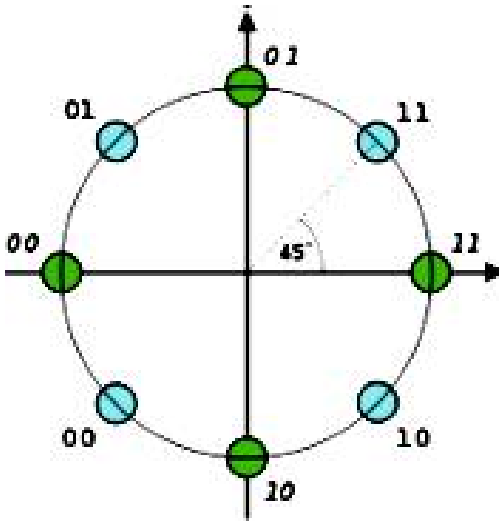
А. В. Володько

СТАТИСТИЧЕСКАЯ ТЕОРИЯ СИСТЕМ

Практикум



Воронеж 2021

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Воронежский государственный технический университет»

А. В. Володько

СТАТИСТИЧЕСКАЯ ТЕОРИЯ СИСТЕМ

Практикум

Воронеж 2021

УДК 681.51.01:519.22(07)
ББК 65.01я7
В68

Рецензенты:
кафедра информационной безопасности и систем связи
Международного института компьютерных технологий (г. Воронеж);
(зав. кафедрой канд. техн. наук, доц. О. С. Хорпяков);
А. В. Останков, д-р техн наук, проф.

Володько, А. В.

В68 **Статистическая теория систем**: практикум [Электронный ресурс]. – Электрон. текстовые и граф. данные (1,5 Мб) / А. В. Володько. Воронеж: ФГБОУ ВО «Воронежский государственный технический университет», 2021. – 1 электрон. опт. диск (CD-ROM): цв. – Систем требования: ПК 500 и выше; 256 Мб ОЗУ; Windows XP; SVGA с разрешением 1024x768; Adobe Acrobat; CD-ROM дисковод; мышь. – Загл. с экрана.

ISBN 978-5-7731-0996-9

Практикум содержит необходимые материалы и задания к проведению лабораторных и практических занятий дисциплины «Статистическая теория систем».

Первая часть практикума посвящена вопросам помехоустойчивого кодирования. В сжатой форме представлены минимальные теоретические сведения, необходимые для освоения материала, а также подробно описан порядок выполнения лабораторно-практических заданий.

Вторая часть содержит описание лабораторно-практических занятий, проводимых с привлечением специального лабораторного оборудования.

В третьей части приведены теоретические сведения теории кодирования информации.

Практикум предназначен для студентов специальности 11.05.01 «Радиоэлектронные системы и комплексы» очной формы обучения.

Ил. 33. Библиогр.: 22 назв.

УДК 681.51.01:519.22(07)
ББК 65.01я7

Издается по решению редакционно-издательского совета
Воронежского государственного технического университета

ISBN 978-5-7731-0996-9

ВВЕДЕНИЕ

Кодирование сообщений является важной и неотъемлемой частью любой современной радиотехнической системы передачи информации. Технологии кодировании позволяют решить многие актуальные задачи связи, такие как увеличение помехоустойчивости сообщений, повышение верности передаваемой информации, большей эффективности использования физического канала связи.

Основной целью выполнения цикла работ является ознакомление студентов с различными методами кодирования, оценки помехоустойчивости сообщений и приобретение практических навыков кодирования / декодирования информации. Лабораторные задания выполняются на лабораторных стендах, на панели которого представлены наборы блоков. Соединяя блоки, можно собрать кодирующее и декодирующее устройства, проверить их функционирование, корректирующие способности декодера. Из дополнительных приборов требуется двухлучевой осциллограф с режимом внешней синхронизации.

В третьей части в сжатой форме приведены необходимые теоретические сведения принципов и методов кодирования, а также вопросы и материалы для самостоятельного контроля пройденного материала

1. КОДИРОВАНИЕ И ДЕКОДИРОВАНИЕ ЦИКЛИЧЕСКИХ КОДОВ

1.1. Помехоустойчивое кодирование. Необходимые теоретические сведения

1.1.1. Основной принцип помехоустойчивого кодирования

Помехоустойчивое кодирование предназначено для повышения помехоустойчивости передачи информации путем коррекции ошибок, возникающих в канале связи. Коррекция ошибок возможна только при наличии избыточности переданного сообщения. При помехоустойчивом кодировании избыточность вносится в сообщение так, чтобы наилучшим образом корректировать ошибки, характерные для данного канала. Коды различаются правилами внесения избыточности.

Прежде всего, помехоустойчивые коды бывают блочными и непрерывными. При блочном кодировании последовательность символов сообщения разбивается на группы по K символов, каждой группе присваивается кодовая комбинация (блок) из n символов, $n > K$. Кодов комбинации из n символов выбираются по каким-то правилам. Различные правила дают различные коды. Возможно случайное помехоустойчивое кодирование. В этом случае имеет место случайное сопоставление группе из K информационных символов кодовой комбинации из n символов. Благодаря наличию избыточности этот код также будет корректировать ошибки, но устройства кодирования и особенно декодирования будут сложными вследствие необходимости большой памяти. Большое распространение получило регулярное кодирование, при котором кодовые комбинации формируются по определенному правилу на основе известных K информационных символов, при этом предыдущие и последующие группы информационных символов на выбор текущей кодовой комбинации не влияют. Мы будем рассматривать исключительно регулярное кодирование.

Непрерывные коды характеризуются тем, что операции кодирования и декодирования производятся непрерывной последовательностью символов сообщения без разбиения ее на группы, блоки. К таким кодам относится сверточный код.

По виду воздействия помех на сообщения различают каналы с независимыми и группирующимися ошибками. Соответственно помехоустойчивые коды можно разделить на два класса: исправляющие независимые ошибки и исправляющие пакеты ошибок. Далее будем рассматривать коды, исправляющие независимые ошибки, они обусловливаются в основном помехами в виде шумов. В случае, если канал характеризуется группирующимися ошибками, целесообразно провести перемещения символов сообщения или декорреляцию ошибок с последующим применением кодов, для независимых ошибок. Далее будем рассматривать, двоичные коды, когда кодовыми являются символы ***1*** и ***0.***

1.1.2. Блочные коды, основные характеристики

Большинство блочных кодов относится к линейным систематическим кодам. Название «систематический» означает, что кодовая комбинация из n символов четко разделяется на информационную часть и проверочные символы. Обычно и информационные символы занимают первые k позиций в кодовой комбинации. Последние r позиций,

$$r = n-k \qquad (1)$$

заняты проверочными символами, которые не несут информацию, являются избыточными и используются для коррекции ошибок.

Название «линейный» означает, что проверочные символы формируются на основе каких-то информационных при использовании определенной линейной операции, чаще всего суммирования по модулю два.

Основными характеристиками блочных кодов являются:

- число разрешенных N_p и запрещенных N_3 кодовых комбинаций,
- хеммингово и кодовое расстояние d,
- веса кодовых комбинаций w.

Поясним коротко каждую характеристику.

Среди всех возможных 2^n кодовых комбинаций длины n только некоторые будут использованы для построения кода. Эти комбинации называются разреженными, их число

$$N_P = 2^K \qquad (2)$$

определяется числом комбинаций по $к$ информационных символов. Остальные комбинации

$$N_3 = 2^n - 2^к \qquad (3)$$

являются запрещенными и при передаче информации не используются.

Любые две кодовые комбинации отстоят друг от друга на какое-то расстояние. Это расстояние называется хеммингом, оно определяется как число позиций, в которых одна комбинация отличается от другой. Например, кодовые комбинации 0101110 и 1110010 имеют хеммингово расстояние $d = 4$. Чтобы проще его определить, целесообразно записать комбинации одну под другой. Сравнение символов в каждой позиции можно заменить суммированием по модулю два. Число «1», полученных в результате суммирования, и даст значение хеммингова расстояния.

0101110
1110010
1 111 d = 4

Для разрешенных кодовых комбинаций будет большое число пар комбинаций, для каждой пары вычисляется хеммингово расстояние. Наименьшее из его возможных значений является важнейшей характеристикой кода и называется кодовым расстоянием. Обозначается также буквой d.

Вес w кодовой комбинации - это число единичных символов в ней. Веса разрешенных кодовых комбинаций могут быть как одинаковыми, так и различ-

ными. О значении этой и других характеристик кода подробнее познакомимся при дальнейшем изучении блочных кодов.

Линейные систематические коды обозначаются (***n,K***), где ***n*** - длина кодовой комбинации, ***K*** - число информационных символов в ней.

1.1.3. Виды декодирования

Коррекция ошибок осуществляется при декодировании принятой кодовой комбинации, при преобразовании ее в последовательность информационных символов. При этом возможны прием «в целом» и последетекторное декодирование. При приеме «в целом» принятая комбинация рассматривается как единый сигнал, который принадлежит к ***m*** - ичным сигналам, $m = 2^K$.

Преобразование этого сигнала в информацию осуществляется уже известными нам методами оптимального приема на основе многоканального корреляционного приемника или согласованных фильтров. При последетекторном декодировании в приемнике сначала выносится решение относительно каждого кодового символа, а затем по принятым кодовым символам выносится решение о переданной информации. Здесь уже можно говорить о кратности ошибки, то есть о числе ошибочных символов в принятой кодовой комбинации. При декодировании ошибки некоторой кратности могут быть исправлены, это декодирование с исправлением ошибки. Ошибки другой кратности могут быть только обнаружены. Это декодирование с обнаружением ошибок. При обнаружении ошибок принятая комбинация получателю не выдается, она стирается. Этот вид декодирования есть смысл использовать в каналах с обратной связью: передается запрос на повторение той комбинации, в которой обнаружена ошибка.

Рассмотрим поподробнее различные виды декодирования и укажем, какие кратности ошибок будут корректироваться гарантированно при использовании заданного кода, с кодовым расстоянием d.

