ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.В.06 Теория информации

Направление подготовки (специальность) *09.03.01 Информатика и вычислительная техника*

Профиль образовательной программы *«Автоматизированные системы обработки информации и управления»*

Форма обучения *заочная*

СОДЕРЖАНИЕ

1. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1.1. Организационно-методические данные дисциплины

№ п.п.	Наименование темы	Общий объем часов по видам самостоятельной работы				
		подготовка курсового проекта (работы)	подготовка реферата/эссе	индивидуальные домашние задания (ИДЗ)	самостоятельное изучение вопросов (СИВ)	подготовка к занятиям (ПкЗ)
1	2	3	4	5	6	7
1	**Раздел 1 Введение. Анализ сигналов, как средства передачи информации**				**12**	
1.1	**Тема 1** Понятие информации. Модели детерминированных и случайных сигналов. Преобразование непрерывных сигналов в дискретные				6	
1.2	**Тема 2** Меры неопределенности дискретных множеств и непрерывных случайных величин. Количество информации как мера снятой неопределенности				6	
2	**Раздел 2 Анализ информационных характеристик источников сообщения и каналов связи**				**12**	
2.1	**Тема 3** Оценка информационных характеристик источников сообщений				6	
2.2	**Тема 4** Информационные характеристики каналов связи				6	
3	**Раздел 3 Теория кодирования**					
3.1	**Тема 5** Эффективное кодирование. Введение в теорию помехоустойчивого кодирования				**24**	
3.2	**Тема 6** Построение групповых кодов. Циклические коды				**24**	

33	**Тема 7** Матричные представления в теории кодирования. Кодирование линейными последовательными машинами			**50**	**24**	
4	**Раздел 4 Методы приема и обработки информации**			20	8	
4.1	**Тема 8** Обнаружение и различение сигналов			20	8	
4.2	**Тема 9** Оценка параметров сигналов			10	8	

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ИНДИВИДУАЛЬНЫХ ДОМАШНИХ ЗАДАНИЙ

Индивидуальное домашнее задание выполняется в виде контрольной работы.

2.1 Темы индивидуальных домашних заданий

Работа №1:

1. Построить неравномерные эффективные коды по методике Шеннона-Фано или Хаффмена для кодирования слов длиной в 1 и 2 символа.
2. Разработать Марковские процедуры кодирования слов длиной 1 и 2 символа.
3. Оценить и сравнить эффективность построенных кодов.
4. Построенными кодами (4 шт.) закодировать фрагмент текста длиной в 30 символов, выбранный источником.

Для источника без памяти:

5. Построить неравномерные эффективные коды по методике Шеннона-Фано или Хаффмена для кодирорвания слов длиной в 1, 2 и 3 символа.
6. Оценить и сравнить эффективность построения кодов.
7. Разработанными кодами (3 шт) закодировать текст длиной в 30 символов, выбранной источником.

Работа №2:

2.2 Содержание индивидуальных домашних заданий

Для источника с памятью (марковского):

1. Построить неравномерные эффективные коды по методике Шеннона-Фано или Хаффмена для кодирования слов длиной в 1 и 2 символа.
2. Разработать марковские процедуры кодирования слов длиной 1 и 2 символа.
3. Оценить и сравнить эффективность построенных кодов.
4. Построенными кодами (4 шт.) закодировать фрагмент текста длиной в 30 символов, выработанный источником.

Для источника без памяти:

1. Построить неравномерные эффективные коды по методике Шеннона-Фано или Хаффмена для кодирования слов длинной в 1, 2 и 3 символа.
2. Оценить и сравнить эффективность построенных кодов.
3. Разработанными кодами (3 шт.) закодировать текст длинной в 30 символов, выработанный источником.

2.3 Порядок выполнения заданий . Работа выполняется по вариантам .

Самостоятельно. Приводятся все необходимые пояснения

2.4 Пример выполнения задания

Работа №1:

1.Теоретические сведения

Эффективное кодирование информации

Понятие о кодировании.

Коды появились в глубокой древности в виде, когда ими пользовались для засекречивания важного сообщения. В наше время коды приобрели иное значение, являясь, прежде всего, средством для экономной, удобной и практически безошибочной передачи сообщений. Новое применение кодов сложилось в результате бурного развития средств связи, неизмеримо возросшего объема передаваемой информации. Решать возникшие в связи с этим задачи было бы невозможно без привлечения самых разнообразных математических методов. Неслучайно поэтому теория кодирования считается сейчас одним из наиболее важных разделов прикладной математики.

Как известно, передача информации от источника к получателю производится посредством сигналов. Для того чтобы сигналы были однозначно поняты, их необходимо составлять по правилу, которое строго фиксировано в течение всего времени передачи данной группы сообщений. Правило, устанавливающее каждому конкретному сообщению строго определенную комбинацию различных символов, называется кодом, а процесс преобразования сообщения в комбинацию различных символов или соответствующих им сигналов - кодированием. Процесс восстановления содержания сообщения по данному коду называется декодированием.

Последовательность символов, которая в процессе кодирования присваивается каждому из множеств передаваемых сообщений, называется кодовым словом. Символы, с помощью которых записано передаваемое сообщение, составляют первичный алфавит, а символы, с помощью которых сообщение трансформируется в код - вторичный алфавит.

Исторически первый код, предназначенный для передачи сообщений, связан с именем изобретателя телеграфного аппарата Сэмюэля Морзе и известен всем как азбука Морзе. Другим кодом, столь же широко распространенным в телеграфии, является код Бодо. Оба они используют два различных элементарных сигнала. Такие коды принято называть двоичными.

Коды, в которых сообщения представлены комбинациями с неравным количеством символов, называются неравномерными, или некомплектными. Коды, в которых сообщения представлены комбинациями с равным количеством символов, называется равномерными, или комплектными.

Примером неравномерного кода может служить азбука Морзе, а равномерного - пятизначный код Бодо.

Коды могут быть представлены формулой, геометрической фигурой, таблицей, графом, многочленом, матрицей и.т.д.

Представление кода числа А в виде многочлена для любой позиционной системы счисления есть сумма произведений коэффициента a_i и веса x_i i-го разряда кода:

$$A = \sum_i a_i x_i \ .$$

В качестве коэффициента a_i используют целое неотрицательное число, причем

$0 \le a_i < \lim_{n\to\infty} \frac{x_n}{x_{n-1}}$,где $\lim_{n\to\infty} \frac{x_n}{x_{n-1}}$ - основание системы счисления.

Представление кода в виде геометрической модели возможно благодаря тому, что кодовые комбинации n-значного кода могут рассматриваться как определенные точки n-мерного пространства. Так, геометрическая модель двузначного кода представляет собой квадрат - фигуру двумерного пространства; трехзначного - куб (фигуру трехмерного пространства).

Принципы эффективного кодирования.

Известно, что максимальное количество информации на символ сообщения можно получить только в случае равновероятных и независимых символов. Реальные коды редко полностью удовлетворяют этому условию, поэтому информационная нагрузка на каждый их элемент обычно меньше той, которую они могли бы переносить. Раз элементы кодов, представляющих сообщения, недогружены, то само сообщение обладает информационной избыточностью.

Различают избыточность естественную и искусственную. Естественная избыточность характерна для первичных алфавитов, а искусственная - для вторичных.

Естественная избыточность может быть подразделена на семантическую и статистическую избыточности.

Семантическая избыточность заключается в том, что мысль, высказанная в сообщении, может быть выражена короче. Все преобразования по устранению семантической избыточности производятся в первичном алфавите.

Статистическая избыточность обусловливается не равновероятностным распределением качественных признаков первичного алфавита и их взаимозависимостью. Например, для английского языка избыточность составляет 50 %.

Устраняется статистическая избыточность путем построения эффективных неравномерных кодов. При этом статистическая избыточность первичного алфавита устраняется за счет рационального построения сообщений во вторичном алфавите.

При передаче сообщений, закодированных двоичным равномерным кодом, обычно не учитывают статистическую структуру передаваемых сообщений . Все сообщения (независимо от вероятности их появления) представляют собой кодовые комбинации одинаковой длины, т.е. количество двоичных символов, приходящихся на одно сообщение, строго постоянно.

Из теоремы Шеннона о кодировании сообщений в каналах без шумов следует, что если передача дискретных сообщений ведется при отсутствии помех, то всегда можно найти такой метод кодирования, при котором среднее число двоичных символов на одно сообщение будет сколь угодно близким к энтропии источника этих сообщений. На основании этой теоремы можно ставить вопрос о построении такого неравномерного кода, в котором часто встречающимся сообщениям присваиваются более короткие кодовые комбинации, а редко встречающимся символам - более длинные.

Таким образом, учет статистических закономерностей сообщения позволяет строить более экономный, более эффективный код.

Эффективным кодированием называется процедура преобразования символов первичного алфавита в кодовые слова во вторичном алфавите, при которой средняя длина сообщений во вторичном алфавите имеет минимально возможную для данного алфавита длину.

Эффективными называются коды, представляющие кодируемые понятия кодовыми словами минимальной средней длины. В литературе вместо термина “эффективное

кодирование” часто используют так же термины оптимальное или статистическое кодирование.
Эффективность кодов видна близостью энтропии источника сообщений и среднего числа двоичных знаков на букву кодов, т.е. в идеальном случае должно выполняться равенство

$$\log_2 m \sum_{i=1}^{n} l(i) P_i = l_{c.p} = H,$$

Для двоичных кодов $L_{cp} = \sum_{i=1}^{n} l(i)\, p_i = -\sum_{i=1}^{n} p_i \log_2 p_i$ и разность ($L_{ср}$ - Н) будет тем меньше, чем больше Н, а Н достигает максимума при равновероятных и взаимно независимых символах. Отсюда вытекают основные свойства эффективных кодов:

- минимальная средняя длина кодового слова оптимального кода обеспечивается в том случае, когда избыточность каждого кодового слова сведена к минимуму (в идеальном случае - к нулю);
- кодовые слова оптимального кода должны строиться из равновероятных и взаимно независимых символов.

Из свойств оптимальных кодов вытекают принципы их построения.
Первый принцип эффективного кодирования: выбор каждого кодового слова необходимо производить так, чтобы содержащееся в нем количество информации было максимальным. Второй принцип эффективного кодирования заключается в том, что буквам первичного алфавита, имеющим большую вероятность, присваиваются более короткие кодовые слова во вторичном алфавите.
Принципы эффективного кодирования определяют методику построения эффективных кодов.

Построение эффективного кода по методу Шеннона-Фано.

Построение эффективного кода по методу Шеннона-Фано сводится к следующей процедуре:

- множество сообщений располагают в порядке убывания вероятностей;
- первоначальный ансамбль кодируемых сигналов разбивают на две группы таким образом, чтобы суммарные вероятности сообщений обеих групп были по возможности равны;
- одной группе присваивается символ 0 , другой группе - символ 1;
- каждую из подгрупп делят на две группы так, чтобы их суммарные вероятности были по возможности равны;
- одним подгруппам каждой из групп вновь присваивают 0, а другим - 1, в результате чего получают вторые цифры кода. Затем каждую из четырех подгрупп вновь делят на равные части и т.д. до тех пор, пока в каждой из подгрупп остается по одной букве.

