МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

А. И. МИТЮХИН

# ТЕОРИЯ КОДИРОВАНИЯ

УЧЕБНОЕ ПОСОБИЕ
по дисциплине «Теория кодирования»
для студентов специальности
«Программное обеспечение информационных технологий»

МИНСК 2014

## Введение

Теория кодирования это новый раздел науки, возникший сравнительно недавно. Умение применять на практике результаты теории кодирования стало важным для специалиста, создающего современные инфокоммуникационные системы. Теория кодирования возникла из статистической теории связи. Лишь частично отвечая на вопросы о путях и способах технической реализации аппаратуры, эта теория позволяет вычислить эффективность любой системы передачи, хранения, обработки информации, определить максимально возможную эффективность радиосистемы. Для широкого класса задач при определенных знаниях или допущениях относительно статистики шумов стало возможным построение аппаратуры, работающей на основе оптимального приема. После того, как выбрана и обоснована конкретная схема оптимального приемника, фильтра, обнаружителя и т.п. возникают вопросы кодирования.

Задача теории кодирования – при известной статистике шумов выбрать такое множество передаваемых сигналов, чтобы правдоподобие правильного декодирования принимаемых сообщений было максимальным. При этом важно найти не только хороший код, но и эффективный алгоритм декодирования.

Теория кодов, контролирующих ошибки является одной из ветвей теории цифровой обработки сигналов (ЦОС). Существует тесная связь теории кодирования и теории ЦОС. Но данные дисциплины развивались различными путями: одна разрабатывалась в основном алгебраистами, а другая – в основном инженерами. Первые результаты по теории кодирования появились в конце 40-х годов в работах К. Шеннона (Shannon Claude), Голея (M.J.E. Golay) и Р. Хэмминга (Hamming R.). Можно определить следующие основные исторические этапы развития теории кодирования:

– 1948 г., Клод Шеннон (американский математик) сформулировал и доказал теоремы кодирования для дискретного канала. К. Шеннон показал, что с каждым каналом передачи информации связано число $C$. Это число определяет пропускную способность канала и измеряется в битах в секунду. Если требуемая от информационной системы скорость передачи информации $R_i$ (измеряемая в битах в секунду) меньше $C$, то используя коды, контролирующие ошибки, для данного канала можно построить такую систему связи, что вероятность ошибки на выходе декодера будет сколь угодно мала;

– 1950 г., Хэмминг описал класс кодов, исправляющих независимые одиночные ошибки;

– 1960 г., Боуз Р.К. (Bose R.C.), Рой-Чоудхури (R.Chaudhari) и независимо Хоквингем (1959) открыли двоичные коды, исправляющие кратные независимые ошибки (БЧХ-коды);

– 1963 г., Рид И.С. (Reed I.C.) и Соломон предложили модификацию БЧХ-кодов для недвоичных каналов (РС-коды). Эти коды нашли применение для исправления пакетов и модулей ошибок;

– (1960 – 1970) г., с появлением микросхем средней степени интеграции началось практическое воплощение методов теории кодирования в каналах с

большим уровнем помех. Применялись низкоскоростные коды максимальной длины (М-последовательности), коды Рида-Маллера (РМ-коды) и др. Кроме того, были разработаны новые эффективные алгоритмы декодирования (Питерсон, Берлекэмп, Мэсси и др.).

Коды используются:

– для защиты данных в памяти вычислительных устройств, для передачи данных в вычислительных системах (такие системы очень чувствительны к очень малой доле ошибок, т.к. даже одиночная ошибка может нарушить всю программу вычислений);

– в цифровых оптических дисках (компакт - дисках);

– в системах со сжатием данных;

– в системах связи с ограничением на передаваемую мощность, например, в системах ретрансляции через спутник, где увеличение мощности обходится очень дорого;

– в системах цифрового телевидения; обработки изображения;

– в системах передачи информации разного назначения, например, в системах с пакетной коммутацией и разделением во времени, где длинные двоичные сообщения разделяются на пакеты, и пакет передается в отведенное временное окно. Из-за нарушения синхронизации пакеты могут быть утеряны. Кодирование позволяет обеспечить надежную синхронизацию в такой системе.

Кодирование применяется для защиты специальных радиотехнических систем гражданского и военного назначения, например, радиолокационных и радионавигационных станций, систем видеографии от воздействия:

– непреднамеренных помех типа белого шума;

– преднамеренных помех специального типа, (например, сосредоточенных в спектре сигнала – узкополосных, или широкополосных с кодовыми видами модуляции).

Кодирование защищает информационные системы от случайного и несанкционированного доступа к информации; повышает надежность радиотехнических и вычислительных устройств, делая их нечувствительными к отказам и сбоям.

Рассмотрение вопросов кодирования начнём с представления некоторых общих моделей информационных каналов.

## 1. МОДЕЛИ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ С КОДИРОВАНИЕМ

Обобщенная модель канала передачи информации с кодированием имеет вид, представленный на рисунке 1.1.

Рассмотрим некоторые особенности представленной модели. Источник сообщений формирует поток непрерывных или дискретных сообщений. Кодер источника сообщения предназначен для устранения информационной избыточности. Он позволяет:

– более эффективно использовать частотный ресурс;

– повысить скорость передачи информации.

Корректирующий кодер вводит информационную избыточность в передаваемое сообщение с целью обнаружения и (или) исправления ошибок сравнительно небольшой, не более 1,2,3,4 кратности.

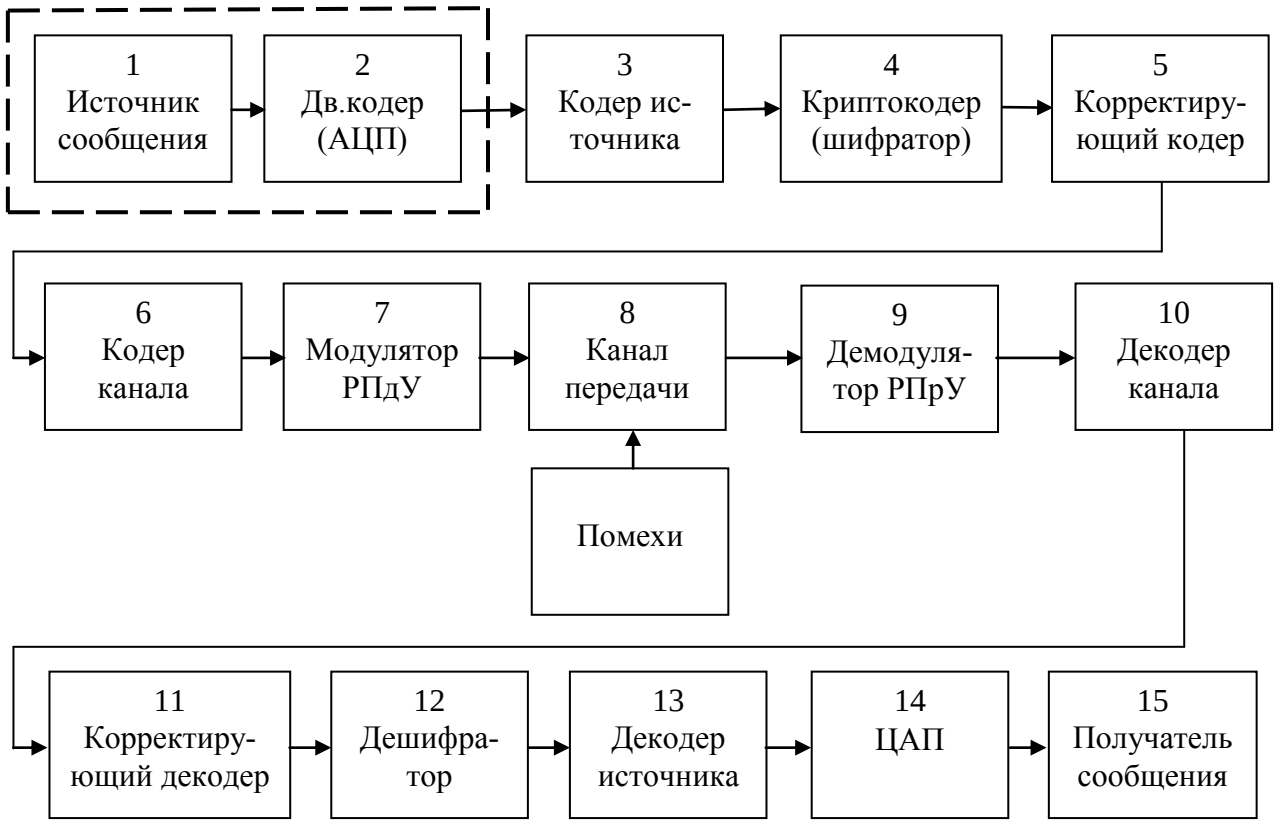



Рисунок 1.1 – Модель канала передачи информации с кодированием

Кодер канала (помехоустойчивый кодер) также предназначен для минимизации влияния помех на передаваемую информацию и в большинстве своем используется в специальных радиотехнических системах:

– системах дальнего космоса;

– спутниковых навигационных системах (например, GPS"NAVSTAR" (Global Positioning System ″NAVSTAR″), ″ГЛОНАСС″ (глобальная навигационная спутниковая система));

– системах скрытной связи;

– радиолокационных системах дальнего обнаружения целей, системах наведения на цель с повышенной точностью (точное оружие);

– системах мобильной и фиксированной связи третьего поколения CDMA (Code Division Multiple Access – кодовое разделение каналов, множественный доступ).

Модулятор преобразует множество дискретных сигналов канального кодера в непрерывные сигналы, которые передаются по каналам.

Каналом передачи информации может служить:

– радиоканал;
– проводной канал;
– оптический канал;
– магнитная лента;
– компакт-диск;
– запоминающее устройство и т.п.

Замечание. Если в качестве канала передачи использовать ЗУ, то это канал передачи информации во времени в отличие, например, от радиоканала передачи информации в пространстве.

В канале формируется смесь сигнала и помехи вида

$$y(t) = x(t)\mu(t) + n(t)$$

где – $x(t)$ передаваемый непрерывный сигнал, $\mu(t)$ мультипликативная помеха, $n(t)$ аддитивная помеха (как правило, шум с гауссовским распределением).

Декодер источника восстанавливает ту избыточность, которая была ранее устранена на передающей стороне.

Замечания.

1. Техническая реализация составляющих рисунка 1.1 с номерами 3, 4, 5, 6, 10, 11, 12, 13 осуществляется на цифровой элементной базе.
2. Криптокодер и корректирующий кодер могут меняться местами.
3. В элементах 1,2 производится дискретизация по времени и квантование по уровню входной аналоговой реализации (сообщения) с формированием символов в двоичном или $q$-ичном алфавите.

## 1.1. Разновидности моделей каналов передачи информации с помехоустойчивым кодированием

### 1.1.1. Канал с неизвестным местоположением ошибок при кодировании и декодировании

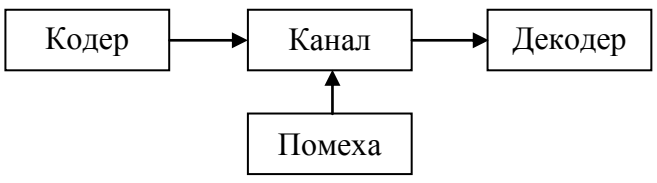



Рисунок 1.2 – Канал без информации о виде и состоянии ошибки

### 1.1.2. Канал со стиранием

Стирание – потеря передаваемого символа в некоторой позиции. Оно отличается от ошибки тем, что известен номер позиции, где это произошло. Состояние символа неизвестно и, кроме того, неизвестно согласованно ли оно с передаваемой информацией или нет. Если передаётся множество $x(n) = (x(1), x(2), \dots, x(N-1))$ $N$-точечной последовательности отчетов сигнала, то возможную форму огибающей последовательности для $N = 7$ и двух стираний можно изобразить, как показано на рисунке 1.3. Здесь обрабатываемая последовательность записывается в виде множества $x(n) = (0,1,s,1,0,s)$

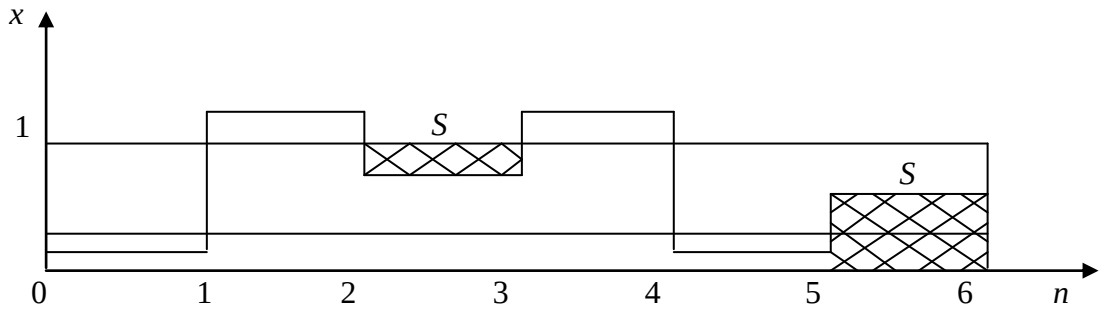



Рисунок 1.3

Канал со стиранием называется каналом с известным местоположением ошибок при декодировании. Примером канала со стиранием может служить ЗУ, рисунок 1.4.

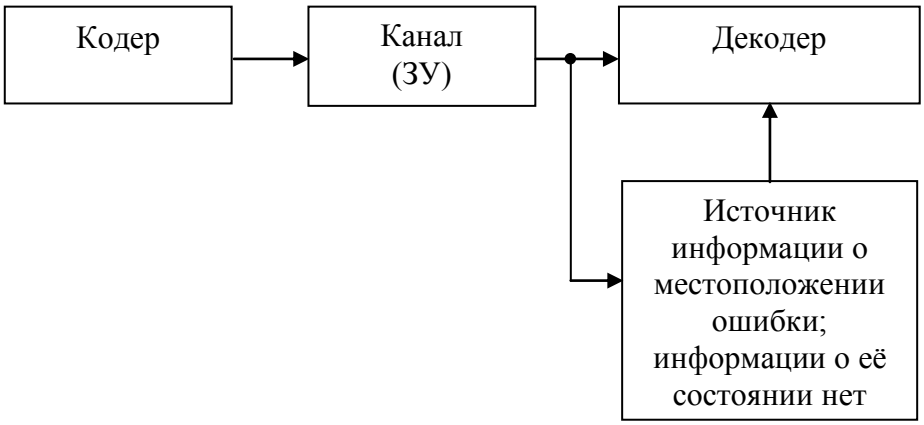



Рисунок 1.4

### 1.1.3. Канал с дефектом

Дефект – отказ какого-либо элемента, местоположение которого известно, а состояние не изменяется при входных воздействиях. Покажем это

на примере матрицы оперативного ЗУ. Дефектной является третья ячейка памяти, рисунок 1.5.

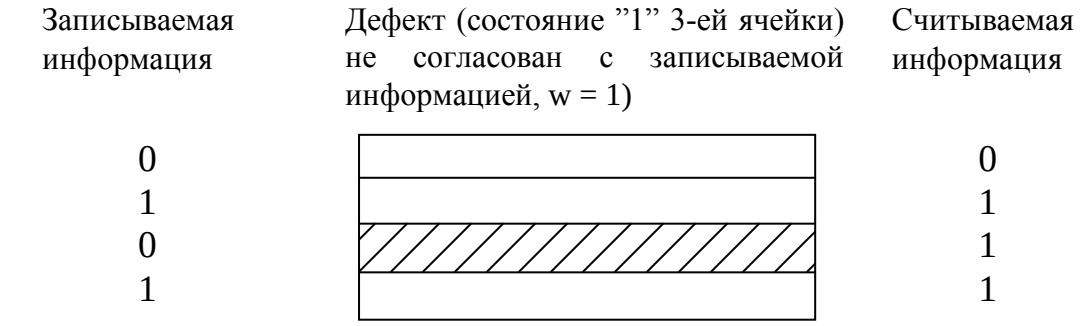



Рисунок 1.5

Канал с дефектом называют каналом с известным местоположением ошибок и их состоянием при кодировании, рисунок 1.6. В этой модели канала передачи, в отличие от канала со стиранием, имеется информация о согласовании или несогласовании дефектов с передаваемой информацией.

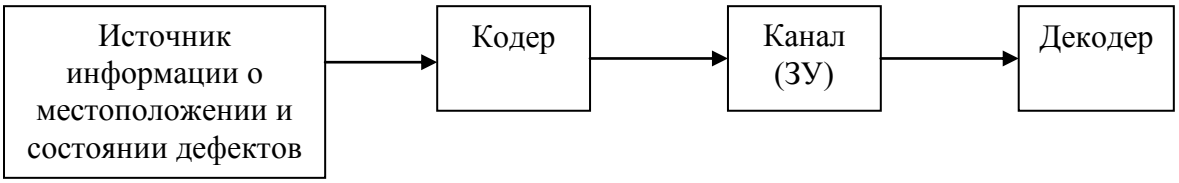



Рисунок 1.6

1.1.4. Канал с известным местоположением ошибок при кодировании и декодировании

В этой модели состояния ошибок неизвестны. Модель такого канала показана на рисунке 1.7. Данная модель используется для создания памяти суперкомпьютера – объекта стратегического значения ведущих мировых стран.

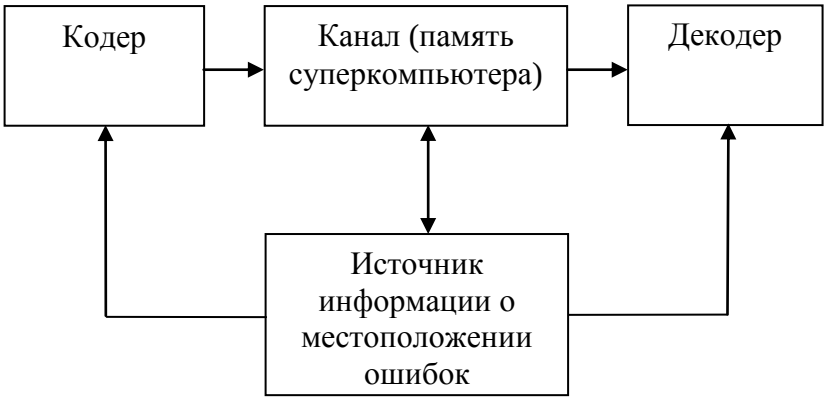



Рисунок 1.7

С помощью суперкомпьютера можно моделировать разные физические

процессы. Например, суперкомпьютер используется для моделирования геофизических процессов Земли. В этом случае имеется возможность решения чрезвычайно актуальной задачи предсказания глобальных землетресений. Всем известны катастрофические последствия такого землетресения в Юго-Восточной Азии в 2004 году. Другим примером служит реализация трехмерного моделирования ядерных взрывов (аналогичных проводимым до начала 60-х годов на полигоне в штате Невада США). Моделирование столь сложных физических процессов во многом заменяет дорогие натурные ядерные испытания, позволяет осуществить идентификацию и различение ядерных взрывов. Масса суперкомпьютера 106 тонн, а занимаемая площадь 800÷2000 кв.м. (3-х этажное здание). Скорость вычислений свыше 1000 триллионов математических операций в секунду. На решение вышеназванной задачи суперкомпьютеру требуется 1месяц работы (≈ 350 лет обычному компьютеру). При создании суперкомпьютера возникает сложная проблема – перегрев. Тепловыделение на одном процессоре-чипе достигает величины 1кВт. Потребляемая суперкомпьютером мощность – 3000кВт = 3МВт. Кроме того на систему охлаждения необходима мощность порядка 2000кВт = 2МВт и зал, уставленный холодильными шкафами. Всего суперкомпьютер требует расхода мощности порядка 5МВт. Для сравнения: 3МВт – мощность, потребляемая сравнительно большим городом. При огромном объеме памяти возрастает вероятность появления дефектных ячеек или ячеек со сбоями, что в конечном итоге приводит к низкой надежности работы суперкомпьютера из-за частой переборки компонентов системы, а следовательно, дополнительным материальным затратам на создание такого компьютера. Модель использует способы кодирования, позволяющие осуществить обход отказавших ячеек памяти.

### 1.1.5. Канал с обратной связью

Иногда бывает так, что ввиду особых требований к системе, устройству (масса, габариты, энергопотребление и пр.) или технической сложности, эффективным является режим обнаружения ошибок. Эта модель применима также в каналах передачи информации, где ошибки встречаются крайне редко: низкоорбитальные и среднеорбитальные космические системы связи, волоконно-оптические линии связи, системы передачи речи (она избыточна сама по себе) и др. Канал с обратной связью допускает повторную передачу информации. На рисунке 1.8 показана модель такого канала.

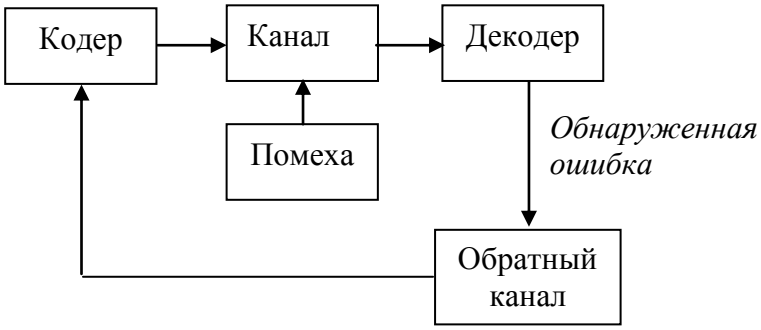



Рисунок 1.8

1.1.6. Широковещательный канал

Канал моделирует передачу (обмен) информации между множеством терминалов (источниками и получателями).

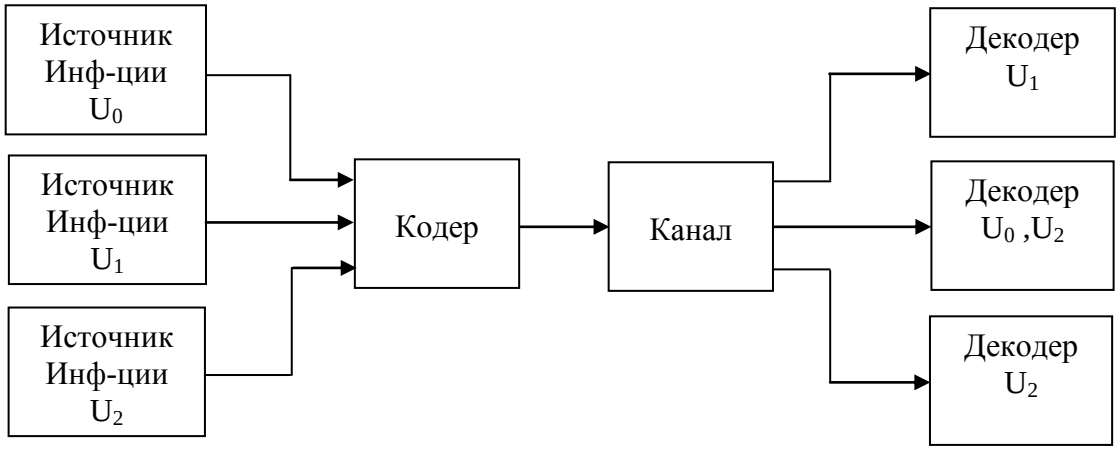



Рисунок 1.9

Модель широковещательного канала во многом отражает спутниковое, цифровое телевидение, цифровое радиовещание, кабельное ТВ, скрытную связь и пр. Эта же модель характерна для систем, где разделение каналов осуществляется по таким признакам, как частота, фаза, время, код.

1.1.7. Канал с подслушиванием

Предполагается, что подслушивающая сторона знает коды, схемы работы кодера и декодера применяемые в основном канале. Однако ошибки в канале подслушивания или большой уровень шума в принятом им сигнале мешают расшифровке данных, передаваемых по основному каналу. Кодер-декодер основного канала должны быть построены так, чтобы обеспечивать секретность передачи данных с наибольшей скоростью *R.* Требование секретности означает, что должна быть максимально возможной ненадежность данных, поступающих к подслушивающему устройству. Ситуация напоминает плохой

радиовещательный канал, но цель преследуется иная. В радиовещательном канале стремятся максимизировать поток информации к обоим приемникам, тогда как в модели с подслушиванием минимизируется информация, поступающая к приемнику канала подслушивания. Модель канала с подслушиванием показана на рисунке 1.10.

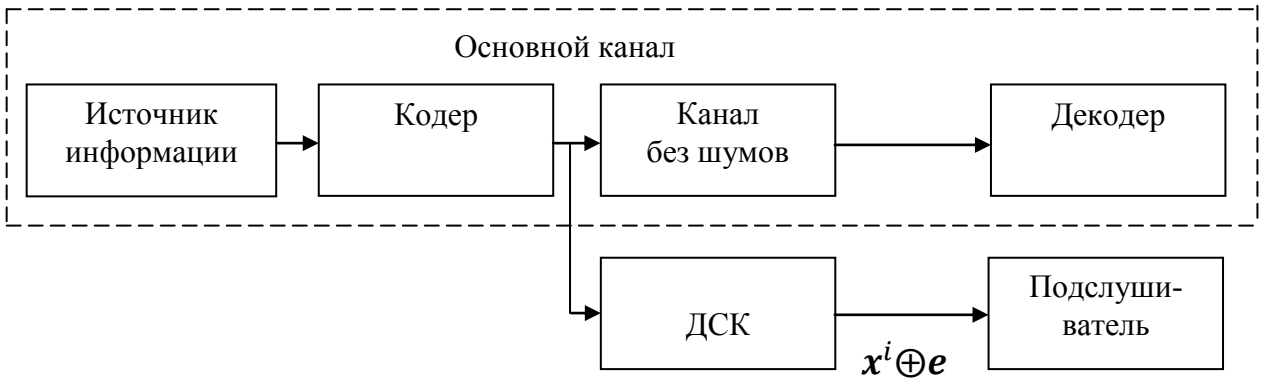



Рисунок 1.10

ДСК – двоичный симметричный канал;
$x^i$– кодированное сообщение;
$e$ – случайный вектор ошибок в канале с подслушиванием.

Очевидно, что представленное выше многообразие моделей каналов передачи информации с помехоустойчивым кодированием требует применения различных классов кодов.

## 1.2. Методы борьбы с ошибками

Повышение надежности передачи, хранения информации в различных каналах достигается применением следующих методов борьбы с ошибками.

1. Технологический, основанный на совершенствовании, модернизации:

а) технологии производства всех компонентов системы;
б) конструкции системы;
в) схемотехники устройств;
г) характеристик каналов передачи информации.

2. Введение структурной избыточности (резервирование систем и устройств).

3. Введение информационной избыточности – помехоустойчивого кодирования.

4. Комбинация вышеперечисленных методов.

1.3. Классификация ошибок

Ошибки бывают:
– случайные (независимые);
– зависимые.

Случайные ошибки возникают независимо друг от друга в передаваемом сообщении. При этом говорят о кратности ошибок *t*.

Зависимые ошибки делятся на:
– пакетные;
– модульные.

Пакет ошибок описывается длиной пакета $p$. Он может находиться в произвольном месте потока передаваемых (записываемых) символов. Говорят, граница (фаза) пакета неизвестна.

Например, в ЗУ длиной 16 следует записать информацию

0001 0110 1111 1010.

Произошла пакетная ошибка длиной $p = 4$. В ЗУ запишется информация

0001 0101 0011 1010.