Декодирование с обнаружением ошибок

Основной принцип такого декодирования - определить, является ли принятая кодовая комбинация разрешенной или запрещенной. Если принята разрешенная комбинация, то информационные символы выдаются получателю, так как считается, что в комбинации нет ошибки (хотя на самом деле она может и быть). Если при декодировании установлен факт, что принята неразрешенная комбинация, то она стирается, то есть информация получателю не выдается. Теперь можно решить вопрос, какие кратности ошибок будут обнаруживаться. Ответ прост: обнаруживаться будут те ошибки, которые не переведут переданную разрешенную кодовую комбинацию в другую разрешенную. Для решения вопроса о кратности обнаруживаемой ошибки вернемся к рассмотрению хемминга расстояния. Его можно рассматривать как число позиций, занятых искаженными символами в одной комбинации, которое переведет ее в другую. Короче, если для рассматриваемых выше комбинаций хеммингово расстояние $d = 4$, то четырехкратная ошибка может перевести одну комбинацию в другую.

Ошибка меньшей кратности никогда не переведет одну комбинацию в другую. Поэтому для всех разрешенных кодовых комбинаций кратность обнаруживаемой ошибки меньше кодового расстояния:

$$\rho_0 \le d - 1 \qquad (4)$$

Здесь следует заметить, что все ошибки таких кратностей будут гарантированно обнаруживаться. Но возможно обнаружение ошибок и большей кратности таких, которые не переводят переданную разрешенную комбинацию в другую разрешенную. Зная структуру кода, его характеристики, можно ответить на вопрос, какие кратности ошибок, более определяемой формулой (4), будут обнаруживаться. Об этом мы будем говорить ниже.

Декодирование с исправлением ошибки

Отличие от предыдущего вида декодирования состоит в том, что здесь надо определить место ошибки, позицию ошибочного символа, и сформировать сигнал исправления. При декодировании определяется сигнал, который указывает на место ошибки. Этот сигнал называется локатором ошибки. Для определения кратности исправляемой ошибки опять вернемся к понятию хеммингова расстояния и его толкованию, которое мы привели при рассмотрении декодирования с обнаружением ошибки. Назовем искажение одного символа комбинации одним шагом. Тогда комбинация 0101110 перейдет в комбинацию 1110010 за четыре шага.

Распишем эти шаги.

0101110 → 1101110 → 1111110 → 1110110 → 1110010
Шаги: 1-й 2-й 3-й 4-й

При каждом шаге переименовывается только один символ, который отмечается точкой внизу. Предположим, что в приведенной выше цепочке две комбинации будут разрешенными: первая 0101110 и вторая 1110010. Остальные комбинации будут запрещенными. Комбинация 1101110 является запрещенной и отстоит от первой разрешенной комбинации на один шаг, а от второй разрешенной - на три шага. Можно сказать, что комбинация 1101110 ближе к первой разрешенной комбинации, чем ко второй. Запрещенная комбинация 1110110 стоит ближе ко второй разрешенной кодовой комбинации, чем к первой. А комбинация 1111110 имеет одинаковые расстояния от первой и второй разрешенной комбинации.

Все возможные комбинации длины ***n*** можно расположить в каком-то пространстве. Вокруг каждой разрешенной комбинации располагаются запрещенные комбинации, причем каждая разрешенная имеет вокруг себя область, содержащую близкие к ней запрещенные комбинации.

Запрещенные комбинации каждой области ближе к своей разрешенной комбинации, чем к любой другой. Ошибка будит исправляться правильно, если она не выведет переданную разрешенную комбинацию из своей области. Тогда исправление ошибки будет сводиться к замене запрещенной кодовой комбина-

ции своей разрешенной. Зная кодовое расстояние кода, можно ответить на вопрос о кратности исправляемой ошибки:

$$\rho_{И} < \frac{d}{2} \qquad (5)$$

Следует обратить внимание, что в этом выражении используется строгое неравенство. Ошибка кратности $\rho_{И} = \frac{d}{2}$ может дать запрещенную комбинацию, которая равноудалена от каких-то разрешенных комбинаций. Эта запрещенная комбинация не принадлежит ни одной области и никакой разрешенной комбинацией не может быть заменена. Ошибки кратности $\rho_{И} = \frac{d}{2}$ не исправляются.

Декодирование с обнаружением и исправлением ошибок

При этом виде декодирования ошибки кратности $\boldsymbol{\rho_o}$ обнаруживаются, а кратности $\rho_и$ исправляются. Обычно ошибка кратности $\boldsymbol{\rho_и < \rho_o}$. Очевидно ошибки, не выводящие разрешенную комбинацию из своей области, исправляются. Но имеются запрещенные комбинации, которые не принадлежат ни одной области. Ошибки, переводящие переданную разрешенную комбинацию в такие запрещенные, не могут быть исправлены, они только обнаруживаются. Соотношение для кратностей $\boldsymbol{\rho_и}$ исправляемой ошибки и $\boldsymbol{\rho_o}$ обнаруживаемой ошибки и кодовым расстоянием $\boldsymbol{d}$ для этого вида декодирования будет следующим

$$\boldsymbol{\rho_и + \rho_o + 1 = d} \qquad (6)$$

Рассмотрим примеры:

Пример 1. Оценить, какие виды декодирования возможны для кода (7,3) с кодовым расстоянием $\boldsymbol{d = 4}$. Указать допустимые кратности ошибок при каждом виде декодирования.

1) Декодирование с обнаружением ошибок. Кратность обнаруживаемой ошибки согласно формуле (4)

$$\boldsymbol{\rho_o \leq 4\text{-}1 = 3}$$

2) Декодирование с исправлением ошибки.

В соответствии с формулой (5) кратность исправляемой ошибки

$$\boldsymbol{\rho_и < 4/2 = 2}$$

3) Декодирование с обнаружением и исправлением ошибок.

Здесь надо помнить, что условие (6) должно выполняться при $\boldsymbol{\rho_и < \rho_o}$, то есть $\boldsymbol{\rho_и = 1, \rho_o = 2.}$

Таким образом, код (7,3) с кодовым расстоянием $\boldsymbol{d = 4}$ допускает все три вида декодирования.

1.1.4. Описание лабораторной установки

Лабораторный стенд (рис. 1.1) содержит панель, на которой представлены следующие устройства: программное, кодирующее, декодирующее и устройство коррекции ошибок.

Программное устройство, представленное отдельным блоком, содержит генератор тактовых импульсов (КТ7), формирователи сигналов: установки нуля «Уст. 0» (КТ8); импульса опроса «ИО» (КТ9); синхронизации осциллографа (КТ13) (в скобках указаны номера контрольных точек, в которых можно наблюдать соответствующие сигналы). В программное устройство входят также формирователи: сигналов переключения кодирующего устройства (КТ2); сигналов информации («ИНФ» – КТ1); сигналов ошибки («ОШ» – КТ3).

На передней панели лабораторного стенда представлена функциональная схема лабораторной работы. Основными блоками являются кодирующее и декодирующее устройства.

Кодирующее и декодирующее устройства содержат наборы блоков, гнезда для их соединения и клеммы контрольных точек.

Кодирующее устройство может быть собрано с использованием следующих блоков: регистр сдвига Д1, схема И-НЕ Д5, сумматор по модулю два Д3, схема 2И Д4 и схема 2И-ИЛИ Д6, формирователь СП Д2, а также гнезда Г1-Г13. Гнезда Г1 - Г4 являются выходами первого, второго, третьего, четвертого разрядов кодирующего регистра. Гнезда Г5 - Г7 являются входами сумматора по модулю два, выход которого через Д4 подключен ко входу регистра.

Гнезда Г1 – Г7 позволяют в соответствии с заданным порождающим полиномом подключить на входы сумматора по модулю два выходы соответствующих разрядов регистра сдвига. Для нормальной работы кодирующего устройства следует правильно выбрать СП, который должен иметь «1» в течение k информационных разрядов.

Выбор СП осуществляется переключением запускающего триггер импульса в 3, 4 или 6 такт. Сигнал в восьмом такте перебрасывает триггер в исходное состояние. Контроль СП проводится в точке КТ2. Гнезда Г9 – Г13 и схема Д5 позволяют подключить к ключам Д4 и Д6 СП прямой или инвертированный в соответствии с требуемой работой ключей. Кодовую комбинацию можно наблюдать в точке КТ5.

В сумматоре Д9 кодовая комбинация складывается по модулю 2 с сигналом ошибки (КТ3) и в контрольной точке КТ6 можно наблюдать сигнал с помехами (кодовая комбинация + ошибка).

На кодирующее устройство подается информация, которая набирается поразрядно с помощью тумблеров и может наблюдаться в КТ1. Верхнее положение тумблера соответствует «1», нижнее – «0». При наборе информации следует помнить, что информационная последовательность – это группа из k двоичных символов, то есть используются первые k тумблеров.