1. Построим двоичные неравномерные эффективные коды
Для получения кодов для кодирования по одному символу используем методику Хаффмена:
P(A) = 0,811
P(B) = 0,040
P(D) = 0,149

Слово	Вероятность	КК	Длина КК	
A	0,811	1	1	
B	0,040	01	2	

D	0,149	00	2	

Для получения кодов для кодирования по два символа используем методику Хаффмена, предварительно рассчитав частоты появления слов, которые состоят из двух символов:
P(AA) = P(A)*P(A) = 0,811*0,811 = 0,6577
P(AB) = P(A)*P(B) = 0,811*0,040 = 0,0324
P(AD) = P(A)*P(D) = 0,811*0,149 = 0,1208
P(BA) = P(B)*P(A) = 0,040*0,811 = 0,0324
P(BB) = P(B)*P(B) = 0,040*0,040 = 0,0016
P(BD) = P(B)*P(D) = 0,040*0,149 = 0,0060
P(DA) = P(D)*P(A) = 0,149*0,811 = 0,1208
P(DB) = P(D)*P(B) = 0,149*0,040 = 0,0060
P(DD) = P(D)*P(D) = 0,149*0,149 = 0,0222

Слово	Вероятность	КК	Длина КК	
AA	0,6577	1	1	
AB	0,0324	00111	5	
AD	0,1208	01	2	
BA	0,0324	00110	5	
BB	0,0016	0010111	7	
BD	0,0060	0010110	7	
DA	0,1208	000	3	
DB	0,0060	001010	6	
DD	0,0222	00100	5	

Для получения кодов для кодирования по три символа используем методику Хаффмена, предварительно рассчитав частоты появления слов, которые состоят из трех символов:
P(AAA) = P(A)*P(A)*P(A) = 0,811*0,811*0,811 = 0,5334
P(AAB) = P(A)*P(A)*P(B) = 0,811*0,811*0,040 = 0,0263
P(AAD) = P(A)*P(A)*P(D) = 0,811*0,811*0,149 = 0,0980
P(ABA) = P(A)*P(B)*P(A) = 0,811*0,040*0,811 = 0,0263
P(ABB) = P(A)*P(B)*P(B) = 0,811*0,040*0,040 = 0,0013
P(ABD) = P(A)*P(B)*P(D) = 0,811*0,040*0,149 = 0,0048
P(ADA) = P(A)*P(D)*P(A) = 0,811*0,149*0,811 = 0,0980
P(ADB) = P(A)*P(D)*P(B) = 0,811*0,149*0,004 = 0,0048
P(ADD) = P(A)*P(D)*P(D) = 0,811*0,149*0,149 = 0,0180
P(BAA) = P(B)*P(A)*P(A) = 0,040*0,811*0,811 = 0,0263
P(BAB) = P(B)*P(A)*P(B) = 0, 040*0,811*0,040 = 0,0013
P(BAD) = P(B)*P(A)*P(D) = 0, 040*0,811*0,149 = 0,0048
P(BBA) = P(B)*P(B)*P(A) = 0, 040*0,040*0,811 = 0,0013
P(BBB) = P(B)*P(B)*P(B) = 0, 040*0,040*0,040 = 0,0001
P(BBD) = P(B)*P(B)*P(D) = 0, 040*0,040*0,149 = 0,0002
P(BDA) = P(B)*P(D)*P(A) = 0, 040*0,149*0,811 = 0,0048
P(BDB) = P(B)*P(D)*P(B) = 0, 040*0,149*0,004 = 0,0002

P(BDD) = P(B)*P(D)*P(D) = 0, 040*0,149*0,149 = 0,0009
P(DAA) = P(D)*P(A)*P(A) = 0,149*0,811*0,811 = 0,0980
P(DAB) = P(D)*P(A)*P(B) = 0, 149*0,811*0,040 = 0,0048
P(DAD) = P(D)*P(A)*P(D) = 0, 149*0,811*0,149 = 0,0180
P(DBA) = P(D)*P(B)*P(A) = 0, 149*0,040*0,811 = 0,0048
P(DBB) = P(D)*P(B)*P(B) = 0, 149*0,040*0,040 = 0,0002
P(DBD) = P(D)*P(B)*P(D) = 0, 149*0,040*0,149 = 0,0009
P(DDA) = P(D)*P(D)*P(A) = 0, 149*0,149*0,811 = 0,0180
P(DDB) = P(D)*P(D)*P(B) = 0, 149*0,149*0,004 = 0,0009
P(DDD) = P(D)*P(D)*P(D) = 0, 149*0,149*0,149 = 0,0033

Слово	Вероятность	КК	Длина КК	
AAA	0,5334	1	1	
AAB	0,0263	010111	6	
AAD	0,0980	001	3	
ABA	0,0263	010110	6	
ABB	0,0013	0100011011	10	
ABD	0,0048	01010011	8	
ADA	0,0980	011	3	
ADB	0,0048	01010010	8	
ADD	0,0180	00011	5	
BAA	0,0263	010101	6	
BAB	0,0013	0100011010	10	
BAD	0,0048	01010001	8	
BBA	0,0013	0101000011	10	
BBB	0,0001	0101000010111	13	
BBD	0,0002	0101000010110	13	
BDA	0,0048	01000111	8	
BDB	0,0002	0101000010101	13	
BDD	0,0009	01010000100	11	
DAA	0,0980	000	3	
DAB	0,0048	01000101	8	
DAD	0,0180	010010	6	

DBA	0,0048	01000100	8	
DBB	0,0002	0101000010100	13	
DBD	0,0009	0101000001	10	
DDA	0,0180	010000	6	
DDB	0,0009	010100000	9	
DDD	0,0033	010001100	9	

2. Сравним между собой построенные коды и их эффективность

Рассчитаем среднюю длину кодовой комбинации в расчете на один символ источника.

l ср (1) = 0,811*1 + 0,040*2 + 0,149*2 = 1,189

l ср (2) = [0,6577*1 + (0,0324 + 0,0324 + 0,0060 + 0,0222)*5 + (0,0016 + 0,0060)*7 + 0,128*3]/2 = 0,8929

l ср (3) = 2,5296/3 = 0,8432

Найдем относительную разницу между средней длиной кодовой комбинации и энтропией источника.

H(x) = 0,8126

Видим, что наиболее эффективным будет код при кодировании по три символа.

3. Построенными кодами закодируем фрагмент текста

AAAAAAAAAAADDAAAAAAAAAAABADAAA

Для кодирования по одному символу:

11111111111000011111111111101100111

Длина двоичной последовательности: L = 34.

Для кодирования по два символа:

11111010001111100110000 1

Длина двоичной последовательности: L = 24.

Для кодирования по три символа:

111001000111010100011

Длина двоичной последовательности: L = 21.

Для источника с памятью

1. Построим двоичные неравномерные эффективные коды для кодирования слов длиной в два символа, предварительно рассчитав вероятности их появления.

P(A) = 0,604

P(B) = 0,175

P(D) = 0,220

P(AA) = P(A)*P (A/A) = 0,604*0,809 = 0,4886

P(AB) = P(A)*P (B/A) = 0,604*0,039 = 0,0236

P(AD) = P(A)*P (D/A) = 0,604*0,152 = 0,0918

P(BA) = P(B)*P (A/B) = 0,175*0,375 = 0,0656

P(BB) = P(B)*P (B/B) = 0,175*0,534 = 0,0935

P(BD) = P(B)*P (D/B) = 0,175*0,091 = 0,0159

P(DA) = P(D)*P (A/D) = 0,220*0,226 = 0,0497

P(DB) = P(D)*P (B/D) = 0,220*0,262 = 0,0576

P(DD) = P(D)*P (D/D) = 0,220*0,512 = 0,1126

Неравномерные двоичные эффективные коды построим по методике Хаффмена.

Слово	Вероятность	КК	Длина КК	
AA	0,4886	1	1	

AB	0,0236	011011	6	
AD	0,0918	0111	4	
BA	0,0656	0101	4	
BB	0,0935	001	3	
BD	0,0159	011010	6	
DA	0,0497	01100	5	
DB	0,0576	0100	4	
DD	0,1126	000	3	

2. Разработаем марковские процедуры для кодирования слов по одному символу:
Для состояния A:
P (A/A) = 0,809
P (B/A) = 0,039
P (D/A) = 0,152

Символ, что ожидается	Условная вероятность	КК	Длина КК	
A	0,809	1	1	
B	0,039	01	2	
D	0,152	00	2	

Для состояния B:
P (A/B) = 0,375
P (B/B) = 0,534
P (D/B) = 0,091

Символ, что ожидается	Условная вероятность	КК	Длина КК	
A	0,375	11	2	
B	0,534	0	1	
D	0,091	10	2	

Для состояния D:
P (A/D) = 0,226
P (B/D) = 0,262
P (D/D) = 0,512

Символ, что ожидается	Условная вероятность	КК	Длина КК	

A	0,226	11	2	
B	0,262	10	2	
D	0,512	0	1	

Разработаем марковские процедуры для кодирования слов по два символа:
двоичный неравномерный код марковский
Для состояния A:
P (AA/A) = P (A/A)*P (A/A) = 0,809*0,809 = 0,6545
P (AB/A) = P (A/A)*P (B/A) = 0,809*0,039 = 0,0316
P (AD/A) = P (A/A)*P (D/A) = 0,809*0,152 = 0,1230
P (BA/A) = P (B/A)*P (A/B) = 0,039*0,375 = 0,0146
P (BB/A) = P (B/A)*P (B/B) = 0,039*0,534 = 0,0208
P (BD/A) = P (B/A)*P (D/B) = 0,039*0,091 = 0,0035
P (DA/A) = P (D/A)*P (A/D) = 0,152*0,226 = 0,0343
P (DB/A) = P (D/A)*P (B/D) = 0,152*0,262 = 0,0398
P (DD/A) = P (D/A)*P (D/D) = 0,152*0,512 = 0,0778

Слово	Вероятность	КК	Длина КК	
AA	0,6545	1	1	
AB	0,0316	0111	4	
AD	0,1230	001	3	
BA	0,0146	000111	6	
BB	0,0208	00010	5	
BD	0,0035	000110	6	
DA	0,0343	0110	4	
DB	0,0398	0000	4	
DD	0,0778	010	3	

Для состояния B:
P (AA/B) = P (A/B)*P (A/A) = 0,375*0,809 = 0,3034
P (AB/B) = P (A/B)*P (B/A) = 0,375*0,039 = 0,0146
P (AD/B) = P (A/B)*P (D/A) = 0,375*0,152 = 0,0570
P (BA/B) = P (B/B)*P (A/B) = 0,534*0,375 = 0,2003
P (BB/B) = P (B/B)*P (B/B) = 0,534*0,534 = 0,2852
P (BD/B) = P (B/B)*P (D/B) = 0,534*0,091 = 0,0486
P (DA/B) = P (D/B)*P (A/D) = 0,091*0,226 = 0,0206
P (DB/B) = P (D/B)*P (B/D) = 0,091*0,262 = 0,0238
P (DD/B) = P (D/B)*P (D/D) = 0,091*0,512 = 0,0466

Слово	Вероятность	КК	Длина КК	

AA	0,3034	11	2	
AB	0,0146	001011	6	
AD	0,0570	0011	4	
BA	0,2003	01	2	
BB	0,2852	10	2	
BD	0,0486	0001	4	
DA	0,0206	001010	6	
DB	0,0238	00100	5	
DD	0,0466	0000	4	

Для состояния D:
P (AA/D) = P (A/D)*P (A/A) = 0,226*0,809 = 0,1828
P (AB/D) = P (A/D)*P (B/A) = 0,226*0,039 = 0,0088
P (AD/D) = P (A/D)*P (D/A) = 0,226*0,152 = 0,0344
P (BA/D) = P (B/D)*P (A/B) = 0,262*0,375 = 0,0983
P (BB/D) = P (B/D)*P (B/B) = 0,262*0,534 = 0,1399
P (BD/D) = P (B/D)*P (D/B) = 0,262*0,091 = 0,0238
P (DA/D) = P (D/D)*P (A/D) = 0,512*0,226 = 0,1157
P (DB/D) = P (D/D)*P (B/D) = 0,512*0,262 = 0,1341
P (DD/D) = P (D/D)*P (D/D) = 0,512*0,512 = 0,2621

Слово	Вероятность	КК	Длина КК	
AA	0,1828	11	2	
AB	0,0088	011111	6	
AD	0,0344	01110	5	
BA	0,0983	0110	4	
BB	0,1399	010	3	
BD	0,0238	011110	6	
DA	0,1157	101	3	
DB	0,1341	100	3	
DD	0,2621	00	2	

3. Сравним между собой разработанные коды и оценим их эффективность.
Для кодирования по одному символу:
Для кодирования по два символа:

4. Разработанными кодами и процедурами закодируем фрагмент текста:
AAAAAAAAAAAAAAAAAADBBAAAAAAAA
При кодировании кодами по два символа:
11111111101110011111
Длина кодовой комбинации: L = 20
Кодирование процедурами будем выполнять в порядке справа налево, считая, что перед появлением первого символа на выходе источника был символ А.
При кодировании процедурами по одному символу:
1111111101010111111111111111111111
Длина кодовой комбинации: L = 33
При кодировании процедурами по два символа:
111100010001010111111111
Длина кодовой комбинации: L = 24

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

3.1 Понятие информации. Модели детерминированных и случайных сигналов. Преобразование непрерывных сигналов в дискретные

Соотношение между длительностью сигналов и шириной их спектров. Спектральная плотность мощности. Квантование сигналов.

