвольного числа циклических сдвигов также принадлежит циклическому коду.

Идея построения циклического кода базируется на понятии неприводимого многочлена, который делится только на самого себя и на единицу, т.е. не может быть разложен на более простые многочлены. Сам же неприводимый многочлен является делителем многочлена xn(+)1 без остатка. Неприводимые многочлены в теории циклических кодов играют роль образующих многочленов или полиномов. Эти полиномы табулированы. P(x)=x+1, P(x2)=x2+x+1, P(x3)=x3+x+1, P(x4)=x3+x2+1. Вектор циклического кода по заданному информационному слову строится следующим образом:

Пусть задано информационное слово Q(x) и многочлен P(xr). Тогда, когда слово F(x)=Q(x)*xr + Res [Q(x)xr / P(xr)], Q(x) – информационное слово, которое надо закодировать. P(x) – порождающий многочлен.

Пример (КОДИРОВАНИЯ В ЦИКЛИЧЕСКОМ КОДЕ): число, которое подлежит кодированию – 0111. P(x3)=x3+x2+1, Q(x)=x2+x+1, r = 3, Q(x)*xr = x5+x4+x3, P(x)=x5+x4+x3+R, столбиком делим Q(x)*xr / P(xr) = x2+1, остаток R=1.

ОТВЕТ: F(x)=x5+x4+x3+1 => 0111 001.

Циклический код, как и всякий систематический код код может быть задан в виде порождающей матрицы. Структура этой матрицы:

G(n, k) = ||ITk x k, Pk x (n-k)||, P – матрица проверочных разрядов.

$$G(7,4)=\begin{matrix}0001\ 101\\0010\ 111\\0100\ 011\\1000\ 110\end{matrix}$$

ПРИМЕР: ПОСТРОИТЬ МАТРИЦУ G(7,4) ЦК

Q1(x)=1, Q2(x)=x, Q3(x)=x2, Q4(x)=x3.

P(x3)=x3+x2+1, Чтобы найти значения, которые потом вписать в правую часть матрицы, надо произвести деления столбиком и найти остатки, которые потом в соответствии с присутствующими степенями x преобразовать в двоичный вид и записать в правую часть. Res[Q(x)x3/P(x3)] - ? Надо 4 раза поделить. Делим на P, соответственно x3, потом x4, x5, x6.

Обнаружение и исправление ошибок в ЦК

$$\left\|\begin{matrix}0001\ 101\\0010\ 111\\0100\ 011\\1000\ 110\end{matrix}\right\|$$

Любое кодовое слово ЦК делится на неприводимый многочлен без остатка, поэтому признаком наличия ошибки в принятом слове является ненулевой остаток от деления принятого слова на неприводимый многочлен. Однако наличие ненулевого остатка лишь говорит о факте существования ошибки, т.е. ошибки обнаруживаются, но по виду остатка нельзя судить о месте возникновения ошибки. Для коррекции t и менее ошибок используется следующий алгоритм: 1) принятое слово делится на неприводимый полином. 2) подсчитывается вес остатка. 3)Если вес не превышает корректирующую способность кода (t), то остаток суммируется с делимым и полученная сумма – есть правильное слово. Если вес остатка больше t, то принятое слово циклически сдвигается влево на один разряд, делится на $P(x^r)$ и анализируется вес остатка. Если вес остатка не больше t, то остаток прибавляется к делимому. Полученная сумма циклически сдвигается вправо на один разряд. Результат этой операции – скорректированное слово. Если вес остатка больше t, то делимое еще раз сдвигается влево.

Пример: ЦК задан порождающей матрицей $G=P(x^3)=x^3+x^2+1$, **t=1**, $d_{min}=3$

Кодовое слово: A=0001101,

слово с ошибкой: $A'=0011101=x^4+x^3+x^2+1$,

делим столбиком A'/ P =x,

остаток Res=x^2+x+1, ω(Res)=3>t (исправлять не надо). Теперь сдвигаем A'^{1y} (сверху стрелка←) = 0111010, и опять также делим Res=x+1 (ω=2)>t, опять значит не то – сдвигаем опять влево и так далее, пока не станет Res=1 (ω=1=t). Исправляем последний символ A'^{3y}(←) на обратный и двигаем,→а 3. Это будет A=0001101.

Необнаруживаемые циклическим кодом ошибки.

Представим вектор одиночных ошибок в виде единичной матрицы с побочной сл. диаг. К такой матрице добавим справа матрицу, полученную от деления каждого вектора ошибок на порождающий многочлен. Дописываемая матрица называется матрицей остатков и имеет r столбцов, где r – степень порождающего многочлена. В итоге получим матрицу M', которую будем анализировать. Матрица одиночных ошибок:

0	0	0	0	0	0	1	**0**	**0**	**1**
0	0	0	0	0	1	0	**0**	**1**	**0**
0	0	0	0	1	0	0	**1**	**0**	**0**
0	0	0	1	0	0	0	1	0	1
0	0	1	0	0	0	0	1	1	1
0	1	0	0	0	0	0	0	1	1
1	0	0	0	0	0	0	1	1	0
			n*n				r		

M' =

a4	a3	a2	a1	p1	p2	p3
0	0	0	0	0	0	1
0	0	0	0	0	1	0
0	0	0	0	1	0	0
0	0	0	1	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
1	0	0	0	0	0	0

$M' = \| I_{n*n}{}^{T} * (I^{T}_{r*r}/R) \|$

Не обязательно знать кодовое слово, достаточно знать ошибочную строку(слово ошибок).