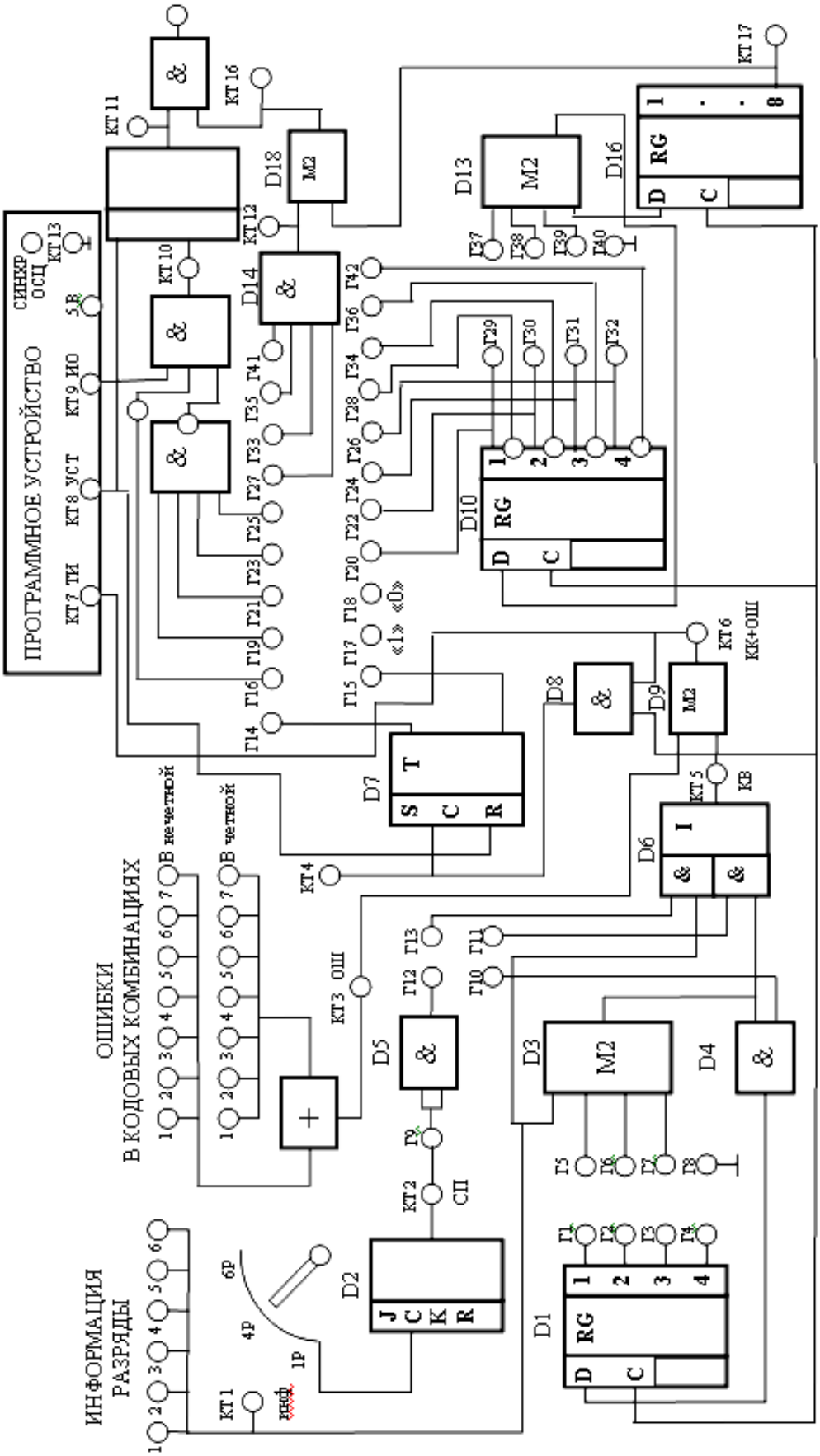


Рис. 1.1 Вид передней панели лабораторной установки

Ошибки набираются в виде комбинации, в которой символ «1» определяет позиции кодовой комбинации, искаженные помехой. В лабораторном стенде предусматривается независимый набор комбинаций ошибок в четных и нечетных кодовых комбинациях. В лабораторной работе используются кодовые комбинации длиной 7, и набор ошибок позволяет проимитировать ошибку в любой из семи позиций. Комбинации ошибок наблюдаются в контрольной точке КТ3.

Для продвижения информации в регистре сдвига Д1 требуются тактовые импульсы, которые вырабатываются в программном устройстве и подаются на кодирующий регистр (их можно наблюдать в КТ7).

Декодирующее устройство (ДКУ) содержит регистр сдвига Д10, сумматор по модулю два Д13, а также гнезда Г29 – Г32, Г37 – Г40.

Связи регистра сдвига с сумматором по модулю два должны быть выбраны с помощью гнезд Г29 – Г32, Г37 – Г40, как и в кодирующем устройстве, в соответствии с порождающим полиномом. Обработка информации в декодирующем регистре осуществляется в течение15 тактов. В 16-м такте регистр устанавливается в нулевое положение сигналом «Уст. 0), который вырабатывается в программном устройстве, его можно наблюдать в контрольной точке КТ8.

Устройство коррекции ошибок содержит: 8-разрядный регистр задержки Д16, триггер четности Д7 с элементом стробирования Д8; схему обнаружения ошибки – два элемента «И-НЕ» Д11 и Д12; триггер Д15; вырабатывающий сигнал сброса информации, если произошла неисправляемая ошибка; ключ – элемент «И» Д17; регистр задержки на 8 разрядов Д16 и схему исправления ошибки: дешифратор 1000 Д14, сумматор по модулю два Д18, а также гнезда Г14 – Г41, позволяющие собирать схему для заданного кода и для заданного вида декодирования.

1.2. Лабораторная работа «Кодирование циклических кодов»

1.2.1. Домашние задания и методические указания по их выполнению

1. Изучить основы теории помехоустойчивого кодирования: основные принципы кодирования, понятие о разрешенных и запрещенных кодовых комбинациях, видах декодирования, кодовом расстоянии, кратности ошибки. Циклические коды и их свойства. Представление кодовых комбинаций в виде полиномов условной переменной ***x***, понятие о порождающем полиноме и его свойствах. Структурную схему кодирующего устройства (назначение регистра сдвига, сумматора «по модулю два» и ключей). Диаграммы состояний кодирующего устройства в течение ***n*** тактов.

Для выполнения заданий следует воспользоваться литературой [1, с. 173-179; 2, с. 180-181].

2. Для кода (7, К) путем деления на порождающий полином определить разрешенную кодовую комбинацию (порождающий полином и информационные символы заданы в таблице вариантом во 2-м и 3-м столбцах).

Для заданного порождающего полинома нарисовать структурную схему кодирующего устройства. Представить в виде таблицы диаграмму состояний при кодировании заданной информации. Сравнить кодовую комбинацию, полученную на выходе кодирующего устройства, с кодовой комбинацией, полученной путем деления.

При получении кодовой комбинации путем деления на порождающий полином следует помнить, что k информационных символов следует представить в виде полинома условной переменной x степени (k – 1), затем этот полином надо умножить на x^r, где r – число проверочных символов, совпадающее со степенью порождающего полинома, а затем разделить на порождающий полином. Остаток от деления и даст проверочные символы. Сказанное можно пояснить на примере получения кодовой комбинации кода (7, 4) с порождающим полиномом $x^3 + x^2 + 1$ при информации $1110 = x^3 + x^2 + x$. Умножение на x^3 дает полином $x^6 + x^5 + x^4$. Деление на порождающий полином можно провести двумя способами: при обычном и двоичном представлениях полиномов.

$$
\begin{array}{l}
\oplus\ x^6 + x^5 + x^4 \ \big|\underline{x^3 + x^2 + 1} \\
\underline{x^6 + x^5 + x^3} \ \big|x^3 + x \\
\oplus\ x^4 + x^3 \\
\underline{x^4 + x^3 + x} \\
x
\end{array}
\qquad
\begin{array}{l}
\oplus\ 1110000 \ \big|\underline{1101} \\
\underline{1101} \qquad\quad \big|101 \\
\oplus\ 01100 \\
\underline{1101} \\
0010
\end{array}
$$

Получается кодовая комбинация $1110010 = x^6 + x^5 + x^4 + x$.