. Анализируя спектр одиночного прямоугольного импульса (см. рис. 1.10), можно установить, что при увеличении его длительности τ от 0 до ∞ спектр сокращается от безграничного (у дельта-функции) до одной спектральной линии в начале координат, соответствующей постоянному значению сигнала. Это свойство сокращения ширины спектра сигнала при увеличении его длительности и наоборот справедливо для сигналов любой формы. Оно вытекает непосредственно из особенностей прямого и обратного интегрального преобразования Фурье, у которых показатель степени экспоненциальной функции в подынтегральных выражениях имеет переменные t и ω в виде произведения.

Рассмотрим функцию u(t) определенной продолжительности и функцию u(λ t), длительность которой при $\lambda>1$ будет в λ раз меньше. Считая, что u(t) имеет спектральную характеристику S(jω), найдем соответствующую характеристику S λ (jω) для u(λ t):

$$S_\lambda(j\omega) = \int_{-\infty}^{\infty} u(\lambda t)\mathrm{e}^{-j\omega t}dt =$$

$$= \frac{1}{\lambda}\int_{-\infty}^{\infty} u(t')\mathrm{e}^{-j\frac{\omega t'}{\lambda}}dt' = \frac{1}{\lambda}S\left(j\frac{\omega}{\lambda}\right),$$

где $t' = \lambda t$.

Следовательно, спектр укороченного в λ раз сигнала ровно в λ раз шире. Коэффициент $1/\lambda$ перед S(jω/λ) изменяет только амплитуду гармонических составляющих

и на ширину спектра не влияет.

Другой важный вывод, также являющийся прямым следствием Фурье-преобразования, заключается в том, что длительность сигнала и ширина его спектра не могут быть одновременно ограничены конечными интервалами: если длительность сигнала ограничена, то спектр его неограничен, и, наоборот, сигнал с ограниченным спектром длится бесконечно долго. Справедливо соотношение

$$\Delta t \Delta f = C ,$$

где Δt — длительность импульса; Δf — ширина спектра импульса; С — постоянная величина, зависящая от формы импульса (при ориентировочных оценках обычно принимают С=1).

Реальные сигналы ограничены во времени, генерируются и передаются устройствами, содержащими инерционные элементы (например, емкости и индуктивности в электрических цепях), и поэтому не могут содержать гармонические составляющие сколь угодно высоких частот.

В связи с этим возникает необходимость ввести в рассмотрение модели сигналов, обладающие как конечной длительностью, так и ограниченным спектром. При этом в соответствии с каким-либо критерием дополнительно ограничивается либо ширина спектра, либо длительность сигнала, либо оба параметра одновременно. В качестве такого критерия используется энергетический критерий, согласно которому практическую длительность $T_п$ и практическую ширину спектра $\omega_п$ выбирают так, чтобы в них была сосредоточена подавляющая часть энергии сигнала.

Для сигналов, начинающихся в момент времени t_0 = О, практическая длительность определяется из соотношения

$$\int_0^{T_п} |u(t)|^2 dt = \eta \int_0^{\infty} |u(t)|^2 dt ,$$

где η — коэффициент, достаточно близкий к 1 (от 0,9 до 0,99 в зависимости от требований к качеству воспроизведения сигнала).

Принимая во внимание равенство Парсеваля (1.56), для практической ширины спектра сигнала соответственно имеем

$$\frac{1}{\pi}\int_0^{\omega_п} |S(\omega)|^2 d\omega = \frac{\eta}{\pi}\int_0^{\infty} |S(\omega)|^2 d\omega .$$

3.2 Меры неопределенности дискретных множеств и непрерывных случайных величин. Количество информации как мера снятой неопределенности

Условная энтропия и её свойства. Распределения, обладающие максимальной дифференциальной энтропией. Избыточность сообщений.

. При оценке неопределенности выбора часто необходимо учитывать статистические связи, которые в большинстве случаев имеют место как между состояниями двух или нескольких источников, объединенных в рамках одной системы, так и между состояниями, последовательно выбираемыми одним источником.

Определим энтропию объединения двух статистически связанных ансамблей U и V. Объединение ансамблей характеризуется матрицей p(UV) вероятностей $p(u_i\upsilon_i)$ всех возможных комбинаций состояний $u_i(1\leq i \leq N)$ ансамбля U и состояний $\upsilon_j(1 \leq j \leq k)$ ансамбля V:

$$p(U,\ V) = \left\| \begin{array}{c} p(u_1v_1)\ldots p(u_iv_1)\ldots p(u_Nv_1) \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ p(u_1v_j)\ldots p(u_iv_j)\ldots p(u_Nv_j) \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ p(u_1v_k)\ldots p(u_iv_k)\ldots p(u_Nv_k) \end{array} \right\|.$$

Суммируя столбцы и строки матрицы (3.14), получим информацию об ансамблях U и V исходных источников u и υ:

$$U = \left| \begin{array}{c} u_1\ldots \quad u_i\ldots \quad u_N \\ p(u_1)\ldots p(u_i)\ldots p(u_N) \end{array} \right|,\ V = \left| \begin{array}{c} v_1\ldots \quad v_j\ldots \quad v_k \\ p(v_1)\ldots p(v_j)\ldots p(v_k) \end{array} \right|.$$

Вероятности $p(u_i\upsilon_i)$ совместной реализации взаимозависимых состояний и, и ν·, можно выразить через условные вероятности $p(u_i/\upsilon_i)$ или $p(\upsilon_j/u_i)$ в соответствии с тем, какие состояния принять за причину, а какие — за следствие:

$$p(u_iv_j) = p(u_i)p(v_j/u_i) = p(v_j)p(u_i/v_j),$$

где $p(u_i/\upsilon_j)$ — вероятность реализации состояний u_i ансамбля U при условии, что реализовалось состояние υ_j ансамбля V; $P(\upsilon_j/u_i)$ — вероятность реализации состояния υ_j ансамбля V при условии, что реализовалось состояние u_i ансамбля U. Тогда выражение (3.11) для энтропии объединения принимает вид

$$H(U,\ V) = -\sum_{i=1}^{N}\sum_{j=1}^{k} p(u_i)p(v_j/u_i)\log p(u_i)\times$$

$$\times p(v_j/u_i) = -\sum_{i=1}^{N} p(u_i)\log p(u_i) - \sum_{i=1}^{N} p(u_i)\times$$

$$\times \sum_{j=1}^{k} p(v_j/u_i)\log (v_j/u_i).$$

Сумма

$$-\sum_{j=1}^{k} p(v_j/u_i)\log p(v_j/u_i)$$

представляет собой случайную величину, характеризующую неопределенность, приходящуюся на одно состояние ансамбля V при условии, что реализовалось конкретное состояние u_i ансамбля U.

Назовем ее частной условной энтропией ансамбля V и обозначим $H_{ui}(V)$:

$$H_{u_i}(V) = -\sum_{j=1}^{k} p(v_j/u_i)\log(v_j/u_i).$$

При усреднении по всем состояниям ансамбля U получаем среднюю неопределенность, приходящуюся на одно состояние ансамбля V при известных состояниях ансамбля U:

$$H_U(V) = \sum_{i=1}^{N} p(u_i)H_{u_i}(V),$$

или

$$H_U(V) = -\sum_{i=1}^{N} p(u_i)\sum_{j=1}^{k} p(v_j/u_i)\log p(v_j/u_i).$$

Величину $H_U(V)$ называют полной условной или просто условной энтропией ансамбля V по отношению к ансамблю U.

Подставляя (3.19) в (3.16), получаем

$$H(UV) = H(U) + H_U(V).$$

Выражая в (3.11) $p(u_i\upsilon_j)$ через другую условную вероятность в соответствии с (3.15), найдем

$$H(UV) = H(V) + H_V(U),$$

где

$$H_V(U) = \sum_{j=1}^{k} p(v_j)H_{v_j}(U)$$

и

$$H_{v_j}(U) = -\sum_{i=1}^{N} p(u_i/v_j)\log p(u_i/v_j).$$

Таким образом, энтропия объединения двух статистически связанных ансамблей U и V равна безусловной энтропии одного ансамбля плюс условная энтропия другого относительно первого.

Распространяя правило (3.19) на объединение любого числа зависимых ансамблей, получим

$$H(UVZ...W) = H(U) + H_U(V) + H_{UV}(Z) + ... + H_{UVZ}(W).$$

Покажем теперь, что в объединении ансамблей условная энтропия любого ансамбля всегда меньше или равна безусловной энтропии того же ансамбля.

Для объединения двух ансамблей U и V данное утверждение принимает вид соотношений

$$H_U(V) \leqslant H(V),$$
$$H_V(U) \leqslant H(U).$$

Из (3.20) и (3.25) следует, что объединение двух произвольных ансамблей удовлетворяет соотношению

$$H(UV) \leqslant H(U) + H(V).$$

Для объединения нескольких произвольных ансамблей соответственно имеем

$$H(UVZ...W) \leqslant H(U) + H(V) + H(Z) + ... + H(W).$$

Действительно, наличие сведений о результатах реализации состояний одного ансамбля никак не может увеличить неопределенность выбора состояния из другого ансамбля. Эта неопределенность может только уменьшиться, если существует взаимосвязь в реализациях состояний из обоих ансамблей.

В случае отсутствия статистической связи в реализациях состояний u_i, из ансамбля U и υ_j из ансамбля V сведения о результатах выбора состояний из одного ансамбля не снижают неопределенности выбора состояний из другого ансамбля, что находит отражение в равенствах

$$H_U(V) = H(V),\ H_V(U) = H(U).$$

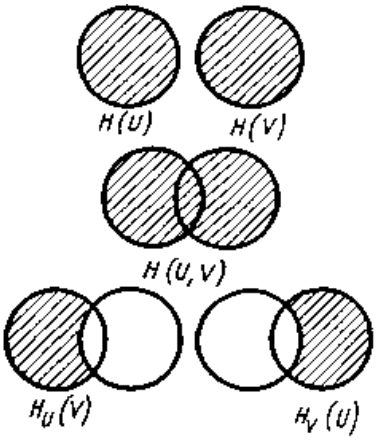


Рис. 3.2

Если имеет место однозначная связь в реализациях состояний $u_i (1 \leq i \leq N)$ из ансамбля U и $\upsilon_j (1 \leq j \leq N)$ из ансамбля V, то условная энтропия любого из ансамблей равна нулю:

$$H_U(V) = 0,\ H_V(U) = 0.$$

Действительно, условные вероятности $p(u_i/\upsilon_j)$ и $P(\upsilon_j/u_i)$ в этом случае принимают значения, равные нулю или единице. Поэтому все слагаемые, входящие в выражения (3.17) и (3.23) для частных условных энтропии, равны нулю. Тогда в соответствии с (3.18) и (3.22) условные энтропии также равны нулю.