V=C+E.

Для изучения свойств кодов принятое слово представляем в виде суммы кодового слова C и слова ошибки E. Известно, что при делении C на порождающий многочлен остаток всегда равен 0. Т. о. для изучения свойств кода достаточно изучать остаток от деления вектора E на порождающий многочлен. Именно на этом основании и построена матрица M'. Как видно из матрицы остатков в M', все остатки ненулевые и различны, что одиночные ошибки исправляются 100%. Кроме того, обнаруживаются 2-кратные ошибки, о чём можно узнать, построив матрицу M'', где в k-той строке будет по 2 ошибки. При этом подматрица остатков не будет содержать 0-вых строк, однако среди них возникнут повторяющиеся строки. Аналогично для любого циклического кода. Следует сказать, что фактическое обнаруж. способность кода больше, чем гарантированная. Так для рассматриваемого кода гарантированная обнаруживающая способность =2, из общего количества 35 3-хкратных ошибок не обнаруживаются только 7, из 4-хкратных - тоже 7, не обнаруживается единственная 7-кратная ошибка. Итого не обнаруживается всего 15 ошибочных комбинаций.

Основная литература: 1[97-119, 150-169, 172-204], 2[162-193, 197-211, 219-236, 239-245], 3 [69-70]

Дополнительная литература: 4[23-29, 130-133, 141-152, 161-215]

Контрольные вопросы:

1. Что такое циклический код?
2. Что является основным свойством циклических кодов?
3. На чем базируются циклические коды?
4. Что является признаком ошибки в циклическом коде?
5. Как задается циклический код?
6. Необнаруживаемые циклическим кодом ошибки.

Лекция 15. *Реализация схем кодирования и декодирования в ЦК.*

Рассмотрим основные структуры кодеров и декодеров циклических кодов. Схемы, построенные на основе регистров сдвига, называются цифровыми фильтрами. Основа – циклический сдвиг. Чаще всего это D-триггер. n-разрядный регистр сдвига используется для циклического сдвига многочлена x^n-1. Каждый раз после сдвига вычисляется $x*V(x)(mod(x^n-1))$,

V(x) – некоторый начальный вектор, который помещен в этот регистр. Структура определяет выражение по модулю x^n-1, где n – количество регистров. x – умножение, в логике – сдвиг. Умножение на x соответствует однократному циклическому сдвигу V(x) вправо, причем старшие разряды слова находятся справа.

Обобщенная схема делительного устройства:

Данная схема делит входной полином на порождающий многочлен g(x). В начальном состоянии все триггеры сброшены и первые r сдвигов на выходе последнего триггера 0, т.е. обратная связь разомкнута. Многочлен d(x) проталкивается в схему начиная со старших коэффициентов. После n сдвигов, где n – степень многочлена d(x) на выходе схемы будет частное, а в самом регистре будет записан остаток от деления d(x) на g(x).

$g(x)=g_r x^r + \ldots+g1x+g0$.

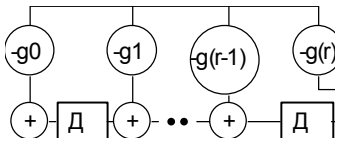
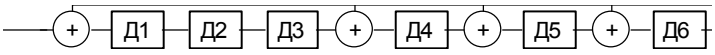


Рисунок 18 – Обобщенная схема делительного устройства

<u>Пример 1:</u> построить схему деления на многочлен $g(x)=x^6+x^5+x^4+x^3+1$

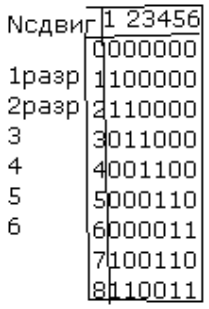


d(x)=11000001, d(x)(→)=10000011.

Разделить $d(x)=x^7+x^6+1$

```
X7+X6+1          | X6+X5+X4+X3+1
X7+X6+X5+X4+X    | X
-------------
   X5+X4+X+1
```

Результат – остаток 110011 ($R=x^5+x^4+x+1$).



Циклические коды, исправляющие пакеты ошибок.

В общем случае любой корректирующий код исправляющий t ошибок исправляет любую конфигурацию из t ошибок. Вместе с тем, если заранее известно, что ошибки расположены пакетом, то можно сконструировать коды более эффективно. Пакет ошибок описывается в виде $e(x)=x^i*b(x)(\mathrm{mod}\ x^n-1)$, где b(x) – многочлен, степень которого не выше чем t-1, x^i – локатор пакета, i – номер разряда.

Синдромные многочлены S(x) для исправляющего пакеты ошибок ЦК должны быть различны для любого пакета длины не более t.

<u>Пример 2:</u> $g(x)=x^6+x^3+x^2+x+1$, n=15 и корректирует пакеты из трёх и менее ошибок.