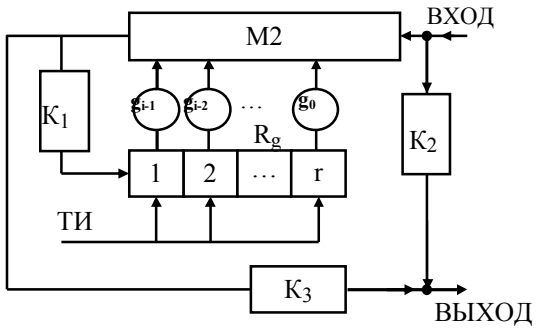


Рис. 1.2. Структурная схема кодирующего устройства

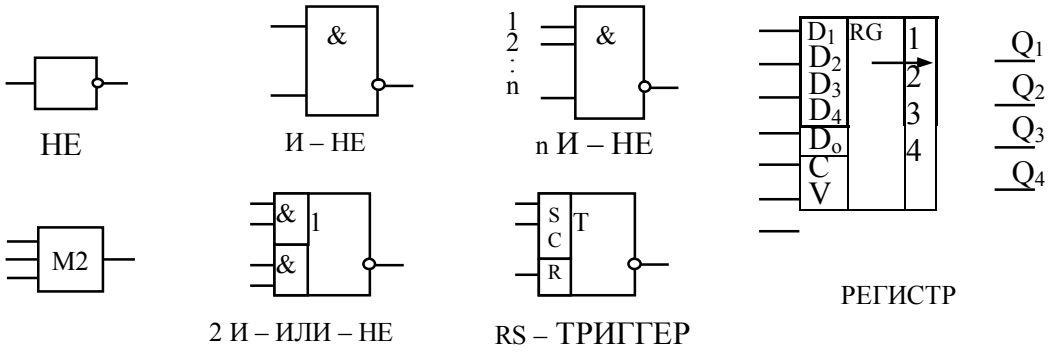


Рис. 1.3. Набор типовых микросхем

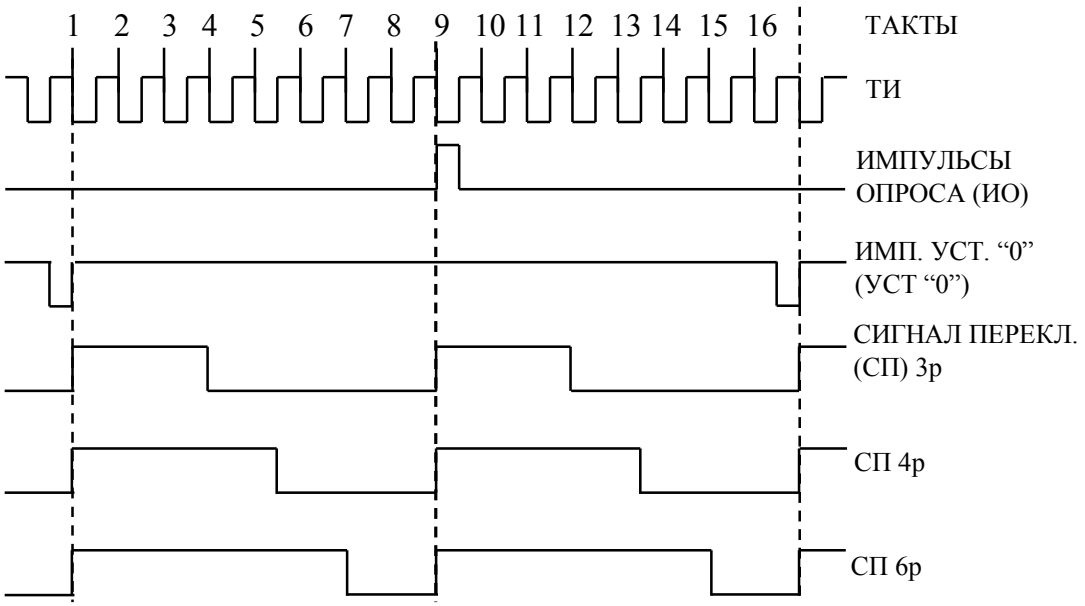


Рис. 1.4. Эпюры устройства кодирования

Реализация кодирующего устройства основана на том, что определение остатка можно осуществить с помощью линейных переключательных схем, называемых также линейными автоматами или многотактными фильтрами Хаффмана. Формирование циклического кода можно осуществить с помощью линейного автомата из ***r*** ячеек со связями, соответствующими порождающему полиному. Структурная схема кодирующего устройства представлена на рис. 1.2.

Регистр сдвига RG состоит из r разрядов. Выход i-го разряда подключается к сумматору по модулю два, если в порождающем полиноме $g(x) = g_r x^r + + g_{r-1} x^{r-1} + \ldots g_1 x + g_o$ коэффициент $g_{r-i} \neq 0$. Если $g_{r-i} = 0$, то связь отсутствует. Продвижение символов в регистре сдвига осуществляется при помощи сигнала сдвига – тактовых импульсов ТИ, и сигнал на выходе каждого разряда регистра равен сигналу на входе в предыдущий такт.

Схема рис. 1.2 работает следующим образом. В течение первых k тактов, когда на вход кодирующего устройства подается информация (k символов), ключ К3 разомкнут.

Ключи К1 и К2 замкнуты: информационная последовательность через ключ К2 подается в канал, а через ключ К1 на вход регистра сдвига подается результат сложения по модулю 2 выходов соответствующих разрядов регистра и информации. После k тактов ключ К3 замыкается, ключи К1 и К2 размыкаются, и линейный автомат начинает формировать остаток от деления, который получается на выходе сумматора и через замкнутый ключ К3 подается в канал, т.е. присоединяется к информационной последовательности. Процесс формирования кодового вектора, соответствующего входной информационной последовательности, заканчивается. На вход кодирующего устройства подаются следующие k информационные символы, процесс кодирования повторяется. Диаграмму состояний кодирующего устройства следует представить в виде табл. 1.1:

Таблица 1.1

Такты		1 2 3 4	5 6 7
Информация		1 1 1 0	0 0 0
Вход 1-го разряда регистра		1	0 0 0
Выходы разрядов регистра	1-го 2-го r-го	0 0 0	
Выход кодирующего устройства			
Замкнутые ключи		К1 К2	К3

В строку «Информация» в первые k тактов записываются информационные символы, а в последующие r тактов – нули. В приведенной таблице записана рассмотренная ранее информация 1110 из четырех символов. Далее следует учитывать, что перед началом работы кодирующего устройства регистр обнуляется, то есть на первом такте на выходе всех разрядов регистра сигнал будет нулевым. Сигнал на входе первого разряда регистра является результатом суммирования по модулю два информационного символа и символов с определенных выходов разрядов регистра.

Строка «Выход 1-го разряда регистра» заполняется в каждом такте последней, после того, как будут определены состояния регистра. На выход кодирующего устройства в первые k тактов, когда замкнут ключ К2, подаются информационные символы, а в последние r тактов, когда замкнут ключ К3, - замкнут ключ К3, - результат суммирования по модулю два. При разомкнутом ключе К1 (в течение последних r тактов) на вход 1-го разряда регистра подается уровень «лог. 0», что и отмечено в приведенной таблице.

Последующие домашние и лабораторные задания выполнять для исходных данных, приведенных в 4 – 5-м столбцах таблицы вариантов (табл. 1.2).

3. Провести расчет общих характеристик кода (7, r). Для заданного порождающего полинома определить число проверочных и информационных символов, обозначение кода, число запрещенных и разрешенных кодовых комбинаций.

Записать какую-нибудь кодовую комбинацию, обозначив в ней информационные и проверочные символы.

Записать все разрешенные кодовые комбинации (для кода (7, 6) – по 2 – 3 кодовые комбинации для каждой из групп, различающихся числом «1» в информационной части).

Определить веса кодовых комбинаций, хемминговы и кодовые расстояния.

Здесь следует еще раз обратиться к порождающему полиному и его свойствам. Именно по порождающему полиному можно определить число проверочных символов, какую-нибудь кодовую комбинацию. Свойства циклических кодов следует вспомнить для получения разрешенных кодовых комбинаций по какой-то одной известной. Для кодов (7, 3) и (7, 4) следует получить все разрешенные кодовые комбинации, проверяя при этом, чтобы информационные части встречались лишь по одному разу. Вес кодовых комбинаций определяется числом единиц в них.

Хемминговы расстояния следует определить для нескольких пар кодовых комбинаций, стараясь определить максимальное и минимальное значения. Для циклических кодов, которые здесь изучаются, минимальное хемминговое (кодовое) расстояние совпадает с расстоянием между нулевой кодовой комбинацией и комбинацией, представляющей порождающий полином, то есть кодовое расстояние совпадает с количеством слагаемых в порождающем полиноме.

Варианты исходных данных.

Таблица 1.2

Номер варианта	Данные для СРК		Данные для домашних и лабораторных заданий			
	порождающий полином	информация	порождающий полином	информация	номер символа с ошибкой	вид декодирования (для составления функциональной, схемы)
1	11101	110	11	100110	1	с триггером четности
2	11101	011	1011	1001	2	с обнаружением ошибок
3	11101	010	1101	1001	3	с исправлением ошибок
4	10111	110	11101	110	4	с обнаружением ошибок
5	11101	100	10111	100	5	с исправлением ошибок
6	10111	011	11	101111	6	с регистром сдвига и сумматором по модулю 2
7	10111	010	1011	1010	7	с исправлением ошибки
8	10111	100	1101	1010	1	с обнаружением ошибок
9	10111	111	11101	100	2	с исправлением ошибки
10	11101	111	10111	110	3	с обнаружением ошибок
11	10111	001	11101	111	4	с исправлением ошибки
12	11101	001	10111	111	5	с обнаружением ошибок

Примечание. Порождающие полиномы представлены в двоичном виде.

Например, $11 = x + 1$; $11101 = x^4 + x^3 + x^2 + 1$.

4. Разработать кодирующее устройство циклического кода.

По заданным информационным символам получить кодовую комбинацию путем деления на порождающий полином, найти ее среди разрешенных, полученных в 3-м задании.

Нарисовать структурную схему кодирующего устройства.

Представить в виде таблицы диаграммы состояний при кодировании заданной информации.

Сравнить полученную на выходе кодирующего устройства кодовую комбинацию с полученной путем деления.

Нарисовать функциональную схему кодирующего устройства.

Представить диаграммы напряжений, поясняющие работу функциональной схемы, и в частности, получение кодовой комбинации из информационной группы символов, сдвиг информации в регистре, работу ключей и т.д.

Функциональную схему кодирующего устройства рекомендуется составлять с использованием набора типовых микросхем, представленных на рис.1.3. При этом целесообразно считать, что срабатывание триггеров, продвижение информации в регистрах проводится по заднему фронту тактовых импульсов, как и в устройствах лабораторного стенда. На рис.1.3 приведена структурная схема универсального четырехразрядного регистра. Для него Д1 - Д4 – входы параллельной записи, С – вход тактовых импульсов, R – вход общего сброса, Q_1 – Q_4 - выходы разрядов регистра, V – разрешение параллельной/последовательной записи. При параллельной записи на вход V подается уровень лог. 1. Сдвиг информации в регистре осуществляется при V = 0 под воздействием тактовых импульсов на входе С (по заднему фронту). Такой регистр целесообразно использовать в кодирующем устройстве, а также при построении декодирующего регистра. На кодирующее устройство подаются сигналы информации, тактовые импульсы, сигнал переключения СП ключей, импульс установки «0» (эпюры трех последних сигналов представлены на рис. 1.4).

1.2.2. Лабораторные задания и методические указания по их выполнению

1. Изучить часть панели лабораторного стенда (рис.1.1), на которой может быть собрано кодирующее устройство, включающее в себя: тумблеры задания информации, переключатель сигнала переключения СП, инвертор Д5, кодирующий регистр Д1, четырехвходовый сумматор по модулю два Д3, элемент 2И – Д4, схему 2 – 2И – ИЛИ – Д3 и соответствующие гнезда.

Верхним положениям тумблеров задания информации соответствуют символы «1» информации, нижним – нулевые значения. Для набора информации следует использовать первые слева k тумблеров.

2. Собрать кодирующее устройство. В соответствии со структурной схемой кодирующего устройства, разработанной в четвертом задании:

наметить соединения гнезд Г1 – Г8 для установления связей регистра сдвига RG с сумматором по модулю два в соответствии с заданным порождающим полиномом, сделать соответствующие соединения;

разобраться, в качестве каких ключей могут использоваться схемы Д4 2И и Д6 2-ЗИ-ИЛИ; сделать соответствующие соединения гнезд Г10, Г11, Г13 с гнездами Г9, Г12.