Равенства (3.30) отражают факт отсутствия дополнительной неопределенности при выборе событий из второго ансамбля.

Уяснению соотношений между рассмотренными энтропиями дискретных

источников информации (ансамблей) способствует их графическое отображение (рис. 3.2).

Пример 3.4. Определить энтропии H(U), H(V), H_v(U), H(UV), если задана матрица вероятностей состояний системы, объединяющей источники u и v:

$$p(v, u) = \begin{Vmatrix} 0{,}4 & 0{,}1 & 0 \\ 0 & 0{,}2 & 0{,}1 \\ 0 & 0 & 0{,}2 \end{Vmatrix}$$

Вычисляем безусловные вероятности состояний каждой системы как суммы совместных вероятностей по строкам и столбцам заданной матрицы:

$$p(v, u) = \left\| \begin{array}{ccc|c} 0{,}4 & 0{,}1 & 0 & 0{,}5 \\ 0 & 0{,}2 & 0{,}1 & 0{,}3 \\ 0 & 0 & 0{,}2 & 0{,}2 \\ \hline p(v_i) & 0{,}4 & 0{,}3 & 0{,}3 \end{array} \right\| \quad p(u_i)$$

$$H(U) = -\sum_i p(u_i) \log p(u_i) = -(0{,}5 \log_2 0{,}5 + 0{,}3 \log_2 0{,}3 + 0{,}2 \log 0{,}2) = 1{,}485 \text{ дв. ед.};$$

$$H(V) = -\sum_i p(v_i) \log p(v_i) = -(0{,}4 \log_2 0{,}4 + 0{,}3 \log_2 0{,}3 + 0{,}3 \log 0{,}3) = 1{,}57 \text{ дв. ед.}$$

Определяем условные вероятности

$$p(u_i/v_j) = \frac{p(u_i v_j)}{p(v_j)}$$

$$p(u_1/v_1) = 0{,}4/0{,}4 = 1;$$

$$p(u_1/v_2) = p(u_2/v_3) = 0{,}1/0{,}3 = 0{,}33;$$

$$p(u_2/v_2) = p(u_3/v_3) = 0{,}2/0{,}3 = 0{,}67;$$

$$p(u_1/v_3) = p(u_2/v_1) = p(u_3/v_1) = p(u_3/v_2) = 0;$$

$$H_V(U) = -\sum_i \sum_j p(v_j) p(u_i/v_j) \log p(u_i/v_j) =$$

$$= -[0{,}4(1 \cdot \log_2 1) + 0{,}3(0{,}33 \log_2 0{,}33 + 0{,}67 \log_2 0{,}67) + 0{,}3(0{,}33 \log 0{,}33 + 0{,}67 \log 0{,}67)] \approx 0{,}55 \text{ дв. ед.};$$

$$H(U,V) = -\sum_i \sum_j p(u_i v_j) \log p(u_i v_j) = -(0{,}4 \log 0{,}4 + 0{,}1 \log 0{,}1 + 0{,}2 \log 0{,}2 + 0{,}1 \log 0{,}1 + 0{,}2 \log 0{,}2) =$$

$$0.529 + 0{,}332 + 0{,}464 + 0{,}332 + 0{,}464 = 2{,}12 \text{ дв. ед.}$$

Проверим результаты по формуле

$$H(U,V) = H(V) + H_V(U) = 1{,}57 + 0{,}55 = 2{,}12 \text{ дв. ед.}$$

3.3 Оценка информационных характеристик источников сообщений

Эпсилон- производительность источника непрерывных сообщений.

Под конкретным непрерывным сообщением z_T(t) подразумевают некоторую реализацию случайного процесса длительностью Т. Источник непрерывных сообщений характеризуется ансамблем его реализаций. Наиболее плодотворной оказалась модель непрерывного сообщения в

виде эргодического случайного процесса.

Для определения производительности источника непрерывных сообщений воспользуемся подходом и результатами § 3.7, где определена ε-энтропия случайной величины.

Под *ε-производительностью источника непрерывных сообщений* $H_\varepsilon(z)$ понимают минимальное количество информации, которое необходимо создать источнику в единицу времени, чтобы любую реализацию $z_T(t)$ можно было воспроизвести с заданной вероятностью ε.

Допустим, что $z_T(t)$ воспроизводится реализацией $u_T(t)$. Наблюдаемые реализации следует рассматривать, как сигналы, обладающие ограниченным, хотя возможно и достаточно широким спектром F [28, 8].

При достаточно большой длительности T как $z_T(t)$, так и $u_T(t)$ могут быть представлены N-мерными (N = 2FT) векторами $(z_1, z_2, ..., z_N)$ и $(u_1, u_2, ..., u_N)$, координатами которых являются отсчеты. Ансамбли сообщений $\{z_T(t)\}$ и воспроизводящих сигналов $\{u_T(t)\}$ характеризуют при этом N-мерными случайными векторами Z и U, составляющими которых являются соответственно случайные величины $Z_1, Z_2, .., Z_N$ и $U_1, U_2, .., U_N$. Статистическое описание каждого из ансамблей задается N-мерными плотностями распределения вероятностей $\rho(Z) = \rho(z_1, z_2, ..., z_N)$ и $p(U) = p(u_1, u_2, ..., u_N)$. Связь между ансамблями отражают условные плотности распределений $p_u(Z) = \rho(z_1, z_2, ..., z_N / u_1, u_2, ..., u_N)$ и $p_z(U) = p(u_1, u_2, ..., u_N / z_1, z_2, ..., z_N)$, а также совместная плотность распределения вероятностей $p(Z,U) = p(z_1, z_2, ..., z_N; u_1, u_2, ..., u_N)$.

Распространяя формулу (4.20) на N-мерные случайные векторы Z и U для количества информации одного из них относительно второго, получим

$$I(\mathbf{Z},\mathbf{U}) = \iint_{\mathbf{ZU}} p(\mathbf{Z},\mathbf{U}) \log \frac{p(\mathbf{Z},\mathbf{U})}{p(\mathbf{Z})p(\mathbf{U})} d\mathbf{Z}d\mathbf{U},$$

где интегралы являются N-мерными.

Используем, как и ранее, среднеквадратический критерий верности $\theta(Z,U)$, который в рассматриваемом случае имеет вид

$$\theta(\mathbf{Z},\mathbf{U}) = \int_{\mathbf{Z}} \int_{\mathbf{U}} p(\mathbf{Z}) p_{\mathbf{Z}}(\mathbf{U}) \rho(\mathbf{Z},\mathbf{U}) d\mathbf{Z}d\mathbf{U},$$

где $p(Z,U)ZU$ представляет собой квадрат расстояния $l(Z,U)$ в N-мерном евклидовом пространстве.

Количество информации, приходящееся в среднем на один отсчет дискретизованных сигналов $Z_T(t)$ и $U_T(t)$, определяется выражением

$$I(\mathbf{Z},\mathbf{U}) = \frac{1}{N} \int_{\mathbf{Z}} \int_{\mathbf{U}} p(\mathbf{Z},\mathbf{U}) \log \frac{p(\mathbf{ZU})}{p(\mathbf{Z})p(\mathbf{U})} d\mathbf{Z}d\mathbf{U}.$$

Тогда в соответствии с определением для ε-пропорциональности источника непрерывных сообщений $H_\varepsilon(Z)$ запишем

$$H_\varepsilon(\mathbf{Z}) = \nu \min_{\{p_{\mathbf{Z}}(\mathbf{U})\}} \bar{I}(\mathbf{Z},\mathbf{U})$$

при выполнении условия

$$\theta(\mathbf{Z},\mathbf{U}) \leqslant \varepsilon^2.$$

Величина v характеризует скорость формирования источником отсчетов (v = =2F).

Пример 4.5. Определить ε-производительность источника, формирующего со скоростью ν_1 некоррелированные отсчеты стационарного нормального случайного сигнала с дисперсией σ^2.

Воспользовавшись полученным в (3.65) значением ε-энтропии для нормально распределенной случайной величины, найдем

$$\overline{H_\varepsilon(\mathbf{Z})} = \nu_1 H_\varepsilon(Z) = \frac{\nu_1}{2} \log_2 \frac{\sigma^2}{\varepsilon^2} \ \frac{\text{дв ед}}{\text{с}}.$$

Возможности воспроизведения любого сообщения $z_T(t)$ с заданной верностью можно дать геометрическое толкование. Поскольку все реализации эргодического процесса достаточно большой длительности являются типичными и обладают практически одной и той же средней мощностью, концы соответствующих им векторов в N-мерном пространстве сообщений составляют непрерывное множество точек, равноудаленных от начала координат (гиперсферу).

Конечное подмножество воспроизводящих сигналов $U_T(t)$ размещается в центрах непересекающихся правильных сферических N-угольников (ε-областей), на которое гиперсфера разбивается без промежутков. Размеры ε-областей определены заданной верностью воспроизведения сообщений. Если источником реализуется сообщение $z^*_T(t)$, конец вектора которого должен попасть в ε-область сигнала $u^*_T(t)$, то воспроизводится сигнал $u^*_T(t)$.

Следует отметить, что заданная верность воспроизведения будет достигнута с вероятностью, близкой к единице, только при достаточно большой длительности сообщений, когда погрешностью от замены непрерывных реализаций последовательностями отсчетов можно будет пренебречь. Для уменьшения указанной погрешности при ограниченной длительности сообщений T необходимо увеличивать число отсчетов N. В пределе при $N \to \infty$ получим непрерывные реализации.

В вычислении ε - производительности источника и геометрическом толковании возможности воспроизведения сообщений с заданной верностью принципиально ничего не изменяется. Следует лишь учесть, что N-мерное евклидово пространство сообщений становится гильбертовым и мерой близости двух сигналов должно быть расстояние в этом пространстве.

3.4 Информационные характеристики каналов связи

Согласование физических характеристик сигнала и канала.

Конкретный канал связи обладает определенными физическими параметрами, от которых зависит возможность передачи по нему тех или иных сигналов. Независимо от назначения непрерывного канала его можно характеризовать тремя основными параметрами: временем, в течение которого он предоставляется для передачи сигнала $T_к$, шириной полосы пропускания сигнала F_K и допустимым превышением сигнала над помехой в канале $H_к$. Превышение $H_к$

характеризуется разностью максимально допустимого сигнала в канале $P_{u\,max}$ и уровня помех P_{ξ} (в логарифмическом масштабе). Для проводных каналов превышение в основном определяется пробивным напряжением и уровнем перекрестных помех, для радиоканалов — возможностями выявления сигнала на соответствующих расстояниях.

Произведение указанных основных параметров канала связи принято называть объемом (емкостью) канала и обозначать V_K:

$$V_к = T_к F_к H_к .$$

При оценке возможностей передачи сигнала по каналу с заданными физическими характеристиками также ограничиваются рассмотрением трех основных параметров сигнала: его длительности T_c, ширины спектра F_c и превышения над помехой H_c, причем

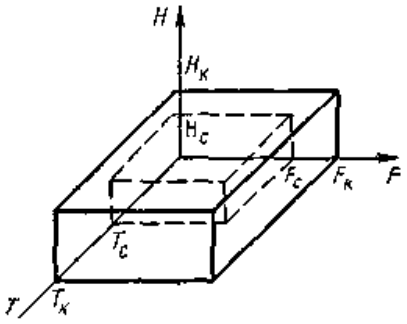
$$H_c = \log (P_u / P_{\xi}) ,$$

где P_u — средняя мощность передаваемого сигнала; P_{ξ} — средняя мощность помехи в канале.