Кратность пакета ошибок обозначается через $q$. Пакет ошибок описывается вектором ошибки $e = (e_0, e_1, \dots, e_{p-1})$. Для двоичных кодов $e_i = \{0, 1\}$. В приведенном примере $e = (1111)$, $q = 1$.

Модульная ошибка – это частный случай пакетной ошибки. В литературе по кодированию ее называют и байтовой ошибкой. Модуль ошибок – это фазированный пакет ошибок. В этом случае граница (фаза) пакета известна. Длина модуля ошибок и кратность модуля ошибок обозначаются соответственно $b$ и $q$. Число возможных конфигураций векторов ошибок равно $2^b - 1$. Для $b = 4$ конфигурации ошибок образуют следующее множество векторов ошибок

$$e = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ . & . & . & . \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Пусть двоичная информация

0001 0110 1111 1010

записывается в ЗУ с модульной ошибкой. Вектор $e = (1010)$; $q = 1$. Тогда на входе декодера двоичное слово представляется в виде

1011 0110 1111 1010.

В реальных системах модульные и пакетные ошибки встречаются чаще, чем отдельно расположенные ошибки. Зависимые ошибки могут вызываться источником периодического шума, например, расположенным поблизости радиолокатором или каким-то вращающимся электромеханизмом, замираниями в линии связи и пр. В этом случае необходимо применение кодов, исправляющих пакетные и модульные ошибки. Заметим, что при наличии таких ошибок может оказаться более правильным использовать процедуру перемежения порядка символов в закодированной последовательности перед передачей и восстановления исходного порядка символов после приема с тем, чтобы рандомизировать ошибки, объединенные в пакеты.

## 1.4. Статистические характеристики ошибок

Различают ошибки:
– симметричные;
– асимметричные;
– однонаправленные.

Симметричные ошибки характерны для двоично-симметричного канала (ДСК). Условно такой канал изображен на рисунке 1.11.

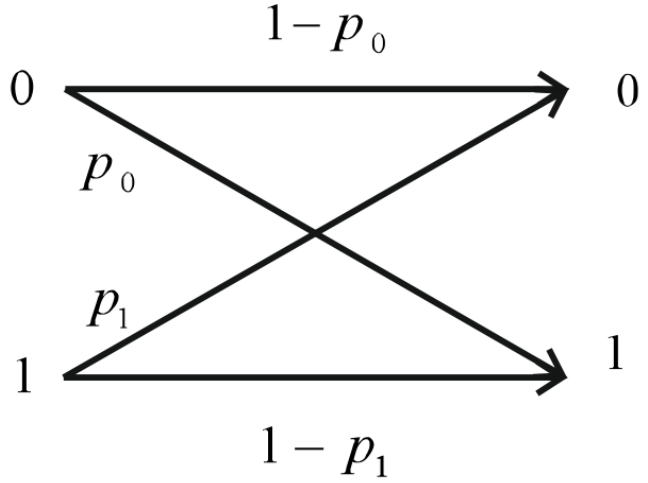



Рисунок 1.11

Входными символами канала являются символы 0 и 1. Возможными выходными символами канала также будут символы 0 и 1. Обозначим $p_0$ вероятность ошибки при передаче символа 0, $p_1$ – вероятность ошибки при передаче символа 1. Тогда выражения (1– $p_0$) и (1– $p_1$) представляют вероятности неискаженной передачи соответственно символов 0 и 1.

Если $p_0 = p_1$, то канал является симметричным.

При $p_0 \gg p_1$ или $p_1 \gg p_0$ – канал асимметричный.

Однонаправленные ошибки возникают, например, при отказе устройства, когда во всех разрядах некоторого его модуля устанавливается только нулевое или единичное состояние.

Проектирование, разработка радиоэлектронных систем различного назначения требует априорного знания значений вероятностей ошибок при передаче информации в том или ином канале. Статистика ошибок в различных каналах к настоящему времени исследована достаточно полно. Опубликованы результаты экспериментов, касающиеся измерения частоты ошибок на информационный бит и характера их группирования в каналах. Вероятность появления ошибок на выходе соответствующего канального приемника по данным отечественной и зарубежной литературы находится в пределах:

– радиорелейного $p_0 = 10^{-4} - 10^{-5}$;

– телефонного $p_0 = 10^{-3} - 10^{-5}$;

– магнитной ленты $p_0 = 10^{-4} - 10^{-5}$;

– телеметрического $p_0 = 10^{-6} - 10^{-10}$;

– оптического диска $p_0 = 10^{-5} - 10^{-6}$;

– космического телеметрического $p_0 = 10^{-12} - 10^{-23}$;

В телеметрическом канале космического корабля многоразовых полетов (Space Shuttle) с помощью (127, 120) БЧХ-кода достигается вероятность ложного приема командной информации менее $p_0 = 6{,}62 \cdot 10^{-23}$.

Для цифровых устройств различают следующие вероятности ошибок:

– вероятность ошибки из-за дефектов (отказа) элементов;

– вероятность ошибки из-за сбоев элементов.

Сбой это перемежающийся переход состояния элемента из правильного в неправильное и обратно (возможен и при входном воздействии).

Для полупроводниковой памяти вероятность ошибки из-за отказа $p_0 = 10^{-5} - 10^{-6}$, а вероятность ошибки из-за сбоев элементов $p_0 = 10^{-4} - 10^{-5}$. Для того чтобы гарантировать высокую надежность памяти необходимо иметь вероятность ошибки из-за отказа $p_0 = 10^{-10} - 10^{-12}$.

## 2.1. Параметры кодов

Определение 2.1. Код – это множество дискретных сигналов, разрешенное для передачи сообщений.

Коды характеризуются следующими параметрами.

1. Основание кода $q$ – число различных элементов множества, выбранное для построения кода. Основание $q$ определяет размерность используемого алфавита. Например, если:

а) $q = \{a,b,c\}$, то $q = 3$ для троичного кода;

б) $q = \{0, 1\}$, q = 2 для двоичного кода.

Практически $q \geq 2$.

Замечание. Эффективность каналов передачи (хранения) информации возрастает с переходом на недвоичные коды.

Определение 2.2. Длина кода $n$ (значность) – число символов кодового слова. Последовательности элементов (символов) длиной $n$ называются кодовыми словами или кодовыми векторами. Говорят, что слово $x = (x_0 x_1 \dots x_{n-1})$ имеет длину $n$, $l = (abbcab), n = 6$.

Параметр $n$ определяет следующие особенности кодов. Коды бывают:

– равномерные (блоковые), $n$ = const;

– неравномерные, $n$ = var;

– бесконечные, $n = \infty$.

К бесконечным относят коды:

а) сверточные (древовидные);

б) цепные;

в) непрерывные.

У равномерных (блоковых) кодов поток данных разделяется на блоки по $k$ информационных символов, и далее они кодируются $n$-символьными кодовыми словами.

Для бесконечного непрерывного кода поток данных разбивается на блоки длиной $k_0 \ll k$, которые называются кадрами информационных символов. Эти кадры кодируются $n_0$ символами кодового слова (кадрами кодового слова). Кодирование каждого кадра информационных символов в отдельные кадры кодового слова производится с учетом предыдущих $m$ кадров информационных символов. На рисунке 2.1 показаны структуры кодирования блоковыми и непрерывными кодами.

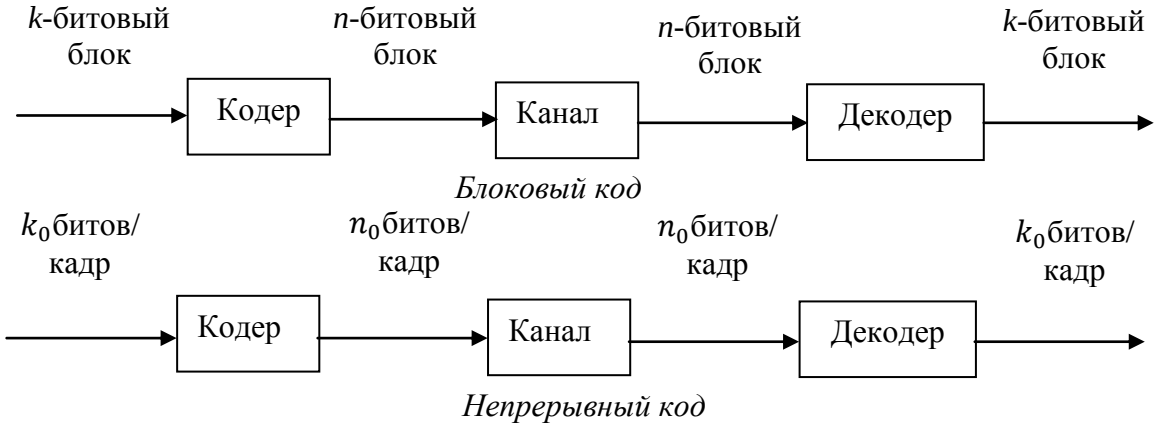



Рисунок 2.1

Определение 2.3. Размерность кода $k$ – число информационных элементов (позиций) кодового слова.

Определение 2.4. Мощность кода $M = q^k$ – число различных кодовых

последовательностей (комбинаций), разрешаемых для кодирования.

Различают $M_{\max} = q^n$ – максимальное число кодовых комбинаций при заданных $q$ и $n$. Например, $q = 3$; $n = 6$; $M_{\max} = 3^6 = 729$.
Код, у которого используются все комбинации, называется полным (безызбыточным). Для него $k = n$.
Если число кодовых слов кода $M < M_{\max}$, то код называется избыточным.

Пример 2.1. Пусть $q = 2$, $n = 5$, $M = 4$. Избыточный код

$$G = \begin{Bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{Bmatrix}.$$

Определение 2.5. Число проверочных (избыточных) позиций кодового слова $r = n - k$. Пусть $n = 7$, $q = 2$, $k = 4$. Тогда на длине слова из семи символов три избыточных.

Определение 2.6. Скорость передачи кода $R = k/n$. Для приведенного примера $R = 4/7$.

Определение 2.7. Кратность ошибки $t$. Параметр $t$ указывает, что все конфигурации из $t$ или менее ошибок в любом кодовом слове могут быть исправлены и (или) обнаружены.

Предположим, что по каналу передается или хранится в памяти кодовое слово $x = (x_0 x_1 \dots x_{n-1})$, а принимается, или считывается из памяти вектор $y = (y_0 y_1 \dots y_{n-1})$. Тогда вектор $y - x = e = (e_0 e_1 \dots e_{n-1})$ называется вектором ошибок, где $e_i \in GF(q)$. Если ошибок не произошло, то $e = 0$. Вектор ошибок указывает место и значение ошибок.

Определение 2.8. Расстояние Хэмминга между двумя векторами (степень удаленности любых кодовых последовательностей друг от друга) – $d_x$.
Если $x = (x_0 x_1 \dots x_{n-1})$ и $y = (y_0 y_1 \dots y_{n-1})$ кодовые векторы, то расстояние Хэмминга равно числу позиций, в которых они различаются. Расстояние Хэмминга может обозначаться и как dist$(x, y)$. Например, dist(*abbcb,cbcaa*) = 4; dist(0122,2212) = 3.

Замечание. С позиции теории кодирования $d_x$ показывает, сколько символов в слове надо исказить, чтобы перевести одно кодовое слово в другое.

Определение 2.9. Наименьшее значение расстояния Хэмминга для всех пар кодовых последовательностей кода $G$ называют кодовым расстоянием $d$ (минимальное расстояние кода),

$$d = \min\{\text{dist}(x, y)\}, \text{ где } x \in G; y \in G; x \neq y.$$

Кодовое расстояние $d$ характеризует корректирующую способность кода

$$t = f(d).$$

Определение 2.10. Код значностью $n$, размерностью $k$ и расстоянием $d$ называется $[n,k,d]$- кодом.

Пример 2.2. Можно построить следующий код:

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

Данный код можно использовать для кодирования 2 – битовых двоичных чисел, используя следующее (произвольное) соответствие:

$$00 \leftrightarrow 0000$$
$$10 \leftrightarrow 1010$$
$$01 \leftrightarrow 0111$$
$$11 \leftrightarrow 1101.$$

Найдем кодовое расстояние этого кода:

$$\text{dist}(1010,0111) = 3;$$
$$\text{dist}(1010,1101) = 3;$$
$$\text{dist}(0111,1101) = 2.$$

Следовательно, для этого кода $d = \min\{\text{dist}(x, y)\} = 2.$

Определение 2.11. Вес Хэмминга вектора $x = (x_0 x_1 \dots x_{n-1})$ равен числу ненулевых позиций вектора $x$; обозначается $\text{wt}(x)$.

Например, wt(1230430) = 5. Используя определение веса Хэмминга, получим очевидное выражение

$$\text{dist}(x, y) = \text{wt}(x - y). \qquad (2.1)$$

Пример 2.3. $x = (1202)^T$, $y = (2012)^T$.

$$\text{dist}(x, y) = \text{wt}(\begin{bmatrix} 1 \\ 2 \\ 0 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 0 \\ 1 \\ 2 \end{bmatrix}) = \text{wt} \begin{bmatrix} 2 \\ 2 \\ 2 \\ 0 \end{bmatrix} = 3.$$

Из выражения (2.1) следует, что минимальное расстояние Хэмминга равно

$$d = \min\{\text{dist}(x, y)\} = \min\{\text{wt}(x - y), \text{где } x \in G; y \in G; x \neq y.$$

Замечание. Для нахождения минимального расстояния линейного кода не

обязательно сравнивать все возможные пары кодовых слов. Если $x$ и $y$ принадлежат линейному коду $G$, то $x - y = u$ также является кодовым словом кода $G$. Такой код является аддитивной группой (определена операция сложения) и, следовательно,

$$d = \min\{\text{dist}(x, y)\} = \min\{\text{wt}(x - y)\} = \text{minwt}(u),$$

где $u \in G; u \neq 0$, т.е. справедлива следующая теорема.

Теорема 2.1. Минимальное расстояние линейного кода равно минимальному весу ненулевых кодовых слов.

Так как $t = f(d)$, то возникает вопрос о величине $d$, такой, чтобы код обеспечивал контроль ошибок, т.е. обнаружение и исправление ошибок.

## 2.2. Контроль ошибок

Передаваемое кодовое слово можно представить в виде вектора с координатами в $n$-мерном векторном пространстве. Например, для $n$ = 3 вектор $x = (x_0 x_1 x_2)$ находится в трёхмерном евклидовом пространстве, рисунок 2.2. Разрешенными словами для передачи выбраны векторы $x_1 = (000)$ и $x_2 = (111)$.

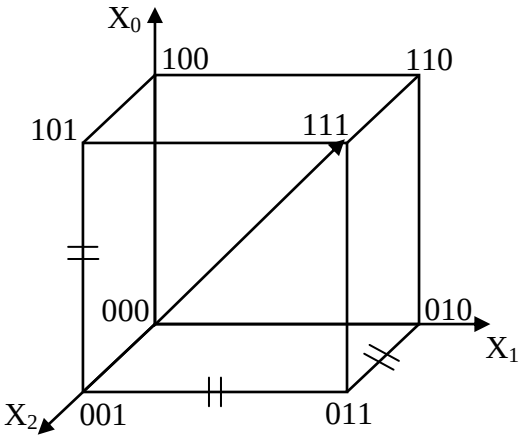



Рисунок 2.2

Рисунок наглядно изображает алгебраическую интерпретацию понятия «мощность кода»:

а) кодовые слова полного кода определяют $n$-мерное пространство, состоящее из $q^n$ последовательностей ($n$ = 3 – трехмерное пространство, включающее при $q$ = 2 восемь последовательностей полного двоичного кода);

б) кодовые слова избыточного кода определяют подпространство (подмножество) $n$-мерного пространства, состоящее из $q^k$ последовательностей.

Под воздействием помех происходит искажение отдельных разрядов

вектора разрешенного подмножества. В результате разрешённые для передачи кодовые векторы переходят в другие векторы (с иными координатами) – запрещённые. Факт перехода разрешённого слова в запрещённое для передачи слово можно использовать для контроля над ошибками.

Возможна ситуация, когда разрешённый вектор переходит в другой разрешённый кодовый вектор: (000)⇔(111). В этом случае ошибки не обнаруживаются, и контроль становится неэффективным.

Из рассмотренной модели можно сделать следующий очевидный, но важный вывод. Для того, чтобы передаваемые векторы можно было бы отличать друг от друга при наличии помех, необходимо располагать эти векторы в $n$-мерном пространстве как можно дальше друг от друга. Из этой же $n$-мерной модели следует геометрическая интерпретация расстояния Хэмминга $d_x$– это число рёбер, которые нужно пройти, чтобы перевести один вектор в другой, т.е. попасть из вершины одного вектора в вершину другого.

### 2.2.1. Обнаружение ошибок

Стратегия обнаружения ошибок в переданном слове заключается в следующем. Можно обнаружить ошибку, если установить, что переданным словом было ближайшее по расстоянию Хэмминга к принятому слову. Покажем применение этого утверждения.

Пример 2.4. Пусть $n = 3$; $q = 2$. Разрешенным для передачи является множество кодовых слов:

$$G = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Очевидно, что множество $G$ имеет $d = 1$. Любая одиночная ошибка трансформирует кодовое слово кода в другое разрешенное для передачи слово. Это случай, когда выбранное для передачи информации множество не обладает корректирующей способностью.

Пример 2.5. Пусть теперь подмножество $G$ разрешённых для передачи кодовых слов представлено в виде двоичных векторов с чётным весом (чётным числом единиц).

$$G = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Заданный код $G$ имеет $d$ = 2. Запрещенные кодовые слова представлены в виде подмножества

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Если $d$ = 2, то ни одно из разрешенных кодовых слов (т.е. кода $G$) при одиночной ошибке не переходит в другое разрешённое слово этого же кода. Таким образом, код $G$ обнаруживает:

– одиночные ошибки;

– ошибки нечетной кратности (для $n$ = 3 – тройные).

Например, тройная ошибка кодового слова $x$ = (110); $e$ =(111), переводит его в запрещенный вектор $y = x \oplus e = (001)$. Рассмотрим процесс декодирования в режиме обнаружения.

Допустим, передавалось кодовое слово $x$ = (101). Возникла одиночная ошибка, вектор которой $e$ = (100). На вход декодера поступил вектор $y = x \oplus e = (001)$. Данный вектор принадлежит запрещенному подмножеству $A$. Следовательно, декодер устанавливает, что при передаче информации произошла ошибка. Таким образом, осуществляется контроль ошибок.

Еще раз рассмотрим утверждение: переданным словом было то, которое является ближайшим по расстоянию Хэмминга к принятому. Вычислим расстояния Хэмминга для всех слов разрешенного подмножества и входным вектором.

$$\begin{aligned} &\mathrm{dist}_1(000{,}001) = 1, \\ &\mathrm{dist}_2(101{,}001) = 1, \\ &\mathrm{dist}_3(011{,}001) = 1, \\ &\mathrm{dist}_4(110{,}001) = 3. \end{aligned}$$

Наиболее вероятно, что передаваемыми словами могли быть следующие:

$$x_1 = (000), x_2 = (101), x_3 = (011).$$

Вывод. В общем случае, при необходимости обнаруживать ошибки кратностью $t$ кодовое расстояние кода должно удовлетворять выражению

$$d \geq t + 1.$$

Пример 2.6. Пусть $n$ = 3; $q$ = 2; код $G$ задан векторами $x_1$=(000) и $x_2$=(111). При возникновении одиночных ошибок или множества векторов

$$\{e\} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

кодовому слову $x_1$ = (000) соответствует следующее запрещенное подмножество

$$A = \{x_1 \oplus e\} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Кодовому слову $x_2$ = (111) соответствует следующее запрещенное подмножество

$$L = \{x_2 \oplus e\} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Таким образом, коду $G$, разрешенному для передачи подмножеств векторов $\{x_1, x_2\}$, соответствуют два запрещенных подмножества векторов $\{A\}$ и $\{L\}$:

$$G = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{matrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = A \\ \rightarrow \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} = L \end{matrix}.$$

Стратегия исправления ошибок заключается в следующем:

– каждая из одиночных ошибок приводит к запрещенному кодовому слову того или иного запрещенного подмножества ($L$ и $A$);

– структура кодового запрещенного подмножества, относящаяся к соответствующему исходному разрешенному подмножеству, позволяет определить местоположение ошибки, т.е. исправить ошибку.

Допустим, передавалось кодовое слово $x_2 = (111)$. Возникла одиночная ошибка, вектор которой $e$ = (100). На вход декодера поступил вектор

$$y = x \oplus e = (011).$$

Вычислим расстояния Хэмминга для всех слов разрешенного подмножества и входным вектором.

$$\text{dist}_1(000,011) = 2,$$
$$\text{dist}_2(111,011) = 1.$$

Наиболее вероятно, что передавалось слово

$$x_2 = (111).$$

Для исправления ошибок кратностью $t$ кодовое расстояние должно удовлетворять соотношению

$$d \geq 2t+1. \qquad (2.2)$$

Используя эту формулу, можно записать

$$t = \lceil (d\text{-l})/2 \rceil,$$

где $\lceil l \rceil$ обозначает целую часть числа $l$.

Замечание. Существуют модели каналов (например, канал с дефектами), в которых величина $t$ может быть больше, чем в выражении (2.2).

## 2.3. Возможность исправления ошибок кодами

### 2.3.1. Теорема К. Шеннона о кодировании в дискретном канале с шумами

Определение 2.12. Пропускная способность двоичного симметричного канала с вероятностью ошибки $p$ равна

$$C = W[1 + p\log_2 p + (1-p)\log_2(1-p)] \text{ бит/с},$$

где $W = 1/\tau$ – тактовая частота следования информационных символов; $\tau$ – длительность символа.

При отсутствии помех $p = 0$ пропускная способность достигает максимума:

$$C_{\max} = W \text{ бит/с}$$

Пропускная способность канала, отнесенная к одному элементарному символу длительностью $\tau$, определяется из выражения

$$C/C_{\max} = f(p) = C(p),$$

где

$$C = [1 + p\log_2 p + (1-p)\log_2(1-p)].$$

Пусть в среднем один из каждых 100 символов принимается ошибочным, т.е. $p = 0{,}01$. Пропускная способность на символ ДСК равна

$$C(p) = [1 + 0{,}01\log_2 0{,}01 + 0{,}99\log_2 0{,}99] \text{ бит/с}.$$

При наличии шумов пропускная способность $C(p)$ в канале всегда меньше одного бита на символ (рисунок 2.3).

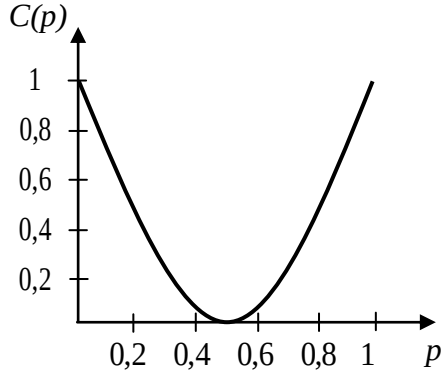



Рисунок 2.3 – Зависимость относительной пропускной способности ДСК от вероятности ошибочного приема

Из рисунка 2.3 видно, что с ростом $p$ от 0 до 0,5 пропускная способность $C(p)$ убывает от своего максимального значения, равного 1 до 0. Среднее

количество передаваемой информации оказывается равным нулю. Если процент ошибок достигает 100%, то среднее количество передаваемой информации также оказывается равным 1 бит/симв. Но в этом случае с вероятностью единица принятый символ не равен переданному символу. Тогда нулевой символ надо читать как единичный и наоборот.

Теорема 2.2. Пусть $C(p)$ – относительная пропускная способность дискретного канала; источник создает информацию со скоростью $R = k/n$. Тогда для любого $\varepsilon > 0$, если $R < C(p)$ и $n$ достаточно велико, существует $[n, k, d]$ – двоичный код со скоростью $R \leq k/n$, вероятность ошибки которого $P_{ош} < \varepsilon$.

Теорема Шеннона состоит из двух утверждений.

Прямое утверждение

При любой производительности источника сообщений, меньшей, чем пропускная способность канала, существует такой способ кодирования, который обеспечивает передачу информации со сколь угодно малой вероятностью ошибки.

Замечания:

1. Под производительностью источника сообщений понимают количество информации, вырабатываемой источником сообщений в единицу времени.

2. Пропускная способность – это предельная скорость передачи информации по каналу, при которой еще возможна передача со сколь угодно малой вероятностью ошибки.

Обратное утверждение теоремы К. Шеннона

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

$$R = \frac{k}{n} > C(p).$$

Теорема с одной стороны – фундаментальна, а с другой стороны – неконструктивна.

Фундаментальность – устанавливается теоретический предел эффективности системы при достоверной передаче информации. При этом:

– помехи в канале не ограничивают точность (достоверность) передачи;

– помехи ограничивают скорость передачи информации, при которой может быть достигнута сколь угодно высокая достоверность передачи;

– при любой конечной скорости передачи информации, вплоть до пропускной способности, сколь угодно малая вероятность ошибки достигается лишь при увеличении длительности кодовых последовательностей и

использовании большого ансамбля кодовых слов.

Неконструктивность теоремы заключается в том, что в ней не затрагиваются пути построения кодов, методы обработки, обеспечивающие безошибочную передачу информации, а лишь утверждается их существование.

### 2.3.2. Формула К. Шеннона

Качество цифровой системы передачи информации характеризуется вероятностью ошибки на бит (частотой ошибок на бит). При передаче дискретных данных по каналу с аддитивным гауссовским шумом вероятность ошибки на бит может быть уменьшена путем увеличения мощности передатчика, которая также является одной из характеристик качества системы. Лучшей из двух систем передачи данных считается та, которая достигает желаемой частоты ошибок на бит при меньшей мощности передатчика.

Сообщение из $k$ информационных бит имеют энергию

$$E_c = \sum_{n=0}^{k-1} |x(n)|^2.$$

Энергия сигнала, соответствующая одному информационному биту, определяется соотношением

$$E_b = \frac{E_c}{k} = \frac{1}{k}\sum_{n=0}^{k-1} |x(n)|^2. \qquad (2.3)$$

Замечание. Проверочные символы, символы синхронизации (например, начала кодового слова, строчные, кадровые или символы канального обмена и др.) не несут информации и поэтому не могут участвовать в вычислении $E_b$.

Для сообщений, передаваемых со скоростью $R_i$ информационных бит/с, величина $E_b$ определяется из выражения

$$E_b = \frac{P_c}{R_i},$$

где $P_c$ – средняя мощность сообщения.

На вход приемника поступает также и белый шум с односторонней спектральной плотностью $N_0$ Вт/Гц. Очевидно, что на частоту ошибок на бит влияет только отношение $\frac{E_b}{N_0}$. Сравнительные качественные характеристики различных способов передачи сигналов можно получить, оценивая зависимости их вероятностей ошибок на бит от отношения $\frac{E_b}{N_0}$. Нижняя, теоретически достижимая в цифровой системе передачи информации, граница $\frac{E_b}{N_0}$ определяется из формулы пропускной способности непрерывного канала (формулы К. Шеннона)

$$C = W \log_2(1 + P_c/P_N), \qquad (2.5)$$

где $C$ – пропускная способность канала; $W$ – ширина полосы частот канала; $P_N = N_0 W$– средняя мощность помех с нормальным законом распределения амплитуд и равномерным спектром в полосе частот канала.