$e(x)=x^i, i=0,\ldots,14$

$e(x)=x^i(1+x)(\mathrm{mod}\ x^{15}-1)$

$e(x)=x^i(1+x^2)(\mathrm{mod}\ x^{15}-1)$

$e(x)=x^i(1+x+x^2)(\mathrm{mod}\ x^{15}-1)$

Непосредственным вычислением проявляется, что синдромы для всех 56 возможных пакетов различны. Следовательно, $g(x)=x^6+x^3+x^2+x+1$ порождает код, исправляющий все пакеты длины 3.

Как правило, ЦК, исправляющие пакеты ошибок синтезируются с помощью ЭВМ.

Основная литература: 1[97-119, 150-169, 172-204], 2[162-193, 197-211, 219-236, 239-245], 3 [69-70]

Дополнительная литература: 4[23-29, 130-133, 141-152, 161-215]

Контрольные вопросы:

1. Что является цифровым фильтром?
2. Обобщенная схема делительного устройства.
3. Чему соответствует умножение?
4. Циклические коды, исправляющие пакеты ошибок.

2.3 Планы практических занятий

Цель работ – научится практически применять знания, полученные во время лекционных занятий.

Практическое занятие № 1. ***(1 час)***

Тема: Количественная оценка информации. Мера Хартли.

Задание:

1. Определить количество информации по Хартли, содержащееся в системе, информационная емкость которой характеризуется десятичным числом Q.

2. Закодировать это число по двоичной системе счисления.

Методические рекомендации: Число Q взять из таблицы вариантов.

Основная литература: 1[31-40], 2[97-106], 3[12-20]

Дополнительная литература: 6[12-15]

Контрольные вопросы:

1. Какова формула Хартли?
2. Чем определяется количество информации?

Практическое занятие № 2. ***(1 час)***

Тема: Количественная оценка информации. Формула Шеннона.

Задание:

1. Изучить формулу Шеннона.

2. Определить количество информации по формуле Шеннона для величины заданной распределением Q.

Методические рекомендации: Вероятности взять из таблицы согласно варианту.

Основная литература: 1[31-40], 2[97-106], 3[12-20]

Дополнительная литература: 6[12-15]

Контрольные вопросы:

1. В чем отличие формулы Шеннона от меры Хартли?
2. Чем определяется основание логарифма в формуле Шеннона?

Практическое занятие № 3. ***(1 час)***

Тема: Способы измерения информации. Энтропия.

Задание:

1. Определить среднее количество информации, содержащееся в сообщении, используемом три независимых символа S_1, S_2, S_3. Известны вероятности появления символов $p(S_1)=p_1$, $p(S_2)=p_2$, $p(S_3)=p_3$. Оценить избыточность сообщения.

2. В условии предыдущего задания учесть зависимость между символами, которая задана матрицей условных вероятностей $P(S_i / S_j)$.

3.Найти энтропию дискретной случайной величины, заданной распределением.

Методические рекомендации: Вероятности взять из таблицы согласно варианту.

Основная литература: 1[41-44], 2[105-111], 3[12-20]

Дополнительная литература: 6[35-41]

Контрольные вопросы:

1. Что такое энтропия?
2. Какие свойства есть у энтропии?

Практическое занятие № 4. ***(1 час)***

Тема: Способы измерения информации. Избыточность.

Задание: Определить избыточность для букв русского, английского и французского языков.

Методические рекомендации: Вероятности распределения взять из справочника.

Основная литература: 1[31-40], 2[97-106], 3[12-20]

Дополнительная литература: 6[12-15]

Контрольные вопросы:

1. Что определяет избыточность?
2. Чем объясняется высокая избыточность языков?

Практическое занятие № 5. ***(1 час)***

Тема: Взаимовероятность и взаимоэнтропия.

Задание:

1. Определить взаимовероятность для двумерной случайной величины.
2. Определить взаимоэнтропию для двумерной случайной величины.

Методические рекомендации: Распеделение вероятностей взять из таблицы вариантов.

Основная литература: 1[31-40], 2[97-106], 3[12-20]

Дополнительная литература: 6[12-15]

Контрольные вопросы:

1. Что такое взаимовероятность?
2. Что такое взаимоэнтропия?

Практическое занятие № 6. ***(1 час)***

Тема: Условная энтропия

Задание: Определить условную энтропию для двумерной случайной величины.

Методические рекомендации: Распеделение вероятностей взять из таблицы вариантов.

Основная литература: 1[31-40], 2[97-106], 3[12-20]

Дополнительная литература: 6[12-15]

Контрольные вопросы:

1. Что показывает условная энтропия?
2. Как определяется условная энтропия?

Практическое занятие № 7. ***(1 час)***

Тема: Пропускная способность канала и скорость передачи информации.

Задание:

Определить пропускную способность канала связи, по которому передаются сигналы S_i. Помехи в канале определяются матрицей условных вероятностей $P(S_i / S_j)$. За секунду может быть передано N сигналов.

Методические рекомендации: Матрицы условных вероятностей взять из таблицы согласно варианту.

Основная литература: 3[45-50], 4[78-85]

Дополнительная литература: 7

Контрольные вопросы:

1. Скорость передачи сигнала.
2. Скорость передачи сообщения.
3. От чего зависит пропускная способность канала?

Практическое занятие № 8. ***(1 час)***

Тема: Сжатие информации. Алгоритм Шеннона-Фэно. Алгоритм Хаффмена.

Задание:

1. Вычислить среднее количество бит на единицу сжатого сообщения о значении каждой из дискретной случайной величины, из заданных распределениями вероятностей, при сжатии методами Шеннона-Фэно, Хаффмена.