Превышение H_c связано с возможностями передатчика и дальностью передачи. Чем больше H_c, тем меньше вероятность ошибочного приема. Аналогично объему канала вводится понятие объема (емкости) V_c передаваемого сигнала:

$$V_c = T_c F_c H_c .$$

Как объем сигнала, так и объем канала могут быть представлены в трехмерном пространстве с соответствующими координатами T, F, H (рис. 4.8).



Необходимым условием принципиальной возможности неискаженной передачи сигнала по данному каналу является выполнение соотношения

$$V_c \leqslant V_к .$$

При этом, однако, могут потребоваться преобразования для обеспечения достаточных условий передачи, а именно:

$$T_c \leqslant T_к, \; F_c \leqslant F_к, \; H_c \leqslant H_к .$$

Когда канал имеет меньшую полосу пропускания, чем практическая ширина спектра, подлежащего передаче сигнала, последнюю можно уменьшить за счет увеличения длительности сигнала. Объем сигнала при этом сохраняется неизменным. Практически такое преобразование можно осуществить, например, посредством записи сигнала на магнитную ленту с высокой скоростью и последующего воспроизведения со скоростью, при которой ширина его спектра равна полосе пропускания канала.

Если, наоборот, широкополосный канал предоставляется на время меньшее длительности сигнала, то согласование осуществляется за счет расширения спектра сигнала. Для реализации также может использоваться накопитель на магнитной ленте, однако в данном случае скорость воспроизведения должна быть выше скорости записи.

При низком допустимом уровне превышения сигнала в канале преобразование

заключается в уменьшении уровня превышения передаваемого сигнала с одновременным увеличением его длительности путем многократного повторения передачи. Возможны и другие виды преобразования.

Рассмотрим, какова связь между объемом канала и количеством информации, которое можно получить о передаваемом по этому каналу сигнале.

В соответствии с выражением (4.37) предельное количество информации, которое может быть передано по каналу связи за время $T_к$,

$$I_{max}(V,U) = T_к F_к \log(1 + P_и/P_ξ).$$

Отсюда следует, что если $P_и/P_ξ >> 1$, то при условии обеспечения посредством преобразования сигнала полного использования физических возможностей канала максимальное количество информации, которое можно получить о сигнале, близко к емкости канала:

$$I_{max}(V,U) = V_к = T_к F_к \log(P_{и\,max}/P_ξ).$$

3.5 Эффективное кодирование. Введение в теорию помехоустойчивого кодирования

Недостатки системы эффективного кодирования. Математическое введение к линейным кодам.

Недостатки системы эффективного кодирования. Причиной одного из недостатков является различие в длине кодовых комбинаций. Если моменты снятия информации с источника неуправляемы (например, при непрерывном съеме информации с запоминающего устройства на магнитной ленте), кодирующее устройство через равные промежутки времени выдает комбинации различной длины. Так как линия связи используется эффективно только в том случае, когда символы поступают в нее с постоянной скоростью, то на выходе кодирующего устройства должно быть предусмотрено буферное устройство («упругая» задержка). Оно запасает символы по мере поступления и выдает их в линию связи с постоянной скоростью. Аналогичное устройство необходимо и на приемной стороне.

Второй недостаток связан с возникновением задержки в передаче информации.

Наибольший эффект достигается при кодировании длинными блоками, а это приводит к необходимости накапливать знаки, прежде чем поставить им в соответствие определенную последовательность символов. При декодировании задержка возникает снова. Общее время задержки может быть велико, особенно при появлении блока, вероятность которого мала. Это следует учитывать при выборе длины кодируемого блока.

Еще один недостаток заключается в специфическом влиянии помех на достоверность приема. Одиночная ошибка может перевести передаваемую кодовую комбинацию в другую, не равную ей по длительности. Это повлечет за собой неправильное декодирование ряда последующих комбинаций, который называют треком ошибки.

Специальными методами построения эффективного кода трек ошибки стараются свести к минимуму

Следует отметить относительную сложность технической реализации систем эффективного кодирования.

Математическое введение к линейным кодам. Основой математического описания линейных кодов является линейная алгебра (теория векторных пространств, теория матриц, теория групп). Кодовые комбинации рассматривают как элементы множества, например кодовые комбинации двоичного кода принадлежат множеству положительных двоичных чисел.

Множества, для которых определены некоторые алгебраические операции, называют *алгебраическими системами*. Под *алгебраической операцией* понимают однозначное сопоставление двум элементам некоторого третьего элемента по определенным правилам. Обычно основную операцию называют сложением (обозначают a + b = c) или умножением (обозначают a·b=c), а обратную ей — вычитанием или делением, даже если эти операции проводятся не над числами и неидентичны соответствующим арифметическим операциям.

Рассмотрим кратко основные алгебраические системы, широко используемые в теории корректирующих кодов.

Группой называют множество элементов, в котором определена одна основная операция и выполняются следующие аксиомы:

1. В результате применения операции к любым двум элементам группы образуется элемент этой же группы (требование замкнутости).

2. Для любых трех элементов группы a, b и c удовлетворяется равенство $(a+b)+c=a+(b+c)$ (если основная операция — сложение) и равенство $a(bc)=(ab)c$ (если основная операция — умножение).

3. В любой группе G_n существует однозначно определенный элемент, удовлетворяющий при всех значениях *a* из G_n условию $a+0=0+a=a$ (если основная операция — сложение) или условию $a\cdot 1=1\cdot a=a$ (если основная операция — умножение).

В первом случае этот элемент называют *нулем* и обозначают символом 0, а во втором — *единицей* и обозначают символом 1.

4. Всякий элемент *a* группы обладает элементом, однозначно определенным уравнением $a+(-a) = -a + a = 0$ (если основная операция сложение) или уравнением $aa^{-1}=a^{-1}a=1$ (если основная операция — умножение).

В первом случае этот элемент называют *противоположным* и обозначают (-*a*), а во втором — *обратным* и обозначают a^{-1}.

Если операция, определенная в группе, коммутативна, т. е. справедливо равенство $a+b=b+a$ (для группы по сложению) или равенство ab = ba (для группы по умножению), то группу называют *коммутативной* или *абелевой*.

Группу, состоящую из конечного числа элементов, называют конечной. Число элементов в группе называют *порядком* группы.

Чтобы рассматриваемое нами множество n-разрядных кодовых комбинаций было конечной группой, при выполнении основной операции число разрядов в результирующей кодовой комбинации не должно увеличиваться. Этому условию удовлетворяет операция символического поразрядного сложения по заданному модулю q (q — простое число), при которой цифры одинаковых разрядов элементов группы складываются обычным порядком, а результатом сложения считается остаток от деления полученного числа на модуль q.

При рассмотрении двоичных кодов используется операция *сложения по модулю 2*. Результатом сложения цифр данного разряда является 0, если сумма единиц в нем четна, и 1, если сумма единиц в нем нечетна, например:

$$\begin{array}{r} 1\ 0\ 1\ 1\ 1\ 0\ 1 \\ \oplus\ 0\ 1\ 1\ 1\ 1\ 0\ 1 \\ \hline 0\ 0\ 0\ 1\ 1\ 1\ 0 \\ \hline 1\ 1\ 0\ 1\ 1\ 1\ 0 \end{array}$$

Выбранная нами операция коммутативна, поэтому рассматриваемые группы будут абелевыми.

Нулевым элементом является комбинация, состоящая из одних нулей. Противоположным элементом при сложении по модулю 2 будет сам заданный элемент. Следовательно, операция вычитания по модулю 2 тождественна операции сложения.

Пример 6.2. Определить, являются ли группами следующие множества кодовых комбинаций:

1) 0001, 0110, 0111, 0011,
2) 0000, 1101, 1110, 0111,
3) 000, 001, 010, 011, 100, 101, 110, 111

Первое множество не является группой, так как не содержит нулевого элемента.

Второе множество не является группой, так как не выполняется условие замкнутости, например сумма по модулю 2 комбинаций 1101 и 1110 дает комбинацию 0011, не принадлежащему исходному множеству.

Третье множество удовлетворяет всем перечисленным условиям и является группой.

Подмножества группы, являющиеся сами по себе группами относительно операции, определенной в группе, называют подгруппами. Например, подмножество трехразрядных кодовых комбинаций: 000, 001, 010, 011 образуют подгруппу указанной в примере группы трехразрядных кодовых комбинаций.

Пусть в абелевой группе G_n задана определенная подгруппа A. Если B — любой не входящий в A элемент из G_n, то суммы (по модулю 2) элементов B с каждым из элементов подгруппы A образуют смежный класс группы G_n по подгруппе A, порождаемый элементом B.

Элемент B, естественно, содержится в этом смежном классе, так как любая подгруппа содержит нулевой элемент. Взяв последовательно некоторые элементы B_j группы, не вошедшие в уже образованные смежные классы, можно разложить всю группу на смежные классы по подгруппе A.

Элементы B_j называют образующими элементами смежных классов подгруппы.

В таблице разложения, иногда называемой *групповой таблицей*, образующие элементы обычно располагают в крайнем левом столбце, причем крайним левым элементом подгруппы является нулевой элемент.

Пример 6.3. Разложим группу трехразрядных двоичных кодовых комбинаций по подгруппе двухразрядных кодовых комбинаций.

Разложение выполняем в соответствии с табл. 6.2.

Таблица 6.2

$A_1 = 0$	A_2	A_3	A_4
000 B_1 100	001 $A_2 + B_1$ 101	010 $A_3 + B_1$ 110	011 $A_4 + B_1$ 111

Пример 6.4. Разложим группу четырехразрядных двоичных кодовых комбинаций по подгруппе двухразрядных кодовых комбинаций.

Существует много вариантов разложения в зависимости от того, какие элементы выбраны в качестве образующих смежных классов. Один из вариантов представлен в табл. 6.3.

Таблица 6.3

$A_1 = 0$ 0000	A_2 0001	A_3 0010	A_4 0011
B_1 0100	$A_2 \oplus B_1$ 0101	$A_3 \oplus B_1$ 0110	$A_4 \oplus B_1$ 0111
B_2 1010	$A_2 \oplus B_2$ 1011	$A_3 \oplus B_2$ 1000	$A_4 \oplus B_2$ 1001
B_3 1100	$A_2 \oplus B_3$ 1101	$A_3 \oplus B_3$ 1110	$A_4 \oplus B_3$ 1111

Кольцом называют множество элементов R, на котором определены две операции (сложения и умножения), такие, что:

1) множество R является коммутативной группой по сложению;

2) произведение элементов $a \in R$ и $b \in R$ есть элемент R (замкнутость по отношению к умножению);

3) для любых трех элементов a, b и c из R справедливо равенство a(bc) = (ab)c (ассоциативный закон для умножения);

4) для любых трех элементов a, b и c из R выполняются соотношения a(b+c) = =ab+ac и (b+c)a = ba+ca (дистрибутивные законы).

Если для любых двух элементов кольца справедливо соотношение ab = ba, кольцо называют *коммутативным*. Кольцо может не иметь единичного элемента по умножению и обратных элементов.

Примером кольца может служить множество действительных четных целых чисел относительно обычных операций сложения и умножения.

Полем F называют множество по крайней мере двух элементов, в котором определены две операции — сложение и умножение, и выполняются следующие аксиомы:

1) множество элементов образует коммутативную группу по сложению;

2) множество ненулевых элементов образует коммутативную группу по умножению;

3) для любых трех элементов множества a, b, c выполняется соотношение (дистрибутивный закон)

$$a(b+c)=ab+ac\,.$$

Поле F является, следовательно, коммутативным кольцом с единичным элементом по умножению, в котором каждый ненулевой элемент обладает обратным элементом. Примером поля может служить множество всех действительных чисел.