Определим границу абсолютного значения отношения $\frac{E_b}{N_0}$. Ширина полосы сигнала в формуле (2.5) не ограничена. Устремим $W$ к бесконечности и найдем предельное значение пропускной способности канала $C_\infty$:

$$C_\infty = \lim_{W\to\infty} C = \lim_{W\to\infty} W \log_2(1 + \frac{P_c}{N_0 W}).$$

Обозначим $\frac{1}{W}$ через $\gamma$, тогда можно записать

$$C_\infty = \lim_{\gamma\to 0} C = \lim_{\gamma\to 0} \frac{1}{\gamma} \log_2(1 + \frac{P_c}{N_0}\gamma). \qquad (2.6)$$

Функция (2.6) в точке $\gamma = 0$, принимая вид 0/0, не определена. Для раскрытия неопределенности и вычисления предела воспользуемся правилом Лопиталя. Продифференцируем числитель и знаменатель (2.6) по $(1 + \frac{P_c}{N_0}\gamma)$.

$$C_\infty = \lim_{\gamma\to 0} \frac{\log_2(1+\frac{P_c}{N_0}\gamma)'}{\gamma'}. \qquad (2.7)$$

Числителю (2.7) соответствует выражение

$$\log_2(x)' = \log_2 e.$$

Дифференцирование знаменателя приводит к

$$\frac{d\gamma}{d(1+\frac{P_c}{N_0}\gamma)} = \frac{N_0}{P_c}.$$

Формулу (2.7) можно записать как

$$C_\infty = \lim_{W\to\infty} C = \frac{P_c}{N_0} \log_2 e = 1{,}443 \frac{P_c}{N_0}.$$

Подставив в последнее выражение значение мощности информационных бит

$$R_i E_b = P_c,$$

получим граничное значение $\frac{E_b}{N_0}$:

$$R_i \le 1{,}443 \frac{P_c}{N_0} = 1{,}443 R_i \frac{E_b}{N_0}; \qquad (2.8)$$

$$N_0 \le 1{,}443 E_b.$$

Замечание. Нужно иметь в виду, что формула Шеннона справедлива только тогда, когда передаваемый сигнал образовывает аддитивную смесь с белым шумом. Кроме того, по своим статистическим свойствам сигнал подобен нормальному стационарному шуму с заданной средней мощностью и равномерной спектральной плотностью внутри полосы частот $W$.

Теорема 2.3. В системе, передающей информацию в условиях белого гауссовского шума односторонней спектральной плотности $N_0$, необходимо, чтобы энергия на бит удовлетворяла неравенствам:

$$E_b \geq 0{,}69N_0;$$

$$\frac{E_b}{N_0} \geq -1{,}6 \text{ dB}.$$

Формула (2.8) приводит к очень важному заключению: для случая малого отношения $\frac{P_c}{P_N} = \frac{\text{сигнал}}{\text{шум}} \ll 1$ на входе приемника пропускная способность канала

$$C_\infty = 1{,}443\frac{P_c}{N_0}$$

не зависит от ширины его пропускания, а определяется средней мощностью передаваемого сигнала и спектральной плотностью мощности шума (мощности, приходящейся на единицу полосы).

Теорема 2.3. определяет нижний предел допустимого отношения $\frac{E_b}{N_0}$. Верхний предел установлен экспериментально. При отношении сигнал/шум $\frac{E_b}{N_0} \geq 12$ dB обеспечивается практически безошибочная передача информации. Следовательно, практическая необходимость применения кодирования и выбора соответствующего кода возникает лишь в том случае, когда соотношение $\frac{E_b}{N_0}$ лежит в диапазоне минус 1,6 dB плюс 12 dB.

Формулу (2.5) можно записать в следующем виде:

$$I = WT\log_2(1 + P_c/P_N), \qquad (2.9)$$

где $I$ характеризует максимальное количество информации, передаваемое по каналу за время $T$.

Из (2.9) следует, что при уменьшении отношения $(P_c/P_N)$ или $\frac{E_b}{N_0}$ можно сохранить количество передаваемой информации, расширяя полосу сигнала или увеличивая время передачи. Выражение (2.9) имеет фундаментальное значение для теории кодирования.

## 2.4. Границы минимального расстояния линейных кодов

Возможна следующая формулировка основной проблемы кодирования:

– требуется построить код как можно с большей скоростью $R = \frac{k}{n}$ (код с большей эффективностью);

– требуется построить код как можно с большим расстоянием $d$ (код с большей исправляющей способностью).

Очевидно, что при увеличении $d$ кратность исправляемой ошибки $t$ растет за счет увеличения числа проверочных символов $r$. При фиксированном $n = \text{const}$ это приводит к уменьшению мощности кода $M = q^k$ и скорости $R$. Отсюда видно, параметры кода $n, d, M$ определяют три возможности построения ″хорошего″ кода:

а) при заданных $M$ и $n$ максимизируется $d$ (т.е. находится максимальное кодовое расстояние); подобным образом полученные коды называют максиминными;

б) при заданных $M$ и $d$ минимизируется $n$ (т.е. отыскиваются коды с минимальной избыточностью);

в) при заданных $n$ и $d$ максимизируется $M$ (т.е. находятся коды с максимальной мощностью).

Замечание. К настоящему времени ни одна из этих задач полностью не решена. Существующие решения не приводят к одному оптимальному результату, найдены лишь частные решения и оценки качества кода.

Если имеются два кода с одинаковыми значениями $n$ и $R$, то следует выбирать код с большей величиной $d$. Функцию, определяющую оптимальный выбор соответствующего класса кода, можно представить в виде

$$d(n, R) = \max d\{G\},$$

где $d\{G\} = \min\{dist(X, Y)\}$, $X \in G, Y \in G, X \neq Y$.

Максимум берется по всем кодам с данной длиной $n$ скоростью $R$. Функция $d(n, R)$ известна только для сравнительно малых значений $n$. Однако получены выражения верхних и нижних границ кодовых расстояний кодов с заданными длиной и скоростью. Наиболее полезными для анализа кодового расстояния являются границы:

– Синглтона;

– Плоткина;

– Хэмминга;

– Варшамова-Гилберта.

### 2.4.1. Граница Синглтона

Теорема 2.4. Кодовое расстояние любого линейного $[n, k, d]$-кода удовлетворяет равенству

$$d \leq 1 + n - k. \qquad (2.10)$$

Доказательство. Ненулевое слово минимального веса в коде имеет вес

$$\min\{\mathrm{wt}(u)\} = d\,, u \neq 0, u \in G.$$

Кодовое слово систематического кода с одним ненулевым информационным символом и $(n - k)$ проверочными символами не может иметь вес, больший $(1 + n - k)$. Следовательно, минимальный вес кода не может быть больше

$$d \leq 1 + n - k.$$

Определение 2.13. Код с кодовым расстоянием, удовлетворяющий равенству

$$d = 1 + n - k = 1 + r$$

называется кодом с максимальным расстоянием.

Граница Синглтона показывает, что для исправления $t$ ошибок код должен иметь не менее $2\,t$ проверочных символов, и что линейные коды с

$$r = d - 1$$

существуют.

Действительно, из $d \geq 2t+1$ и (2.10) следует, что

$$1 + n - k \geq 2t + 1,$$
$$r \geq 2t.$$

Замечание. Большинство кодов имеют намного больше проверочных символов, чем требует граница Синглтона. Коды с максимальным расстоянием имеют точно два проверочных символа на ошибку, т.е.

$$r = 2t.$$

## 3. Линейные коды

Среди корректирующих кодов наибольшее распространение получили линейные коды с символами из некоторой группы или некоторого поля Галуа $GF(q)$.

Определение 3.1. Линейный $[n,k,d]$-код есть подпространство размерностью $k$ линейного $n$-мерного пространства над $GF(q)$. Подмножество, состоящее из $q^k$ последовательностей длиной $n$, называется $q$-ичным блоковым кодом длиной $n$.

Замечания:

1. Если $q = \{0,1\}$, векторное пространство кода над полем $GF(2)$. образует аддитивную подгруппу группы всех двоичных последовательностей длиной $n$. Очевидно, что для этой подгруппы должны выполняться все аксиомы группы, и для нее определена одна основная операция – сложение.

2.Так как операция суммирования является линейной операцией, то и код называется линейным.

Примером линейного группового кода является двоичный код Хэмминга. Пусть $q = 2$. Для каждого целого положительного числа $m$ существует код Хэмминга с параметрами:

$$[2^m–1, 2^m–1–m, 3]; R = (2^m –1– m)/(2^m –1); r = m; t = 1.$$

Заметим, что для больших значений $m$ , скорость кода $R \approx 1$. Например, для $m$ = 8 получаем величину

$$R = (2^8– 1– 8)/(2^8–1) = 247/255 = 0{,}968.$$

Линейные коды делятся на:

– систематические (разделимые);

– несистематические (неразделимые).

У систематического кода первые $k$ символов кодового слова – информационные.

Несистематические – нет деления на информационные и проверочные символы (все символы являются кодовыми символами).

### 3.1. Кодер систематического кода

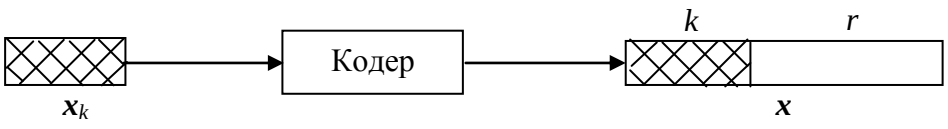



Рисунок 3.1

Действия систематического кодера, рисунок 3.1:

1) кодер разбивает входную информационную последовательность

символов на блоки $x_{k_l} = (x_0 x_1 \dots x_{k-1})$ длиной $k$;

2) для каждого блока $x_{k_l}$ находит слово $x_l$, первые $k$ символов которого совпадают с $x_{k_l}$;

3) кодер обрабатывает каждый поступающий блок независимо от других так, что каждое новое слово на его выходе оказывается не связанным с предыдущими кодовыми словами.

Замечание. Кодер сверточного систематического кода формирует кодовое слово, зависящее от предыдущего блока.

В качестве примера линейного кода приведем [7,4,3]-код Хэмминга мощностью $M = 2^4 = 16$. Ненулевые кодовые слова $x_l = (x_0 x_1 \dots x_{n-1})$ кода Хэмминга [7,4,3] в порядке возрастания величины информационных весов $\mathrm{wt}\{x_k\}$ векторов кода записаны в таблице 3.1.

Таблица 3.1 – Код Хэмминга [7,4,3].

| | $x_l$ | $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | |
|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{wt}\{x_k\}=1$ | $x_0$ | 1 | 0 | 0 | 0 | 1 | 1 | 0 | |
| | $x_1$ | 0 | 1 | 0 | 0 | 1 | 1 | 1 | |
| | $x_2$ | 0 | 0 | 1 | 0 | 0 | 1 | 1 | |
| | $x_3$ | 0 | 0 | 0 | 1 | 1 | 0 | 1 | |
| $\mathrm{wt}\{x_k\}=2$ | $x_4$ | 1 | 1 | 0 | 0 | 0 | 0 | 1 | $x_0 + x_1$ |
| | $x_5$ | 1 | 0 | 1 | 0 | 1 | 0 | 1 | $x_0 + x_2$ |
| | $x_6$ | 1 | 0 | 0 | 1 | 0 | 1 | 1 | $x_0 + x_3$ |
| | $x_7$ | 0 | 1 | 1 | 0 | 1 | 0 | 0 | $x_1 + x_2$ |
| | $x_8$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | $x_1 + x_3$ |
| | $x_9$ | 0 | 0 | 1 | 1 | 1 | 1 | 0 | $x_2 + x_3$ |
| $\mathrm{wt}\{x_k\}=3$ | $x_{10}$ | 1 | 1 | 1 | 0 | 0 | 1 | 0 | $x_0 + x_1 + x_2$ |
| | $x_{11}$ | 1 | 1 | 0 | 1 | 1 | 0 | 0 | $x_0 + x_1 + x_3$ |
| | $x_{12}$ | 1 | 0 | 1 | 1 | 0 | 0 | 0 | $x_0 + x_2 + x_3$ |
| | $x_{13}$ | 0 | 1 | 1 | 1 | 0 | 0 | 1 | $x_1 + x_2 + x_3$ |
| $\mathrm{wt}\{x_k\}=4$ | $x_{14}$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | $x_0 + x_1 + x_2 + x_3$ |

Если информационный вес $\mathrm{wt}\{x_k\} = i$, то число кодовых слов данного информационного веса определяется биноминальным коэффициентом $C_k^i$. Тогда [7,4,3]-код Хэмминга содержит$(C_k^1 + C_k^2 + C_k^3 + C_k^4) = 15$ ненулевых слов. Обозначения $x_0, x_1, x_2, x_3$ соответствуют информационным символам. Проверочные символы кода задаются равенствами:

$$x_4 = x_0 + x_1 + x_3,$$
$$x_5 = x_0 + x_1 + x_2,$$
$$x_6 = x_1 + x_2 + x_3.$$

Все множество кодовых слов кода образуется путем суммирования первых четырех строк (базовых векторов) по 2, по 3, по $k$, таблица 3.1. Таким образом, кодовые слова являются линейными комбинациями строк задающей код матрицы. С точки зрения алгебры все ненулевые слова кода образуют некоторое векторное пространство, базисом которого являются строки базовой (порождающей) матрицы.

### 3.2. Способы задания линейных кодов

Линейные коды задаются с помощью:

а) порождающей матрицы $G$ размерностью $k \times n$;

б) проверочной матрицы $H$ размерностью $r \times n$.

Матрицы связаны основным уравнением кодирования

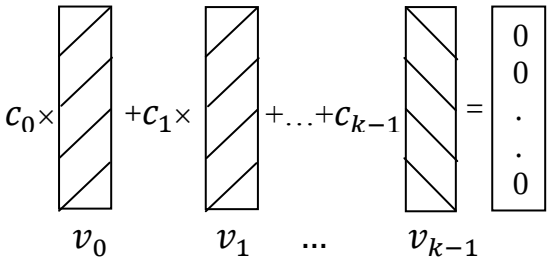
$$G \times H^T = 0 \qquad (3.1)$$

Из (3.1) следует, что для всякой матрицы $G$ существует матрица $H$, удовлетворяющая этому равенству. И наоборот, заданной матрице $H$ будет соответствовать только одна матрица $G$. В качестве строк матрицы $G$ выбираются линейно-независимые слова длиной $n$, отстоящие друг от друга на заданное кодовое расстояние $d$. Рассмотрим векторное пространство $v$ над полем $GF(q)$ .

Определение 3.2. Векторы $v_0, v_1, \dots, v_{k-1}$ из $v$ называются линейно зависимыми, если в $GF(q)$ существуют такие элементы $c_0, c_1, \dots, c_{k-1}$, для которых

$$c_0 v_0 + c_1 v_1 + \cdots + c_{k-1} v_{k-1} = 0.$$

Наглядно условие линейной независимости векторов над полем $GF(q)$ можно изобразить как




где $c_i \in \{q\}$. Для двоичных кодов $c_i \in \{0,1\}$, линейная независимость означает, что суммирование базисных двоичных векторов не образует нулевой вектор. Максимальное число линейно независимых векторов в $v$ называется размерностью векторного пространства $v$ над полем $GF(q)$.

Замечание. Поскольку линейно независимые векторы могут быть выбраны произвольным образом, то, очевидно, можно построить множество матриц $G$ с одним и тем же кодовым расстоянием $d$. Например, второй вариант задания [7,4,3]-кода Хэмминга в виде матрицы $G$ представляется как

| | $x_l$ | $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ |
|---|---|---|---|---|---|---|---|---|
| $G'$ | $x_0$ | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| | $x_1$ | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| | $x_2$ | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| | $x_3$ | 0 | 0 | 0 | 1 | 0 | 1 | 1 |

Линейно независимые векторы инвариантны относительно двух операций, при выполнении которых минимальное расстояние кода не изменяется.

Возможны:

– произвольные перестановки столбцов и строк матрицы $G$;

– элементарные операции (например, сложение) над строками матрицы $G$.

Замечание. Перестановка символов кода эквивалентна перестановке столбцов порождающей матрицы.

### 3.3. Эквивалентные коды

Определение 3.3. Два кода эквивалентны тогда, когда их порождающая матрица получается одна из другой на основе свойства инвариантности.

Примеры.

3.1. Множества $G$ и $G'$ порождают эквивалентные коды

$$G = \begin{pmatrix} x_0 & 1 & 1 & 0 & 0 \\ x_1 & 0 & 1 & 1 & 0 \\ x_2 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad G' = \begin{pmatrix} x_0 + x_1 + x_2 & 1 & 0 & 0 & 1 \\ x_1 + x_2 & 0 & 1 & 0 & 1 \\ x_2 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

3.2. Эквивалентные коды Хэмминга [7,4,3] заданы матрицами $G$ и $G'$:

| | $x_l$ | $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ |
|---|---|---|---|---|---|---|---|---|
| $G$ | $x_0$ | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| | $x_1$ | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| | $x_2$ | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| | $x_3$ | 0 | 0 | 0 | 1 | 1 | 0 | 1 |

| | $x_l$ | $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ |
|---|---|---|---|---|---|---|---|---|
| $G'$ | $x_0$ | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| | $x_1$ | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| | $x_2$ | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| | $x_3$ | 0 | 0 | 0 | 1 | 0 | 1 | 1 |

Замечание. Следует различать эквивалентный и эквидистантный коды.

Определение 3.4. Эквидистантный код – это множество слов, отстоящих друг от друга на одно и то же расстояние Хэмминга $d_x$.

Пример эквидистантного [7, 3, 4]-кода ($m$-кода) представлен матрицей

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

3.4. Порождающая и проверочная матрица линейного кода

Следствием свойства инвариантности векторов относительно выше названных операций является, приведено ступенчатая (каноническая) форма матриц $G$ и $H$. Порождающая матрица кода в канонической форме записывается так

$$G = [I_k | G^*] \quad (3.2)$$

где $I_k$ – единичная подматрица размером $k \times k$, а $G^*$ есть $k \times (n-k)$ подматрица.

С учётом формы матрицы (3.2) уравнение кодирования представим как

$$GH^T = [I_k | G^*] \left[\frac{-G^*}{I_r}\right] = -G^* + G^* = 0.$$

Отсюда определяем проверочную матрицу $H$ в канонической форме

$$H = [-G^{*T} | I_r]. \quad (3.3)$$

где $I_r$ единичная матрица размером $r \times r$.

В поле $GF(2)$ $-G^{*T} = G^{*T}$, поэтому

$$H = [G^{*T} | I_r].$$

Матрицы (3.2) и (3.3) задают систематический линейный код. Если известна проверочная матрица систематического кода

$$H = [H^* | I_r],$$

то матрица $G$ записывается в виде

$$G = [I_k | H^{*T}].$$

Таким образом, код можно задавать перечислением всех $q^k$ разрешенных для передачи кодовых слов, или перечислением только базисных векторов кодового подпространства. Очевидно, второй способ гораздо компактнее и удобнее для описания кодов. Например, если $q = 2$, $R = \frac{1}{2}$; $n = 256$, число кодовых слов достигает порядка $M = 2^{128}$. Полная их запись требует $2^{128} \cdot$

$2^8 = 2^{136}$ битов. Порождающая матрица этого же кода требует только 128× $256 = 2^7 \cdot 2^8 = 2^{15} = 32768$ битов.

Замечание. Любое максимальное множество линейно независимых кодовых слов, выбранное из данного кода, может использоваться в качестве строк порождающей матрицы этого кода.

## 3.5. Кодирование линейным кодом

Кодирование представляет собой операцию умножения вектора сообщения $u$ на порождающую матрицу $G$,

$$x = uG. \tag{3.4}$$

При умножении вектора $u$ на $G$ в форме (3.2) образуется систематический код, т.к. умножение $uI_k = u$ не изменяет входного сообщения. Первые $k$ символов кодового слова равны соответствующим символам сообщения. Проверочные символы выбираются так, чтобы кодовые слова удовлетворяли основному уравнению кодирования

$$xH^T = (x_0 x_1 \dots x_{k-1} \dots x_{n-1})H^T = (00 \dots 0). \tag{3.5}$$

Запишем выражение (3.5) иначе

$$Hx^T = 0.$$

$$[H^*|I_r]\begin{bmatrix} x_0 \\ \vdots \\ x_{k-1} \\ x_k \\ \vdots \\ x_{n-1} \end{bmatrix} = \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}.$$

Найдем из этого уравнения проверочные символы.

$$\begin{bmatrix} x_k \\ \vdots \\ x_{n-1} \end{bmatrix} = -H^* \begin{bmatrix} x_0 \\ \vdots \\ x_{k-1} \end{bmatrix}.$$

В поле $GF(2)$ $-H^* = H$. Поэтому перепишем последнее выражение как

$$\begin{bmatrix} x_k \\ \vdots \\ x_{n-1} \end{bmatrix} = H^* \begin{bmatrix} x_0 \\ \vdots \\ x_{k-1} \end{bmatrix}. \tag{3.6}$$

Таким образом, в общем виде проверочные символы записываются по формуле (3.6).

Пример 3.1. Пусть имеется матрица $H$ размерностью 3×6. Обозначим элементы матрицы $H$ через $h_{ij}$. Тогда получаем:

$$\begin{bmatrix} h_{11} & h_{12} & h_{13} & 1 & 0 & 0 \\ h_{21} & h_{22} & h_{23} & 0 & 1 & 0 \\ h_{31} & h_{32} & h_{33} & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

$$\begin{bmatrix} h_{11}x_0 & + & h_{12}x_1 & + & h_{13}x_2 & + & x_3 \\ h_{21}x_0 & + & h_{22}x_1 & + & h_{23}x_2 & + & x_4 \\ h_{31}x_0 & + & h_{23}x_1 & + & h_{33}x_2 & + & x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

$$\begin{bmatrix} x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \\ h_{31} & h_{32} & h_{33} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix}. \qquad (3.7)$$

Из формулы (3.7) следует, что для двоичных кодов:

– каждый проверочный символ есть сумма информационных символов;

– в вычислении $i$ -го проверочного символа участвуют те информационные, которым соответствуют единицы в $i$-ой строке матрицы $H$;

– $i$-ый проверочный символ определяется по $i$ -му столбцу подматрицы $G^*$.

## 3.6. Коды Рида-Маллера

Как правило, в результате кодирования информации кодом Рида-Маллера (РМ-кодом) получается неразделимый код. При этом используется однородная и регулярная структура порождающей матрицы $G$, позволяющая упростить процедуры кодирования и декодирования.

Практическое применение этого кода осуществлено сравнительно давно в американской специальной системе «Диджилок». В 1972 году РМ коды использовались в американской космической программе «Маринер» по передаче изображений марсианской поверхности. РМ-код имеет следующие параметры.

1. Значность кода $n = 2^m$, $m \geqslant 2$.
2. Кодовое расстояние $d = 2^{m-l}$ .
3. Порядок кода $l$.
3. Размерность кода $k = 1 + \sum_{i=1}^{l} C_m^l$.

Порождающая матрица РМ-кода порядка $l$ строится из определения операции пересечения двоичных векторов. Пусть заданы векторы

$$x = (x_0 x_1 \ldots x_{n-1}),\ y = (y_0 y_1 \ldots y_{n-1}).$$

Результат операции пересечения:

$$x \cdot y = ((x_0 \cdot y_0)(x_1 \cdot y_1) \dots (x_{n-1} \cdot y_{n-1})).$$

При таком определении векторы образуют коммуникативную группу. Например, совокупность векторов, образованная пересечением трех векторов $x_i$ взятых по 2

$$A = \begin{Bmatrix} x_0 & \cdot & x_1 \\ x_0 & \cdot & x_2 \\ x_1 & \cdot & x_2 \end{Bmatrix}.$$

Код Рида-Маллера порядка $l$ определяется как код, базисом которого являются векторы $x_0, x_1, \dots, x_{m-1}$ и все векторные пересечения из $m$ или меньшего числа этих векторов.

Пример 3.2. Построим код Рида-Маллера первого порядка $l = 1, m = 3$. Получаем РМ-код со следующими параметрами:

$$n = 2^3 = 8;$$
$$d = 2^{3-1} = 4;$$
$$k = 1 + \sum_{i=1}^{1} C_3^i = 1 + C_3^1 = 4.$$

Имеем $[8,4,4,]$-код. В общем случае кодовое расстояние РМ-кода первого порядка равно $d = n\ /\ 2$. Код Рида-Маллера первого порядка задается порождающей матрицей $G$, первая строка которой состоит из $n$ единиц. В качестве столбцов остальных $m$ строк используются все двоичные числа длиной $m$. Порождающая матрица РМ-кода первого порядка при $m = 3$ имеет вид

$$G = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} \Leftrightarrow \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \quad (3.8)$$

Пример 3.3. Записать матрицу $G$ РМ-кода второго порядка для $m = 3$. Код характеризуется параметрами:

$$n = 8;$$
$$k = 1 + \sum_{i=1}^{2} C_3^i = 1 + C_3^1 + C_3^2 = 1 + 3 + 3 = 7;$$
$$d = 2^{m-l} = 2.$$

$$G = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 = x_1 \cdot x_2 \\ x_5 = x_1 \cdot x_3 \\ x_6 = x_2 \cdot x_3 \end{bmatrix} \Leftrightarrow \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Векторы $x_0, x_1, x_2, x_3$ линейно независимы.

Пример 3. 4. Закодировать сообщение $u = (1001)$ несистематическим [8,4,4] РМ-кодом.
Решение. Кодовое слово $x = uG = (1\ 1\ 1\ 1\ 0000)$.