2. Распаковать сообщение и рассчитать длину кода сжатого и несжатого сообщения в битах.

Методические рекомендации: Вероятности взять из таблицы согласно варианту.

Основная литература: 3[21-25, 28-33, 35-42]

Дополнительная литература: 7

Контрольные вопросы:

1. Как определяется степень сжатия информации?
2. Какие алгоритмы сжатия наиболее эффективны?
3. Перечислите алгоритмы сжатия?

Практическое занятие № 9. ***(1 час)***

Тема: Сжатие информации. Арифметическое кодирование.

Задание:

1. Вычислить среднее количество бит на единицу сжатого сообщения о значении каждой из дискретной случайной величины, из заданных распределениями вероятностей.

2. Распаковать сообщение и рассчитать длину кода сжатого и несжатого сообщения в битах.

Методические рекомендации: Вероятности взять из таблицы согласно варианту.

Основная литература: 3[21-25, 28-33, 35-42]

Дополнительная литература: 7

Контрольные вопросы:

1. Как определяется степень сжатия информации?
2. Какие алгоритмы сжатия наиболее эффективны?
3. Перечислите алгоритмы сжатия?

Практическое занятие № 10. ***(1 час)***

Тема: Алгоритмы Лемпеля-Зива.

Задание:

1. Выбрать размер словаря.
2. Выбрать размер буфера.
3. Закодировать сообщение алгоритмами Лемпеля-Зива.
4. Вычислить длины полученных кодов.

Методические рекомендации: Тексты для кодирования взять из таблицы вариантов.

Основная литература: 1[31-40], 2[97-106], 3[12-20]

Дополнительная литература: 6[12-15]

Контрольные вопросы:

1. К какому классу кодов относятся алгоритмы Лемпеля-Зива?
2. Как определить размер словаря и размер буфера?

Практическое занятие № 11. ***(1 час)***

Тема: Оптимальное кодирование.

Задание:

1. Провести кодирование по одной и блоками по две и по три букве, используя метод Шеннона – Фэно. Сравнить эффективности кодов.

2. Алфавит передаваемых сообщений состоит из независимых букв S_i. Вероятности появления каждой буквы в сообщении заданы. Определить и сравнить эффективность кодирования сообщений методом Хаффмена при побуквенном кодировании и при кодировании блоками по две буквы.

Методические рекомендации: Вероятности взять из таблицы согласно варианту.

Основная литература: 1[97-119], 2[162-193]

Дополнительная литература: 6[23-29]

Контрольные вопросы:

1. Какие алгоритмы относятся к оптимальным?
2. Чем определяется оптимальность кодирования?
3. Как определяются основные показатели оптимальности?

Практическое занятие № 12. ***(1 час)***

Тема: Помехоустойчивое кодирование.

Задание:

1. Закодировать сообщение.

2. Декодировать полученное сообщение *c*, если известно, что использовался (4, 7) – код Хэмминга.

3. Провести кодирование кодом с проверкой четности.

Методические рекомендации: Сообщения взять из таблицы согласно варианту.

Основная литература: 3[50-57]

Дополнительная литература: 6[130-141]

Контрольные вопросы:

1 . Как определяется избыточность кодов?

2. Какие алгоритмы относятся к помехоустойчивым кодам?

3. Как зависит помехоустойчивость кода от его избыточности?

Практическое занятие № 13. ***(1 час)***

Тема: Линейно-групповые коды.

Задание:

Для кодирующих матриц E_1 и E_2

1. Построить соответственно (2, 5)-код и (3, 4) код.

2. Описать основные характеристики полученных кодов.

3. Построить таблицы декодирования.

Методические рекомендации: Кодирующие матрицы взять из таблицы согласно варианту.

Основная литература: 1[60-93, 150-169], 2[19-236], 3[58-61].

Дополнительная литература: 6[141-152]

Контрольные вопросы:

1. Как характеризуются линейные групповые коды?

2. Как определяется синдром?

3. Как строится проверочная матрица?

Практическое занятие № 14. ***(1 час)***

Тема: Совершенные и квазисовершенные коды.

Задание:

1. Построить совершенный код.
2. Построить квазисовершенный код.

Методические рекомендации: Первоначальные данные взять из таблицы вариантов

Основная литература: 1[31-40], 2[97-106], 3[12-20]

Дополнительная литература: 6[12-15]

Контрольные вопросы:

1. Какой код может быть совершенным?
2. Какой код может быть квазисовершенным?

Практическое занятие № 15. ***(1 час)***

Тема: Полиномиальные коды.

Задание: Построить полиномиальный код.

Методические рекомендации: Первоначальные данные взять из таблицы вариантов

Основная литература: 1[31-40], 2[97-106], 3[12-20]

Дополнительная литература: 6[12-15]

Контрольные вопросы:

1. Какие коды относятся к полиномиальным?
2. Обнаруживает ли ошибки полиномиальный код?