Поле GF(P), состоящее из конечного числа элементов P, называют *конечным полем* или *полем Галуа*. Для любого числа P, являющегося степенью простого числа q, существует поле, насчитывающее P элементов. Например, совокупность чисел по модулю q, если q — простое число, является полем.

Поле не может содержать менее двух элементов, поскольку в нем должны быть по крайней мере единичный элемент относительно операции сложения (0) и единичный элемент относительно операции умножения (1). Поле, включающее только 0 и 1, обозначим GF (2). Правила сложения и умножения в поле с двумя элементами следующие:

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

Двоичные кодовые комбинации, являющиеся упорядоченными последовательностями из n элементов поля GF (2), рассматриваются в теории кодирования как частный случай последовательностей из n элементов поля GF(P). Такой подход позволяет строить и анализировать коды с основанием, равным степени простого числа.

В общем случае суммой кодовых комбинаций A_j, и A_i называют комбинацию $A_f = A_i+A_j$, в которой любой символ A_k (k=1, 2, ..., n) представляет собой сумму k-х символов исходных комбинаций, причем суммирование производится по правилам поля GF(P). При этом вся совокупность n-разрядных кодовых комбинаций оказывается абелевой группой.

В частном случае, когда основанием кода является простое число q, правило сложения в поле GF(q) совпадает с правилом сложения по заданному модулю q.

Линейный код как подпространство линейного векторного пространства. В рассмотренных алгебраических системах (группа, кольцо, поле) операции относились к одному классу математических объектов (элементов). Такие операции называют *внутренними законами*

композиции элементов.

В теории кодирования широко используются модели, охватывающие два класса математических объектов (например, L и Ω). Помимо внутренних законов композиции в них задаются внешние законы композиции элементов, по которым любым элементам $\omega \in \Omega$ и $a \in L$ ставится в соответствие элемент $c \in L$.

Линейным векторным пространством над полем элементов F (скаляров) называют множество элементов V (векторов), если для него выполняются следующие аксиомы:

1) множество V является коммутативной группой относительно операции сложения;

2) для любого вектора ν из V и любого скаляра c из F определено произведение c*v*, которое содержится в V (замкнутость по отношению умножения на скаляр);

3) если u и ν из V векторы, а c и d из F скаляры, то справедливо $c(\mathbf{c}+\mathbf{v}) = c\mathbf{u} + c\mathbf{v}, \ (c+d)\mathbf{v} = c\mathbf{v} + d\mathbf{v}$ (дистрибутивные законы);

4) если ν — вектор, а c и d — скаляры, то (cd)v = c(dv) и 1 · ν = ν (ассоциативный закон для умножения на скаляр).

Выше было определено правило поразрядного сложения кодовых комбинаций, при котором вся их совокупность образует абелеву группу. Определим теперь операцию умножения последовательности из n элементов поля GF(P) (кодовой комбинации) на элемент поля a_i из GF(P) аналогично правилу умножения вектора на скаляр:

$$a_i(a_1, a_2, \ldots, a_n) = (a_i a_1, a_i a_2, \ldots, a_i a_n)$$

[умножение элементов производится по правилам поля GF(P)].

Поскольку при выбранных операциях дистрибутивные законы и ассоциативный закон (п. 3, 4) выполняются, все множество n-разрядных кодовых комбинаций можно рассматривать как векторное линейное пространство над полем GF(P), а кодовые комбинации — как его векторы.

В частности, при двоичном кодировании векторы состоят из элементов поля GF (2) (т. е. 0 и 1). Сложение проводят поразрядно по модулю 2. При умножении вектора на один элемент поля (1) он не изменяется, а умножение на другой (0) превращает его в единичный элемент векторного пространства, обозначаемый символом 0= (0 0...0).

Если в линейном пространстве последовательностей из n элементов поля GF(P) дополнительно задать операцию умножения векторов, удовлетворяющую определенным условиям (ассоциативности, замкнутости, билинейности по отношению к умножению на скаляры), то вся совокупность n-разрядных кодовых комбинаций превращается в линейную коммутативную алгебру над полем коэффициентов GF(P).

Подмножество элементов векторного пространства, которое удовлетворяет аксиомам векторного пространства, называют *подпространством*.

Линейным кодом называют множество векторов, образующих подпространство векторного пространства всех n-разрядных кодовых комбинаций над полем GF(P).

В случае двоичного кодирования такого подпространство комбинаций над полем GF (2)

образует любая совокупность двоичных кодовых комбинаций, являющаяся подгруппой группы всех n-разрядных двоичных кодовых комбинаций. Поэтому любой двоичный линейный код является групповым.

2.6 Построение групповых кодов. Циклические коды

Определение проверочных равенств и уравнений кодирования. Методы формирования комбинаций и декодирования циклического кода.

. **Определение проверочных равенств.** Итак, для любого кода, имеющего целью исправлять наиболее вероятные векторы ошибок заданного канала связи (взаимно независимые ошибки или пачки ошибок), можно составить таблицу опознавателей одиночных ошибок в каждом из разрядов. Пользуясь этой таблицей, нетрудно определить, символы каких разрядов должны входить в каждую из проверок на четность.

Рассмотрим в качестве примера опознаватели для кодов предназначенных исправлять единичные ошибки (табл. 6.6).

Таблица 6.6

Номер разрядов	Опознаватель	Номер разрядов	Опознаватель	Номер разрядов	Опознаватель
1	0001	7	0111	12	1100
2	0010	8	1000	13	1101
3	0011	9	1001	14	1110
4	0100	10	1010	15	1111
5	0101	11	1011	16	10000
6	0110				

В принципе можно построить код, усекая эту таблицу на любом уровне. Однако из таблицы видно, что оптимальными будут коды (7, 4), (15, 11), где первое число равно n, а второе k, и другие, которые среди кодов, имеющих одно и то же число проверочных символов, допускают наибольшее число информационных символов.

Усечем эту таблицу на седьмом разряде и найдем номера разрядов, символы которых должны войти в каждое из проверочных равенств.

Предположим, что в результате первой проверки на четность для младшего разряда опознавателя будет получена единица. Очевидно, это может быть следствием ошибки в одном из разрядов, опознаватели которых в младшем разряде имеют единицу. Следовательно, первое проверочное равенство должно включать символы 1, 3, 5 и 7-го разрядов;

$$a_1 \oplus a_3 \oplus a_5 \oplus a_7 = 0,$$

Единица во втором разряде опознавателя может быть следствием ошибки в разрядах, опознаватели которых имеют единицу во втором разряде. Отсюда второе проверочное равенство должно иметь вид

$$a_2 \oplus a_3 \oplus a_6 \oplus a_7 = 0.$$

Аналогично находим и третье равенство:

$$a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 0.$$

Чтобы эти равенства при отсутствии ошибок удовлетворялись для любых значений информационных символов в кодовой комбинации, в нашем распоряжении имеется три проверочных разряда. Мы должны так выбрать номера этих разрядов, чтобы каждый из них входил только в одно из равенств. Это обеспечит однозначное определение значений символов в проверочных разрядах при кодировании. Указанному условию удовлетворяют разряды, опознаватели которых имеют по одной единице. В нашем случае это будут первый, второй и четвертый разрядыТаким образом, для кода (7, 4), исправляющего одиночные ошибки, искомые правила построения кода, т. е. соотношения, реализуемые в процессе кодирования, принимают вид:

$$\begin{aligned} a_1 &= a_3 \oplus a_5 \oplus a_7, \\ a_2 &= a_3 \oplus a_6 \oplus a_7, \\ a_4 &= a_5 \oplus a_6 \oplus a_7. \end{aligned}$$

Поскольку построенный код имеет минимальное хэммингово расстояние d_{min} = =3, он в соответствии с (6.15) может использоваться с целью обнаружения единичных и двойных ошибок. Обращаясь к табл. 6.6, легко убедиться, что сумма любых двух опознавателей единичных ошибок дает ненулевой опознаватель, что и является признаком наличия ошибки.

Пример 6.5. Построим групповой код объемом 15 слов, способный исправлять единичные и обнаруживать двойные ошибки.

В соответствии с (6.17) код должен обладать минимальным хэмминговым расстоянием, равным 4. Такой код можно построить в два этапа. Сначала строим код заданного объема, способный исправлять единичные ошибки. Это код Хэмминга (7, 4). Затем добавляем еще один проверочный разряд, который обеспечивает четность числа единиц в разрешенных комбинациях.

Таким образом, получаем код (8, 4). В процессе кодирования реализуются соотношения:

$$\begin{aligned} a_1 &= a_3 \oplus a_5 \oplus a_7, \\ a_2 &= a_3 \oplus a_6 \oplus a_7, \\ a_4 &= a_5 \oplus a_6 \oplus a_7, \\ a_8 &= a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7. \end{aligned}$$

Обозначив синдром кода (7, 4) через S_i, результат общей проверки на четности через $S_2 (S_2 = \sum_{i=1}^{8} a_i)$

и пренебрегая возможностью

$$S_2 (S_2 = \sum_{i=1}^{8} a_i)$$

возникновения ошибок кратности 3 и выше, запишем алгоритм декодирования:

при $S_1 = 0$ и $S_2 = 0$ ошибок нет;

при $S_1 = 0$ и $S_2 = 1$ ошибка в восьмом разряде;

при S_1=0 и S_2 = 0 двойная ошибка (коррекция блокируется, посылается запрос повторной передачи),

при S_1=0 и S_2=1 одиночная ошибка (осуществляется ее исправление).

Пример 6.6. Используя табл. 6.6, составим правила построения кода (8,2), исправляющего все одиночные и двойные ошибки.

Усекая табл. 6.5 на восьмом разряде, найдем следующие проверочные равенства:

$$a_1 \oplus a_5 \oplus a_8 = 0,$$
$$a_2 \oplus a_5 \oplus a_8 = 0,$$
$$a_3 \oplus a_5 = 0,$$
$$a_4 \oplus a_5 = 0,$$
$$a_6 \oplus a_8 = 0,$$
$$a_7 \oplus a_8 = 0.$$

Соответственно правила построения кода выразим соотношениями

$$a_1 = a_5 \oplus a_8 \quad (6\ 26\ а)$$
$$a_2 = a_5 \oplus a_8 \quad (6.26\ б)$$
$$a_3 = a_5 \quad (6.26\ в)$$
$$a_4 = a_5 \quad (6\ 26\ г)$$
$$a_6 = a_8 \quad (6.26\ д)$$
$$a_7 = a_8 \quad (6.26\ е)$$

Отметим, что для построенного кода d_{min}=5, и, следовательно, он может использоваться обнаружения ошибок кратности от 1 до 4.

Соотношения, отражающие процессы кодирования и декодирования двоичных линейных кодов, могут быть реализованы непосредственно с использованием сумматоров по модулю два. Однако декодирующие устройства, построенные таким путем для кодов, предназначенных исправлять многократные ошибки, чрезвычайно громоздки. В этом случае более эффективны другие принципы декодирования.

Мажоритарное декодирование групповых кодов. Для линейных кодов, рассчитанных на исправление многократных ошибок, часто более простыми оказываются декодирующие устройства, построенные по мажоритарному принципу. Это метод декодирования называют также принципом голосования или способом декодирования по большинству проверок. В настоящее время известно значительное число кодов, допускающих мажоритарную схему декодирования, а также сформулированы некоторые подходы при конструировании таких кодов.

Мажоритарное декодирование тоже базируется на системе проверочных равенств. Система последовательно может быть разрешена относительно каждой из независимых переменных, причем в силу избыточности это можно сделать не единственным способом.