Пример 3. 5. Закодировать сообщение $u = (1001)$ систематическим [8,4,4] РМ-кодом.
Решение. Получим порождающую матрицу. Для этого:

а) просуммируем все строки матрицы (3.8) и запишем суммарный вектор вместо 1-ой строки матрицы (3.8)

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix};$$

в) переставим столбцы единичного веса, приведя их к единичной матрице

$$G_{8,4} = [I_k | G^*] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Проверочная матрица систематического РМ-кода имеет вид:

$$H_{8,4} = [G^{*T} | I_r] = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \qquad (3.9)$$

Из (3.9) запишем уравнения для вычисления проверочных символов:

$$x_4 = x_0 + x_1 + x_2;$$
$$x_5 = x_0 + x_1 + x_3;$$
$$x_6 = x_0 + x_2 + x_3;$$
$$x_7 = x_1 + x_2 + x_3.$$

Кодовое слово, соответствующее сообщению $u = (1001)$, есть

$$x = (10011001).$$

Пример 3.6. Удовлетворяют ли матрицы $G$ и $H$ основному уравнению кодирования? Для ответа на этот вопрос найдем произведение матриц $G$ и $H^T$ канонического вида.

$$\begin{bmatrix}1&0&0&0&1&1&1&0\\0&1&0&0&1&1&0&1\\0&0&1&0&1&0&1&1\\0&0&0&1&0&1&1&1\end{bmatrix}\begin{bmatrix}1&1&1&0\\1&1&0&1\\1&0&1&1\\0&1&1&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}=\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}.$$

Упражнения

3.1. Построить в приведено ступенчатой форме матрицы $G$ и $H$ кода с проверкой на четность $[n,(n-1),2];n=8.$

3.2. Показать, что матрицы $G$ и $G'$ порождают эквивалентные коды

$$G=\begin{bmatrix}1&1&0&0&0&0\\0&0&1&1&0&0\\0&0&0&0&1&1\end{bmatrix},G'=\begin{bmatrix}1&1&1&1&1&1\\0&1&1&0&1&1\\0&0&1&0&0&1\end{bmatrix}.$$

3.3. Построить канонические матрицы $G$ и $H$ кода с повторением $[n,1,n],n=6.$

3.7. Кодирование над полем $GF(q)$

Рассмотрим пример задания порождающей и проверочной матрицы в канонической форме над полем $GF(3)$. Необходимо построить [4,2,3]- код (троичный код), содержащий $M=3^2=9$ кодовых слов. Возможный вид порождающей матрицы

$$G=[I_k|G^*]=\begin{bmatrix}1&0&2&2\\0&1&1&2\end{bmatrix}.$$

Проверочная матрица

$$H=[-G^{*T}|I_r]=\left[-\begin{bmatrix}2&1\\2&2\end{bmatrix}\begin{matrix}1&0\\0&1\end{matrix}\right]=\begin{bmatrix}1&2&1&0\\1&1&0&1\end{bmatrix}.$$

Троичные сообщения $u$ запишем в виде матрицы

$$u=\begin{bmatrix}0&0\\0&1\\0&2\\1&0\\1&1\\1&2\\2&0\\2&1\\2&2\end{bmatrix}. \qquad (3.10)$$

Пусть необходимо закодировать сообщение $u = [21]$. Тогда

$$x_7 = [2 \quad 1]\begin{bmatrix}1 & 0 & 2 & 1\\ 0 & 1 & 1 & 1\end{bmatrix} = 2120.$$

Информационной матрице (3.10) соответствует матрица кодовых слов кода

$$x = \begin{bmatrix}0 & 0 & 0 & 0\\ 0 & 1 & 1 & 1\\ 0 & 2 & 2 & 2\\ 1 & 0 & 2 & 1\\ 1 & 1 & 0 & 2\\ 1 & 2 & 1 & 0\\ 2 & 0 & 1 & 2\\ 2 & 1 & 2 & 0\\ 2 & 2 & 0 & 1\end{bmatrix}.$$

Данный код является аддитивным групповым линейным кодом. Действительно, если $x_1 \in G$ и $x_3 \in G$, то

$$(x_1 + x_3)\mathrm{mod}3 = (0111) + (1021)\mathrm{mod}3 = x_4 = 1102 \in G.$$

Если элемент $c \in GF(q)$ или группе, то

$$cx \epsilon G.$$

Действительно, если $x_1 \in G$, $c = 2$, то

$$2(0111) = 0222 = x_2.$$

Запишем уравнение проверок для данного кода. Из основного уравнения кодирования $GH^T = 0$ ранее было получено выражение для значений проверочных символов кодов

$$\begin{bmatrix} x_k \\ \vdots \\ x_{n-1}\end{bmatrix} = -H^* \begin{bmatrix} x_0 \\ \vdots \\ x_{k-1}\end{bmatrix},$$

где

$$H = \begin{bmatrix}1 & 2 & 1 & 0\\ 1 & 1 & 0 & 1\end{bmatrix}.$$

Для рассматриваемого $[4, 2, 3]$ - кода вектор проверочных символов

$$\begin{bmatrix}x_2\\ x_3\end{bmatrix} = -\begin{bmatrix}1 & 2\\ 1 & 1\end{bmatrix}\begin{bmatrix}x_0\\ x_1\end{bmatrix} = \begin{bmatrix}2 & 1\\ 2 & 2\end{bmatrix}\begin{bmatrix}x_0\\ x_1\end{bmatrix}.$$

Элементы этого вектора вычисляются по формулам

$$x_2 = 2x_0 + x_1,$$
$$x_3 = 2x_0 + 2x_1.$$

Например, для информационного вектора $u = [21]$ получаем значения проверочных символов:

$$x_2 = 2 \cdot 2 + 1 = 2.$$
$$x_3 = 2 \cdot 2 + 2 \cdot 1 = 0.$$

Сообщению $u = [21]$ соответствует кодовое слово $x_7 = (2120)$.

### 3.8. Определение смежного класса по подгруппе

Для заданной конечной группы $G$ и подгруппы $H$ существует операция, которая устанавливает взаимосвязь между $G$ и $H$. Эта операция называется разложением группы $G$ на смежные классы по $H$. Обозначим элементы группы $G$ через $\{g_1 g_2 \dots g_N\}$, а элементы подгруппы $H$ этой группы через $\{h_1 h_2 \dots h_M\}$. Рассмотрим таблицу, построенную следующим образом:

1) запишем элементы подгруппы $H$ в строку с нейтральным элементом в качестве первого элемента строки;

2) выберем произвольным способом элемент группы $g_i$ не принадлежащий подгруппе $H$, и запишем его первым элементом второй строки;

3) просуммировав $g_i$ со всеми элементами $H$, получим вторую строку таблицы;

4) далее, выбрав произвольным способом элемент $g_i$, не принадлежащий ни первой, ни второй строке таблицы, и просуммировав его со всеми элементами $H$, получим третью строку и т. д. для всех элементов группы. Построение заканчивается тогда, когда после некоторой итерации оказывается, что каждый элемент группы $G$ записан в некоторой ячейке таблицы. В результате получается таблица.

Таблица 3.2

| $h_1 = e$ | $h_2$ | $h_3$ | … | $h_M$ |
|---|---|---|---|---|
| $h_1+g_1$ | $h_2+g_1$ | $h_3+g_1$ | … | $h_M+g_1$ |
| $h_1+g_2$ | $h_2+g_2$ | $h_3+g_2$ | … | $h_M+g_2$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $h_1+g_i$ | $h_2+g_i$ | $h_3+g_i$ | … | $h_M+g_i$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $h_1+g_j$ | $h_2+g_j$ | $h_3+g_j$ | … | $h_M+g_j$ |

Подобным способом построенная таблица называется таблицей смежных классов. Строки таблицы называются смежными классами по подгруппе $H$. Элементы первого столбца называются образующими смежных классов

(лидерами смежных классов).

Пример 3.7. Заданы группа $G$ и подгруппа $H$ группы $G$:

$$G = \langle\{0,1,2,3,4,5\}_6; +\rangle; H = \langle\{0,3\}_6; +\rangle.$$

Построить таблицу смежных классов. По определению смежного класса получим:

Таблица 3.2

| | |
|---|---|
| 0 | 3 |
| 1 | 4 |
| 2 | 5 |

Теорема 3.1. Каждый элемент группы принадлежит одному и только одному смежному классу. Теорема используется для декодирования кодов по таблице смежных классов. Декодирование основывается на анализе стандартного расположения элементов таблицы.

Утверждение 3.1. Два смежных класса не пересекаются. Объединение всех смежных классов совпадает с множеством группы $G$.

Для приведённого примера справедливы выражения:

$$(0 + H) \cap (1 + H) \cap (2 + H) = \emptyset,$$

$$(0 + H) \cup (1 + H) \cup (2 + H) = G,$$

где символ $\emptyset$ обозначает пустое множество, а символы $\cap$ и $\cup$ – соответственно операции пересечения и объединения.

Следствие из теоремы 3.1. Если $H$ – подгруппа конечной группы $G$, то число элементов в $H$ делит число элементов в $G$. Доказательство следует из прямоугольности таблицы смежных классов. Следовательно, порядок $G$ равен порядку $H$ умноженному на число смежных классов разложения $G$ по $H$.

Теорема 3.2. Ж. Лагранжа (фр. математик J. L. Lagrange, 1736-1813). Порядок любой подгруппы конечной группы является делителем порядка группы.

3.8.1. Определение смежного класса кода

Пусть имеем код $G$ над полем $GF(q)$ мощностью $M = q^k$. Для произвольного вектора $a \in \{F_n\}$ запишем выражение

$$a + G = \{a + x; x \in G\}.$$

Определение 3.5. Сумма вектора $a$ со всеми векторами $x$ множества $G$ называется смежным классом кода $G$. Произвольный вектор $b \in \{F_n\}$ находится в некотором смежном классе.

Теорема 3.3. Два вектора $a$ и $b$ лежат в одном и том же смежном классе тогда и только тогда, когда $a - b \in G$.

Действительно, если $x \in G$, $y \in G$ и $a = x + e$, $b = y + e$,

$$a - b = x + e - y - e = x - y = \{G\}.$$

Множество всех векторов $\{F_n\}$ может быть разбито на смежные классы кода $G$:

$$\{F_n\} = G \cup (a_1 + G) \cup \ldots \cup (a_t + G), \qquad (3.11)$$

где $t = q^{n-k} - 1 = q^r - 1$.

3.8.2. Таблица стандартного расположения для кода

Первая строка таблицы состоит из всех кодовых слов кода $x_1, x_2, \ldots, x_M$ (включая нулевое слово). Другие строки – это смежные классы $(a + G)$, т.е.

$$(a_1 + x_1), (a_1 + x_2), \ldots, (a_1 + x_M),$$
$$(a_2 + x_1), (a_2 + x_2), \ldots, (a_2 + x_M),$$
$$\ldots$$
$$(a_t + x_1), (a_t + x_2), \ldots, (a_t + x_M).$$

Напомним, что $a_i$ не принадлежит коду.

Таблица 3.3. Стандартное расположение для кода

| $x_1$ | $x_2$ | $x_3$ | … | $x_M$ |
|---|---|---|---|---|
| $a_1$+$x_1$ | $a_1$+$x_2$ | $a_1$+$x_3$ | … | $a_1$+$x_M$ |
| $a_2$+$x_1$ | $a_2$+$x_2$ | $a_2$+$x_3$ | … | $a_2$+$x_M$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $a_i$+$x_1$ | $a_i$+$x_2$ | $a_i$+$x_3$ | … | $a_i$+$x_M$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $a_t$+$x_1$ | $a_t$+$x_2$ | $a_t$+$x_3$ | … | $a_t$+$x_M$ |

Для $q = 2$ таблица содержит:

– $2^r$ смежных классов (строк);

– каждый смежный класс содержит $2^k$ векторов;

– $2^k$ столбцов;

– $2^r \cdot 2^k = 2^{r+k} = 2^n$ векторов длиной $n$.

Например, таблица стандартного расположения для [7,4,3]-кода Хэмминга имеет размеры 8×16 и содержит $2^3 \cdot 2^4 = 128$ элементов (векторов).

Пример 3.8. Пусть [4,2,2] – код есть подгруппа некоторой двоичной группы $F_n$.

Код предназначен для передачи сообщений:

$$u_0 = (00) \to 0;$$
$$u_1 = (10) \to 1;$$
$$u_2 = (01) \to 2;$$
$$u_3 = (11) \to 3.$$

Сообщениям $u_i$ соответствуют слова кода

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}. \qquad (3.12)$$

Стандартное расположение элементов таблицы смежных классов кода $G$ показано ниже.

Таблица 3.4

| | | | |
|---|---|---|---|
| 0000 | 1011 | 0101 | 1110 |
| 1000 | 0011 | 1101 | 0110 |
| 0100 | 1111 | 0001 | 1010 |
| 0010 | 1001 | 0111 | 1100 |

Замечание. Вектор [0001] не входит в образующие смежных классов.

### 3.8.3. Декодирование кода по таблице смежных классов

Предположим, что на вход декодера поступил вектор $y$. Этот вектор должен принадлежать некоторому смежному классу.

$$y = (a_i + x), x \in G.$$

Если было передано кодовое слово $x'$, то вектор ошибок $e$ равен

$$e = y - x' = (a_i + x - x') = (a_i + x''), x'' \in G,$$

$$e = (a_i + x'') \in (a_i + G). \qquad (3.13)$$

Из (3.13) следует, что возможными векторами ошибок являются все векторы из смежного класса, содержащего $y$.

Стратегия декодирования кодов будет следующей:

– необходимо выбрать из смежного класса, содержащего $y$, вектор $e$ с наименьшим весом;

– декодировать $y$ как $x = y - e$.

Замечания.

1. Вектор из смежного класса, имеющий минимальный вес, называется

лидером смежного класса. Лидер смежного класса есть вектор ошибок $e$.

2. Если имеется более одного вектора с минимальным весом, то в качестве лидера смежных классов выбирается любой из таких векторов.

3. В формуле (3.13) лидерами смежных классов являются векторы $a_i$.

Пример 3.9. Декодировать входной вектор по таблице 3.4. На вход декодера поступает вектор $y = [0110]$.

Вектор [0110] принадлежит смежному классу – второй строке таблицы 3.4. Этому классу соответствует лидер смежного класса $e = [1000]$.

Тогда переданным кодовым словом является

$$x^T = y^T - e^T = \begin{bmatrix}0\\1\\1\\0\end{bmatrix} - \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}1\\1\\1\\0\end{bmatrix}.$$

Из таблицы 3.4 также видно, что векторы [0100] и [0001] принадлежат одному и тому же смежному классу (третья строка таблицы 3.4) поскольку их разность

$$\begin{bmatrix}0\\1\\0\\0\end{bmatrix} - \begin{bmatrix}0\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\1\end{bmatrix} = x_2$$

есть кодовый вектор кода (3.13). Если рассматривать эти векторы в качестве векторов ошибок, то соответствующие им конфигурации ошибок (с минимальным одинаковым весом) не могут быть исправленными. Обе конфигурации можно выбрать в качестве лидеров своего смежного класса. Ввиду неоднозначного определения лидера смежного класса невозможно исправление ошибок этих конфигураций. О корректирующей способности рассмотренного кода говорят, что он исправляет не все ошибки веса 1, а только однократные определенной конфигурации. Это справедливо во всех случаях, когда используются кодовые слова веса 2. Поскольку только минимальный вес $\min wt(x) = d = 3$ является необходимым и достаточным условием для исправления всех конфигураций одиночных ошибок.

## 4. Декодирование линейных кодов

Известны и применяются четыре основных метода декодирования:

1) декодирование по синдрому;

2) декодирование по максимальному правдоподобию;

3) спектральное декодирование;

4) мажоритарное декодирование или декодирование по большинству проверок.

Первый и четвертый методы применяются для коррекции независимых, модульных и пакетных ошибок кратностью $t = 1 \div 4$. Второй и четвертый

методы декодирования используются, как правило, в радиоэлектронных системах, работающих при низких отношениях сигнал/помеха на входе декодера, сложной помеховой обстановке.

## 4.1. Декодирование по синдрому

Определение 4.1. Вектор $s = Hy^T$ называется синдромом вектора $y$, где $y$ – вектор на входе декодера.

Свойства синдрома.

1. Синдром $s$ – представляет собой вектор-столбец размером $(n-k) \times 1$.

2. Синдром $s$ равен нулю, если и только если $y$ – кодовое слово кода.

Пусть $y = x + e$, где $x \in G$.

$$s = Hy^T = H(x+e)^T = Hx^T + He^T = He^T. \qquad (4.1)$$

3. Если в кодовом слове имеются ошибки на позициях с номерами $a, b, c, \ldots$ так, что $e = [0 \ldots \overset{a}{\overset{\frown}{1}} \ldots \overset{b}{\overset{\frown}{1}} 00 \ldots \overset{c}{\overset{\frown}{1}} \ldots 00]$, то из (4.1) получаем, что

$$s = \sum_i e_i H_i = H_a + H_b + H_c + \cdots,$$

где $H_i$ $i$ – ый столбец матрицы $H$. Вычисление синдрома можно рассматривать как линейное преобразование вектора ошибок.

Теорема 4.1. Для двоичного кода синдром равен сумме тех столбцов матрицы $H$, где произошли ошибки.

Замечание. Вектор $s$ называется синдромом, так как выделяет совокупность ошибок (гр. Syndrome – стечение). Синдром кодового слова является индикатором вектора ошибок.

Теорема 4.2. Имеется взаимно однозначное соответствие между синдромами и смежными классами, а именно: два вектора находятся в одном и том же смежном классе кода $G$, если и только если имеют один и тот же синдром.

Действительно, векторы $a$ и $b$ находятся в одном смежном классе, если и только если $(a-b) \in G$, что эквивалентно $H(a-b)^T = 0$, или $Ha^T = Hb^T$.

Пусть имеется код мощностью $M = q^k$. Кодовые слова множества $\{x\}=\{x_1, x_2, \ldots, x_s, \ldots, x_M\}$ передаются по каналу с шумами. На вход декодера поступает множество векторов $\{y\} = \{x + e\}$.

Таблица стандартного расположения для кода $\{x\}$ вместе со столбцом синдромов будет иметь вид

Таблица 4.1

| $x_1$ | $x_2$ | $x_3$ | … | $x_s$ | … | $x_M$ | $s_0$ |
|---|---|---|---|---|---|---|---|
| $e_1$+$x_1$ | $e_1$+$x_2$ | $e_1$+$x_3$ | … | $e_1 + x_s$ | … | $e_1$+$x_M$ | $s_1$ |
| $e_2$+$x_1$ | $e_2$+$x_2$ | $e_2$+$x_3$ | … | $e_2 + x_s$ | … | $e_2$+$x_M$ | $s_2$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $e_i$+$x_1$ | $e_i$+$x_2$ | $e_i$+$x_3$ | … | $e_i + x_s$ | … | $e_i$+$x_M$ | $s_i$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $e_t$+$x_1$ | $e_t$+$x_2$ | $e_t$+$x_3$ | … | $e_t + x_s$ | … | $e_t$+$x_M$ | $s_t$ |

Здесь $s_1$ – вектор одиночных ошибок; синдром $s_t$ соответствует исправлению $t$ ошибок (сфере декодирования). Если принимаются векторы

$$y_s = e_i + x_s$$
$$y_j = e_i + x_j,$$

то соответствующие им синдромы равны

$$s_{i_s} = Hy_s^T = Hx_s^T + He_i^T = He_i^T,$$
$$s_{i_j} = Hy_j^T = Hx_j^T + He_i^T = He_i^T.$$

Таким образом, $s_{i_s} = s_{i_j}$

Пример 4.1. Найти соответствие между синдромами и смежными классами [4,2,2]-кода (таблица 3.4)

После вычисления синдромов, таблица примет вид

Таблица 4.2

| | | | | |
|---|---|---|---|---|
| 0000 | 1011 | 0101 | 1110 | $s = \begin{bmatrix}0\\0\end{bmatrix}$ |
| 1000 | 0011 | 1101 | 0110 | $s = \begin{bmatrix}1\\1\end{bmatrix}$ |
| 0100 | 1111 | 0001 | 1010 | $s = \begin{bmatrix}0\\1\end{bmatrix}$ |
| 0010 | 1001 | 0111 | 1100 | $s = \begin{bmatrix}1\\0\end{bmatrix}$ |

Алгоритм декодирования по синдрому состоит в следующем. Синдром позволяет определить, в каком смежном классе находится принятый вектор $y$. Зная смежный класс, определяется вектор ошибок $e$ и, следовательно, искомое кодовое слово и соответствующее ему сообщение. Правило декодирования состоит из операций:

$$s_{i_s} = Hy_s^T;$$

$s_{i_s} \to e_i$ **лидер смежного класса;**

$x_s = y_s - e_i;$

$x_s \to u_s$ сообщение.

По свойству 2 синдрома декодирование состоит в сравнении синдромов с нулем. Для этого:

а) вычисляются проверочные символы, используя принятые информационные;

б) сравниваются полученные проверочные символы с принятыми проверочными.

Замечание. Следствием а) является то, что синдромный декодер содержит кодирующее устройство.

Если в качестве образующих выбраны векторы, имеющие минимальный вес в своем смежном классе, то декодирование по синдрому совпадает с декодированием по минимуму расстояния Хэмминга. В этом случае обеспечивается минимальная вероятность ошибки декодирования в двоично-симметричном канале.

Тот факт, что все элементы одного и того же смежного класса имеют один и тот же синдром, позволяет упростить процедуру декодирования в сравнении с декодированием по таблице стандартного расположения для кода. Сравним техническую сложность декодирования по таблице смежных классов и синдромного декодированием также с использованием таблицы синдромов.

Процесс декодирования по таблице стандартного расположения для кода требует память объемом

$$V = n2^n \text{ бит.}$$

Таблица стандартного расположения содержит $2^r$ смежных классов или $2^r$ разных синдромов. Для хранения всех векторов столбца лидеров смежных классов потребуется объем памяти величиной

$$V' = n2^r \text{ бит.}$$

Выигрыш по объему памяти декодера составит значение

$$L = \frac{V}{V'} = 2^k.$$

## 4.2. Коды Хэмминга

Для практических целей желательно иметь код, который можно легко кодировать и декодировать. Важным семейством кодов, которые отвечают этому требованию, является семейство кодов Хэмминга, исправляющие одну ошибку.

Теорема 4.3. Коды Хэмминга являются совершенными кодами.

Согласно теореме 4.1, синдром принятого вектора равен сумме тех столбцов матрицы $H$, где произошли ошибки. Для того, чтобы построить код, исправляющий одну ошибку, необходимо выбрать столбцы матрицы $H$

следующим образом:

– столбцы должны быть ненулевыми (иначе ошибка в этой позиции будет необнаруженной);

– столбцы должны быть различными (иначе, если два столбца матрицы $H$ одинаковы, то ошибки в соответствующих двух позициях будут неразличимы).

Если матрица $H$ имеет $r$ строк, то существует только $2^r - 1$ допустимых ненулевых двоичных векторов длиной $r$. Проверочная матрица кода Хэмминга содержит столбцы, которые являются двоичными представлениями чисел от 1 до $r$.

Параметры кода Хэмминга:

– длина $2^r - 1, r = 2,3, \ldots$;

– размерность $k = 2^r - 1 - r$;

– кодовое расстояние $d = 3$;

– распределение лидеров смежных классов веса $a_{i=0} = 1, a_{i=1} = n$.

В таблице 4.3 приведены значения некоторых параметров семейства кодов Хэмминга.

Таблица 4.3

| $r$ | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|
| $n$ | 7 | 15 | 31 | 63 | 127 |
| $k$ | 4 | 11 | 26 | 57 | 120 |

## 4.3. Формы представления матрицы $H$ кода Хэмминга

1. Классическая (несистематический код Хэмминга). Например,

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \qquad (4.2)$$

Используя такую матрицу, в которой $i$ -ый столбец $H_i$ равен двоичному представлению числа $i$, по синдрому легко определяется номер ошибочного символа принятого слова.

Замечание. Более простой технической реализацией алгоритма синдромного декодирования, чем по матрице классического вида не существует.

2. Приведенно-ступенчатая (систематический код Хэмминга). Например,

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

Из этой матрицы легко можно получить порождающую матрицу [7,4,3]-кода Хэмминга.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

## 4.4. Представление элементов поля Галуа $GF(q^m)$

Удобное описание многих вычислительных алгоритмом, процессов помехоустойчивого и криптографического кодирования и декодирования реализуется с помощью, степенного, полиномиального, векторного и логарифмического представления элементов расширенного поля Галуа.

Элементы поля $GF(q^m)$ могут интерпретироваться как класс вычетов полиномов от $x$ с коэффициентами из $GF(q)$ по модулю неприводимого над $GF(q)$ полинома степени $m$.

Пример 4.2. Определим основные операции в поле неприводимого над полем $GF(2)$ полинома $p(x) = 1 + x + x^2, m = 2$.

Операция сложения в поле $GF(2^2)$, элементы которого записываются в виде полиномов, задается в виде

Таблица 4.4

| + | 0 | 1 | $x$ | $1 + x$ |
|---|---|---|---|---|
| 0 | 0 | 1 | $x$ | $1 + x$ |
| 1 | 1 | 0 | $1 + x$ | $x$ |
| $x$ | $x$ | $1 + x$ | 0 | 1 |
| $1 + x$ | $1 + x$ | $x$ | 1 | 0 |

Записывая коэффициенты полиномов, получим следующее соответствие между полиномами и двоичными векторами:

Таблица 4.5

| | |
|---|---|
| 0 | 0 0 |
| 1 | 1 0 |
| $x$ | 0 1 |
| $1 + x$ | 1 1 |

Таблица Кэли в поле $GF(2^2)$, элементы которого записываются в виде двоичных чисел, имеет вид

Таблица 4.6

| + | 0 0 | 1 0 | 0 1 | 1 1 |
|---|---|---|---|---|
| 0 0 | 0 0 | 1 0 | 0 1 | 1 1 |
| 1 0 | 1 0 | 0 0 | 1 1 | 0 1 |
| 0 1 | 0 1 | 1 1 | 0 0 | 1 0 |
| 1 1 | 1 1 | 0 1 | 1 0 | 0 0 |

Аналогично построим таблицы умножения элементов поля $GF(2^2)$. Операция умножения в поле $GF(2^2)$, элементы которого записываются в виде полиномов, задается в виде

Таблица 4.7

| × | 0 | 1 | $x$ | $1+x$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $x$ | $1+x$ |
| $x$ | 0 | $x$ | $1+x$ | 1 |
| $1+x$ | 0 | $1+x$ | 1 | $x$ |

Таблица умножения, представленная двоичными векторами, имеет вид

Таблица 4.8

| × | 0 0 | 1 0 | 0 1 | 1 1 |
|---|---|---|---|---|
| 0 0 | 0 0 | 0 0 | 0 0 | 0 0 |
| 1 0 | 0 0 | 1 0 | 0 1 | 1 1 |
| 0 1 | 0 0 | 0 1 | 1 1 | 1 0 |
| 1 1 | 0 0 | 1 1 | 1 0 | 0 1 |

Например, элемент таблицы 10 с координатами (01, 11) получен следующим образом.

1. Воспользуемся обычным умножением в «столбик» со старшим разрядом числа слева:

$$\begin{array}{r} 10 \\ \underline{11} \\ 1\,0 \\ \underline{1\,0} \\ 1\;\;1\,0. \end{array}$$

2. Результат умножения приведем по модулю полинома $p(x)$ (вектора – коэффициентов $p(x)$):

$$\begin{array}{l} \underline{1\,1\,0|}\;\underline{1\,1\,1} \\ \underline{1\,1\,1}\;\;1 \\ 0\;\;0\,1. \end{array}$$

3. Выполним инверсию двоичного числа: 0 0 1|1 0 0. Получим вектор 1 0.

Теорема 4.4. В расширенном поле полиномов $GF(q^m)$ существует примитивный элемент $\alpha$ порядка $(q^m-1)$, т.е.

$$\alpha^{(q^m-1)} = 1.$$

Каждый элемент $\beta$ поля $GF(q^m)$ может быть представлен как некоторая степень $\alpha$, т.е. $\beta = \alpha^i$.

Теорема 4.5. Если $\alpha$ – примитивный элемент поля, то $\alpha^\kappa$ тоже примитивный элемент, если $\kappa$ и $q^m$ – взаимно простые числа. Тогда в поле $GF(q^m)$ имеется $\varphi(q^m - 1)$ примитивных элементов.

Пример 4.3. Пусть $GF(2^3)$ – расширенное поле Галуа. Найти примитивные элементы поля.

Решение. Функция Эйлера $\varphi(2^3 - 1) = \varphi(7) = 6$. Следовательно, поле содержит 6 примитивных элементов. Примитивным элементом поля является элемент $\alpha^\kappa$, где $\kappa$ и $q^m = 2^3 = 8$ – взаимно простые числа. (НОД) $d$ = (8, 3) = (8, 5) = 1. Тогда $\alpha^3$ $\alpha^5$ – примитивные элементы. Заметим, что $\alpha^7 \equiv ((1))$.
$\alpha^5, (\alpha^5)^2 = \alpha^3, (\alpha^5)^3 = \alpha, (\alpha^5)^4 = \alpha^6, (\alpha^5)^5 = \alpha^4, (\alpha^5)^6 = \alpha^2, (\alpha^5)^7 = 1.$

Определение 4.2. Неприводимый над полем $GF(q)$ полином степени $m$ называется примитивным, если его корнем является примитивный элемент $\alpha$ поля $GF(q^m)$.