2.4 Планы занятий в рамках самостоятельной работы студентов под руководством преподавателя (СРСП)

№	Задание	Формы проведения	Методические рекомендации по выполнению заданий	Рекомендуемая литература с указанием страниц
1	2	3	4	5
1	Структурная мера информации	Коллоквиум, опрос	Изучить структурные меры информации	1[19-31], 4[19-39]
2	Основные требования к информационным системам	Коллоквиум, опрос	Рассмотреть основные требования к информационным системам	3[45-50]
3	Количество информации	Решение задач	Определить количес-тво информации в заданном условии	3[12-20]
4	Энтропия	Решение задач	Определить энтропии русского, казахского языков	3[12-20]
5	Квантование сигналов	Коллоквиум, опрос	Изучить методы квантования сигналов	1[60-93]
6	Условная энтропия	Решение задач	Определить условную энтропию двух источников	3[12-20]
7	Избыточность информации	Решение задач	Определить избыточность русского и казахского языка	3[12-20]
8	Дискретизация символов	Коллоквиум, опрос	Изучить методы дискретизации сигналов	1[67-97]
9	Пропускная способность каналов	Решение задач	Определить пропуск-ную способность кана-лов	3[45-50]
10	Код Лемпеля-Зива	Решение задач	Изучить код и привести примеры кодирования	3[35-41]
11	Метод Шеннона-Фано	Решение задач	Изучить код и привести примеры кодирования	3[21-28]
12	Метод контрольных сумм	Решение задач	Изучить код и привести примеры кодирования	7
13	Линейный групповой код	Решение задач	Изучить код и привести примеры кодирования	3[58-61]

14	Циклический код	Решение задач	Изучить код и привести примеры кодирования	2[239-254], 3[69-70], 6[209-215]
15	Циклические коды, исправляющие пакеты ошибок	Решение задач	Изучить код и привести примеры кодирования	3[69-70]

2.5 Планы занятий в рамках самостоятельной работы студентов (СРС)

№	Задание	Методические рекомендации по выполнению заданий	Рекомендуемая литература с указанием страниц
1	**2**	**3**	**4**
1	История развития теории информации	Рассмотреть историю развития теории информации.	3[4-6]
2	Измерение семантической информации	Рассмотреть методы измерения семантической информации и привести примеры.	1[54-63], 3[20-21], 6[75-80]
3	Измерение геометрической информации.	Рассмотреть методы измерения геометрической информации и привести примеры.	6[75-80]
4	Эпсилон-энтропия.	Рассмотреть понятие эпсилон-энтропии и ее свойства	1[40-44], 2[8-13], 4[40-50]
5	Дифференциальная энтропия.	Рассмотреть свойства дифференциальной энтропии.	4[30-40]
6	Свойства условной энтропии.	Рассмотреть своства условной энтропии.	3[12-20]
7	Избыточность информации.	Рассмотреть степень избыточности информации в файлах различного формата.	3[12-20]
8	Формы представления сигналов	Рассмотреть формы представления сигналов. Привести примеры.	3[7-10]
9	Преимущества цифровой формы представления сигналов	Рассмотреть преимущества цифрового представления сигналов	7
10	Программы-архиваторы.	Рассмотреть принцип работы программ-архиваторов и степень сжатия.	3[42-44], 6[23-29]
11	Арифметическое кодирование	Рассмотреть особенности построения и привести примеры.	3[25-28, 33-35], 6[130-141]
12	Матричное кодирование	Рассмотреть особенности построения и привести примеры.	3[57-58]
13	Совершенные и квазисовершенные коды	Рассмотреть особенности построения и привести примеры.	3[61-65]
14	Полиномиальные коды	Рассмотреть особенности построения и привести примеры.	3[65-67]

15	Коды Боуза-Чоудхури-Хоккенгема	Рассмотреть особенности построения и привести примеры.	3[67-69]

2.6 Тематика письменных работ по курсу

Тематика контрольных работ

1. Энтропия. Свойства энтропии.
2. Каналы связи.
3. Кодирование информации.
4. Сжатие информации.

Рекомендуемая литература лекции, основная и дополнительная литература

2.7 Тестовые задания для самоконтроля с указанием ключей правильных ответов (30 вопросов)

&&& 1. За единицу измерения информации в теории кодирования принимается:

А) 1 кг;

Б) 1 фут;

В) 1 бар;

Г) 1 бит;

Д) 1 бод.

&&& 2. В теории информации количество информации в сообщении определяется как:

А) количество различных символов в сообщении;

Б) мощность физического сигнала - носителя информации;

В) объем памяти компьютера, необходимый для хранения сообщения;

Г) мера уменьшения неопределенности, связанного с получением сообщения;

Д) сумма произведений кодируемого символа на среднюю вероятность его выбора из алфавита.

&&& 3. Даны три сообщения:

1) «Монета упала цифрой вверх»;

2) «Игральная кость упала вверх гранью с тремя очками»;

3) «На светофоре горит красный свет».

Какое из них согласно теории информации содержит больше информации:

А) второе;

Б) третье;

В) первое;

Г) количество информации во всех сообщениях одинаково;

Д) вопрос некорректен?

&&& 4. Можно ли измерить информацию, исходя из того, что количество информации в сообщении зависит от новизны этого сообщения для получателя:

А) может быть да;

Б) да, разумеется;

В) скорее нет, чем да;

Г) нельзя;

Д) на сегодняшний день дать категорический ответ на данный вопрос принципиально невозможно?

&&& 5. Каково значение избыточных символов?

А) применение для обнаружения и исправления ошибок.

Б) применение для перехвата информации.

В) применение для анализа свойств источника.