Любой символ a_i, выражается d (минимальное кодовое расстояние) различными независимыми способами в виде линейных комбинаций других символов. При этом может использоваться тривиальная проверка $a_i = a_i$. Результаты вычислений подаются на соответствующий этому символу мажоритарный элемент. Последний представляет собой схему, имеющую d входов и один выход, на котором появляется единица, когда возбуждается больше половины его входов, и нуль, когда возбуждается число таких входов меньше половины. Если

ошибки отсутствуют, то проверочные равенства не нарушаются, и на выходе мажоритарного элемента получаем истинное значение символа. Если число проверок d^{2s+1} и появление ошибки кратности s и менее не приводит к нарушению более s проверок, то правильное решение может быть принято по большинству неискаженных проверок. Чтобы указанное условие выполнялось, любой другой символ a_j(j неравно i) не должен входить более чем в одно проверочное равенство. В этом случае мы имеем дело с системой разделенных проверок.

Пример 6.7. Построим систему разделенных проверок для декодирования информационных символов рассмотренного ранее группового кода (8,2).

Поскольку код рассчитан на исправление любых единичных и двойных ошибок, число проверочных равенств для определения каждого символа должно быть не менее 5. Подставив в равенства (6.26 а) и (6.26 б) значения a_8, полученные из равенств (6.26д) и (6.26е), и записав их относительно a_5 совместно с равенствами (6.26 в) и (6.26г) и тривиальным равенством $a_5 = a_5$, получим следующую систему разделенных проверок для символа a_5:

$$a_5 = a_6 \oplus a_1,$$
$$a_5 = a_7 \oplus a_2,$$
$$a_5 = a_3,$$
$$a_5 = a_4,$$
$$a_5 = a_5.$$

Для символа a_8 систему разделенных проверок строим аналогично

$$a_8 = a_3 \oplus a_1,$$
$$a_8 = a_4 \oplus a_2,$$
$$a_8 = a_6,$$
$$a_8 = a_7,$$
$$a_8 = a_8.$$

3.7 Матричные представления в теории кодирования. Кодирование линейными последовательными машинами

Границы для числа разрешенных комбинаций. Образующая матрица АЛПМ

Матрицу, составленную из любой совокупности векторов линейного кода, образующей базис пространства, называют порождающей (образующей) матрицей кода.

Если порождающая матрица содержит k строк по n элементов поля GF(q), то код называют (n, k)-кодом. В каждой комбинации (n, k)-кода k информационных символов и n — k проверочных. Общее число разрешенных кодовых комбинаций (исключая нулевую) Q == qk-1.

Зная порождающую матрицу кода, легко найти разрешенную кодовую комбинацию, соответствующую любой последовательности A_{ki} из k информационных символов. Она получается в результате умножения вектора A_{ki} на порождающую матрицу $M_{n,k}$:

$$\mathbf{A}_{ni} = \mathbf{A}_{ki} \cdot \mathbf{M}_{n,k}.$$

Найдем, например, разрешенную комбинацию кода (8,2), соответствующую информационным символам a_5=1, a_8=1:

$$|1\,1|\mathbf{M}_{8,2} = |1\,1|\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} = 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1.$$

Пространство строк матрицы остается неизменным при выполнении следующих элементарных операций над строками: 1) перестановка любых двух строк; 2) умножение любой строки на ненулевой элемент поля; 3) сложение какой-либо строки с произведением другой строки на ненулевой элемент поля, а также при перестановке столбцов.

Если образующая матрица кода M_2 получена из образующей матрицы кода М1 с помощью элементарных операций над строками, то обе матрицы порождают один и тот же код. Перестановка столбцов образующей матрицы кода приводит к образующей матрице эквивалентного кода. Эквивалентные коды весьма близки по своим свойствам. Корректирующая способность таких кодов одинакова.

Для анализа возможностей линейного (n, k)-кода, а также для упрощения процесса кодирования удобно, чтобы порождающая матрица ($M_{n,k}$) состояла из двух матриц: единичной матрицы размерности kXk и дописываемой справа матрицы-дополнения (контрольной подматрицы) размерности k*(n-k), которая соответствует n — k проверочным разрядам:

$$\mathbf{M}_{n,k} = [\mathbf{I}_k \mathbf{P}_{k\,n-k}] = \begin{bmatrix} 1\ 0\ldots 0 p_{1,k+1} p_{1,k+2}\ldots p_{1,j}\ldots p_{1,n} \\ 0\ 1\ldots 0 p_{2,k+1} p_{2,k+2}\ldots p_{2,j}\ldots p_{2\,n} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0\ldots 1\ldots 0 p_{i,k+1} p_{i,k+2}\ldots p_{i,j}\ldots p_{i\,n} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0\ 0\ldots 1 p_{k,k+1} p_{k,k+2}\ldots p_{k,j}\ldots p_{k\,n} \end{bmatrix}$$

Разрешенные кодовые комбинации кода с такой порождающей матрицей отличаются тем, что первые k символов в них совпадают с исходными информационными, а проверочными оказываются (n — k) последних символов.

Действительно, если умножим вектор-строку $A_{ki} = (a_1\ a_2 \ldots a_i \ldots a_n)$ на матрицу получим

$$\mathbf{M}_{n,k} = [\mathbf{I}_k \mathbf{P}_{k,n-k}],$$

вектор

$$\mathbf{A}_{ni} = (a_1 a_2 \ldots a_i \ \ldots a_k \ldots a_{k+1} \ldots a_j \ldots a_n),$$

где проверочные символы $a_j (k+1 \leqslant j \leqslant n)$ являются линейными комбинациями информационных:

$$a_j = \sum_{i=1}^{k} a_i p_{ij}.$$

Коды, удовлетворяющие этому условию, называют систематическими. Для каждого линейного кода существует эквивалентный систематический код.

Как следует из (6.27), (6.28), информацию о способе построения такого кода содержит матрица-дополнение. Если правила построения кода (уравнения кодирования) известны, то значения символов любой строки матрицы-дополнения получим, применяя эти правила к символам соответствующей строки единичной матрицы.

Пример 6.9. Запишем матрицы I_k, $P_{k,n-k}$ и $M_{n,k}$ для двоичного кода (7,4)

Единичная матрица на четыре разряда имеет вид

$$\mathbf{I}_4 = \begin{bmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{bmatrix}$$

Один из вариантов матрицы дополнения можно записать, используя соотношения (6.25)

$$\mathbf{P}_{4,3} = \begin{bmatrix} 110 \\ 101 \\ 011 \\ 111 \end{bmatrix}$$

Тогда для двоичного кода Хэмминга имеем·

$$\mathbf{M}_{7,4} = \begin{bmatrix} a_3 a_5 a_6 a_7 a_1 a_2 a_4 \\ 1\ 0\ 0\ 0\ 1\ 1\ 0 \\ 0\ 1\ 0\ 0\ 1\ 0\ 1 \\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \\ 0\ 0\ 0\ 1\ 1\ 1\ 1 \end{bmatrix}$$

Запишем также матрицу для систематического кода (7,4)·

$$\mathbf{M}_{7,4} = \begin{bmatrix} a_1 a_2 a_3 a_4 a_5 a_6 a_7 \\ 1\ 0\ 0\ 0\ 1\ 1\ 0 \\ 0\ 1\ 0\ 0\ 1\ 0\ 1 \\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \\ 0\ 0\ 0\ 1\ 1\ 1\ 1 \end{bmatrix}$$

В свою очередь, по заданной матрице-дополнению $P_{k,n-k}$ можно определить равенства, задающие правила построения кода. Единица в первой строке каждого столбца указывает на то, что в образовании соответствующего столбцу проверочного разряда участвовал первый информационный разряд. Единица в следующей строке любого столбца говорит об участии в образовании проверочного разряда второго информационного разряда и т. д.

Так как матрица-дополнение содержит всю информацию о правилах построения кода, то систематический код с заданными свойствами можно синтезировать путем построения соответствующей матрицы-дополнения.

Так как минимальное кодовое расстояние d для линейного кода равно минимальному весу его ненулевых векторов, то в матрицу-дополнение должны быть включены такие k строк, которые удовлетворяли бы следующему общему условию: вектор-строка образующей матрицы, получающаяся при суммировании любых l $(1 \leqslant l \leqslant k)$ строк, должна содержать не менее d-l отличных от нуля символов.

Действительно, при выполнении указанного условия любая разрешенная кодовая комбинация, полученная суммированием l строк образующей матрицы, имеет не менее d ненулевых символов, так как l ненулевых символов она всегда содержит в результате суммирования строк единичной матрицы.

Синтезируем таким путем образующую матрицу двоичного систематического кода (7,4) с минимальным кодовым расстоянием d = 3.

В каждой вектор - строке матрицы - дополнения согласно сформулированному условию

(при l= 1) должно быть не менее двух единиц. Среди трехразрядных векторов таких имеется четыре: 011, 110, 101, 111.

Эти векторы могут быть сопоставлены со строками единичной матрицы в любом порядке. В результате получим матрицы систематических кодов, эквивалентных коду Хэмминга, например:

$$\mathbf{M}_{7,4} = \begin{bmatrix} 1\,0\,0\,0 & 0\,1\,1 \\ 0\,1\,0\,0 & 1\,1\,1 \\ 0\,0\,1\,0 & 1\,0\,1 \\ 0\,0\,0\,1 & 1\,1\,0 \end{bmatrix}$$

Нетрудно убедиться, что при суммировании нескольких строк такой матрицы (l>1) получим вектор-строку, содержащую не менее d = 3 ненулевых символов.

Имея образующую матрицу систематического кода Mn,k = [I_k $P_{k,n-k}$], можно построить так называемую проверочную (контрольную) матрицу H размерности (n---k)Xn:

$$\mathbf{H} = [-\mathbf{P}^T_{k,n-k}\mathbf{I}_{n-k}] = \begin{bmatrix} p_{1,k+1}, p_{2,k+1}\ldots p_{k,k+1} & -1 & 0\ldots 0 \\ p_{1,k+2}, p_{2,k+2}\ldots p_{k,k+2} & 0 & -1\ldots 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & & \\ p_{1,n}\ \ p_{2,n}\ \ \ldots p_{k,n} & 0 & 0\ldots -1 \end{bmatrix}.$$

При умножении неискаженного кодового вектора A_{ni} на матрицу, транспонированную к матрице H, получим вектор, все компоненты которого равны нулю:

$$\mathbf{A}_{ni}\mathbf{H}^T = |a_1 a_2,\ldots,a_k,a_{k+1},\ldots,a_j,\ldots,a_n| \cdot \begin{bmatrix} p_{1,k+1}\ldots p_{1,j}\ldots p_{1,n} \\ p_{2,k+1}\ldots p_{2,j}\ldots p_{2,n} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ p_{k,k+1}\ldots p_{k,j}\ldots p_{k,n} \\ -1\ \ldots\ 0\ \ldots\ 0 \\ 0\ldots -1\ \ldots\ 0 \\ 0\ \ldots\ 0\ldots -1 \end{bmatrix} =$$

$$= |S_{k+1}, S_{k+2}, \ldots, S_j, \ldots, S_n| = |0,0..0..0|.$$

Каждая компонента S, является результатом проверки справедливости соответствующего уравнения декодирования:

$$S_j = \sum_{i=1}^{k} a_i P_{ij} - a_j = 0.$$

В общем случае, когда кодовый вектор A_{ni} = (a_1, a_2,...ai,...,a_k, a_{k+1},...a_j,...,a_n) искажен вектором ошибки $\xi_{ni} = (\xi_1, \xi_2, \ldots, \xi_i, \ldots, \xi_k, \xi_{k+1}, \ldots, \xi_j, \ldots, \xi_n)$, умножение вектора ($A_{ni}$ + ξ_{ni}) на матрицу H^t дает ненулевые компоненты:

$$S_j = \sum_{i=1}^{k} \xi_i P_{ij} - \xi_j.$$

Отсюда видно, что $S_j (k+1 \leqslant j \leqslant n)$ представляют собой символы, зависящие только от вектора ошибки, а вектор S = (S_{k+1}, S_{k+2}, ..., S_j,...S_n) является не чем иным как опознавателем ошибки (синдромом).