Пример 4.4. Полином $p(x) = 1 + x + x^2$ неприводим над полем $GF(2)$. Этот полином примитивный, так как примитивный элемент $\alpha$ поля $GF(q^m)$ является корнем $p(x)$. Действительно,
$p(\alpha) = 1 + \alpha + \alpha^2 = 0$, так как $x^2 \equiv (1 + x)\ mod\ (1 + x + x^2)$. Тогда $p(\alpha) = 1 + \alpha + \alpha^2 = 1 + \alpha + 1 + \alpha = 0$.

В таблице 4.9 приведены четыре формы представления элементов поля $GF(2^2)$. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x) = 1 + x + x^2$. Порядок элемента $\alpha$ равен 3, так как $\alpha^{(2^2-1)} = \alpha^3 \equiv 1\ mod\ (1 + \alpha + \alpha^2)$.

Таблица 4.9 – Формы представления элементов поля $GF(2^2)$.

| В виде степени примитивного элемента | В виде полинома | В виде двоичного числа | В виде логарифма |
|---|---|---|---|
| – | 0 | 0 0 | – |
| $\alpha^0$ | 1 | 1 0 | 0 |
| $\alpha^1$ | $\alpha$ | 0 1 | 1 |
| $\alpha^2$ | 1 + $\alpha$ | 1 1 | 2 |

Используя разные формы элементов поля можно эффективно производить алгебраические операции в поле $GF(q^m)$.

1. Умножение с представлением элементов поля в виде степеней примитивного элемента выполняется следующим образом:

$$\beta_1 \cdot \beta_2 = \alpha^i \cdot \alpha^j = \alpha^{i+j} = ((\alpha^{Rest\left[\frac{i+j}{N}\right]})),$$

где $Rest\left[\frac{i+j}{N}\right]$ – остаток от деления $(i+j)$ на порядок $N$ примитивного элемента $\alpha$ поля $GF(q^m)$. Например, используя таблицу 4.9, имеем

$$\alpha^2 \cdot \alpha^2 = \alpha^4 = \alpha^1.$$

2. Деление на элемент поля

Теорема 4.6. Если полином $p(x)$ степени $m$ неприводим над полем $GF(q)$, то каждый ненулевой полином $c(\alpha)$ степени не более $(m-1)$ имеет единственный обратный полином $c(\alpha)^{-1}$такой, что

$$c(\alpha) \cdot c(\alpha)^{-1} \equiv 1 mod\ p(\alpha).$$

Нахождение обратных элементов легко выполнять, если воспользоваться представлением элементов поля в виде степеней примитивного элемента или логарифмов. Пусть $c = c(\alpha) -$ произвольный элемент поля $GF(q^m)$ с коэффициентами из поля $GF(q)$, т.е.

$$c = c(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{m-1}\alpha^{m-1}.$$

Требуется разделить элемент $c$ на элемент поля

$$b = b_0 + b_1\alpha^1 + b_2\alpha^2 + \cdots + b_{m-1}\alpha^{m-1}.$$

Для того чтобы найти $c/b$, вычислим обратный элемент $b^{-1} = 1/b$, а затем представим

$$c/b = \text{с}\cdot 1/b.$$

Пример 4.5. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x) = 1 + x + x^2$. Вычислить $\alpha/1 + \alpha$.

Решение. Полиному $(1+\alpha)$ соответствует $\alpha^2$. Тогда $(\alpha/1+\alpha) = \frac{\alpha}{\alpha^2} = \alpha^{-1} =$

$$= \alpha^3\alpha^{-1} = \alpha^2 = 1 + \alpha.$$

Пример 4.6. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x) = 1 + x + x^3$. Вычислить $\sqrt{110}$.

Решение. Вектору (110) соответствует элемент поля $\alpha^3$. Квадратный корень $\sqrt{\alpha^3} = \sqrt{1\alpha^3} = \sqrt{\alpha^7\alpha^3} = \sqrt{\alpha^{10}} = \alpha^5 = 111$.

Упражнения

4.1. Найти все примитивные элементы расширенного поля Галуа $GF(2^4)$.

4.2. Привести четыре формы представления элементов поля $GF(2^4)$. Поле образовано неприводимым над полем $GF(2)$ полиномом $p(x) = 1 + x + x^4$.

4.3. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x) = 1 + x + x^3$. Вычислить:

а) полином, обратный полиному $a = 1 + \alpha + \alpha^2$;

б) полином, обратный полиному $b = \alpha + \alpha^2$;

в) $a / b$;

г) $\sqrt{\alpha + \alpha^2}$;

д) $(111)^{-1}$.

4.5. Задание кода Хэмминга с помощью элементов расширенного поля Галуа $GF(2^m)$

Если $\alpha$ – примитивный элемент поля $GF(2^m)$, то все элементы поля различны и представляются ненулевыми двоичными векторами. Это свойство используется для построения проверочной матрицы кода Хэмминга,

$$H = [1 \quad \alpha \quad \alpha^2 \quad \dots \quad \alpha^{2^m-2}].$$

Пример 4.7. Пусть $\alpha \in GF(2^3)$ – корень уравнения $\alpha^3 + \alpha + 1 = 0$. Тогда

$$H = [1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6].$$

Все элементы поля могут быть представлены как различные ненулевые двоичные $m$-векторы. Проверочная матрица двоичного [7, 3, 4] – кода Хэмминга записывается как

$$H = \begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{matrix}$$
$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Сопоставим каждому вектору $c = (c_0, c_1, \dots, c_{n-1})$ из некоторого конечного поля $F^n$ многочлен $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$. Например, коду

$$G = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

соответствует множество многочленов вида

$$c(x) = \begin{Bmatrix} 0 & & & & \\ 1 & + & x & & \\ & & x & + & x^2 \\ 1 & + & & & x^2 \end{Bmatrix}.$$

Из свойств синдрома следует, что вектор $c = (c_0, c_1, \dots, c_{n-1})$ принадлежит коду, Хэмминга, $c \in G$ тогда и только тогда, когда нулевое значение синдрома

$$S = Hc^T = 0.$$

Это условие можно записать и следующим образом:

$$\rightleftarrows \sum_{i=0}^{n-1} c_i \alpha^i = 0;$$

$$\rightleftarrows c(\alpha) = 0, \qquad (4.3)$$

где $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$.

Пример 4.8. Пусть $H = [1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6]$, $\alpha \in GF(2^3)$ – корень уравнения $x^3 + x + 1 = 0$. Синдром равен

$$S = [1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6] \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} =$$

$$= c_0 + \alpha c_1 + \alpha^2 c_2 + \alpha^3 c_3 + \alpha^4 c_4 + \alpha^5 c_5 + \alpha^6 c_6 = \sum_{i=0}^{n-1} c_i \alpha^i = 0.$$

Если многочлен $c(x)$ принадлежит коду, то примитивный элемент поля $GF(2^r)$ является корнем этого многочлена и выполняется условие (4.3). Например, для некоторого кодового слова выполняется равенство

$$c_l(x) = 1 + x + x^3 \rightarrow c_l(\alpha) = 1 + \alpha + \alpha^3 = 1 + \alpha + 1 + \alpha = 0.$$

Любой многочлен $c(x) \in G$ определяется уравнением кодирования в поле многочленов

$$c(x) = g(x) f(x),$$

где $g(x)$ – порождающий многочлен степени $r$ ($\deg g(x) = r$), $f(x)$ – информационный многочлен степени ($\deg f(x) \leq n - r - 1$).

Пример 4.9. Задан порождающий многочлен кода Хэмминга $g(x) = 1 + x + x^3$ над полем $GF(2)$. Информационный многочлен $f(x) = 1 + x$.
Соответствующее кодовое слово кода Хэмминга

$$c(x) = g(x) f(x) = (1 + x + x^3)(1 + x) = 1 + x^2 + x^3 + x^4.$$

Слово принадлежит коду, т.к.

$$c(\alpha) = 1 + \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha^2 + 1 + \alpha + \alpha + \alpha^2 = 0$$

Этому слову соответствует вектор

$$c = (1011100).$$

Пример 4.10. Найти элементы синдрома $s^T = (s_0 s_1 s_2)$, используя форму (4.2) матрицы $H$, для входного вектора $y = (y_0 y_1 y_2 y_3 y_4 y_5 y_6)$.

$$H(y_0 y_1 y_2 y_3 y_4 y_5 y_6)^T = (s_0 s_1 s_2)^T$$

$$s_0 = y_0 + y_2 + y_4 + y_6,$$
$$s_1 = y_1 + y_2 + y_5 + y_6,$$
$$s_2 = y_3 + y_4 + y_5 + y_6.$$

На рисунке 4.2 показана функциональная схема вычисления синдрома

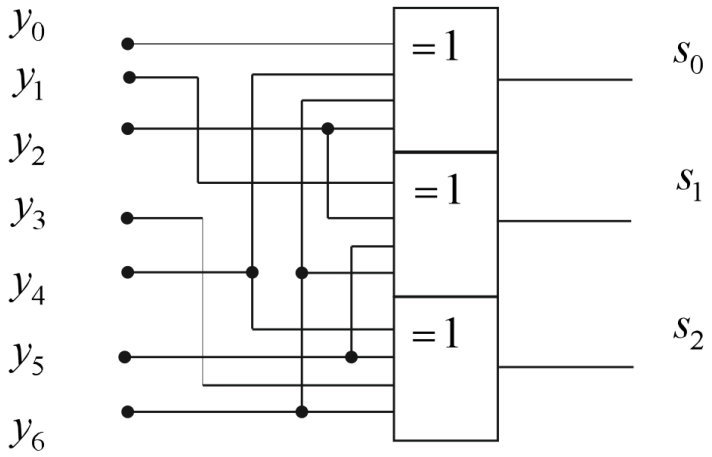



Рисунок 4.2 – Вычислитель синдрома

Упражнение 4.4. Записать все кодовые слова [7,4,3]- кода Хэмминга, используя $g(x) = 1 + x^2 + x^3$ над полем $GF(2)$.

Упражнение 4.5. Построить проверочную матрицу кода (упражнение 4.4), используя элементы расширенного поля $GF(2^3)$. Поле порождается многочленом $g(x) = 1 + x^2 + x^3$.

## 4.6. Коррекция двукратных ошибок

Согласно границе Синглтона для минимального кодового расстояния любого линейного $[n, k, d]$-кода, кодовое расстояние удовлетворяет равенству

$$d \leq 1 + n - k.$$

Напомним простое доказательство этого утверждения. Ненулевое слово минимального веса в коде имеет вес

$$\min\{\mathrm{wt}(u)\} = d\,, u \neq 0, u \in G.$$

Кодовое слово систематического кода с одним ненулевым информационным символом и $(n-k)$ проверочными символами не может иметь вес больший величины $(1+n-k)$. Следовательно, минимальный вес кода не может быть больше чем

$$d \leq 1 + n - k.$$

Подставляя значение $d \geq 2t+1$ в последнее выражение, получаем

$$2t + 1 \leq 1 + n - k = 1 + r,$$

$$r \geq 2t.$$

Исправление $t$ ошибок требует использования не менее $2\,t$ проверочных символов. Для исправления двукратных ошибок нужно иметь не менее $2\,t = 4$ проверочных символов.

Код Хэмминга исправляет одиночные ошибки. Двоичный код Хэмминга длиной $n = 2^r - 1$ имеет $r$ проверочных символов. Проверочная матрица этого кода имеет $r$ строк. Построим на его основе код, исправляющий две ошибки. Естественно предположить, что его проверочная матрица будет иметь $2r$ строк. Проверочную $H'$ матрицу кода, исправляющего две ошибки, построим исходя из следующего. Пусть $n = 7,\ r = 3$. Первую строку матрицы $H'$ запишем в виде строки

$$[1,2,\dots,i,\dots,j,\dots,7].$$

Здесь обозначениям $i$ и $j$ соответствуют двоичные векторы-столбцы длиной 3 кода Хэмминга. Добавим еще одну строку, записанную таким способом:

$$[f(1), f(2), \dots, f(i), \dots, f(j), \dots, f(7)],$$

где $f(i)$ и $f(j)$ также некоторые двоичные векторы-столбцы матрицы длиной 3 кода Хэмминга. Матрица $H'$будет иметь вид

$$H' = \begin{bmatrix} 1, & 2, & \dots, & i, & \dots, & j, & \dots, & 7 \\ f(1), f(2), \dots, f(i), \dots, f(j), \dots, f(7) \end{bmatrix},$$

где $H_i = \begin{bmatrix} i \\ f(i) \end{bmatrix}$ и $H_j = \begin{bmatrix} j \\ f(j) \end{bmatrix}$ – есть векторы-столбцы длиной 6. Какой должна быть функция $f(i)$, чтобы по форме (структуре) синдрома однозначно определить местоположение двукратных ошибок.

Предположим, что произошли две ошибки на позициях $i$ и $j$. Синдром пример форму $S = (\frac{S_1}{S_2})$, где $S_1$и $S_2$ – это части синдрома, соответствующие первой и второй строке матрицы $H'$. По форме синдрома $S = (\frac{S_1}{S_2})$ декодер

должен определить $i$ и $j$, т.е. найти решения уравнений

$$\begin{cases} i + j = S_1 \\ f(i) + f(j) = S_2 \end{cases} \tag{4.4}$$

относительно $i$ и $j$ при заданных $S_1$и $S_2$. Напомним, что $i, j, f(i), f(j), S_1, S_2$ являются элементами расширенного поля Галуа $GF(2^r)$. Пусть код Хэмминга задается примитивным неприводимым многочленом $p(x) = 1 + x + x^3$ степени 3 над полем $GF(2)$. Необходимо так выбрать функции $f(i), f(j)$ в системе уравнений (4.4), чтобы она имела решения в поле $GF(2^3)$. Рассмотрим несколько вариантов решений (4.4).

1) $\begin{cases} i + j = S_1 \\ ci + cj = S_2 \end{cases}$, (4.5)

где $f(i) = ci, f(j) = cj, c \in GF(2)$.

Система (4.5) не имеет решения, так как невозможно выразить $i$ и $j$ через $S_1$ и $S_2$. Действительно, из первого уравнения имеем

$$i = S_1 - j.$$

Подставляя значение $i$ во второе уравнение, получаем

$$c(S_1 - j) + cj = S_2,$$
$$cS_1 = S_2$$

Замечание. Одним из возможных способов нахождения корней уравнения (4.4) является проверка по очереди каждого элемента поля.

2) Пусть $f(i) = i^2, f(j) = j^2$.
Тогда система (4.4) примет вид

$$\begin{cases} i + j = S_1, \\ i^2 + j^2 = S_2 \end{cases}. \tag{4.6}$$

Так как в поле коэффициентов $GF(2)$

$$(i + j)^2 = i^2 + 2ij + j^2 = i^2 + j^2,$$

то система уравнений

$$\begin{cases} i + j = S_1, \\ (i + j)^2 = S_2 \end{cases},$$
$$S_1^2 = S_2$$

также не имеет решения.
3) Далее рассмотрим такой вариант функциональной зависимости

$$f(i) = i^3, f(j) = j^3.$$

Систему уравнений (4.4) представим в виде

$$\begin{cases} i + j = S_1, \\ i^3 + j^3 = S_2 \end{cases}. \qquad 4.7$$

В алгебре полиномов с коэффициентами из $GF(2)$

$$a^3 + b^3 = (a + b)(a^2 + ab + b^2) = a^3 + a^2b + ab^2 + ba^2 + b^2a + b^3 =.$$
$$= a^3 + 2a^2b + 2ab^2 + b^3 = a^3 + b^3.$$

Систему уравнений (4.7) представим в виде

$$\begin{cases} i + j = S_1, \\ i^3 + j^3 = (i + j)(i^2 + ij + j^2) = S_2 \end{cases}. \qquad (4.8)$$

Систему (4.8) перепишем следующим образом:

$$\begin{cases} i + j = S_1; \\ i^3 + j^3 = (i + j)[(i^2 + j^2) + ij] = S_2 \end{cases}.$$

После преобразования уравнений имеем

$$\begin{cases} i + j = S_1, \\ S_1[{S_1}^2 + ij] = S_2 \end{cases};$$

$$\begin{cases} i + j = S_1 \\ ij = \frac{S_2}{S_1} + {S_1}^2 \end{cases}. \qquad (4.9)$$

Напомним из алгебры, что для приведенного квадратного уравнения

$$x^2 + px + q = 0$$

произведение корней $(x_1 \cdot x_2) = q$, а сумма корней $(x_1 + x_2) = -p$. Если рассматривать

$$ij = q = \frac{S_2}{S_1} + {S_1}^2,$$
$$(i + j) = -p = S_1,$$

то $i$ и $j$ являются корнями квадратного уравнения

$$x^2 + S_1x + \frac{S_2}{S_1} + {S_1}^2 = 0, S_1 \neq 0. \qquad (4.10)$$

4.6.1. Алгоритм декодирования кода, исправляющего две ошибки

По принятому вектору $Y = X + E$ вычисляется синдром

$$S = HY^T = (\frac{S_1}{S_2}).$$

1. Если $S_1 = S_2 = 0$, то ошибок нет.

2. Если $S_1 \neq 0$, а $S_2 = i^3 = {S_1}^3$, то произошла одиночная ошибка на позиции $i = S_1$, которая исправляется. При возникновении одиночной ошибки номера $j$ нет.

3. Если $S_1 \neq 0$, $S_2 \neq 0$, а $S_2 \neq {S_1}^3$, то формируется признак неодиночной ошибки и составляется квадратное уравнение (4.10). Если уравнение имеет два различных корня $x_1 = i$ и $x_2 = j$, то исправляются ошибки на этих позициях.

4. Если уравнение (4.10) не имеет корней или $S_1 = 0$, а $S_2 \neq 0$, то событие идентифицируется как обнаружение ошибок (произошло, по крайней мере, три ошибки).

Замечание. Общие формулы, выражающие корни алгебраических уравнений вида $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$через их коэффициенты $c_i$ и содержащие только конечное число сложений, вычитаний, делений, умножений и извлечений корня, существуют только для уравнений степеней: первой (линейные уравнения), второй (квадратные уравнения), третьей (кубические уравнения) и четвёртой (уравнения четвёртой степени). В нашем случае, один из возможных путей отыскания корней в поле $GF(2^r)$ – подстановка по очереди каждого элемента поля.

### 4.6.2. БЧХ-код, исправляющий две ошибки

Пусть задана проверочная матрица [7,4,3]-кода Хэмминга; $\alpha$ – примитивный элемент поля $GF(2^r)$ есть корень уравнения $\alpha^3 + \alpha + 1 = 0$ Проверочная матрица БЧХ-кода, исправляющего две ошибки записывается в виде

$$H = \begin{bmatrix} 1 & \alpha & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} \end{bmatrix}. \qquad (4.11)$$

С учетом свойства периодичности элементов поля для примитивного элемента, когда $\alpha^{2^r-1} = 1, \alpha^7 = 1$, матрица (4.11) преобразуется как

$$H = \begin{bmatrix} 1 & \alpha & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{bmatrix}. \qquad (4.12)$$

Замечания.

1. Элемент $\alpha$ действительно является примитивным элементом поля, т.к. и во второй строке матрицы (4.12) появляются все степени $\alpha$;

2. БЧХ-код может строиться и с помощью порождающего элемента расширенного поля Галуа $GF(2^r)$. В этом случае не все степени $\alpha$ появляются

во второй строке.

Используя двоичное представление элементов поля, проверочную матрицу $H$ представим в следующей форме:

$$H' = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}. \qquad (4.13)$$

Пример 4.11. Декодирование БЧХ-кода

1. Пусть произошли две ошибки на позициях 1 и 6 (нумерация начинается с нуля). Им соответствуют столбцы матрицы (4.15):

$$1\rightarrow \begin{bmatrix} \alpha \\ \alpha^3 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}; 6\rightarrow \begin{bmatrix} \alpha^6 \\ \alpha^4 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix};$$

Находим $$S_1 = i + j = \alpha + \alpha^6 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \alpha^5$$

и

$$S_2 = i^3 + j^3 = \alpha^3 + \alpha^4 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \alpha^6.$$

Так как $S_1 \neq 0$, $S_2 \neq 0$, а $S_2 \neq {S_1}^3$, то формируется признак неодиночной ошибки и составляется квадратное уравнение (4.10).

$$x^2 + S_1 x + \frac{S_2}{S_1} + {S_1}^2 = 0, S_1 \neq 0.$$

Вычисляем свободный член уравнения

$$\frac{S_2}{S_1} + {S_1}^2 = \frac{\alpha^6}{\alpha^5} + {\alpha^5}^2 = \alpha + \alpha^3 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \alpha^0.$$

Квадратное уравнение для нахождения $i$ и $j$ имеет вид

$$x^2 + \alpha^5 x + \alpha^0 = 0.$$

Корнями этого уравнения являются $\alpha$ и $\alpha^6$. Действительно, разложение на линейные двучлены уравнения приводит к тождеству

$$x^2 + \alpha^5 x + \alpha^0 = (x - \alpha)(x - \alpha^6) = x^2 - x\alpha^6 - \alpha x + \alpha^7 =$$
$$= x^2 - x(\alpha^6 + \alpha) + \alpha^0 = x^2 + x\left(\begin{bmatrix}1\\0\\1\end{bmatrix} + \begin{bmatrix}0\\1\\0\end{bmatrix} = \begin{bmatrix}1\\1\\1\end{bmatrix}\right) + \alpha^0 =$$
$$= x^2 + \alpha^5 x + \alpha^0.$$

2. Предположим, произошли три ошибки на позициях 0, 1 и 6. Им соответствуют столбцы матрицы (4.15):

$$0\rightarrow \begin{bmatrix}\alpha^0\\ \alpha^0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\1\\0\\0\end{bmatrix}; 1\rightarrow \begin{bmatrix}\alpha\\ \alpha^3\end{bmatrix} = \begin{bmatrix}0\\1\\0\\1\\1\\0\end{bmatrix}; 6\rightarrow \begin{bmatrix}\alpha^6\\ \alpha^4\end{bmatrix} = \begin{bmatrix}1\\0\\1\\0\\1\\1\end{bmatrix};$$

Находим составляющие $S_1$ и $S_2$ синдрома $S$.

$$S_1 = z + i + j = \alpha^0 + \alpha + \alpha^6 = \begin{bmatrix}1\\0\\0\end{bmatrix} + \begin{bmatrix}0\\1\\0\end{bmatrix} + \begin{bmatrix}1\\0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\1\end{bmatrix} = \alpha^4.$$

$$S_2 = z^3 + i^3 + j^3 = \alpha^3 + \alpha^4 = \begin{bmatrix}1\\0\\0\end{bmatrix} + \begin{bmatrix}1\\1\\0\end{bmatrix} + \begin{bmatrix}0\\1\\1\end{bmatrix} = \begin{bmatrix}0\\0\\1\end{bmatrix} = \alpha^2.$$

Так как $S_1 \neq 0$, $S_2 \neq 0$, а $S_2 \neq {S_1}^3$, то формируется признак неодиночной ошибки и составляется квадратное уравнение (4.10).

$$x^2 + S_1 x + \frac{S_2}{S_1} + {S_1}^2 = 0, S_1 \neq 0.$$

Вычисляем свободный член уравнения

$$\frac{S_2}{S_1} + {S_1}^2 = \frac{\alpha^2}{\alpha^4} + {\alpha^4}^2 = \alpha^5 + \alpha^1 = \begin{bmatrix}1\\1\\1\end{bmatrix} + \begin{bmatrix}0\\1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\1\end{bmatrix} = \alpha^6.$$

Квадратное уравнение для нахождения $z, i$ и $j$ имеет вид

$$x^2 + \alpha^4 x + \alpha^6 = 0.$$

Проверяя каждый элемент по очереди, декодер обнаруживает, что уравнение не имеет корней в поле Галуа $GF(2^r)$ и поэтому принимает решение, что произошли по крайней мере три ошибки.

Двоичный БЧХ-код, исправляющий две ошибки имеет параметры

$$[(2^m - 1), (2^m - 1 - 2m), 5].$$

Для рассмотренных примеров $m = 3, n = 7, k = 1, r = 6$. Если $m = 4$, то имеем [15, 7, 5]-БЧХ код, исправляющий две ошибки.

В общем случае проверочная матрица двоичного БЧХ-кода, исправляющего две ошибки, имеет вид

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(2^m-2)} \end{bmatrix} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \end{bmatrix},$$

где каждый элемент поля $m \in GF(2^m)$ должен быть заменен соответствующим двоичным $m$-вектором.

Замечания

1. Рассмотренный алгоритм декодирования является неполным, т.к. он не исправляет те тройные ошибки, которые код в состоянии исправить.

2. Можно построить двоичный БЧХ-код, исправляющий более чем две независимые ошибки. Проверочная матрица такого кода записывается как

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(2^m-2)} \\ 1 & . & . & \dots & . \\ 1 & \alpha^{2t-1} & \alpha^{(2t-1)2} & \dots & \alpha^{(2t-1)(2^m-2)} \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ 1 & . & . & \dots & . \\ 1 & \alpha^{2t-1} & \alpha^{(2t-1)2} & \dots & \alpha^{(2t-1)(n-1)} \end{bmatrix}.$$

Пример 4.11. Двоичный БЧХ-код со значениями $m = 4, t = 3$ имеет параметры $[(2^4 - 1), (2^4 - 1 - 3 \cdot 4), 7] = [15, 3, 7]$. Проверочная матрица имеет вид

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \dots & \left((\alpha^{3\cdot 14})\right) = \alpha^{12} \\ 1 & \alpha^{2t-1} & \alpha^{(2t-1)2} & \dots & \alpha^{(2t-1)(n-1)} \end{bmatrix} =$$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{12} \\ 1 & \alpha^5 & \alpha^{10} & \dots & ((\alpha^{(5\cdot 14)})) = \alpha^{10} \end{bmatrix}.$$

4.7. Описание структурных схем для выполнения операций в поле $GF(q^m)$

Алгебру полей Галуа можно технически реализовать с помощью логических (арифметических) цепей и схем запоминания элементов поля.

1. Умножитель на скаляр (константу), показанный на рисунке 4.3, реализует функцию одной переменной. Умножает входную переменную (входной символ) на константу, которой может быть элемент поля $GF(q)$. Введение в схему умножителя константы $h$ = 1 эквивалентно соединению. Константа $h$ = 0 эквивалентна отсутствию соединения.

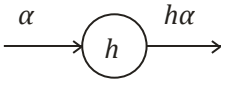



Рисунок 4.3

2. Сумматор, рисунок 4.4, реализует функцию двух переменных, принадлежащих полю Галуа $GF(q)$. Если $q$ = 2, сумматор – это схема „Исключающее ИЛИ“.

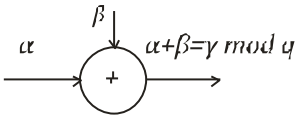



Рисунок 4.4

3. Умножитель, показанный на рисунке 4.5, реализует функцию двух переменных, принимающих значение из поля $GF(q)$. Для $q$ = 2 умножитель – это схема „Логическое И“.