Г) применение для улучшения пропускной способности канала.

Д) применение для увеличения количества ошибок.

&&& 6. Как определяется существенность информации?

А) по степени простоты информации о том или ином событии.

Б) по степени гарантированности информации о том или ином событии.

В) по степени корректности информации о том или ином событии.

Г) по степени важности информации о том или ином событии.

Д) по стоимости информации о том или ином событии.

&&& 7. Как осуществляется динамическая энтропия?

А) обращением в нуль неопределенности ситуации.

Б) обращением в нуль прагматической составляющей.

В) обращением в нуль определенности ситуации.

Г) обращением в единицу определенности ситуации.

Д) обращением в единицу неопределенности ситуации.

&&& 8. Как оценивается содержательность информации?

А) на основе семантического анализа.

Б) на основе сигматического анализа.

В) на основе математической логики.

Г) на основе статистического анализа.

Д) на основе логистики.

&&& 9. Как образуются сигналы?

А) физическими процессами, параметры которых содержат информацию.

Б) физическими процессами, параметры которых не содержат информацию.

В) физическими процессами, параметры которых содержат сообщения.

Г) физическими процессами, которых содержат информацию.

Д) некоторыми процессами, которых содержат информацию.

&&& 10. Как образуются циклические коды?

А) сдвигом последней комбинации.

Б) сдвигом образующей комбинации.

В) сдвигом канала.

Г) сдвигом сообщения.

Д) сдвигом источника.

&&& 11. Как определяются оптимальные коды?

А) по обеспечению максимальной корректирующей способности при минимально возможной избыточности.

Б) по обеспечению заданной корректирующей способности при максимально возможной избыточности.

В) по обеспечению минимальной корректирующей способности при максимально возможной избыточности.

Г) по обеспечению корректирующей способности при случайной избыточности.

Д) по обеспечению заданной корректирующей способности при минимально возможной избыточности.

&&& 12. Как определяется избыточность?

А) по степени оптимизации кодовой комбинации.

Б) по степени укорочения кодовой комбинации для не достижения определенной корректирующей способности.

В) по степени удлинения кодовой комбинации для не достижения определенной корректирующей способности.

Г) по степени удлинения кодовой комбинации для достижения определенной корректирующей способности.

Д) по степени укорочения кодовой комбинации для достижения определенной корректирующей способности.

&&& 13. Как осуществляется оптимальное кодирование информации?

А) обеспечивается заданная достоверность при передаче и хранении информации путем дополнительного внесения избыточности.

Б) обеспечивается заданная плотность при передаче и хранении информации путем дополнительного внесения избыточности.

В) обеспечивается заданная информативность при передаче и хранении информации путем дополнительного внесения избыточности.

Г) обеспечивается заданная компактность при передаче и хранении информации путем дополнительного внесения избыточности.

Д) обеспечивается заданная гарантированность при передаче и хранении информации путем дополнительного внесения избыточности.

&&& 14. Как выполняется эффективное кодирование?

А) путем повышения избыточности существенно повышается минимальное число символов на букву сообщения.

Б) путем повышения избыточности существенно снижается среднее число символов на букву сообщения.

В) путем понижения избыточности существенно снижается максимальное число символов на букву сообщения.

Г) путем повышения избыточности существенно повышается среднее число символов на букву сообщения.

Д) путем понижения избыточности существенно снижается среднее число символов на букву сообщения.

&&& 15. Что выполняется при кодировании сообщений?

А) осуществляется преобразование сообщений в сигналы.

Б) осуществляется представление сообщений в форме, удобной для передачи по данному каналу.

В) осуществляется отображение сообщений в форме, удобной для человека.

Г) осуществляется обработка сообщений для представления человеку.

Д) осуществляется восстановление сообщений для повторной передачи по данному каналу.

&&& 16. Что измеряет энтропия?

А) качество передачи.

Б) структуру канала.

В) смысл сообщений.

Г) содержание сообщений.

Д) количество информации.

&&& 17. Что передает дискретный канал?

А) объекты.

Б) последовательности символов.

В) помехи и ошибки.

Г) аналоговые сигналы.

Д) произвольные предметы.

&&& 18. Кем была предложена логарифмическая мера информации?

А) Шенноном.

Б) Котельниковом.

В) Хартли.

Г) Бородиным.

Д) Фано.

&&& 19. Как определяется понятие «тезаурус»?

А) запас объектов, используемый приемником.

Б) запас знаний или словарь, используемый передатчиком.

В) запас знаний или словарь, используемый каналом.

Г) запас знаний или словарь, используемый преобразователем.

Д) запас знаний или словарь, используемый приемником.

&&& 20. Для какого кода минимальное расстояние определяется выражением $n-k+1$?

А) Шеннона-Фано.

Б) БЧХ.

В) Рида-Соломона.

Г) Хэмминга.

Д) Блэйхута.

&&& 21. Как описывается пропускная способность?

А) $C = \min\limits_{N\to\infty} \dfrac{\log N(T)}{T}$

Б) $C = \inf\limits_{N\to\infty} \dfrac{\log N(T)}{T}$

В) $C = \sup\limits_{N\to\infty} \dfrac{\log N(T)}{T}$

Г) $C = \lim\limits_{N\to\infty} \dfrac{tgN(T)}{T}$

Д) $C = \lim\limits_{N\to\infty} \dfrac{\log N(T)}{T}$

&&& 22. Что означает следующее выражение $C = \max\left|H(x) - H_y(x)\right|$?