Для двоичных кодов (операция сложения тождественна операции вычитания) проверочная матрица имеет вид

$$\mathbf{H} = [\mathbf{P}^{T}_{k,n-k}, \mathbf{I}_{n-k}] = \begin{bmatrix} p_{1,k+1} & p_{2,k+1} \ldots p_{k,k+1} & 1\ 0 \ldots 0 \\ p_{1,k+2} & p_{2,k+2} \ldots p_{k,k+2} & 0\ 1 \ldots 0 \\ p_{1,n} & p_{2,n} \quad\quad p_{k,n} & 0\ 0 \ldots 1 \end{bmatrix}.$$

Пример 6.10. Найдем проверочную матрицу H для кода (7,4) с образующей матрицей M:

$$\mathbf{M}_{7,4} = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,0 \\ 0\,1\,0\,0\,1\,0\,1 \\ 0\,0\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \end{bmatrix}.$$

Определим синдромы в случаях отсутствия и наличия ошибки в кодовом векторе 1100011.

Выполним транспонирование матрицы $P_{4,3}$

$$\mathbf{P}^{T}_{4,3} = \begin{bmatrix} 1\,1\,0\,1 \\ 1\,0\,1\,1 \\ 0\,1\,1\,1 \end{bmatrix}.$$

Запишем проверочную матрицу:

$$\mathbf{H} = \begin{bmatrix} 1\,1\,0\,1\,1\,0\,0 \\ 1\,0\,1\,1\,0\,1\,0 \\ 0\,1\,1\,1\,0\,0\,1 \end{bmatrix}.$$

Умножение на H^t неискаженного кодового вектора 1100011 дает нулевой синдром:

$$[1100011] \begin{bmatrix} 110 \\ 101 \\ 011 \\ 111 \\ 100 \\ 010 \\ 001 \end{bmatrix} = [000]$$

$$[1101011] \begin{bmatrix} 110 \\ 101 \\ 011 \\ 111 \\ 100 \\ 010 \\ 001 \end{bmatrix} = [111]$$

При наличии в кодовом векторе ошибки, например, в 4 м разряде (1101011) получим

Следовательно, вектор-строка 111 в данном коде является опознавателем (синдромом) ошибки в четвертом разряде. Аналогично можно найти и синдромы других ошибок. Множество всех опознавателей идентично множеству опознавателей кода Хэмминга (7,4), но сопоставлены они конкретным векторам ошибок по-иному, в соответствии с образующей матрицей данного (эквивалентного) кода.

3.8 Обнаружение и различение сигналов

Различение сигналов.

Обнаружение и первичное различение сигналов обеспечивается рецепторами, а детектирование и опознание сигналов – нейронами коры больших полушарий. Передачу, преобразование и кодирование сигналов осуществляют нейроны всех слоев сенсорных систем.

Обнаружение сигналов начинается в рецепторе – специализированной клетке, эволюционно приспособленной к восприятию раздражителя определенной модальности из внешней или внутренней среды и преобразованию его из физической или химической формы в форму нервного возбуждения.

Различение сигналов. Важная характеристика сенсорной системы – способность замечать различия в свойствах одновременно или последовательно действующих раздражителей. Различение начинается в рецепторах, но в этом процессе участвуют нейроны всей сенсорной системы. Оно характеризует то минимальное различие между стимулами, которое сенсорная система может заметить (дифференциальный, или разностный, порог).

Передача и преобразование сигналов. Процессы преобразования и передачи сигналов в сенсорной системе доносят до высших центров мозга наиболее важную (существенную) информацию о раздражителе в форме, удобной для его надежного и быстрого анализа.

Кодирование информации. Кодированием называют совершаемое по определенным правилам преобразование информации в условную форму – код.

Детектирование сигналов – это избирательное выделение сенсорным нейроном того или иного признака раздражителя, имеющего поведенческое значение. Такой анализ осуществляют нейроны-детекторы, избирательно реагирующие лишь на определенные параметры стимула.

Опознание образов представляет собой конечную и наиболее сложную операцию сенсорной системы. Она заключается в отнесении образа к тому или иному классу объектов, с которыми ранее встречался организм, то есть в классификации образов. Синтезируя сигналы от нейронов-детекторов, высший отдел сенсорной системы формирует «образ» раздражителя и сравнивает его с множеством образов, хранящихся в памяти. Опознание завершается принятием решения о том, с каким объектом или ситуацией встретился организм. В результате этого происходит восприятие, то есть мы осознаем, чье лицо видим перед собой, кого слышим, какой запах чувствуем.

3.9 Оценка параметров сигналов

Байесовские оценки.

. Наиболее просто задача построения оптимального приемника решается для случая амплитудной телеграфии с пассивной паузой, что соответствует принятию решения о том, что передавался символ 0 (сигнала нет) или символ 1 (сигнал есть).

Предполагается, что помеха в канале представляет собой гауссовский шум с нулевым средним и известной дисперсией, который взаимодействует с сигналом аддитивно (суммируется). Результатом обработки наблюдаемого колебания является случайная величина y, которая может иметь различное распределение в зависимости от того, есть ли сигнал в наблюдаемом колебании, а именно: распределение при гипотезе H_0 – «сигнала нет» – является гауссовским с нулевым средним, а распределение при гипотезе H_1 – «сигнал есть» – отличается сдвигом на величину a, зависящую от способа обработки (например, если обработка сводится к взятию отсчета в момент, когда несущее колебание достигает максимума, величина a представляет собой его амплитуду). Значение a предполагается известным.

Таким образом, проверяемые гипотезы описываются двумя условными плотностями распределения вероятностей $w(y/H_0)$ и $w(y/H_1)$, изображенными на рисунке 17.2.

Приемник в таком случае должен сравнить y с некоторым фиксированным значением (порогом) $y_п$ и если y больше порога, принять решение о наличии сигнала, в противном случае – о его отсутствии, что можно кратко записать в следующей символической форме:

$$y \geq y_п \rightarrow «1»;$$
$$y \leq y_п \rightarrow «0».$$

Каким бы ни был порог $y_п$, очевидно, есть некоторая ненулевая вероятность p_{01} принять решение о наличии сигнала при его фактическом отсутствии. Эта вероятность называется условной вероятностью *ошибки первого рода* («ложной тревоги») и определяется выражением:

$$p_{01} = \int_{y_п}^{+\infty} w(y \mid H_0)dy$$

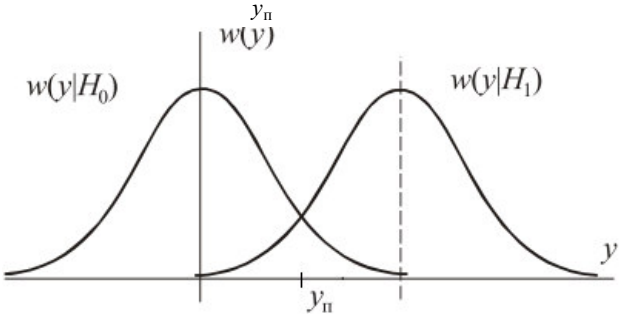


Рис. 17.2. Условные плотности распределения вероятностей величины *y* при простых гипотезах

Аналогично, существует ненулевая вероятность принять решение об отсутствии сигнала, в то время как на самом деле он есть (условная вероятность ошибки второго рода, или пропуска сигнала):

$$p_{10} = \int_{-\infty}^{y_п} w(y \mid H_1)dy .$$

Анализ рисунка 17.2 показывает, что сумма указанных условных вероятностей минимальна, если порог $y_п$ находится как абсцисса точки пересечения условных плотностей $w(y/H_0)$ и $w(y/H_1)$.

Очевидно, при таком выборе порога приемник является оптимальным по критерию *минимума суммарной условной вероятности* ошибки (17.4) и принятие решения основывается на сравнении значений функций $w(y/H_0)$ и $w(y/H_1)$ при наблюдаемом значении *y*:

$w(y|H_0 < w(y|H_1) \rightarrow$ “1”

$w(y|H_0 \geq w(y|H_1) \rightarrow$ “0”

Это правило принятия решения можно переписать также в форме:

$$\frac{w(y \mid H_1)}{w(y \mid H_0)} > 1 \;\rightarrow\; \text{"1"}; \qquad \frac{w(y \mid H_1)}{w(y \mid H_0)} \leq 1 \;\rightarrow\; \text{"0"}.$$

Решение, таким образом, принимается в пользу той гипотезы, которая представляется более правдоподобной при данном значении *y*, поэтому отношение $\frac{w(y \mid H_1)}{w(y \mid H_0)}$ называется отношением правдоподобия и обозначается $\Lambda(y)$. Правило (17.5) называют правилом максимального правдоподобия. Заметим, что критерий (17.4) часто называют критерием максимума правдоподобия.

Критерий идеального наблюдателя предполагает учет априорных вероятностей гипотез, и оптимальный в смысле этого критерия приемник обеспечивает минимум средней вероятности ошибки, т.е. наименьшую сумму безусловных вероятностей ошибок первого и второго рода. Иначе говоря, сравнению подлежат функции $w(y/H_0)$ и $w(y/H_1)$, умноженные на соответствующие априорные вероятности. Правило принятия решения в таком приемнике можно записать в форме:

$$\frac{p_1 w(y \mid H_1)}{p_0 w(y \mid H_0)} > 1 \;\rightarrow\; \text{"1"}; \qquad \frac{p_1 w(y \mid H_1)}{p_0 w(y \mid H_0)} \leq 1 \;\rightarrow\; \text{"0"}$$

Используя понятие *отношения правдоподобия*, можно записать правило в виде:

$$\Lambda(y) > \frac{p_0}{p_1} \quad \rightarrow \quad \text{"1"}; \qquad \Lambda(y) \leq \frac{p_0}{p_1} \quad \rightarrow \quad \text{"0"},$$

при этом *отношение правдоподобия* сравнивается с пороговым значением, зависящим от априорных вероятностей.

Наконец, в случае *байесовского* критерия решение принимается по правилу:

$$\frac{\Pi_{10} p_1 w(y \mid H_1)}{\Pi_{01} p_0 w(y \mid H_0)} > 1 \;\rightarrow\; \text{"1"}; \qquad \frac{\Pi_{10} p_1 w(y \mid H_1)}{\Pi_{01} p_0 w(y \mid H_0)} \le 1 \;\rightarrow\; \text{"0"},$$

или

$$\Lambda(y) > \frac{p_0 \Pi_{01}}{p_1 \Pi_{10}} \;\rightarrow\; \text{"1"}; \qquad \Lambda(y) \le \frac{p_0 \Pi_{01}}{p_1 \Pi_{10}} \;\rightarrow\; \text{"0"}.$$

Итак, во всех случаях оптимальный приемник (демодулятор, или решающее устройство) «устроен одинаково»: для наблюдаемого значения у, зависящего от принятой реализации z(t), вычисляется значение отношения правдоподобия, которое сравнивается с порогом; порог равен $\frac{p_0 \Pi_{01}}{p_1 \Pi_{10}}$ для оптимального приемника по критерию минимума среднего риска, p_0 / p_1 для идеального приемника Котельникова и 1 для приемника максимального правдоподобия.

Следует отметим, что иногда удобнее вычислять не отношение правдоподобия, а его логарифм. В силу монотонности логарифмической функции это не влияет на условные вероятности ошибок, если порог также прологарифмировать.