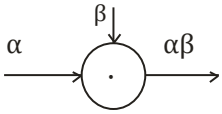



Рисунок 4.5

4. Цепи записи (хранения) двоичных элементов поля элементов поля Галуа $GF(2^m)$ представляют собой $m$-битовые последовательные и параллельные схемы на основе регистров сдвига и хранения.

Определение 4.3. Символ $Y$ на выходе ячейки памяти (элемента задержки) может быть записан в форме

$$Y = DX,$$

где $X$ – входной символ, а $D$ – оператор задержки или отношение выходной величины задержки к входной задержке.

Символ $D^i$ является алгебраическим оператором задержки, действие которого заключается в задержке входного символа на $i$ тактов.

Схемы, состоящие из различных сочетаний элементов, изображенных на рисунках 4.3 – 4.5, называются линейными переключательными схемами. Символ, появляющийся на выходе такой схемы, может зависеть только от одного символа, который присутствует на входе, или от нескольких символов, которые появились на входе в данный и предыдущий момент времени. В первом случае схема будет однотактной, а во втором – многотактной.

### 4.7.1. Линейная многотактная переключательная схема

Функциональную зависимость между выходными и входными символами многотактной переключательной схемы можно выразить как

$$Y = \varphi(X). \qquad (4.16)$$

Ограничимся только линейной логической функциональной зависимостью выход – вход. Многотактная переключательная схема называется линейной, если выходной символ равен сумме по модулю $q$ некоторых входных символов. Для такой схемы применим аппарат линейной алгебры.

Для двоичного случая, когда $q = 2$, выходной символ схемы есть сумма по модулю 2 множества входных сигналов.

Рассмотрим принцип работы многотактной переключательной схемы, изображенной на рисунке 4.6. Пусть все константы $h$ равны 1.

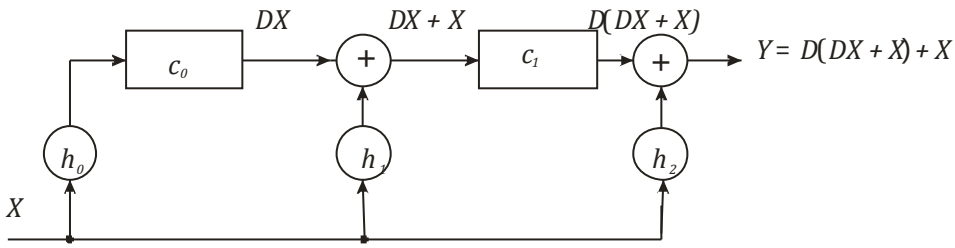



Рисунок 4.6

Зависимость между входной и выходной последовательностями определяется выражением

$$Y = D(DX + X) + X. \qquad (4.17)$$

Отношение выходной последовательности к входной называется передаточной функцией $P(D)$ схемы. Запишем уравнение (4.17) в другой форме

$$Y = D^2X + DX + X) = X(D^2 + D + 1), \qquad (4.18)$$

где 1 = $D^0$– это тождественный или единичный оператор.

Передаточная функция многотактной переключательной схемы (линейного фильтра), рис. 4.6, равна

$$P(D) = \frac{Y}{X} = D^2 + D + 1.$$

Видно, что передаточная функция представляет собой полином задержки, записанный в порядке возрастания степеней оператора $D$. Передаточная функция однозначно определяет свойства линейной многотактной переключательной схемы (устройства преобразования входных последовательностей).

Пример 4.11. Пусть на входе схемы, рисунок 4.6, имеется единичное воздействие $X$ = (1 0 0 0…). Изменения состояний ячеек памяти регистра в тактовые моменты времени приведены в таблице 4.1

Таблица 4.10

| № такта | Вход $X$ | $c_0$ | $c_1$ | Выход $Y$ |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 1 |
| 2 | 0 | 0 | 1 | 1 |
| 3 | 0 | 0 | 0 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

На выходе получим импульсную реакцию $Y$ = (1 1 1 0…). Положение единицы в импульсной реакции соответствует степеням оператора $D$ в передаточной функции. Импульсная реакция затухает через два такта. Здесь выходная последовательность является функцией только последовательности входных символов (формула 4.16).

Далее рассмотрим случай, когда выход является функцией не только символов входной последовательности, но и выходной. Функциональную зависимость между выходными и входными символами такой многотактной переключательной схемы можно выразить как

$$Y = \varphi(X, Y). \qquad (4.19)$$

Из выражения (4.19) следует, что при определенных условиях возможно появление выходных символов $Y$ после окончания поступления входных символов $X$. Разрешим уравнение (4.18) относительно входной последовательности

$$X = {}^{Y}\!/_{(D^2 + D + 1)}. \qquad (4.20)$$

Если принять, что $Y$– это входная последовательность, а $X$– выходная, то передаточная функция примет вид

$$\frac{1}{(D^2 + D + 1)}.$$

Схемная реализация такой многотактной схемы показана на рисунке 4.7.

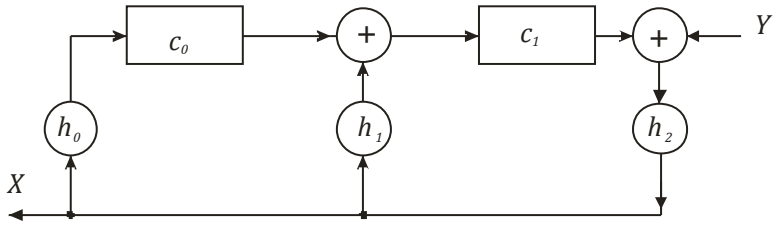



Рисунок 4.7

Схема отличается от схемы, приведенной на рисунке 4.6 тем, что вход и выход поменялись местами и изменилось направление прохождение входного символа. Поскольку в схеме имеются обратные связи, при определенных условиях можно получить выходную последовательность при отсутствии входной. Этот режим формирования вытекает из решения уравнения

$$X = {Y}/{(D^2 + D + 1)},$$ когда $Y = 0$, т.е.

$$X(D^2 + D + 1) = 0.$$

Напомним, для рассматриваемой схемы $X$ означает выходную последовательность. Таким образом, схема, приведенная на рисунке 4.7, при определенных условиях может генерировать последовательность двоичных символов. Чтобы началась генерация, достаточно записать в элемент памяти единицу.

### 4.7.2. Генератор псевдослучайной последовательности

На рисунке 4.8 изображена линейная генераторная схема на основе регистра сдвига (РС) с обратной связью. Структура линейных обратных связей описывается проверочным полиномом $h(x) = 1 + x + x^3$. Также как и передаточная функция $P(D)$, проверочный полиномом $h(x)$ однозначно определяет свойства линейной схемы генератора.

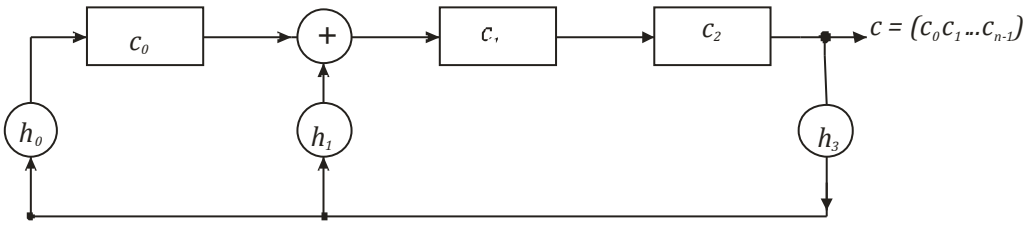



Рисунок 4.8

Обозначим состояния содержимого РС $(c_0 c_1 c_2 \ldots c_m)$. Начальное состояние РС примем равным $c_0 = 1, c_1 = 0\ c_2 = 1 \ldots c_m = 0$, (однотактная запись по параллельным входам). Изменение состояний РС после $(n+1)$ тактов приведены в таблице 4.11.

Таблица 4.11

| № такта | $c_0$ | $c_1$ | $c_2$ | ПСП $c = (c_0 c_1 \ldots c_{n-1})$ | $\beta = \alpha^i$ | $\alpha^0 + \alpha^1 + \cdots + \alpha^{m-1}$ | Дв. вектор |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 | $\alpha^0$ | $\alpha^0$ | 1 0 0 |
| 2 | 0 | 1 | 0 | 0 | $\alpha^1$ | $\alpha^1$ | 0 1 0 |
| 3 | 0 | 0 | 1 | 1 | $\alpha^2$ | $\alpha^2$ | 0 0 1 |
| 4 | 1 | 1 | 0 | 0 | $\alpha^3$ | $1 + \alpha$ | 1 1 0 |
| 5 | 0 | 1 | 1 | 1 | $\alpha^4$ | $\alpha + \alpha^2$ | 0 1 1 |
| 6 | 1 | 1 | 1 | 1 | $\alpha^5$ | $1 + \alpha + \alpha^2$ | 1 1 1 |
| 7 | 1 | 0 | 1 | 1 | $\alpha^6$ | $1 + \alpha^2$ | 1 0 1 |
| 8 | 1 | 0 | 0 | 0 | $\alpha^7$ | $\alpha^0$ | 1 0 0 |

Если некоторое состояние (фазу) ( $c_0 c_1 c_2 \ldots c_m$) регистра выбрать в качестве начального, то регистр принимает $(2^m - 1)$ возможных двоичных состояний, прежде чем состояния начинают повторяться. С выхода третьей ячейки генератора формируется $m$-последовательность $c$ = (0 0 1 0 111). Последовательность символов является периодической с периодом 7. Это – максимально возможный период для 3-х ячеек памяти. Имеется только $2^3 - 1 = 7$ ненулевых состояний. Выходные последовательности значностью 7 представляет собой кодовые слова кода максимальной длины.

Для сравнения в таблице 4.11 также приведены три формы представления элементов расширенного поля Галуа $GF(2^3)$, порождаемого неприводимым над полем $GF(2)$ полиномом $h(x) = 1 + x + x^3$. Любой элемент поля представляется $m$-разрядным двоичным числом и может храниться в $m$-разрядном регистре памяти. Как видно, двоичные состояния РС эквивалентны степеням примитивного элемента поля $\alpha$ и формам полиномов. Таким образом, схема, показанная на рисунке 4.8, является генератором элементов расширенного поля Галуа.

Это устройство умножает содержимое РС на элемент $\alpha$ в поле $GF(2^3)$. Например, если в начальный момент времени регистр содержит 100 $\rightarrow$ $\alpha^0 = 1$,

то в последующие моменты времени он будет содержать $\alpha, \alpha^2, \ldots \alpha^7 = ((1))$, так как $\alpha$ – примитивный элемент поля.

Пример 4.12. Умножить $\alpha\beta = \alpha(c_0 + c_1\alpha + c_2\alpha^2)$,
где элемент поля $\beta = (c_0 + c_1\alpha + c_2\alpha^2)$ пусть будет начальным содержанием регистра хранения, $c_i \in \{0,1\}$.

Решение. $\alpha\beta = \alpha(c_0 + c_1\alpha + c_2\alpha^2) = c_0\alpha + c_1\alpha^2 + c_2\alpha^3$. Так как $\alpha^3 \equiv (\alpha + 1) \bmod(\alpha^3 + \alpha + 1)$, то $\alpha\beta = (c_0\alpha + c_1\alpha^2 + c_2(\alpha + 1)) = (c_0\alpha + c_1\alpha^2 +$ *c2α+c2=(c2+c0+c2α+c1α2).* На рисунке 4.9 показано состояние регистра памяти после умножения на $\alpha$.

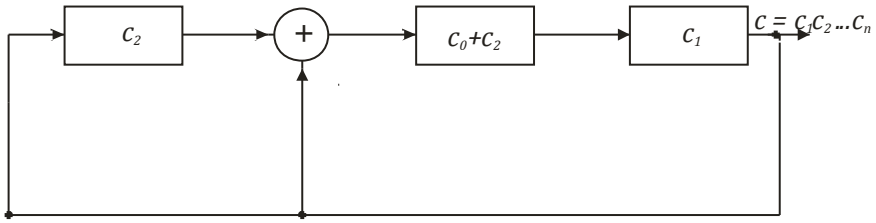



Рисунок 4.9

Пример 4.13. Умножение на фиксированный элемент поля.

Задан произвольный элемент поля $GF(2^4)$ поля $\beta = (c_0 + c_1\alpha + c_2\alpha^2 +$ ***c3α3*** Его надо умножить на фиксированный элемент поля $(1+\alpha^2)$.

Решение. $(c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3)(1 + \alpha^2) = c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + c_0\alpha^2 + c_1\alpha^3 + c_2\alpha^4 + c_3\alpha^5 = c_0 + c_1\alpha + (c_0 + c_2)\alpha^2 + (c_1 + c_3)\alpha^3 + (1 + \alpha)c_2 + (\alpha + \alpha^2)c_3 = (c_0 + c_2) + (c_1 + c_2 + c_3)\alpha + (c_2 + c_0 + c_3)\alpha^2 + (c_3 + c_1)\alpha^3$.

На рис. 4.10 показана функциональная схема умножения на произвольный элемент поля фиксированного элемента поля $(1+\alpha^2)$.

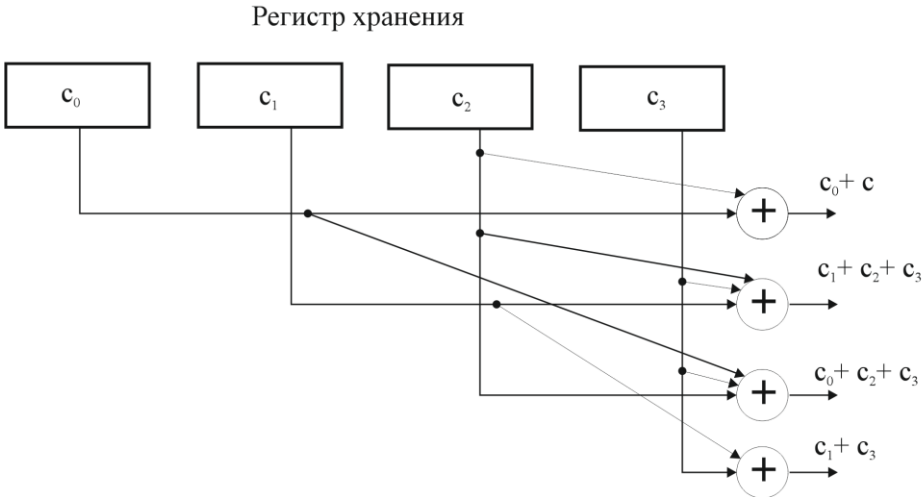



Рис. 4.10

Замечание. Создать генератор действительно случайных последовательностей чисел невозможно. Кодер псевдошумовых

последовательностей работает исходя из точных алгоритмов, а точность и случайность несовместимые понятия. Поэтому любая последовательность, сгенерированная кодером является псевдослучайной. Основа же случайных последовательностей – это последовательность равномерно распределенных чисел.

### 4.7.3. Псевдошумовые последовательности

Определение 4.4. Слова циклического $[2^m-1,\ m, 2^{m-1}]$ $m$ – кода или расширенного кода Рида – Маллера первого порядка $[2^m,\ m+1, 2^{m-1}]$, порождаемые неприводимым проверочным полиномом

$$h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_m x^m$$

степени $m$ над полем $GF(2)$ образуют псевдошумовые последовательности.
Если $c = c_0\, c_1\, \ldots c_{n-1}$ − некоторое слово этого кода, то он обладает свойствами, характерными для последовательностей, которые получаются при случайном подбрасывании монеты $(2^m-1)$ раз. Например, число единиц и нулей в $c$ практически равно друг другу, как и должно быть при длительном подбрасывании монеты.

Псевдошумовые последовательности генерируются при помощи регистров сдвига с линейной обратной связью. Состояния регистра сдвига соответствуют элементам расширенного поля Галуа $GF(2^m)$, порожденного примитивным элементом поля $\alpha$ (корнем уравнения $h(x)$) Устройство генерирования псевдошумовой последовательности эквивалентно устройству, выполняющему умножение на $\alpha$ в поле $GF(2^m)$.

Длительность псевдошумовой последовательности

$$T = n\tau_0 = (2^m-1)\tau_0,$$

где $\tau_0$ – длительность элементарного дискрета последовательности $c$.
Если тактовая частота в сдвигающем регистре равна

$$f = \frac{1}{\tau_0}, \text{ то } \quad T = n\tau_0 = (2^m-1)/f.$$

В таблице 4.12 приведены значения длительности периода псевдошумовой последовательности для $m \in \{7, 8, \ldots, 89\}$ с тактовой частотой $f$ = 1 Мгц.

Таблица 4.12

| Регистр длиной $m$ | Длина последовательности | Длительность периода последовательности |
|---|---|---|
| 7 | 127 | $1{,}27 \cdot 10^{-4}$ с. |
| 8 | 255 | $2{,}55 \cdot 10^{-4}$ с. |
| 9 | 511 | $5{,}11 \cdot 10^{-4}$ с. |
| 10 | 1023 | $1{,}023 \cdot 10^{-3}$ с. |
| 11 | 2047 | $2{,}047 \cdot 10^{-3}$ с. |
| 12 | 4095 | $4{,}095 \cdot 10^{-3}$ с. |
| 13 | 8191 | $8{,}191 \cdot 10^{-3}$ с. |
| 15 | 32767 | $0{,}32767 \cdot 10^{-1}$с. |
| 17 | 131071 | $1{,}31 \cdot 10^{-1}$ с. |
| 19 | 524287 | $5{,}24 \cdot 10^{-1}$ с. |
| 23 | 8388607 | 8,388с. |
| 27 | 134217727 | 13,421 с. |
| 31 | 2147483647 | 35,8 мин. |
| 43 | 879609302207 | 101,7 дня |
| 61 | 2305843009213693951 | $7{,}3 \cdot 10^{4}$ лет |
| 89 | 618971119642691137449562111 (27 десятичных символов) | $1{,}95 \cdot 10^{9}$лет |

Как видно, на практике легко получить бесконечные ключевые последовательности.

В качестве примера использования псевдошумовых последовательностей можно привести систему связи с непилотируемым межпланетным космическим аппаратом и его управление по программе «Венера 15». С помощью автоматической межпланетной станции "Венера-15" осуществлялось радиолокационное картографирование поверхности Венеры. Применением кодированных сигналов обеспечивалось совместное измерение скорости движения и дальности до аппарата. При измерении дальности осуществляется оценка задержки между излученным и принятым сигналами:

$$\tau_{\delta} = \frac{2Д(t)}{c},$$

где $Д(t)$ – дальность до объекта измерений, $c$ – скорость света.

При измерении скорости оценивалось допплеровское приращение частоты

$$F = \frac{2\dot{Д}(t)f}{c},$$

где $\dot{Д}(t)$ – скорость движения объекта; $f$ – несущая частота. В качестве переносчика информации использовались $m$-последовательности длиной 127, 511 и 32767 двоичных символов. Система должна была обеспечивать связь с космическим аппаратом на расстоянии до 105 млн. км. и выполнять следующие задачи:

– передавать командную и телеметрическую информацию на борт космического аппарата с Земли;

– передавать технические и научные данные с космического аппарата на Землю;

– обеспечивать автоматическое слежение за частотой Допплера и слежение по угловым координатам.

Периодическая 127-элементная $m$ -последовательность использовалась для фазовой манипуляции сигналов радара с синтезированной апертурой. Разрешение радиолокационных изображений составляло 1—2 км. По американской программе на тот момент разрешение изображений составляло 20 км; в настоящее время: 200 – 300 м. Кроме того, техническим заданием на разработку радиолинии дальней космической связи задавалась необходимость осуществить радиосвязь на расстоянии 260 миллионов километров. Был разработан канал обработки телеметрических сигналов многоканальной совмещенной системы связи, где также применялись низкоскоростные коды разной значности для решения задачи передачи эксплуатационных данных о работе спутниковой бортовой аппаратуры и исследовательских данных. Позднее результаты разработки использовались в проекте "Венера-Галлей" при создании аппарата "Вега". Две автоматические межпланетные станции "Вега-1" и "Вега-2" этого проекта осуществили комплексное исследование кометы Галлея, космического пространства с попутным облетом и изучением планеты Венера.

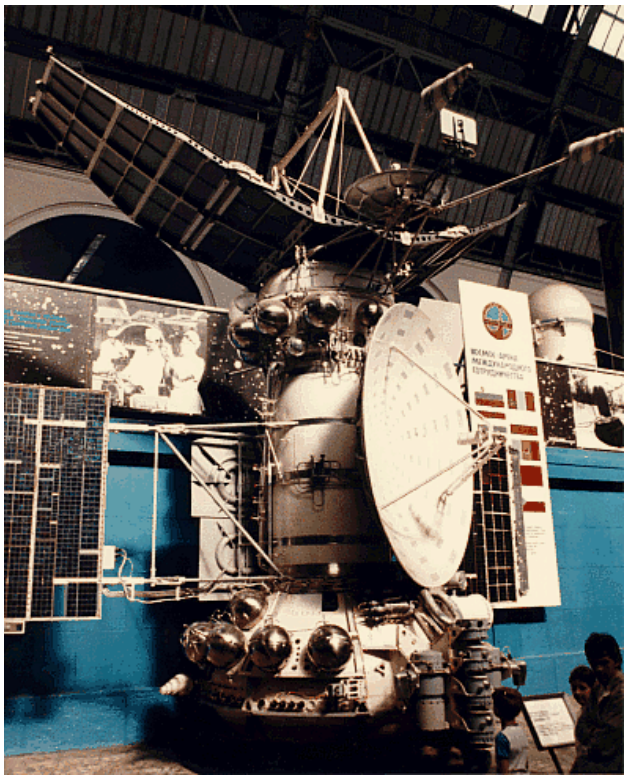


Рис.4.11. Автоматическая межпланетная станция "Венера-16"

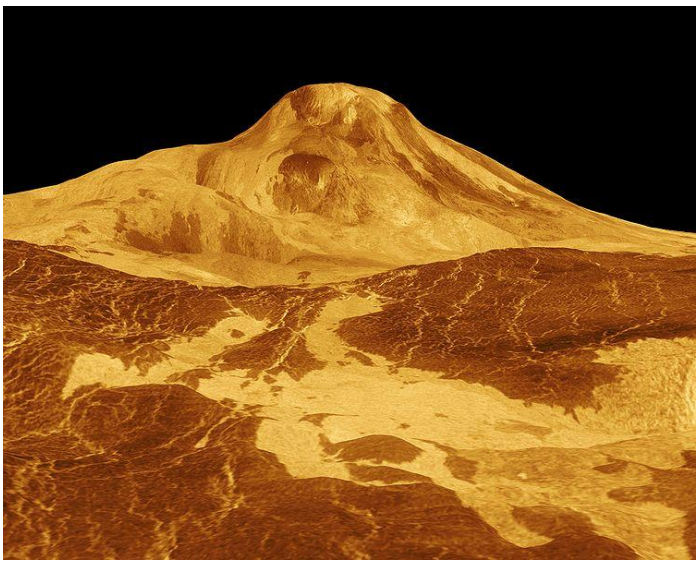


Рис.4.12. Радиолокационное изображение поверхности Венеры

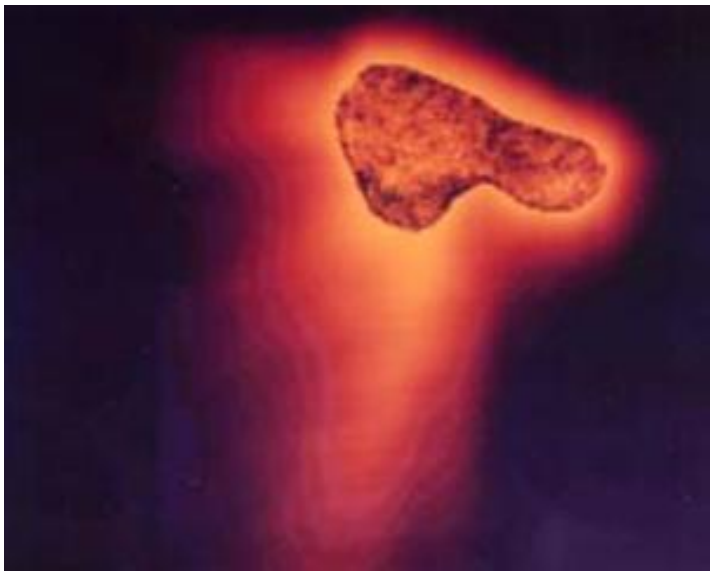


Рис.4.13. Снимок ядра кометы Галлея

## 4.8. Скрытность сигналов

Различают три вида скрытности сигналов:
– энергетическая;
– структурная;
– информационная.

Энергетическая скрытность характеризует способность противостоять мерам, направленным на обнаружение сигнала подслушивателем (разведывательным приемником). Прием информации может осуществляться при мощности сигнала, приходящейся на единицу полосы частот, меньшей спектральной плотности помех в $n$ раз. Для любого отношения $P_s/P_N$ на входе приемника можно подобрать такое значение длины кода, которое обеспечит требуемое для заданной достоверности приема информации отношение сигнал/шум. Если

обнаружение сигнала происходит в условиях, когда на разведывательное устройство действуют шумы, то процесс обнаружения носит вероятностный характер. При этом возможны ошибки двух типов: пропуск сигнала при его наличии на входе приемника и ложное обнаружение (ложная тревога) при отсутствии сигнала. Количественной мерой энергетической скрытности может являться вероятность правильного обнаружения $p_o$ при заданной вероятности ложной тревоги $p_л$. Эти вероятности зависят от отношения сигнал/шум в канале передачи информации и правила принятия решения на обнаружение сигнала.

Структурная скрытность характеризует способность противостоять мерам радиотехнической разведки, направленным на раскрытие сигнала. Это означает распознавание формы сигнала, определяемой способами его кодирования и модуляции, т.е. отождествление обнаруженного сигнала с одним из множества априорно известных сигналов. Следовательно, для увеличения структурной скрытности необходимо иметь по возможности большую мощность используемых кодов и достаточно часто изменять форму сигналов. Скрытность наличия в сигнале информации обеспечивается шумоподобностью сигнала, полученного в результате кодирования. При приеме на обычный широкополосный приемник, в котором не используется информация о способе формирования сигнала данного передатчика, его сигнал будет восприниматься как обычный шум.

Задача определения структуры сигнала является статистической, а количественной мерой структурной скрытности может служить вероятность раскрытия структуры сигнала $p_c$ при условии, что сигнал обнаружен. Таким образом, $p_c$ является условной вероятностью.

Информационная скрытность определяется способностью противостоять мерам, направленным на раскрытие смысла передаваемой информации. Раскрытие смысла информации означает отождествление каждого принятого сигнала с тем сообщением (символом алфавита), которое передается. Эта задача решается выяснением ряда признаков сигнала, например, частости его появления. Наличие априорной и апостериорной неопределенностей делает эту задачу вероятностной, а в качестве количественной меры информационной скрытности принимают вероятность раскрытия (дешифрования) смысла передаваемой информации $p_E$, при условии, что сигнал обнаружен и структура его раскрыта. Следовательно, $p_E$ также является условной вероятностью. Скрытность самой информации достигается с ростом длины и мощности кода. При этом извлечение информации даже из обнаруженного сигнала требует наличия специальной анализирующей аппаратуры, сложность которой возрастает с ростом длины и мощности кода.