А) пропускная способность канала с шумами.
Б) пропускная способность источника информации.
В) пропускная способность приемника.
Г) пропускная способность передатчика.
Д) пропускная способность получателя.

&&& 23. Как вычисляется избыточность?

А) $R = 2 - \dfrac{H}{H_{\max}}$

Б) $D = 1 + \dfrac{H}{H_{\max}}$

В) $D = 1 - \dfrac{H}{H_{\max}}$

Г) $D = 1 - \dfrac{H_{\min}}{H_{\max}}$

Д) $K = T - \dfrac{H}{H_{\max}}$

&&& 24. Чему равна пропускная способность канала с шумом?

А) $C = \max\left|H(x) - H_x(y)\right|$

Б) $C = \max\left|H(x) - H_y(x)\right|$

В) $C = \min\left|H(x) - H_y(x)\right|$

Г) $C = \min\left|H(y) - H_y(x)\right|$

Д) $C = \inf \left| H(x) - H_y(x) \right|$

&&& 25. Что определяет величина $\frac{\log n(q)}{N}$?

А) число бит на символ, необходимых для задания анализируемого процесса.

Б) число бит в секунду, необходимых для получения последовательностей.

В) число бит на символ, необходимых для получения последовательностей.

Г) число бит секунду, необходимых для задания последовательностей.

Д) число бит на символ, необходимых для задания последовательностей.

&&& 26. Как называется следующее отношение $\frac{H}{H_{\max}}$?

А) относительная энтропия.

Б) условная энтропия.

В) минимальное сжатие.

Г) среднее сжатие.

Д) средняя энтропия.

&&& 27. Что означает величина H (x, y)?

А) энтропия условных событий.

Б) энтропия совместных событий.

В) энтропия случайных событий.

Г) энтропия закономерных событий.

Д) энтропия зависимых событий.

&&& 28. Что такое «циклические коды»?

А) коды, которые могут быть получены сдвигом сообщения.

Б) коды, которые могут быть получены сдвигом образующей комбинации.

В) коды, которые могут быть получены сдвигом источника.

Г) коды, которые могут быть получены сдвигом канала.

Д) коды, которые могут быть получены сдвигом последней комбинации.

&&& 29. Что является условием исправления любой одиночной ошибки?

А) $2^{n-k} - 1 \le C_n^1 = n$

Б) $2^{n-k} + 1 \ge C_n^1 = n$

В) $2^{n-k} - 1 \ge C_n^1 \ne n$

Г) $2^{n-k} - 1 \ge C_n^1 = n$

Д) $2^{n-k} - 1 = C_n^1 = n$

&&& 30. Что определяет следующее неравенство $Q \le \frac{2^n}{\sum_{i=0}^{s} C_n^i}$?

А) границу разрешенных комбинаций.
Б) число возможных проверочных разрядов.
В) границу ненадежности.
Г) условие корректности.
Д) условие эффективности.

Таблица 31

Правильные ответы

Номера вопросов	**Правильный ответ**	**Номера вопросов**	**Правильный ответ**	**Номера вопросов**	**Правильный ответ**
1	Д	11	Д	21	Д
2	Г	12	Г	22	А
3	Г	13	А	23	В
4	Б	14	Б	24	Б
5	А	15	Б	25	Д
6	Г	16	Д	26	А
7	А	17	Б	27	Б
8	В	18	В	28	Б
9	А	19	Д	29	Г
10	Б	20	В	30	А

2.8 Перечень экзаменационных вопросов (80 вопросов)

1. Понятие информации. Свойства информации.
2. Знаки и сигналы. Сигнал, его характеристики.
3. Передача информации в информационной системе.
4. Измерение информации (меры информации)
5. Квантование сигналов.
6. Синтаксическая и семантическая информация.
7. Энтропия и ее свойства.
8. Количество информации.
9. Энтропия непрерывных сообщений.
10. Условная энтропия и взаимная информация – дискретные системы передачи информации.
11. Условная энтропия и взаимная информация – непрерывные системы передачи информации.
12. Избыточность информации. Взаимная информация.
13. Информационные характеристики квантованного сигнала.
14. Пропускная способность канала связи при отсутствии шумов.
15. Пропускная способность канала связи с шумом.
16. Дискретизация информации. Теорема Котельникова.
17. Структура канала связи.

18.Формула К.Шеннона.

19. Понятие о помехоустойчивом кодировании.

20. Пространственная и временная избыточность.

21. Сжатие данных

22. Код с повторением.

23. Кодирование сообщений в дискретном канале: кодирующее отображение, равномерный и неравномерный коды.

24. Эффективное кодирование.

25. Код Хаффмена.

26. Код Шеннона-Фано.

27. Расстояние по Хэммингу.

28. Вес слова. Кодовое расстояние.

29. Связь обнаруживающей и корректирующей способности кода с кодовым расстоянием.

30. Геометрическая интерпретация связи кодового расстояния и корректирующей способности кода.

31. Линейные групповые коды.

32. Порождающая матрица – технология построения.

33. Задача построения линейного группового кода с заданными свойствами.

34. Кодирование в линейных групповых кодах: систематическое и несистематическое.