Полученную схему зарисовать в отчет, представить преподавателю. После получения разрешения на проведение эксперимента включить источник питания стенда и тумблер «сеть» осциллографа, установить внешнюю синхронизацию на осциллографе сигналом с контрольной точки КТ13 панели лабораторного стенда.

Кодирующее устройство можно собрать с использованием блоков Д1, Д3, Д4 и Д6 путем соответствующего соединения гнезд Г1 – Г7, Г9 – Г13. Гнезда Г1 – Г7 используются для установки связей в кодирующем регистре в соответствии с порождающим полиномом. При соединении гнезд Г5 – Г7 следует помнить, что свободные входы сумматора М2 следует подключать к земляному гнезду Г8. Надо быть внимательным и не подключить к земле свободные выходы регистра. Гнезда Г9 – Г13 служат для подключения к ключам кодирующего устройства сигнала переключения нужной полярности. Прежде чем установить соединения гнезд, следует уточнить, роль какого ключа играют блоки Д4 и Д6-1, Д6-2. На ключи, замкнутые в течение первых k тактов, подается прямой сигнал переключения с Г9, а на остальные – инвертированный с Г12.

При установке синхронизации осциллографа следует иметь в виду, что информационные символы и, следовательно, кодовые комбинации на выходе кодирующего устройства повторяются каждые 16 тактов, из них первые 7 тактов отводятся на кодирование, 8-й такт – на обнаружение ошибки, 9 – 15-й такты – на декодирование и выдачу информации получателю, 16-й такт – на установку нулевых состояний в кодирующем и декодирующем устройстве. Устанавливать длительность развертки осциллографа целесообразно, наблюдая в точке КТ8 сигнал «Уст. 0», который появляется в конце каждого 16-го такта. При наблюдении эпюр напряжений надо четко знать номер позиции каждого символа на экране осциллографа.

3. Проверить функционирование кодирующего устройства. Наблюдая сигнал в точке КТ2, поставить переключатель СП в нужное положение. Задать информацию и наблюдать ее в КТ 1. Наблюдать сформированную кодовую комбинацию на выходе кодирующего устройства в КТ 5, сравнить ее с полученной в третьем задании.

Меняя информацию, просмотреть все кодовые комбинации и сравнить их с разрешенными, полученными в третьем задании.

Ввести ошибки в кодовые комбинации, кодовые комбинации с ошибками наблюдать в КТ6. Записать несколько искаженных кодовых комбинаций при различной кратности ошибок. Указать кратности ошибок, при которых искаженная кодовая комбинаций попадает в разряд разрешенных.

Зарисовать эпюры напряжений в точках: КТ7 ТИ, КТ8 Уст. «0», КТ1 инф., КТ2 СП, КТ5 КК, КТ3 ОШ, КТ6 КК+ОШ.

Сделать выводы о работе кодирующего устройства, об искажении кодовых комбинаций ошибками.

В лабораторном стенде формируются три возможных вида сигнала переключения, эпюры которых представлены на рис. 1.4. Условно их обозначим 3-5, 4-4, 6-2. Это означает, что из восьми позиций первые 3 (4, 6) имеют уровень «ЛОГ 1», остальные 5 (4, 2) – уровень «ЛОГ 0». Сигнал переключения наблюдается на КТ2. С помощью элемента НЕ Д5 можно сформировать инвертированный сигнал переключения.

Ввод ошибок в кодовые комбинации осуществляется с помощью двух рядов тумблеров. Верхний ряд вводит ошибки в нечетные комбинации (считая от начала развертки луча на экране осциллографа), а нижний ряд – четные. Просмотреть искаженные кодовые комбинации на КТ6 следует для кратности ошибки от 1 до 7. Здесь надо иметь в виду, что искаженная кодовая комбинация может совпасть с какой-то разрешенной при кратностях ошибки, равных весам кодовых комбинаций.

1.2.3. Содержание отчета

В отчет по лабораторной работе должны входить:

- результаты выполнения домашнего задания;
- результаты выполнения лабораторного задания;
- выводы по работе.

1.2.4. Контрольные вопросы

1. Дайте определение циклического кода.

2. Приведите основные характеристики кодов (n , n-1). Для конкретной длины кода дать ответы на следующие вопросы.

Чему равен вес кодовых комбинаций? Укажите два способа получения разрешенных кодовых комбинаций. Привести примеры разрешенных кодовых комбинаций. Нарисовать структурную схему кодирующего устройства. Представить таблицу состояний кодирующего регистра в течение n тактов, показать правильность работы кодирующего устройства.

3. Дайте характеристику кода (7, 3). Определить число разрешенных и запрещенных кодовых комбинаций. Чему равны веса кодовых комбинаций и кодовое расстояние кода? Привести примеры разрешенных кодовых комбинаций, получив одну из них путем деления на порождающий полином. Представить структурную схему кодирующего устройства и таблицу состояний при получении одной из кодовых комбинаций.

Порождающие полиномы: а) $x^4 + x^3 + x^2 + 1$;

б) $x^4 + x^2 + x + 1$.

4. Для кода (7, 4) определить число разрешенных и запрещенных кодовых комбинаций. Получить одну разрешенную кодовую комбинацию путем деления на порождающий полином. Как можно получить другие разрешенные кодовые комбинации? Чему равно кодовое расстояние этого кода. Представить структурную схему кодирующего устройства и таблицу состояний при получении одной из разрешенных кодовых комбинаций:

а) $g(x) = x^3 + x + 1$;

б) $g(x) = x^3 + +x^2 + 1$.

5. Перечислить свойства порождающего полинома.

1.3. Лабораторная работа «Декодирование циклических кодов»

1.3.1. Домашние задания и методические указания по их выполнению

1. Для кода (7, 3) нарисовать структурную схему декодирующего регистра. Составить таблицу состояний схемы при подаче на вход декодирующего регистра кодовой комбинации без ошибок и с ошибками. Указать признаки наличия ошибок, а также их места в кодовой комбинации.

Составить структурную схему декодирующего устройства с обнаружением и исправлением ошибки.

Обнаружение ошибок основано на том, что разрешенная кодовая комбинация делится на порождающий полином без остатка, а запрещенная – с остатком. Деление на порождающий полином, как и при кодировании, осуществляется регистром сдвига с сумматором по модулю два в обратной связи (ключ К1 замкнут всегда, а ключи К2, К3 отсутствуют).

Связи с сумматором по модулю два декодирующего регистра устанавливаются в соответствии с порождающим полиномом, как и в кодирующем устройстве. При делении без остатка все разряды декодирующего устройства в (n + 1)-м такте будут в нулевых состояниях. Наличие хотя бы одного символа «1» на выходах разрядов декодирующего регистра в (n + 1)-м такте свидетельствует о делении входной комбинации с остатком, т.е. о наличии в ней ошибки. Если код позволяет исправить однократную ошибку, то декодирующее устройство должно найти место ошибки, т.е. определить ошибочную позицию в коде. Таблица состояний декодирующего регистра составляется в течение 15 тактов; 8-й такт используется для обнаружения ошибки, а последующие семь тактов (9 – 15-й) – для исправления ошибки, если это возможно, и выдачи кодовой комбинации получателю. На ошибочную позицию и принятой кодовой комбинации указывает состояние 100 ….. 0 декодирующего регистра, то есть все разряды регистра, кроме первого, должны иметь нулевые состояния. При этом первая позиция исправляемой кодовой комбинации соответствует 9-му такту, а последняя – 15-му.

Структурная схема декодирующего устройства с обнаружением ошибок содержит декодирующий регистр с сумматором по модулю два, анализатор состояний регистра в 8-м такте и формирователь импульса сброса, сигнал с выхода которого используется для запирания выходного элемента. На второй вход этого элемента подается задержанная с помощью восьмиразрядного регистра входная кодовая комбинация. При наличии сигнала сброса (нулевого уровня) кодовая комбинация не проходит на выход декодирующего устройства, то есть она стирается.

Для кода (7, 3) кодовое расстояние, равное 4, гарантирует обнаружение ошибки кратности, не более 3. В действительности могут быть обнаружены некоторые ошибки большей кратности – те ошибки, которые переводят кодовую комбинацию в запрещенную. Для уточнения кратности обнаруживаемой ошибки надо использовать следующее свойство циклических кодов: сумма по модулю два двух разрешенных кодовых комбинаций дает разрешенную комбинацию. Таким образом, обнаружены будут все ошибки, комбинации которых совпадают с разрешенными кодовыми комбинациями. Для кода (7, 3), называемого кодом с постоянным весом (вес равен 4), обнаруживаются ошибки любой кратности, за исключением некоторых четырехкратных ошибок.

Декодирующее устройство с исправлением ошибки, кроме декодирующего регистра и 8-разрядного регистра задержки, содержит дешифратор комбинации 10….0 и сумматор по модулю два.

Рассматриваемый код (7, 3) имеет кодовое расстояние, равное 4, поэтому для него можно построить декодирующее устройство с исправлением одно- и обнаружением двукратной ошибок. Оно должно содержать оба такта: обнаружения и исправления. Но выходной элемент «И» должен запираться при неисправляемых ошибках, то есть при двукратных ошибках. Здесь следует учесть, что при двукратной ошибке вес принятой кодовой комбинации будет четным, а при однократной – нечетным. Определение четной кратности ошибки осуществляется с помощью триггера четности – RS-триггера, в котором подсчитывается число «1» в принятой кодовой комбинации. При четном числе «1» на выходе триггера четности формируется уровень «ЛОГ 1», который разрешает формирование импульса сброса и принятая кодовая комбинация стирается. При нечетном числе «1» (при однократной ошибке) импульс сброса не формируется и работает только тракт исправления ошибки. Здесь следует отметить, что в таком устройстве обнаруживаются все ошибки четной кратности за исключением некоторых четырехкратных ошибок. Исправляются только однократные ошибки, а остальные ошибки нечетной кратности приводят к не обнаруживаемой ошибке так же, как и четырехкратные ошибки, комбинации которых совпадают с разрешенными.