Скрытность сигнала определяется вероятностью получения исходной информации после последовательного решения трех задач: обнаружения

сигнала в смеси сигнал + шум, определение структуры обнаруженного сигнала (параметров кодирования) и раскрытие (дешифрование), содержащейся в сигнале информации, поэтому

$$P = p_o \cdot p_c \cdot p_E.$$

4.8.1. Защита информации в системе GPS „Navstar“

В глобальной спутниковой навигационной системе „Navstar“ используются два сигнала несущей частоты $f_1 = 1575,42\ Мгц$ и $f_2 = 1227,6\ Мгц$. Первая несущая манипулируеся периодической последовательностью кода Голда по фазе по закону $\{0, \pi\}$ с тактовой частотой $f_{T1} = 1{,}023$ Мгц и образует сигнал С/А-кода (Clear or Coarse Acqustion – легко обнаруживаемый или не точный). Несущее колебание другого сигнала манипулируется по фазе с тактовой частотой $f_{T2} = 10,23$ Мгц и образует сигнал Р-кода (Protected or precise – санкционированный или точный). Таким образом, используется частотное, фазовое и кодовое разделение сигналов. Кодовая последовательность кода Голда определяет закон фазовой манипуляции.

Каждому i-му $(1 \le i \le 24)$ космическому аппарату спутниковой группировки GPS „Navstar“ соответствуют свои слова $(\mathrm{C/A}_i)$и $P_i$ кодов Голда, которые непрерывно передаются потребителям системы GPS.

В системе „Navstar“ используются две псевдошумовые последовательности кода Голда. Первая получается за счет комбинации по модулю два последовательностей 10-разрядных сдвиговых регистров с обратной связью. Вторая кодовая последовательность строится на комбинировании двух $m$ – последовательностей, генерируемых 24-разрядными регистрами с соответствующими обратными связями и укороченным циклом. Каждая из $m$-последовательностей задается неприводимым примитивным полиномом степени $m$.

Структура кодового слова Р-кода определяется по формуле

$$X = c \oplus D^i v,$$

где $c$ и $v$ – кодовые последовательности, $D^i$ – оператор задержки последовательности $v$ на $i$ тактов, $(1 \le i \le 24)$.

Значности последовательностей $n_c = 15345000$ и $n_v = 15345047$.

Длительность элементарного дискрета последовательности

$$\tau = \frac{1}{f_{T2}}.$$

Длительность периода последовательности $c$

$$T_c = n_c\tau = 15345000 \cdot \frac{1}{10{,}23 \cdot 10^{-6}} = 1{,}5\text{с}.$$

Период последовательности $v$ имеет несколько большую величину длительности

$$T_v = n_v\tau = 15345047 \cdot \frac{1}{10{,}23 \cdot 10^{-6}} = 1{,}5000045\text{с}.$$

При сложении двух двоичных периодических последовательностей с различными длинами получается новая длина комбинированной (составной) кодовой последовательности Голда

$$n = n_c n_v = 15345000 \cdot 15345047.$$

Период составной последовательности, выраженный в сутках

$$T_{cv} = \frac{n}{f_{T2} 3600 \cdot 24} = 266{,}4 \text{ суток.}$$

7-суточные сегменты Р-последовательности приписаны как Р-коды различным спутникам системы GPS. Неперекрывающиеся 7-суточные сегменты имеют следующую величину значности кода

$$n' = \frac{7 \cdot 24 \cdot 3600}{f_{T2}} = 7 \cdot 24 \cdot 3600 \cdot 10{,}23 \cdot 10^6 = 6{,}187104 \cdot 10^{12}.$$

Число возможных различных неприводимых полиномов степени $m$, задающих $m$-коды и, следовательно, коды Голда определяется по формуле

$$L = \frac{\varphi(n)}{m},$$

где $\varphi(n) -$ функция Эйлера. Напомним, если $n$ – простое число, то $\varphi(n) = n - 1$. С ростом $m$ величина $L$ возрастает, как показано в таблице 4.13

Таблица 4.13.

| $m$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|
| $L$ | 2 | 2 | 6 | 6 | 18 | 16 | 48 | 60 | 176 |
| | | | | | | | | | |
| $m$ | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | |
| $L$ | 144 | 630 | 756 | 1800 | 2048 | 7710 | 7776 | 27594 | |

Каждый порождающий полином степени $m$ образует $m$-код мощностью

$$M = 2^m - 1.$$

Количество кодовых слов, генерируемых $m$-разрядным РС достигает величины

$$M_\Sigma = L(2^m - 1).$$

Например, для $m$ =10, путем изменения структуры обратной связи РС можно сформировать 60 последовательностей максимальной длины разного вида. Каждый порождающий полином степени $m$ образует М-код мощностью

$$M = 2^{10} - 1 = 1023.$$

Таким образом, общее количество слов формируемых одним 10-разрядным РС

$$M_{\Sigma} = L(2^m - 1) = 60 \cdot 1023 = 61380.$$

Предполагается, что структура кода Голда может изменяться. Все это говорит о чрезвычайной сложности раскрытия структуры даже С/А-кода, не говоря уже о Р-коде.

На рисунке 4.14 показана структурная схема генератора псевдошумовых последовательностей С/А-кода Голда. Из 1023 возможных сдвигов выбираются такие 24 сдвигов (по максимальному числу обслуживаемых космических аппаратов), при которых последовательности Голда будут иметь наименьший уровень боковых лепестков.

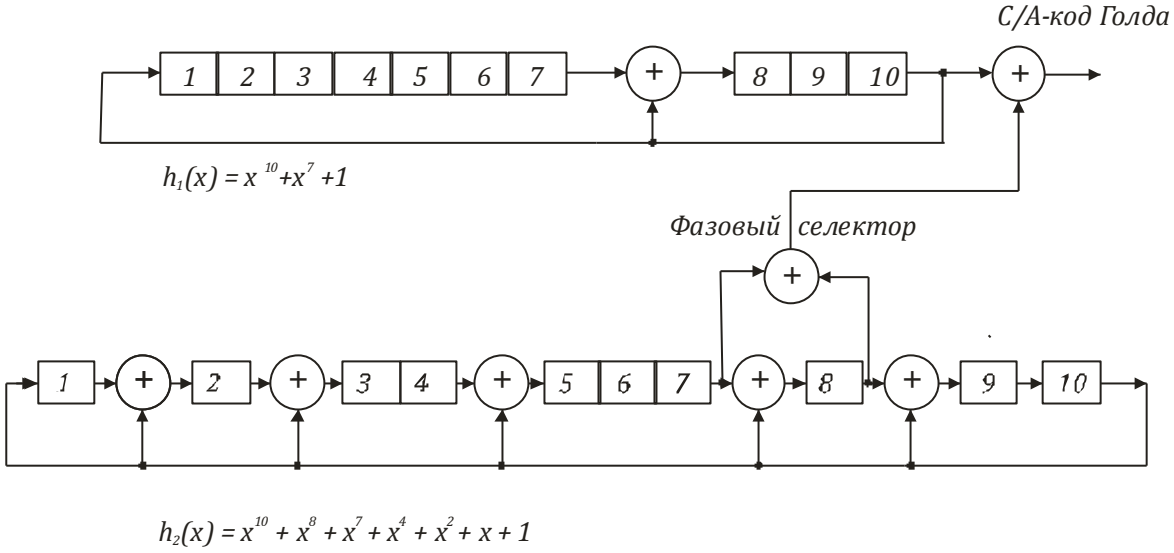



Рис. 4.14

Фазовый селектор позволяет формировать при разных обратных связях для $1 \leq i \leq 24$ (для всех космических аппаратов) последовательности Голда.

Министерство обороны США уполномочило разработчиков GPS предусмотреть и криптозащиту, которая реализована на основе шифра Вернама. В этом случае последовательность Р-кода суммируется по модулю 2 с секретным ключом в виде W-кода. Результатом гаммирования является Y-код. Один символ W-кода перекрывает 20 символов Р-кода. Для взлома ключа перебором пришлось бы протестировать до $2^{n'/20} = 2^{6{,}187104 \cdot 10^{12}/20} > 2^{10000000000}$ вариантов. По этой причине Y-код практически невозможно взломать.

Отношения мощности сигнала $P_s$ к мощности шума $P_N$ в полосе частот, занимаемой сигналом (на выходе избирательной системы, частотная характеристика которой согласована с длительностью элементарного дискрета С/А и Р-кодов соответствуют величинам:

$$\frac{P_{s(\text{С/А})}}{P_N} = -24{,}4 \text{ дБ} < 0{,}01,$$

где $P_N = N_0 f_{T1}$, $N_0-$ односторонняя спектральная плотность шума;

$$\frac{P_{s(P)}}{P_N} = -40{,}4 \text{ дБ} < 0{,}0001,$$

где $P_N = N_0 f_{T2}$.

Из приведенных выражений следует, что на входе декодера мощность шума более чем в 100 раз для С/А-кода и более чем в 10000 раз для Р-кода превышает мощность полезного сигнала. При неизвестной структуре полиномов $h(x)$ сигнал системы практически не может быть обнаружен и декодирован.

Основные операции обработки сигналов в приемнике GPS типичны для любой системы с кодовым разделением. В процессе частотно-временного поиска декодирование кода Голда осуществляется на основе принципа максимального правдоподобия. Так как, полоса частот $\Delta f$, занимаемая информационным сигналом при скорости передачи 50 бит/с составляет 100 Гц, то в этой полосе на выходе демодулятора – декодера отношения мощности сигнала к мощности шума соответственно для С/А и Р-кодов равны:

$$\frac{P_{s(\text{C/A})}}{P_{N\text{вых}}} = 12{,}6 \text{ дБ},$$

где $P_{N\text{вых}} = N_0 \cdot \Delta f$;

$$\frac{P_{s(P)}}{P_{N\text{вых}}} = 18{,}6 \text{ дБ}.$$

Такие величины значений отношений сигнал/шум на выходе декодеров позволяют получить высокие параметры достоверности приема информации. Заметим, что для повышения надежности передачи информационного потока применятся кодирование расширенным [32, 26, 4]-кодом Хэмминга.

## 4.9. Минимальные многочлены

Пусть $F$ – произвольное расширенное поле Галуа $GF(q^m)$порядка $q^m$. Любое конечное поле содержит $q^m$ элементов для некоторого простого $q$ и некоторого целого $m \geq 1$. Существует только одно такое поле $GF(q^m)$для каждого $q$ и $m$.

Конечное поле содержит, по крайней мере, один примитивный элемент $\alpha$, такой, что все ненулевые элементы поля $\beta$ могут быть представлены в виде разных степеней $\alpha^j$. Элементы поля могут быть выражены и через отрицательные степени $\alpha$, так как поле содержит мультипликативный обратный элемент каждого ненулевого элемента.

### 4.9.1. Теорема Ферма

Каждый элемент $\beta$ поля $GF(q^m)$ является корнем уравнения

$$x^{q^m} - x = 0, \qquad (4.21)$$

или, эквивалентно удовлетворяет множеству

$$\beta^{q^m} = \beta.$$

Это означает, что многочлен (4.21) представляется произведением двучленов вида

$$x^{q^m} - x = \prod_{\beta \in F} (x - \beta).$$

Перепишем уравнение (4.21) как

$$x(x^{q^m - 1}) - 1 = 0.$$

Для $x \neq 0$ получаем выражение

$$x^{q^m - 1} - 1 = 0. \qquad (4.22)$$

Многочлену (4.22) также соответствует двучлен

$$x^{q^m - 1} - 1 = \prod_{\beta \in F} (x - \beta).$$

Для двоичного случая (простого поля, $q$ = 2) каждый элемент $\beta$ поля $GF(q^m)$ является корнем уравнения

$$x^{2^m - 1} - 1 = 0.$$

Во многих приложениях для некоторого целого числа $m \geq 1$принимают

$$2^m - 1 = n,$$

где $n$ определяет значность (длину) кода.

Тогда каждый элемент $\beta$ поля $GF(q^m)$ является корнем уравнения

$$x^n - 1 = 0. \qquad (4.23)$$

Многочлен $x^n - 1$ выражается произведением двучленов вида

$$x^n - 1 = \prod_{\beta \in F} (x - \beta).$$

Если $\beta$ корень уравнения (4.23), то

$$\beta^n = \alpha^{jn} = 1,\ 1 \leq j \leq n - 1.$$

Известно, что любой многочлен (двучлен) типа (4.21) и (4.23) может быть представлен произведением всех неприводимых многочленов, степени которых являются делителями числа $m$ (от 1 до $m$ включительно).

Согласно теореме Ферма корни уравнений (4.21), (4.23.) принадлежат различным неприводимым в поле $GF(q)$ многочленам на которые разлагается

двучлен. Например, если $q$ = 2, $m$ = 4. По таблице неприводимых многочленов находим

$x^{15} + 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$. (4.24)

Заметим, что степени неприводимых многочленов (4.24) – числа 1, 2, 4 являются делителями числа $m$ = 4.

С каждым элементом поля связан неприводимый многочлен, называемый минимальным многочленом. Многие циклические коды в своей основе имеют минимальные многочлены.

Определение 4.5. Минимальным многочленом элемента $\beta$ над полем $GF(q)$ называется нормированный многочлен $M(x)$ с коэффициентами из $GF(q)$, наименьшей степени такой, что $M(\beta) = 0$.

Теорема 4.5. Если известен один из корней $\beta$ неприводимого многочлена степени $m$, то все другие корни этого многочлена являются степенями $\beta$, а именно

$$\beta, \beta^2, \dots, \beta^{2^{m-1}}.$$

Например, при $m$ = 3 корнями являются элементы поля $\beta, \beta^2, \beta^{2^{3-1}} = \beta^4$. $M^1(x) = M^2(x) = M^4(x)$. Если $M^1(x) = 1 + x + x^3$, то $M^2(x) = M^4 = 1 + x + x^3$. Воспользовавшись данными таблицы 4.11, имеем

$$M^2(\beta^2) = 1 + \beta^2 + \beta^{2^3} = 1 + \beta^2 + \beta^6 = 1 + \beta^2 + 1 + \beta^2 = 0.$$

Следовательно, $M^2(x) = 1 + x + x^3$.

Пример 4.14. Найти минимальный многочлен $M^3(x)$ элемента $\beta$, $m$ = 3. Корень $\alpha$ рассматриваем как элемент поля, построенного с использованием неприводимого многочлена $g(x) = 1 + x + x^3$.

Решение. Многочлен $M^3(x)$ может быть представлен в виде

$$M^3(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3),$$

где $\beta_1 = \alpha^3$, $\beta_2 = \alpha^{3^2}$, $\beta_3 = \alpha^{3^4}$. Корнями уравнения $M^3(x)$ являются следующие различные элементы: $\beta_1 = \alpha^3$, $\beta_2 = \alpha^6$, $\beta_3 = \alpha^5$. Тогда $M^3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5) = (x^2 - x\alpha^6 - x\alpha^5 - \alpha^9)(x-\alpha^5) = (1 + x^2 + x^3)$.

$M^3(\alpha^3) = (1 + (\alpha^3)^2 + (\alpha^3)^3) = (1 + \alpha^6 + \alpha^9) = (1 + (1 + \alpha^2) + \alpha^2) = 0$.

$M^3(x) = M^6(x) = M^5(x)$.

Упражнение 4.6. Показать, что задавая поле $GF(2^4)$ корнем уравнения $\alpha^4 + \alpha + 1 = 0$ минимальные многочлены имеют вид:

| Элемент | Минимальные многочлены |
|---|---|
| 0 | $x$; |
| 1 | $M^0(x) = x + 1$; |
| $\alpha, \alpha^2, \alpha^4, \alpha^8$ | $M^1(x) = M^2(x) = M^4(x) = M^8(x) = 1 + x + x^4$; |
| $\alpha^3, \alpha^6 \alpha^{12}, \alpha^9$ | $M^3(x) = M^6(x) = M^{12}(x) = M^9(x) = 1 + x + x^2 + x^3 + x^4$; |

4.9.2. Свойства минимальных многочленов

1. Пусть $M(x)$ – минимальный многочлен элемента $\beta \in GF(q^m)$. $M(x)$ неприводим.
2. Если $c(x)$ – некоторый многочлен с коэффициентами из $GF(q)$ такой, что $c(\beta) = 0$, то $M(x) \mid c(x)$ ($M(x)$ делит c($x$)).
3. $M(x) \mid x^{q^m} - x$.
4. $\deg M(x) \leq m$.
5. Степень минимального многочлена примитивного элемента поля $GF(q^m)$ равна $m$. Такой многочлен называется примитивным.
6. Минимальные многочлены элементов поля $\beta$ и $\beta^q$ равны.

Замечание. Если неприводимый многочлен $p(x)$ используется для построения поля $GF(q^m)$ и $\alpha$ является корнем $p(x)$, то многочлен $p(x)$– минимальный.

4.9.3. Кольцо

Определение 4.6. Кольцо – это алгебраическая структура или множество элементов $R$, в котором определены две основные операции (сложение и умножение) и операция, обратная первой из них (вычитание).

В кольце должны выполняться следующие аксиомы:

– $<R; +>$ – абелева группа;

– $<R; \cdot>$ – полугруппа;

– дистрибутивность ( для любых элементов множества $R = \{ a, b, c \}$, $a \cdot (b + c) = a \cdot b + a \cdot c$).

Определение 4.7. Множество $G$ с заданной на нем бинарной операцией и выполнением аксиом замкнутости и ассоциативности называется полугруппой.

Примеры полугрупп

4.15. $<N;\ +>$ – аддитивная полугруппа натуральных чисел.

4.16. Пусть $q$– это конечный набор символов (алфавит). Например, $q$ – множество символов белорусского алфавита, или $q$ двоичное множество {0, 1}. Слово символов из множества имеет вид $a_1\ a_2\ \dots a_n$, где $a_i \in q$. Пусть $G$ обозначает множество слов алфавита $q$. Введем бинарную операцию ○ называемую конкатенацией над $G$ следующим образом: если $a_1\ a_2\ \dots\ a_n$ и $b_1\ b_2\ \dots\ b_m \in G$, то $a_1\ a_2\ \dots\ a_n \circ b_1\ b_2\ \dots\ b_m = a_1\ a_2\ \dots\ a_n\ b_1\ b_2\ \dots\ b_m$.
Например, если $q$ = {0, 1}, то 11011 ○ 1010110 =110111010110.
Пусть $a_1\ a_2\ \dots\ a_n,\ b_1\ b_2\ \dots\ b_m$ и $c_1\ c_2\ \dots\ c_t \in G$. Тогда
$(a_1\ a_2\ \dots\ a_n \circ b_1\ b_2\ \dots\ b_m) \circ (c_1\ c_2\ \dots\ c_t) = (a_1\ a_2\ \dots\ a_n\ b_1\ b_2\ \dots\ b_m) \circ c_1\ c_2\ \dots\ c_t$ $= a_1\ a_2\ \dots a_n\ b_1\ b_2\ \dots b_m\ c_1\ c_2\ \dots c_t$. Бинарная операция конкатенации ассоциативна на множестве $G$ и это множество вместе с операцией конкатенации образует полугруппу.

Кольцо можно определить и так: кольцо $R$ является группой относительно операции сложения и полугруппой относительно операции умножения. В кольце для операции умножения могут не выполнятся аксиомы существования нейтрального и обратного элементов группы.

Примеры колец

4.17. Все действительные числа образуют кольцо относительно операций сложения и умножения;

4.18. Алгебраическая система целых чисел $< Z; +;\cdot >$;

4.19. Множество квадратных матриц размеров $n \times n$. Нейтральным элементом относительно операции умножения в кольце матриц является единичная матрица;

4.20. Кольцо целых чисел по модулю $M$. Например, $M$ = 14. Тогда система $< \{0, 1, 2, \dots, 13\}; +;\cdot;\ 0; 1 >$ – кольцо, в котором для элемента 2 не существует обратного элемента, т.к. $2 \cdot 2^{-1} \neq 1 \bmod 14$.

4.9.4. Идеал кольца

Определение 4.8. Пусть $R$ – кольцо, а $R'$ есть подкольцо – подмножество множества $R$. Подкольцо $R'$ определяется операциями кольца.

Примеры подколец

4.21. Целые числа образуют подкольцо кольца рациональных чисел

$$R' < \{Z = 0, \pm 1, \pm 2, \dots, \}; +;\cdot;\ 0; 1 >.$$

4.22. Рациональные числа образуют подкольцо кольца действительных чисел;

4.23. Действительные числа образуют подкольцо кольца комплексных чисел;

4.24. Множество квадратных матриц размером $n \times n$ с целыми значениями элементов образуют подкольцо кольца матриц размером $n \times n$ с рациональными элементами.

Определение 4.9. Подмножество $I$ элементов кольца $R$ называется идеалом в $R$, если выполняются следующие условия:

– $I$ является подкольцом кольца $R$, т.е. для любого множества $\{a, b\} \in I$ выполняется $(a + b) \in I$ и $a \cdot b \in I$;

– для любого элемента $a \in I$ и любого элемента $r \in R$ произведения $a \cdot r$ и $r \cdot a$ принадлежат $I$.

Упражнение 4.7. Показать, что множество $R' = \{0, 2, 4\}$ это подкольцо кольца $\{Z_6 = 0, 1, 2, 3, 4, 5\}; +; \cdot; 0; 1 >$.

4.9.5. Главный идеал

Определение 4.10. Пусть $R$ – коммутативное кольцо. Идеал $I$ кольца $R$ называется главным идеалом, порожденным элементом $a$ (обозначается $< a >$), если $I$ состоит из всех произведений $a$ на элементы кольца $R$, т.е. $I = < a > = \{ a \cdot r: r \in R\}$.

Теорема 4.6. Совокупность целых чисел образует главный идеал тогда и только тогда, когда она состоит из всех чисел, кратных некоторому числу.

Пример 4.25. Множество целых чисел $Z = \{0, 1, 2, 3\}_4$ является коммутативным кольцом с единицей. Найти главный идеал кольца $Z$.

Решение. Если $a$ – минимальное целое число из $I$, то по определению идеала $b = r \cdot a$. Выберем в качестве $a = 2$, т.е. $I = < 2 >$. Тогда множество всех чисел, кратных $a$, запишем в виде

$$I = < 2 >. = \{0 \cdot 2 = 0; 1 \cdot 2 = 2; 2 \cdot 2 = ((0))_4; 3 \cdot 2 = ((2))_4\} = \{0, 2\}.$$

Пример 4.26. Рассмотрим кольцо целых чисел и два главных идеала, порожденных целыми числами 8 и 12:

$< 8 >$ = {…, – 48, – 40, – 32, – 24, – 16, – 8, 0, 8, 16, 24, 32, 40, 48,…};

$< 12 >$ = {…,– 48, – 36, – 24, – 12, 0, 12, 24, 36, 48,…}.

Найти главный идеал пересечения множеств $< 8 > \cap < 12 >$.

Решение. Пересечения множеств $< 8 > \cap < 12 >$ есть множество {…, – 48, – 24, 0, 24, 48,…}. Главный идеал порождается числом 24, которое является наименьшим общим кратным чисел 8 и 12. В общем случае

$$< a > \cap < b > = < HOK(a, b) >.$$

4.9.6. Кольцо полиномов

Рассмотрим кольцо вида $R_n = \frac{R(x)}{x^n-1}$, состоящее из класса вычетов кольца полиномов $R(x)$ по модулю полинома $x^n - 1$.

Определение 4.11. Идеалом $I_n$ кольца $R_n$ называется линейное подмножество полиномов от $x$ такое, что если $c(x) \in I_n$, то $r(x) \cdot c(x) \in I_n$, для всех $r(x) \in R_n$.

Пример 4.27. Пусть $n = 3$. Подмножество полиномов вида $I_n = \{0, (1 + x), (x + x^2), (1 + x^2)\}$ есть идеал в $R_3$. Действительно:

– подмножество замкнуто относительно сложения (линейно). Например, $(1 + x) + (1 + x^2) = (x + x^2)$;

– выполняется условие $r(x) \cdot c(x) \in I_n$. Например, $x^2(1 + x^2) = (x^2 + x^4) \equiv (x + x^2) mod\ (x^3 - 1)$.

4.10. Циклические корректирующие коды

Алгебраическое описание циклических корректирующих кодов

Теория линейных циклических кодов основывается на полиномиальном представлении, когда построение кода осуществляется с помощью операций сложения, вычитания и умножения полиномов по модулю полинома $x^n - 1$. Множество слов циклического кода $C = \{c(x)\}$ попадает в класс вычетов многочленов в степени не больше $(n - 1)$, т.е. $\{c(x)\} \in R(x)$.

Сопоставим каждому вектору $c = c_0\ c_1\ c_2 \ldots c_{n-1}$ многочлен $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$. Умножая в кольце $R_n$ многочлен $c(x)$ на $x$, получаем

$$xc(x) = c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n = c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1}. \quad (4.24)$$

В кольце $R_n$ имеет место равенство

$$x^n - 1 \equiv 0 \bmod x^n - 1, \text{ отсюда } (( x^n)) \equiv 1.$$

Многочлену (4.24) соответствует вектор $(c_{n-1}\ c_0\ c_1 \ldots c_{n-2})$. Следовательно, в кольце $R_n$ операция умножения на $x$ эквивалентна операции циклического сдвига элементов вектора.

Пусть $n = 4$, $p(x) = x^4 - 1$, $c(x) = (x + x^3)$. Умножая $x(x + x^3) \equiv (1 + x^2) \bmod (x^4 - 1) \equiv ((1 + x^2))$.

Определение 4.12. Циклический код $C = \{c(x)\}$ длиной $n$ есть ненулевой

идеал $I_n$ в кольце многочленов $R_n$ по модулю многочлена $x^n - 1$.

Утверждение 4.1. Если $c(x) \in I_n$ то $x\,c(x) \in I_n$. Любое, кратное многочлену $c(x) \in I_n$, опять лежит в $I_n$.

Пример 4.28. Циклический код Хэмминга задается порождающим многочленом $g(x) = M^1(x)$ идеала.

Из определения 4.11 следует, что любой многочлен $c(x) \in I_n$ в кольце $R_n$ определяется как

$$c(x) = f(x) \cdot g(x) \in I_n. \qquad (4.25)$$

В этом случае информация $f(x)$ кодируется многочленом

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

Многочлену $c(x)$ соответствует вектор $c = (c_0 c_1 \ldots c_{n-1})$, где $c_i \in GF(q)$.

Вектор $c = c_0 c_1 \ldots c_{n-1}$ принадлежит циклическому коду Хэмминга

$$\rightleftarrows c(\alpha) = 0,$$

минимальных многочленов и понятия главного идеала (теорема 2.10) следует, что вектор $c$ принадлежит коду тогда и только тогда, когда $g(x)$ делит $c(x)$. Следовательно,

где $\alpha \in GF(q^m)$ – корень уравнения, порождающего поле. Из свойства

$$g(x) = M^1(x).$$

4.10. Циклотомические классы

Пусть задано поле $GF(2^4)$. Согласно свойству 6 минимальных многочленов, в этом поле равны минимальные многочлены элементов $\beta$ и $\beta^2$.

Определение 4.13. Элементы поля, минимальные многочлены которых равны, называются сопряженными.

Например, если $\beta = \alpha^5$, то $M^5(x) = M^{10}(x)$. Элементы $\alpha^5$ и $\alpha^{10}$ будут сопряженными.