35. Декодирование в линейных групповых кодах.

36. Фактические возможности линейных групповых кодов по обнаружению ошибок.

37. Проверочная матрица – ее структура и связь с порождающей матрицей.

38. Коды Хэмминга.

39. Систематический и несистематический коды Хэмминга.

40. Понятие о циклических кодах. Порождающие многочлены. Структура кодового слова.

41. Порождающая матрица циклического кода.

42. Систематический и несистематический циклический коды.

43. Алгоритм построения циклического кода с заданными свойствами.

44. Алгоритм коррекции ошибок в циклическом коде.

45. Процедура выбора порождающего многочлена.

46. Схемы аппаратной реализации кодеров и декодеров циклического кода.

47. Циклические коды, исправляющие пакеты ошибок.

48. Формула для построения кода, близкого к эффективному.

49. Декодирование сообщений в дискретном канале

50. Взаимная энтропия.

51. Виды информации

52. Хранение и обработка информации

53. Способы измерения информации

54. Вероятностный подход к измерению информации
55. Кодирование информации
56. Арифметическое кодирование
57. Адаптивные алгоритмы сжатия
58. Адаптивный алгоритм Хаффмена
59. Упорядоченный алгоритм Хаффмена
60. Подстановочные или словарно-ориентированные алгоритмы сжатия информации
61. Методы Лемпеля-Зива
62. LZ77
63. LZ78
64. LZSS
65. LZW
66. Особенности программ-архиваторов
67. Сжатие информации с потерями
68. Информационный канал
69. Определение длины кода
70. Определение степени сжатия
71. Адаптивное арифметичекое кодирование
72. Декодирование адаптивных кодов
73. Распаковка подстановочных кодов сжатия
74. Мера Хартли
75. Математическая модель систем связи
76. Матричное кодирование
77. Совершенные коды
78. Квазисовершенные коды
79. Полиномиальные коды
80. Коды Боуза-Чоудхури-Хоккенгема

Глоссарий по курсу

Бит	минимальная единица количества информации, соответствующая одному двоичному разряду.
Декодирование	преобразование данных в исходную форму, которую они имели до кодирования; операция, обратная кодированию.
Дискретный канал передачи информации	совокупность средств, предназначенных для передачи дискретных сигналов.
Знаки	реальноразличимые получаемые материальными объектами: ёмкость, знаки, иероглифы.
Избыточность	понимают использование больших ресурсов для передачи сообщения, чем минимально необходимо.
Информация	сведения о лицах, предметах, фактах, событиях,

	явлениях и процессах независимо от формы их представления, хранящиеся или циркулирующие в обществе, биологических, технических и технологических системах.
Информационные системы	системы, выполняющие автоматизированную обработку официальной документированной информации в целях удовлетворения потребностей в информации.
Канал	часть коммуникационной системы, связывающая между собой источник и приемник сообщений.
Кодирование	представление символа какого-либо алфавита при помощи символов или строк символов из другого алфавита.
Линия связи	Физическая среда, по которой происходит передача сигналов от передатчика к приемнику
Передатчик	устройство, являющееся источником данных.
Помеха	любые мешающие внешние возмущения или воздействия (атмосферные помехи, влияние посторонних источников сигналов), а также искажения сигналов в самой аппаратуре (аппаратурные помехи), вызывающие случайное отклонение принятого сообщения (сигнала) от передаваемого
Помехоустойчивость	способность информации противостоять вредному воздействию помех.
Приемник	устройство, принимающее данные.
Пропускная способность	наибольшая теоретически достижимая для данного канала скорость передачи информации.
Распознавание	это отожествление знаков и сигналов с объектами и их отношениями в реальном мире.
Семантическая (смысловая) информация	Информация, основанная на однозначной связи знаков и сигналов с объектами реального мира,
Сигнал	материальный переносчик сообщения, т.е. изменяющаяся физическая величина, обеспечивающая передачу информации по линии связи.
Синтаксическая информация	Информация, заключенная в порядке следования символов, называется
Система кодирования	совокупность символов и правил кодирования.

Скорость передачи информации	среднее количество информации, передаваемое по каналу в единицу времени.
Сообщение	это форма представления информации.
Средства передачи	физическая передающая среда и специальная аппаратура, обеспечивающая передачу сообщений
Тезаурус	это совокупность сведений, которыми располагает пользователь или система.
Теория информации	это наука о получении, преобразовании, накоплении, отображении и передаче информации.
Энтропия	это количественная мера неопределенности сообщений.

Жулдыз Кенесхановна Алимсеитова

ТЕОРИЯ ИНФОРМАЦИИ

Учебно-методический комплекс дисциплины

(для специальности 5В100200 – Системы информационной безопасности)

Редактор
Техн. редактор

Протокол заседания кафедры
«Вычислительная техника» №___ «__» _____2011г.

Протокол заседания УМС института
«Информационных и
телекоммуникационных технологий» №___ «__» _____2011г.

Подписано в печать _____201__г.

Тираж ____ экз. Формат 60x84 1/16. Бумага типографская № 1.
Объем ___ п.л. Заказ № _____. Цена договорная

Издание Казахского национального технического университета
имени К.И. Сатпаева
Научно-технический издательский центр КазНТУ
г. Алматы, ул. Ладыгина 32