Структурная схема декодирующего устройства с обнаружением и исправлением ошибки представлена на рис. 1.5.

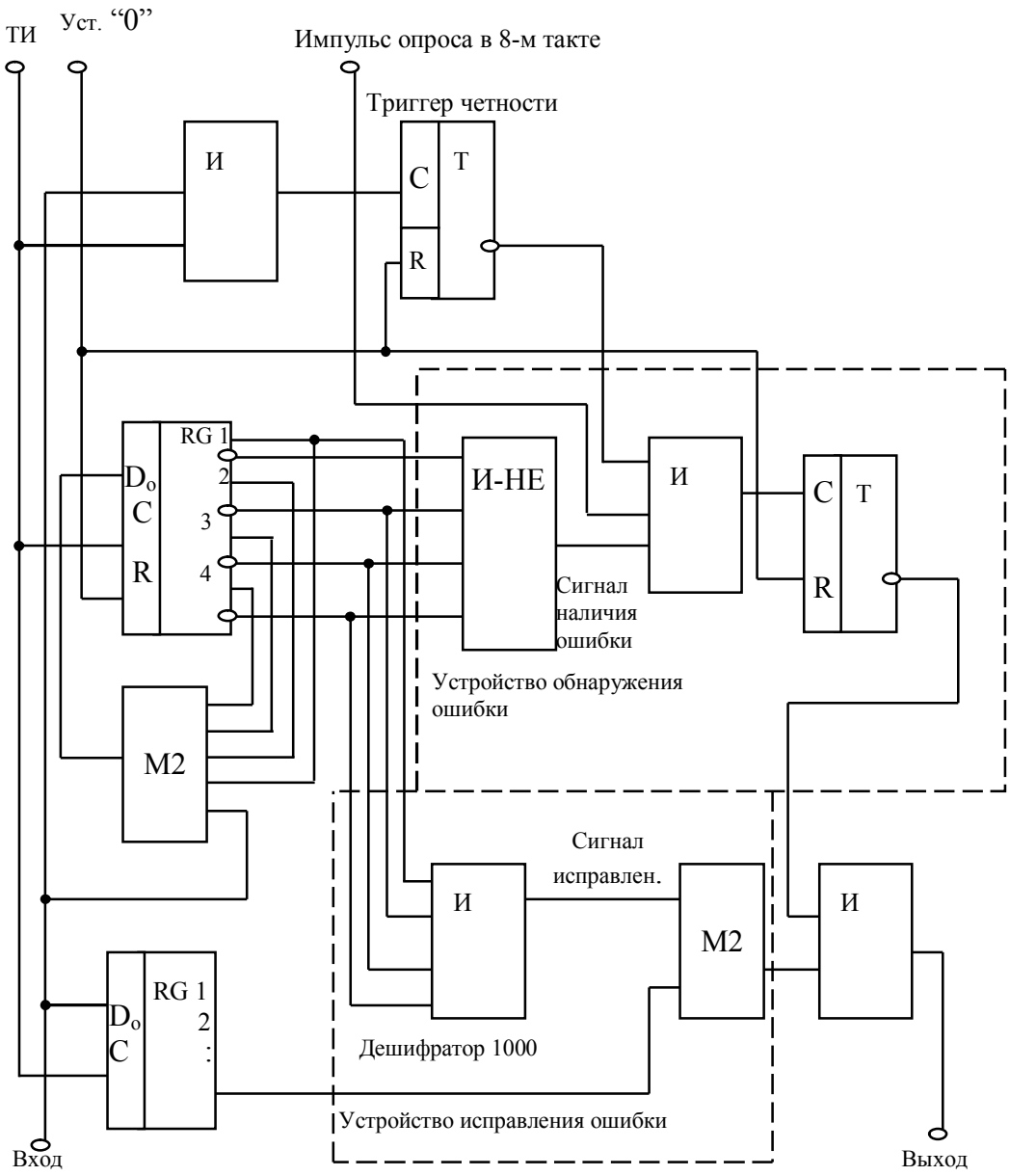


Рис. 1.5. Декодирующее устройство с обнаружением и исправлением ошибки для кода (7,3)

2. Для кода, заданного для домашних лабораторных заданий предыдущей лабораторной работы, определить возможные виды декодирования, для каждого вида указать кратность корректируемых ошибок (в том числе больше гарантированной кодовым расстоянием).

Нарисовать структурную схему декодирующего регистра. Составить таблицы состояний при подаче на вход декодирующего регистра кодовой комбинации без ошибок и с ошибками (ошибка – однократная, ее позиция указана в предпоследнем столбце таблицы вариантов (табл. 1.2)).

При выполнении этого задания следует иметь в виду, что декодирование возможно следующих видов:

а) декодирование с обнаружением ошибки, при котором гарантируется обнаружение ошибок, кратность ρ_o которых меньше кодового расстояния d: $\rho_o \le d - 1$;

б) декодирование с исправлением ошибок, при котором гарантируется исправление ошибок, кратность $\rho_и$ которых меньше d/2, $\rho_и < d/2$;

в) декодирование с обнаружением ошибок кратности ρ_o и исправлением ошибок кратности $\rho_и$, $\rho_o > \rho_и$. В этом случае связь кратностей корректируемых ошибок с кодовым расстоянием устанавливается соотношением:

$\rho_o + \rho_и + 1 = d$.

Кроме ошибок рассмотренных кратностей могут корректироваться некоторые ошибки большей кратности. Например, в декодере с обнаружением ошибок обнаруживаются все ошибки, которые переводят переданную разрешенную кодовую комбинацию в запрещенную. Таким образом можно обнаружить все ошибки, кратность которых отлична от весов разрешенных кодовых комбинаций, и некоторые ошибки, кратности которых совпадают с ними.

Таблицу состояний декодирующего регистра составлять в течение 15-ти тактов (для кода (7, 6) в течение 8 тактов).

3. Составить структурные схемы декодирующих устройств двух видов: с обнаружением ошибки, с исправлением. При коде (7, 6) составить два варианта декодирующего устройства с обнаружением ошибки: на основе регистра сдвига с сумматором по модулю два и на основе триггера четности – RS-триггера со счетным входом.

При выполнении этого задания следует обратиться к методическим указаниям к первому заданию.

4. Составить функциональную схему декодирующего устройства вида, указанного в последнем столбце таблицы вариантов (табл. 1.2).

Представить эпюры напряжений в точках: вход декодирующего устройства (кодовая комбинация с одной ошибкой), выходы декодирующего регистра, выход 8-разрядного регистра и др. Эпюры должны подтверждать правильность работы схемы.

Функциональная схема декодирующего устройства составляется с использованием элементов, представленных на рис. 1.3. Для декодирующего устройства с обнаружением ошибок анализатор состояний декодирующего регистра в 8-м такте рекомендуется строить на последовательно соединенных элементах И-НЕ с r входами (к ним подключаются инвертированные выходы разрядов регистра) и элемента 2И-НЕ, на второй вход которого подается импульс опроса ИО в 8-м такте (ИО наблюдается в КТ9).

Импульс опроса имеет уровень ЛОГ «1», и на выходе элементов 2И-НЕ в течение всех тактов кроме 8-го, будет действовать уровень ЛОГ «1», а в восьмом такте может появиться уровень ЛОГ «0» при наличии ошибок в кодовой комбинации. Длительность импульса на выходе этого элемента определяется длительностью ИО. В качестве устройства формирования импульса сброса можно использовать RS-триггер со счетным входом. Триггер в начальный мо-

мент устанавливается в единичное состояние с помощью сигнала «Уст. 0», благодаря чему следующий за ним элемент И открыт. Сигнал с выхода элемента 2И-НЕ подается на счетный (тактовый) вход триггера и при наличии ошибки по переднему фронту (отрицательному перепаду) импульса на этом входе происходит переход триггера в нулевое состояние, которое закрывает последующий элемент И. Последний элемент И должен иметь три входа: первый вход подключен к выходу RS-триггера, второй – к выходу разрядного регистра задержки, а на третий вход подается сигнал переключения СП для выделения информационных символов, которые должны поступать к получателю информации (проверочные символы не передаются, так как они используются только для коррекции ошибок).

В декодирующем устройстве с исправлением ошибок дешифратор рекомендуется реализовать на элементе «И» с r входами, на один из входов подается сигнал с выхода первого разряда регистра, а на остальные – инвертированные сигналы других разрядов. В этом случае на выходе элемента будет действовать уровень ЛОГ «1» при состоянии регистра 10 …. 0, а при остальных состояниях – уровень ЛОГ «0». Таким образом, на выходе этого элемента появится символ «1» в той позиции кодовой комбинации (задержанной на 8 тактов), в которой произошла ошибка. Суммирование этого сигнала с задержанной на 8 тактов кодовой комбинацией осуществляется в сумматоре по модулю два. На его выходе, который является выходом декодирующего устройства с исправлением ошибки, формируется исправленная кодовая комбинация. Здесь следует обратить внимание на задержку декодирования и выдачи информации получателю не менее, чем на длину кодовой комбинации. При построении эпюр напряжений в качестве управляющих сигналов в схеме следует взять сигналы, представленные на рис. 1.4 , а на вход декодирующего устройства подать кодовую комбинацию с ошибкой в символе, номер которого указан в таблице вариантов.