Из упражнения 4.6:

| Элемент поля | Минимальные многочлены |
|---|---|
| 0 | $x$; |

| | |
|---|---|
| 1 | $M^0(x) = x + 1;$ |
| $\alpha, \alpha^2, \alpha^4, \alpha^8$ | $M^1(x) = M^2(x) = M^4(x) = M^8(x) = 1 + x + x^4;$ |
| $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ | $M^3(x) = M^6(x) = M^{12}(x) = M^9(x) = 1 + x + x^2 + x^3 + x^4;$ |
| $\alpha^5$ | $M^5(x) = M^{10}(x) = 1 + x + x^2;$ |
| $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ | $M^7(x) = M^{14}(x) = M^{13}(x) = M^{11}(x) = 1 + x + x^4.$ |

видно, что степени примитивного элемента поля $GF(2^4)$ всех минимальных многочленов образуют непересекающиеся множества сопряженных элементов поля. Эти подмножества множества элементов поля называются циклотомическими классами.
Следовательно, совокупность циклотомических классов разделяет множество элементов поля $GF(q^m)$ на непересекающиеся подмножества.

Определение 4.14. Множество целых чисел по модулю $(q^m - 1)$ относительно операции умножения на $q$ разделяется на непересекающиеся подмножества – циклотомические классы.

Циклотомический класс, содержащий целое число $s$, это подмножество чисел
вида

$$\{s, qs, q^2s, \dots, q^{m_s-1}s\}, \tag{4.26}$$

где $m_s$– наименьшее натуральное число такое, что

$$q^{m_s} \cdot s \equiv s \bmod q^m - 1. \tag{4.27}$$

Обозначим через $C_s$– циклотомический класс целого наименьшего числа $s$ в классе. Например, циклотомическими классами по модулю $(2^3 - 1)$ являются:

$$C_0 = \{0\};$$
$$C_1 = \{1, 2, 4\};$$
$$C_3 = \{3, 6, 5\}.$$

В циклотомическом классе $C_3$ число $s = m_s = 3$– это наименьшее натуральное число такое, что выполняются выражения (4.26) и (4.27):

$$q^{m_s} \cdot s \equiv 2^3 \cdot 3 \equiv 3 \bmod 2^3 - 1,$$
$$q \cdot s = 2 \cdot 3 = 6,$$
$$q^{m_s-1} \cdot s = 2^{3-1} \cdot 3 = 12 \equiv 5 \bmod 2^3 - 1.$$

Минимальный многочлен элемента $\alpha^s$равен:

$$M^s(x) = \prod_{i \in C_s} (x - \alpha^i).$$

По определению 4.5 $M^s(x)$ – это нормированный многочлен с коэффициентами из $GF(q)$, наименьшей степени такой, что $M(\beta = \alpha^s) = 0$. Из теоремы Ферма получаем выражение разложения двучлена вида

$$x^n - 1 = \prod_s M^s(x). \qquad (4.28)$$

Формула (4.28) представляет собой разложение многочлена $x^n - 1$ над полем $GF(q)$ на неприводимые множители. Многие конструкции циклических кодов получаются с использованием таблицы циклотомических классов разложения (4.28).

## 4.11. БЧХ-код, исправляющий ошибки кратностью $t$

Теорема 4.6. БЧХ-код, исправляющий две ошибки – это циклический код над полем $GF(q)$ с порождающим многочленом $g(x) = M^1(x)M^3(x)$.

Например, для $n = 7$ и $q = 2$ имеем поле $GF(2^3)$. Поле порождается неприводимым над полем $GF(2)$ полиномом $p(x) = 1 + x + x^3$. Корнем уравнения $p(x) = 1 + x + x^3$ является элемент $\alpha \in GF(2^3)$. Тогда,

$$M^1(x) = 1 + x + x^3.$$

Корнем уравнения $p(x) = 1 + x^2 + x^3$ является элемент $\alpha^3 \in GF(2^3)$. Следовательно,

$$M^3(x) = 1 + x^2 + x^3.$$

Искомый порождающий многочлен БЧХ-кода

$g(x) = M^1(x)M^3(x) = (1 + x + x^3)(1 + x^2 + x^3) = 1 + x + x^2 + x^3 + x^4 + +x^5 + x^6$.

Теорема 4.7. Двоичный БЧХ-код, исправляющий $t$ ошибок, имеет порождающий многочлен

$$g(x) = \text{НОК}\,\{M^1(x),\ M^3(x), \dots, M^{2t-1}(x)\},$$

где НОК обозначает наименьшее общее кратное минимальных многочленов.

Пример 4.29. БЧХ-код длиной 15, исправляющий трехкратные ошибки, определяется порождающим многочленом

$$g(x) = \text{НОК}\,\{M^1(x),\ M^3(x),\ M^5(x)\}.$$

Минимальные многочлены элементов поля $GF(2^4)$ выпишем из упражнения 4.6

$$M^1(x) = x^4 + x + 1,$$
$$M^3(x) = x^4 + x^3 + x^2 + x + 1,$$

$$M^5(x) = x^2 + x + 1.$$

Согласно свойству 1 минимальных многочленов, $M^1(x)$, $M^3(x)$, $M^5(x)$ – неприводимы. Тогда

$$\text{НОК}\{M^1(x),\ M^3(x),\ M^5(x)\} = M^1(x) \cdot M^3(x) \cdot M^5(x).$$

$g(x)$ $=(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = (x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1).$

Теорема 4.7. Пусть $C-$ циклический $[n,\ k,\ d]$-код с порождающим многочленом $g(x)$. Тогда $g(x)$ делит $x^n - 1$ и выполняется сравнение

$$c(x) \equiv 0 \bmod g(x),$$

при этом

$$g(\alpha) = 0,$$
$$g(x) = \prod_{i \in L}\left(x - \alpha^i\right), \qquad (4.29)$$

где $L \subseteq \{1, 2, \dots, n-1\}$, т.е $L$ и $i$ – это подмножество чисел множества $\{1,2, \dots, n-1\}$. Множество $L$ образуется объединением циклотомических классов. Кодовое слово $c(x) \in C$ тогда и только тогда, когда

$$c\left(\alpha^i\right) = 0 \text{ для всех } i \in L.$$

Например, циклотомическими классами по модулю $(2^4 - 1)$ являются:

$$C_0 = \{0\};$$
$$C_1 = \{1, 2, 4,8\};$$
$$C_3 = \{3, 6, 12,9\};$$
$$C_5 = \{5, 10\};$$
$$C_7 = \{7, 14, 13,11\}.$$

Множество $L$ образуется объединением циклотомических классов $C_1 = \{1, 2, 4,8\}$, $C_3 = \{3, 6, 12,9\}$, $C_5 = \{5, 10\}$. Множество $L = \{1,2,3,4,5,6,8,9,10,12\}$. БЧХ-код длиной 15, исправляющий трехкратные ошибки, определяется порождающим многочленом

$$g(x) = \prod_{i \in L}\left(x - \alpha^i\right) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)(x - \alpha^5)(x - \alpha^6) \times.$$

$$\times (x - \alpha^8)(x - \alpha^9)(x - \alpha^{10})(x - \alpha^{12}).$$

$$g(x) = (x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1).$$

*Определение 4.15.* Корни порождающего многочлена называются нулями кода. Нули кода принадлежат множеству $\{\alpha^i : i \in L\}$.

Теорема 4.8. (Граница БЧХ). Пусть $C-$ циклический $[n, k, d]$-код с порождающим многочленом $g(x)$. Если выполняется равенство

$$g(\alpha) = g(\alpha^2) = g(\alpha^3) =\ldots= g(\alpha^{d-1}), \qquad (4.30)$$

то кодовое расстояние кода равно $d$.

Замечание. Теорема 4.8 справедлива только, тогда когда $(d - 1)$ последовательных степеней примитивного элемента $\alpha$ являются нулями кода.

Пример 4.30. Определить параметры циклического БЧХ-кода, исправляющего трехкратные ошибки. Поле $GF(2^4)$ порождается неприводимым над $GF(2)$ многочленом $p(x) = x^4 + x + 1$.

Решение. Величина кратности ошибки $t = 3$ приводит к $d = 7$. По теореме 4.8 получается множество последовательных нулей БЧХ-кода вида

$$\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}.$$

Циклотомические классы на $L$, содержащие числа {1, 2, 3, 4, 5, 6}, являются следующие множества:

$$C_1 = \{1, 2, 4, 8\};$$
$$C_3 = \{3, 6, 12, 9\};$$
$$C_5 = \{5, 10\}.$$

Циклу $C_1$ соответствует минимальный многочлен $M^1(x) = 1 + x + x^4$; циклу $C_3$ соответствует $M^3(x) = 1 + x + x^2 + x^3 + x^4$, циклотомическому классу $C_5$ соответствует $M^5(x) = 1 + x + x^2$.

Из формулы (4.29)

$$g(x) = \prod_{i\in L}\left(x - \alpha^i\right) = M^1(x)M^3(x)M^5(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}.$$

Число проверочных символов кода определяет deg $g(x)$ = 10 или сумма длин каждого циклотомического класса. Число информационных символов $k$ = 15 – 10 = 5.

Упражнение 4.8. Показать, что порождающий многочлен БЧХ-кода, исправляющего две ошибки длиной $n$ = 15,

$$g(x) = (1 + x^4 + x^6 + x^7 + x^8).$$

## 4.12. Коды Рида – Соломона

Коды Рида – Соломона (РС-коды) относятся к подклассу циклических БЧХ- кодов. Для заданных параметров $n$ и $k$ они имеют наибольшее кодовое расстояние

$$d = n - k + 1, \qquad (4.31)$$

и удовлетворяют границе Синглтона (см. (2.10)).

*Определение 2.44.* Код Рида – Соломона над полем $GF(q)$ – это БЧХ-код длиной $n = q - 1$.

Длина РС-кода равна числу ненулевых элементов в поле Галуа $GF(q)$.

Ранее был определен БЧХ-код в поле $GF(q^m)$ разложения многочлена

$$x^{q^m-1} - 1 = \prod_{\beta \in F}(x - \beta), \beta \in GF(q^m).$$

РС-код определяется в поле $GF(q)$, т.е. в поле разложения многочлена

$$x^{q-1} - 1 = \prod_{\beta \in F}(x - \beta), \beta \in GF(q).$$

*Замечание.* В качестве $q$ для построения РС-кода выбирают $q = p^m$, где $p$ – простое число, $m > 1$.

Степень порождающего многочлена циклического кода $\deg g(x) = n - k = r$. С учетом границы Синглтона ($r = 2t$), для исправления ошибок кратностью $t$, порождающий многочлен будет иметь степень

$$\deg g(x) = r = 2t.$$

Если $M(x) = (x - \beta)$ – минимальный многочлен элемента $\beta$ поля $GF(q)$, а $\beta_i = \alpha^i$, то порождающий многочлен РС-кода равен:

$$g(x) = \prod_{i=1}^{2t} M^{\beta_i}(x) = \prod_{i=1}^{2t}(x - \beta_i) = \prod_{i=1}^{2t}(x - \alpha^i) =$$

$$= (x - \alpha)(x - \alpha^2) \dots (x - \alpha^{2t}).$$

Так как $r = 2t = d - 1$,

$$g(x) = \prod_{i=1}^{d-1}(x - \alpha^i) = \prod_{i=1}^{d-1}(x - \alpha)(x - \alpha^2) \dots (x - \alpha^{d-1}). \qquad (4.32)$$

*Утверждение 4.2.* Размерность РС- кода равна

$$k = (q - 1 - 2t). \qquad (4.33)$$

Для $k = (q - 1 - 2t)$ существует $[q - 1, q - 1 - 2t, n - k + 1]$ - код Рида-Соломона над полем $GF(q)$.

Пример. 4.31. Записать порождающий многочлен РС-кода над полем $GF(5)$ длиной $n = q - 1 = 4$ и кодовым расстоянием $d$ = 3. Определить параметры кода.

Решение. В качестве примитивного элемента $GF(5)$ возьмём элемент $\alpha$ = 2 Порождающий многочлен (4.32)

$g(x) = (x - \alpha)(x - \alpha^2) = (x - 2)(x - 4) = (x + 3)(x + 1) = (x^2 + x + 3x + 3) = x^2 + 4x + 3.$

Находим параметры $[n, k, d]$ РС- кода. Из формулы (4.33)

$$k = n - d + 1 = 2.$$

Пусть информационный полином $f(x) = 1 + x$. Кодовое слово РС-кода $c(x) = f(x)g(x) = (1 + x)(x^2 + 4x + 3) = x^2 + 4x + 3 + x^3 + 4x^2 + 3x = x^3 + 5x^2 + 7x + 3 = x^3 + 2x + 3.$

Полиному $c(x)$ соответствует вектор над $GF(5)$ – (3 2 0 1).

Мощность кода $M = q^k = 5^2 = 25.$

Пример 4.32. Найти порождающий полином РС-кода над $GF(4) = \{0, 1, \alpha, \beta = \alpha^2\}$ с кодовым расстоянием $d$ = 2. Примитивный элемент поля $\alpha \in GF(4)$ – корень уравнения $(1 + x + x^2) = 0$.

Решение. Для РС-кодов над $GF(4)$ длиной $n = q - 1 = 3$ с расстоянием $d$ = 2 из формулы (4.32) следует

$$g(x) = (x - \alpha).$$

Число информационных символов вычисляется из выражения (4.33).

$$k = n - d + 1 = 2.$$

Мощность кода $M = q^k = 4^2 = 16.$

Получаем [3, 2, 2] РС-код. $q$-ичная запись информационных векторов и, соответствующих им полиномов, приведена в табл. 2.26 и 2.27.

Таблица 4.14

| | | | |
|---|---|---|---|
| 00 | 10 | $\alpha 0$ | $\beta 0$ |
| 01 | 11 | $\alpha 1$ | $\beta 1$ |
| $0\alpha$ | $1\alpha$ | $\alpha\alpha$ | $\beta\alpha$ |
| $0\beta$ | $1\beta$ | $\alpha\beta$ | $\beta\beta$ |

Таблица 4.15

| | | | |
|---|---|---|---|
| 0 | 1 | $\alpha$ | $\beta$ |
| $x$ | $1+ x$ | $\alpha + x$ | $\beta + x$ |
| $\alpha x$ | $1+ \alpha x$ | $\alpha + \alpha x$ | $\beta + \alpha x$ |
| $\beta x$ | $1+ \beta x$ | $\alpha + \beta x$ | $\beta + \beta x$ |

Множество кодовых слов $\{c(x)\}$ РС-кода над полем $GF(4)$ определяется на основе операций сложения и умножения, задаваемых таблицами Кэли (табл. 4.16 и 4.17).

Таблица 4.16

| + | 0 | 1 | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| 0 | 0 | 1 | $\alpha$ | $\beta$ |
| 1 | 1 | 0 | $\beta$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $\beta$ | 0 | 1 |
| $\beta$ | $\beta$ | $\alpha$ | 1 | 0 |

Таблица 4.17

| × | 0 | 1 | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $\alpha$ | $\beta$ |
| $\alpha$ | 0 | $\alpha$ | $\beta$ | 1 |
| $\beta$ | 0 | $\beta$ | 1 | $\alpha$ |

Ненулевые кодовые слова запишем в двух формах: в виде многочленов и векторов, координатами которых являются элементы поля $GF(q)$.

$$c(x) = f(x)g(x),$$
$$c(x) = \gamma_0 + \gamma_1 x^1 + \gamma_2 x^2,$$
$$c = (\gamma_0\ \gamma_1\ \gamma_2),$$

где $f(x)$ – информационный полином, $\gamma_j \in GF(4)$.

$c_1(x) = f_1(x)q(x) = 1(x-\alpha) = (x-\alpha);$ $\quad c_1 = \alpha\ 1\ 0.$

$c_2(x) = f_2(x)q(x) = \alpha(x-\alpha) = (\alpha x - \alpha^2) = (\alpha x - \beta);$ $\quad c_2 = \beta\ \alpha\ 0.$
$c_3(x) = f_3(x)q(x) = \beta(x-\alpha) = (\beta x - \beta\alpha) = (\beta x - 1);$ $\quad c_3 = 1\ \beta\ 0.$
$c_4(x) = f_4(x)q(x) = x(x-\alpha) = (x^2 - \alpha x);$ $\quad c_4 = 0\ \alpha\ 1.$
$c_5(x) = f_5(x)q(x) = \alpha x(x-\alpha) = (\alpha x^2 - \alpha^2 x);$ $\quad c_5 = 0\ \beta\ \alpha.$
……
$c_{10}(x) = f_{10}(x)q(x) = (\alpha + x)(x-\alpha) = (\alpha x - \alpha^2 + x^2 - \alpha x) = (\beta + x^2);$
$c_{10} = \beta\ \ 0\ 1.$
……
$c_{15}(x) = f_{15}(x)q(x) = (\beta + \beta x)(x-\alpha) = (\beta x - \beta\alpha + \beta x^2 - \beta\alpha x) =$
$(1 + (\beta - \beta\alpha)x + \beta x^2) = (1 + (\beta - 1)x\ + \beta x^2) = (1 + \alpha x\ + \beta x^2);$ $\quad c_{15} =$
$1\ \alpha\ \beta.$

5. Вероятность ошибки декодирования кода

Пусть ДСК характеризуется вероятностью ошибки на символ $p$. Введем вектор ошибки $E = (e_1 \ldots e_j \ldots e_n)$; $e_j = 1$ с вероятностью $p$ и $e_j = 0$ с вероятностью $(1-p)$. Найдем вероятность возникновения следующих конфигураций векторов ошибок $E$ для кодового слова длиной $n = 5$.

Prob$\{E = (00000)\} = (1-p)^5$ – есть вероятность правильного приема кодового слова длиной 5.

$\text{Prob}\{\ E = (10000)\} = p(1-p)^4.$

$\text{Prob}\{\ E = (10010)\} = p^2(1-p)^3.$

В общем случае, вероятность возникновения вектора ошибок $E$ веса $i$ запишется в виде

$$\text{Prob}\{\ E_{wt(i)}\} = p^i(1-p)^{n-1}. \qquad (5.1)$$

Вероятность правильного приема кодового слова длиной $n$ равна

$$\text{Prob}\{\ E_{wt(0)}\} = (1-p)^n.$$

Пример 5.1. Пусть $p = 0{,}2;\ n = 5$. Рассмотрим следующие возможные вероятности возникновения векторов ошибок.

1. Вероятность того, что не произошло ни одной ошибки на длине кодового слова:

$$\text{Prob}\{\ E_{wt(0)} = (00000)\} = (1-0{,}2)^5 \cong 0{,}32.$$

2. Вероятность того, что на длине кодового слова имеется ошибка единичного веса

$$\text{Prob}\{\ E_{wt(1)} = (10000)\} = p^1(1-p)^4 = 0{,}2(1-0{,}2)^4 \cong 0{,}081.$$

3. Вероятность того, что произошли две ошибки на длине кодового слова:

$$\text{Prob}\{\ E_{wt(2)} = (10010)\} = p^2(1-p)^3 = 0{,}2^2(1-0{,}2)^3 \cong 0{,}01.$$

Из приведенного примера следует:

– вектор ошибок единичного веса более вероятен, чем вектор ошибок веса два и т.д.;

– ошибки малого веса необходимо обнаруживать и исправлять в первую очередь.

## 5.1. Распределение весов ошибок

На длине $n$ кодового слова возможны следующие ошибки:

– одиночные, $t = 1$;

– двойные, $t = 2$;

– трехкратные, $t = 3$ и т.д.

На длине кодового слова возможны различные конфигурации ошибок – векторы ошибок различного веса и формы. Обозначим $t_i$ – число всех конфигураций ошибок веса $i$. Это число определяется биноминальным коэффициентом

$$C_n^i = \frac{A_n^i}{P_i} = \frac{n(n-1)\ldots(n-i+1)}{i!}.$$

Пример 5.2. Найти распределение весов ошибок на длине кодового слова $n = 5$. Число конфигураций однократных ошибок равно

$$t_1 = C_5^1 = 5.$$

Соответственно находим число следующих конфигураций ошибок:

$$t_2 = C_5^2 = \frac{A_5^2}{P_2} = \frac{n(n-1)}{2!} = \frac{5\cdot 4}{2} = 10.$$

$$t_3 = C_5^3 = \frac{A_5^3}{P_3} = \frac{n(n-1)(n-2)}{3!} = \frac{5\cdot 4\cdot 3}{2\cdot 3\cdot} = 10.$$

$$t_4 = 5, t_5 = 1.$$

Суммарное число возможных конфигураций ошибок на длине $n$ составит

$$t_\Sigma = 2^n - 1 = \sum_{i=1}^n t_i = \sum_i^n C_n^i.$$

Для приведенного примера

$$t_\Sigma = t_1 + t_2 + t_3 + t_4 + t_5 = 5 + 10 + 10 + 5 + 1 = 31.$$

Вероятность того, что в слове длиной $n$ содержится хотя бы одна однократная ошибка, определяется выражением

$$\text{Prob}\{ E_{wt(1_n)}\} = C_n^1 p^1 (1-p)^{n-1}.$$

Для рассматриваемого примера получаем вероятность возникновения хотя бы одной конфигурации однократной ошибки

$$\text{Prob}\{ E_{wt(1_n)}\} = C_n^1 p^1 (1-p)^{n-1} \cong 5 \cdot 0{,}081 \cong 0{,}4.$$

Вероятность того, что имеется хотя бы одна конфигурация двукратной ошибки

$$\text{Prob}\{ E_{wt(2_n)}\} = C_n^2 p^2 (1-p)^{n-2} \cong 10 \cdot 0{,}01 \cong 0{,}1.$$

Вновь подтверждается, что ошибки малого веса необходимо обнаруживать и исправлять в первую очередь.

В общем случае, вероятность того, что в слове длиной $n$ содержится хотя бы одна ошибка кратностью $t$ или величины веса $i$ равна

$$\text{Prob}\{ E_{wt(i_n)}\} = C_n^i p^i (1-p)^{n-i}. \qquad (5.2)$$

## 5.2. Вероятность ошибки декодирования кодового слова

Вероятностью ошибки декодирования кодового слова называется вероятность появления неправильного кодового слова на выходе декодера.

Пусть имеется код мощностью $M$. Слова кода $X^1, X^2, \dots, X^s, \dots, X^M$ передаются по каналу с равной вероятностью. Тогда средняя вероятность ошибки декодирования на кодовое слово

$$P_f = \frac{1}{M}\sum_{s=1}^{M} \text{Prob}\{\text{слово на выходе декодера } \neq X^s | X^s \text{было передано.}$$

При декодировании используем стандартное расположение для кода. Напомним, что выбранный декодером вектор ошибки всегда есть один из лидеров смежных классов. Ошибка декодирования происходит тогда и только тогда, когда вектор ошибок не является лидером смежного класса, т.е.

$$P_f = \text{Prob}\{E \neq \text{лидер смежного класса.}$$

Предположим, что в таблице стандартного расположения имеется $a_i$ лидеров смежных классов веса $i$, т.е. число векторов ошибок веса $i$ равно $a_i$. Используя (5.1), найдем вероятность того, что вектор ошибки $E$ является лидером смежного класса

$$\text{Prob}\{E = \text{лидер смежного класса}\} = \sum_{i=0}^{n} a_i p^i (1-p)^{n-i}. \qquad (5.3)$$

Выражение (5.3) характеризует правильное декодирование. Вероятность непоявления события (5.3) представляется как вероятность ошибки декодирования (вероятность появления неправильного кодового слова на выходе декодера):

$$P_f = 1 - \sum_{i=0}^{n} a_i p^i (1-p)^{n-i}. \qquad (5.4)$$

Если код имеет кодовое расстояние $d = 2t + 1$, он исправляет все $t$- кратные конфигурации ошибок. В этом случае диапазон весов $i$ исправляемых векторов ошибок лежит в пределах

$$0 \leq i \leq t.$$

Тогда каждый вектор ошибок веса не более $t$ является лидером смежного класса. Число лидеров смежного класса веса $i$ для кода с минимальным расстоянием $d = 2t + 1$ находится их выражения, полученного ранее для возможного числа ошибок кратностью $t$ на длине $n$ кодового слова, т.е.

$$a_i = C_n^i.$$

Большинство известных кодов могут исправлять некоторые конфигурации ошибок для значений $i > t$. Вычисление числа лидеров смежных классов для значений $i > t$ не простая задача. Эти числа известны только для немногих

кодов. Но если вероятность ошибки $p$ в канале такова, что

$$(1-p) \cong 1 \text{ и } p^i(1-p)^{n-i} \gg p^{i+1}(1-p)^{n-i-1},$$

в этом случае в формуле (5.4) пренебрегают членами с большими значениями $i$. Тогда вероятность ошибки $P_f$ декодирования кодового слова на основе таблицы стандартного расположения определяется по формуле

$$P_f \cong 1 - \sum_{i=0}^{t} C_n^i p^i (1-p)^{n-i}. \quad (5.5)$$

Пример 5.3. Определить ошибку декодирования кодового слова кода [4,2,2], используя стандартное расположение для кода табл. 4.2; вероятность ошибки на символ $p = 0{,}2$.

Таблица 4.2

| | | | | |
|---|---|---|---|---|
| 0000 | 1011 | 0101 | 1110 | $s = \begin{bmatrix}0\\0\end{bmatrix}$ |
| 1000 | 0011 | 1101 | 0110 | $s = \begin{bmatrix}1\\1\end{bmatrix}$ |
| 0100 | 1111 | 0001 | 1010 | $s = \begin{bmatrix}0\\1\end{bmatrix}$ |
| 0010 | 1001 | 0111 | 1100 | $s = \begin{bmatrix}1\\0\end{bmatrix}$ |

Решение. По таблице находим число лидеров смежных классов веса $i$:

$$a_{i=0} = 1, a_{i=1} = 3.$$

$$P_f = 1 - \sum_{i=0}^{n} a_i p^i (1-p)^{n-i} = 1 - \sum_{i=0}^{4} a_i p^i (1-p)^{4-i} =$$
$$= 1 - p^0(1-p)^4 - 3p^1(1-p)^3 = 1 - 0{,}8^4 - 3 \cdot 0{,}2 \cdot 0{,}8^3 = 0{,}2832.$$

Упражнение 5.1. Определить ошибку декодирования кода [6,3,3], используя стандартное расположение для кода, представленного матрицей

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix},$$

вероятность ошибки на символ $p = 0{,}01$.

## 5.4. Совершенные и несовершенные коды

Если число лидеров смежных классов веса $i$ равно $a_i = 0$ при

$$i > t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

то оценка ошибки декодирования определяется по точной формуле

$$P_f = 1 - \sum_{i=0}^{t} C_n^i p^i (1-p)^{n-i}$$

Оценка справедлива для, так называемых, совершенных кодов. Для такого кода нет ни одной конфигурации ошибок веса большего, чем кратность исправляемых. Совершенный код, исправляющий $t$ ошибок, может исправлять все ошибки веса не более $t$ и не может исправлять ни одной ошибки веса больше, чем $t$.

Если число лидеров смежных классов веса веса $i$ равно $a_i = 0$, при

$$i > t + 1,$$

код называется квазисовершенным. Для него точной формулой $P_f$ декодирования кодового слова будет выражение

$$P_f = 1 - \sum_{i=0}^{t} C_n^i p^i (1-p)^{n-i} - a_{t+1} p^{t+1} (1-p)^{n-(t+1)}.$$

Квазисовершенный код может исправлять:

– все ошибки веса не более $t$;

– некоторые ошибки веса $t + 1$;

– не может исправлять ни одной ошибки веса больше, чем $t + 1$.