Подобный триггер иногда называют триггером четности, поскольку его выходное напряжение зависит от того, четное или нечетное число «1» в принятой кодовой комбинации. Этот триггер перед началом работы должен устанавливаться в одно из состояний по сигналу «Уст. 0». В лабораторном стенде такой сигнал подается на R вход триггера, поэтому его прямой выход устанавливается в нулевое состояние, а инверсный – в единичное. Триггер должен срабатывать от каждого из единичных импульсов независимо от порядка их следования. Для этого перед подачей на тактовый вход триггера кодовая комбинация должна пройти через элемент И (можно И-НЕ), в котором осуществляется ее перемножение с тактовыми импульсами, в результате чего продолжительность единичных импульсов уменьшается вдвое, и следующие подряд единичные импульсы будут восприниматься триггером раздельно. В остальном декодирующее устройство с обнаружением ошибок строится аналогично тому, как это описано выше.

1.3.2. Лабораторные задания и методические указания по их выполнению

1. Собрать кодирующее устройство и проверить правильность его функционирования путем сравнения полученных кодовых комбинаций в КТ5 с разрешенными.

Здесь следует использовать результаты предыдущей лабораторной работы.

2. Собрать декодирующий регистр, проверить правильность его работы по виду сигнала на выходах регистра. Что подтверждает отсутствие ошибки?

Ввести ошибку в четные или нечетные комбинации. Как изменяются сигналы на выходах декодирующего регистра? Что указывает на наличие ошибки?

Связи в декодирующем регистре Д10 с сумматором по модулю два Д13 устанавливаются в соответствии с заданным порождающим полиномом.

3. Собрать схему декодирующего устройства с обнаружением ошибок. (Для кода (7, 6) собирается схема на основе триггера четности).

Собрать схему декодирующего устройства с исправлением ошибки. (Для кода (7, 6) собирается схема декодирующего устройства с обнаружением ошибок на основе сумматора по модулю два). Зарисовать эпюры напряжений в основных точках схемы при подаче на вход декодирующего устройства комбинации, совпадающей с двоичным представлением числа, равного $N_{ст} \cdot 5 + N_{гр}$, где $N_{ст}$ - номер студента по журналу старосты, $N_{гр}$, - номер группы. Какая информация передается данной кодовой комбинацией?

Сделать выводы по работе в отношении корректирующих способностей заданного кода, алгоритма декодирования, результатов решения в декодирующем устройстве.

Декодирующие устройства различных корректирующих способностей содержат следующие блоки: декодирующий регистр Д10, сумматор по модулю два Д13, 8-разрядный регистр Д16.

Декодирующее устройство с обнаружением ошибок кроме указанных содержит также блоки: 4И-НЕ Д11, ЗИ-НЕ Д12, RS-триггер Д15, ЗИ-НЕ Д17. Выходом декодирующего устройства с обнаружением ошибок является КТ 15. При сборке схемы следует иметь в виду, что неиспользованные входы элементов И должны быть либо запараллены с другими входами, либо подключены к уровню ЛОГ1 (гнездо Г17). Если элемент 4И-НЕ Д11 (для кода (7, 6) требуется исключить из схемы, то для этого надо подключить к уровню ЛОГ «0» хотя бы один ее вход. Тогда на выходе Д11 будет действовать уровень ЛОГ «1» и следующий элемент Д12 будет эквивалентен двухвходовой схеме совпадения. Для всех кодов при декодировании с обнаружением ошибки хотя бы один вход элемента Д14 подключается к уровню ЛОГ «0» (гнезда 16, 18 и 40), поэтому на его выходе будет уровень ЛОГ «0» и задержанная кодовая комбинация с выхода

восьмиразрядного регистра Д16 будет проходить через сумматор по модулю два Д18 без изменения.

Для кода (7, 6) декодирующее устройство собирается с использованием схемы И-НЕ Д8 и триггера четности Д7. Надо использовать тот выход с триггера Д7, на котором в 8-м такте устанавливается уровень ЛОГ «1» при нечетном числе единиц в кодовой комбинации. Этот выход через гнездо 16 подключается ко входу элемента Д12 для формирования импульса сброса. На выходе элемента Д11 должен быть уровень ЛОГ «1». Для этого хотя бы один его вход должен быть подключен к уровню ЛОГ «0».

Декодирующее устройство с исправлением ошибки, кроме элементов Д10, Д13 и Д16, содержит элементы 4И Д14 и сумматор по модулю два Д18, выход которого КТ16 является выходом декодирующего устройства.

В декодирующем устройстве с обнаружением ошибок для кода (7, 6), построенном на основе одного разряда регистра сдвига Д10 и сумматора по модулю два Д13, свободные входы сумматора Д13 должны быть подключены к уровню ЛОГ «0» (например Г40), элемент Д11 должен иметь хотя бы на одном входе уровень ЛОГ «0», а соответствующий выход регистра подключается через гнезда Г16 ко входу элемента Д12.

1.3.3. Содержание отчета

В отчет по лабораторной работе должны входить:

- результаты выполнения домашнего задания;
- результаты выполнения лабораторного задания;
- выводы по работе.

1.3.4. Контрольные вопросы

1. Какие виды декодирования Вы знаете? Какие виды декодирования возможны для кодов: а) (n, n – 1), d = 2; б) (7, 3), d = 4; в) (7, 4), d = 3?

2. В чем заключается принцип обнаружения ошибок для циклических кодов и как можно реализовать декодирующее устройство с обнаружением ошибок?

3. В чем заключается принцип исправления однократной ошибки для циклических кодов? Как можно реализовать декодирующее устройство с исправлением однократной ошибки?

4. Нарисовать структурную схему декодирующего устройства с обнаружением ошибок и представить таблицу состояний декодирующего регистра в течение n + 1 тактов при подаче на его вход кодовой комбинации с ошибкой. Что указывает на наличие ошибок? Какие кратности ошибок будут обнаруживаться? Ответы дать для следующих порождающих полиномов: а) $x + 1$; б) $x^3 + x + 1$; в). $x^3 + x^2 + 1$;.г) $x^4 + x^3 + x^2 + 1$; д) $x^4 + x^2 + x + 1$.

2. КОДИРОВАНИЕ И МОДУЛЯЦИЯ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ

2.1. Описание лабораторной установки

Отличительной особенностью лабораторного стенда является использование современных специализированных микропроцессорных систем кодирования, декодирования и визуализации информации.

Лабораторный стенд формирует одно рабочее место для двух студентов и обеспечивает проведение серии экспериментов учебного лабораторного практикума.

Лабораторный стенд выполнен в виде единого моноблока и содержит все необходимые для проведения лабораторных занятий узлы и устройства. Для изучения принципов кодирования/декодирования рекомендуется использовать внешний цифровой осциллограф.

Лабораторный стенд состоит из следующих функциональных узлов:

1. Передающий блок, выполняющий функцию оконечного передатчика линии связи. В состав передающего блока входит микропроцессорный кодер/модулятор с возможностью выбора типа кодирования и режима запуска, возможностью ручного набора данных с клавиатуры или автоматической генерации случайного числа, индикации передаваемого числа, ручного управления запуска цикла передачи (старт/стоп/сброс), а также индикации активации режима передачи сообщения.

2. Линия связи, моделирующая искажения сигнала в канале связи. В состав линии связи входит аддитивный сумматор и управляемый источник помех-генератор шума.

3. Приемный блок, выполняющий функции оконечного приемника – декодера линии связи. В состав блока входят микропроцессорный демодулятор/декодер с возможностью выбора типа кодирования, индикации принятой комбинации, а также индикатора режима приема сообщения. Встроенный блок индикации отображает ткущую информацию: тип кодирования, количество переданных и приняты комбинаций, количество обнаруженных ошибок, действующие напряжения сигнала S и шума N.

Лабораторный стенд позволяет изучать особенности цифрового кодирования следующих видов:

– Бинарное кодирование стандарта NRZ, NRZI, код «Манчестер» и «Дифференциальный Манчестер»;

– Тринарное кодирование RZ, AMI, HDB3, MLT-3, 4B/3T;

– Тетрадное кодирование стандарта 2B1Q;

– Кодирование с использованием кодов замещения 4B/5B;

– Амплитудная модуляция;

– Частотная модуляция;

– Фазовая модуляция;

– Квадратурная модуляция QAM;

Предусмотрена оценка влияния помех (помехоустойчивость) при различных методах кодирования.

Порядок сборки и включения установки

– Провести внешний осмотр установки и убедится в отсутствии механических повреждений корпуса и шнура питания.

– Подсоединить шнур питания к установке.

Примечание: контакт защитного заземления подключен к центральному электроду разъема электропитания стандарта «EURO»;

– Шнур питания подключить к однофазной сети переменного тока напряжением 220 В частотой 50 Гц и заземленным центральным электродом по стандарту «EURO».

Запрещается эксплуатировать установку при снятом кожухе.

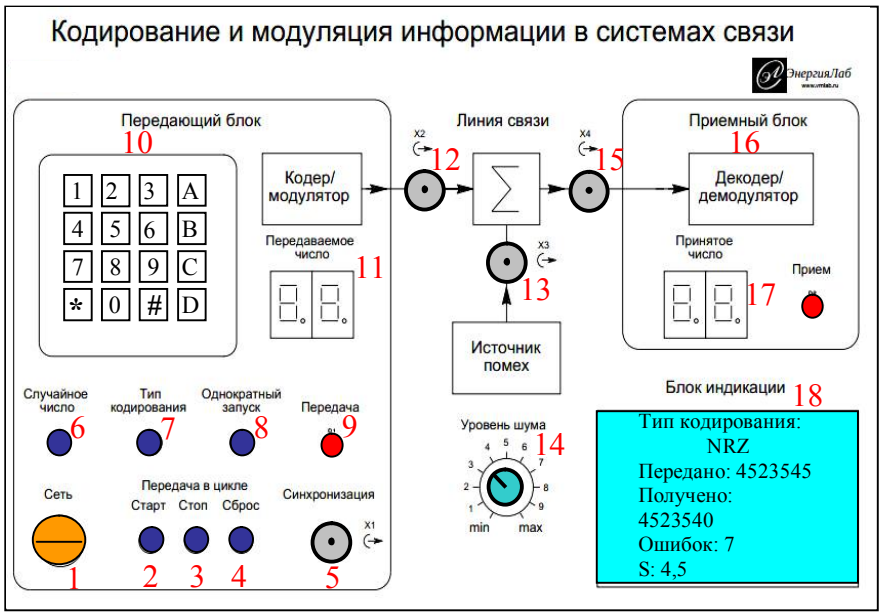


Рис. 2.1. Вид передней панели лабораторного стенда «Кодирование и модуляция информации в системах связи».

Здесь цифрами красного цвета обозначены:

1. Переключатель «Сеть» сетевого электропитания стенда. В верхнем положении электропитание включено, в нижнем – отключено.

2. Кнопка «Старт» запуска циклической передачи информации.

3. Кнопка «Стоп» остановки циклической передачи информации.

4. Кнопка «Сброс» обнуления всех текущих параметров режима передачи комбинации.

5. Коаксиальный контакт «Синхронизация» для синхронизации внешнего осциллографа.

6. Кнопка «Случайное число» однократной генерации числа датчиком случайных чисел.

7. Кнопка «Тип кодирования» выбора текущего вида кодирования: NRZ, NRZI, Манчестер, Дифф. Манчестер, RZ, AMI, HDB3, MLT-3, 4B/3T, 2B1Q, АМ, ЧМ, ФМ, QPSK, QAM, 4B/5B(NRZ), 4B/5B(NRZI), 4B/5B(MLT-3).

8. Кнопка «Однократный запуск» ручной передачи одиночной комбинации.

9. Индикатор «Передача» сигнализирующий о процессе передачи комбинации.

10. Клавиатура ручного ввода шестнадцатеричной цифровой комбинации. Кнопка «#» – вызов меню установки параметров лабораторной установки:

Пункт «A: Синхронизация», выбор параметров осуществляется последовательным нажатием кнопки «A» клавиатуры.

Возможные варианты режима синхронизации:

– «Импульс», синхронизация в виде импульса, определяющего начало передачи выбранной восьмибитной комбинации;

– «Тактовый сигнал», синхронизация в виде тактовых синхроимульсов, определяющих каждый байт комбинации;

– «NRZ», при этом осуществляется генерация текущей кодовой комбинации без кодирования. Используется для сравнения осциллограмм последовательного потока информации, подлежащей кодированию и результирующему коду.

Пункт «B: Тип ввода». Выбор параметров осуществляется последовательным нажатием кнопки «B» клавиатуры.

Возможные варианты выбора типа ввода информации:

– «Hex», ввод информации осуществляется в шестнадцатиричной системе счисления (с использованием кнопок «0-9» и «A-D» клавиатуры);

– «Bin», ввод информации осуществляется в двоичной системе счисления (с использованием кнопок «0» и «1» клавиатуры).

Пункт «C: Запуск генератора случайного числа». Выбор параметров осуществляется последовательным нажатием кнопки «C» клавиатуры.

Возможные варианты запуска генератора случайных чисел:

– «В цикле», при этом в каждом последующем цикле будет сгенерировано новое случайное число;

– «Постоянно», при этом в каждом последующем цикле будет повторятся одно и тоже случайное число, сгенерированное в первом цикле.

Пункт «D: режим отображения информации». Выбор параметров осуществляется последовательным нажатием кнопки «D» клавиатуры.

Возможные режимы отображения информации:

– «Отображать», при этом текущая передаваемая кодовая комбинация будет отображаться индикатором «Передаваемое число» (11 рис. 2.1).

– «Скрывать», при этом текущая кодовая комбинация не будет отображаться индикатором «Передаваемое число» (11, рис. 2.1). Режим «Скрывать»

используется для тренировки и приобретения студентами навыков «ручного декодирования» передаваемой комбинации по осциллограмме сигналов кода.

11. Индикатор «Передаваемое число», индицирующий текущую комбинацию (в шестнадцатеричной системе счисления), подлежащую передаче.

12. Коаксиальный контакт X2 контроля сигнала входа имитатора Линии связи.

13. Коаксиальный контакт X3 контроля сигнала Источника помех Линии связи.

14. Регулятор «Уровень шума» установки амплитуды сигнала генератора шума.

15. Коаксиальный контакт X4 контроля сигнала выхода имитатора Линии связи.

16. Индикатор «Принятое число», индицирует (в шестнадцатеричной системе счисления) текущую принятую комбинацию.

17. Индикатор «Прием», сигнализирующий о процессе приема комбинации.

18. Многофункциональный индикатор лабораторной установки. Индицирует вид кодирования, количество переданных и принятых комбинаций, количество обнаруженных ошибок, величина эффективного напряжения сигнала (S) и шума (N).

2.2. Лабораторная работа «Исследование бинарных кодов NRZ, NRZi, манчестерский, дифференциальный манчестерский код»

Необходимые теоретические сведения

Последовательность двоичных информационных комбинаций, представленных в параллельном виде, в процессе передачи преобразуется в последовательные коды в виде отдельных сигналов, например видеоимпульсов. В настоящее время разработано значительное количество последовательных двоичных (бинарных) кодов, из которых наибольшее распространение получили следующие методы:

Код NRZ (non-return-to-zero) (рус. «Без возврата к нулю»). При передаче логического нуля устройство кодирования формирует напряжение низкого потенциала (0 В при однополярном сигнале, U при двуполярном). В результате на выходе устройства кодирования формируется следующая последовательность [3]:

NRZ (прямой):

– биты 0 представляются нулевым напряжением 0 (В);

– биты 1 представляются значением U (В).

NRZ (обратный):

– биты 0 представляются значением U (В);

– биты 1 представляются нулевым напряжением 0 (В).

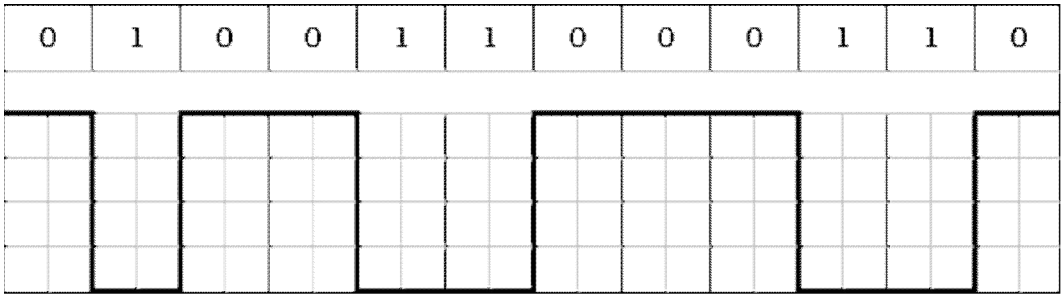


Рис. 2.2. Вид осциллограммы NRZ (обратный) кода (внизу) в зависимости от вида передаваемой информации (вверху) [3]

Одной из разновидностей NRZ кода является **NRZI** (Non return to zero, inverted). Особенностью кода является то, что смена сигнала происходит только при передаче единицы, а при передаче нуля не происходит изменения текущего значения напряжения.

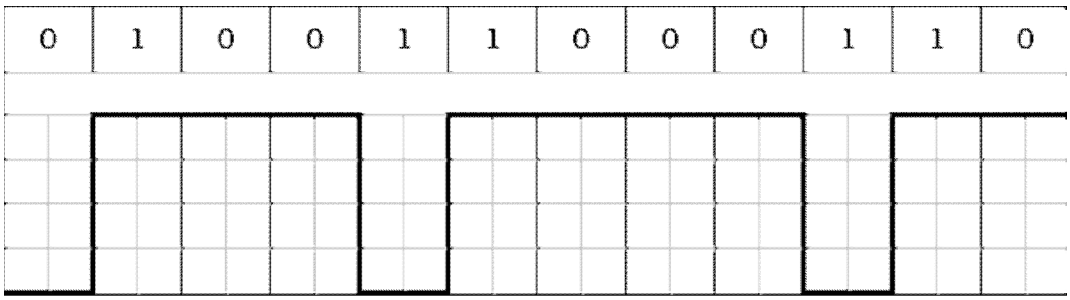


Рис. 2.3. Вид осциллограммы NRZI (потенциального) кода (внизу) в зависимости от вида передаваемой информации (вверху) [3]

Согласно [3], NRZ код имеет следующие преимущества и недостатки:

Достоинства метода NRZ:

– простота реализации;

– метод обладает хорошей распознаваемостью ошибок (благодаря наличию двух резко отличающихся потенциалов);

– основная гармоника f_0 имеет достаточно низкую частоту (равную N/2 Гц, где N – битовая скорость передачи дискретных данных (бит/с)), что приводит к узкому спектру.

Недостатки метода NRZ:

– метод не обладает свойством самосинхронизации. Даже при наличии высокоточного тактового генератора, приёмник может ошибиться с выбором момента съёма (выборки) данных, так как частоты двух генераторов никогда не бывают полностью идентичными. Поэтому при высоких скоростях обмена данными и длинных последовательностях единиц или нулей, небольшое рассогласование тактовых частот может привести к ошибке в целый такт и, соответственно, считыванию некорректного значения бита;

– наличие низкочастотной составляющей, которая приближается к постоянному потенциалу при передаче длинных последовательностей единиц и нулей. Из-за этого многие линии связи, не обеспечивающие прямого гальванического соединения между приёмником и источником, этот вид кодирования не поддерживают. Поэтому в сетях код NRZ в основном используется в виде различных его модификаций, в которых устранены как плохая самосинхронизация кода, так и проблемы постоянной составляющей.

Код Манчестер (Manchester encoding) [4]

При манчестерском кодировании каждый такт делится на две части. Информация кодируется перепадами потенциала в середине каждого такта. Единица кодируется перепадом от низкого уровня сигнала к высокому, а ноль – обратным перепадом ***(в различных стандартах возможны отличия – прим. автора.).*** В начале каждого такта может происходить служебный перепад сигнала, если нужно представить несколько единиц или нулей подряд.

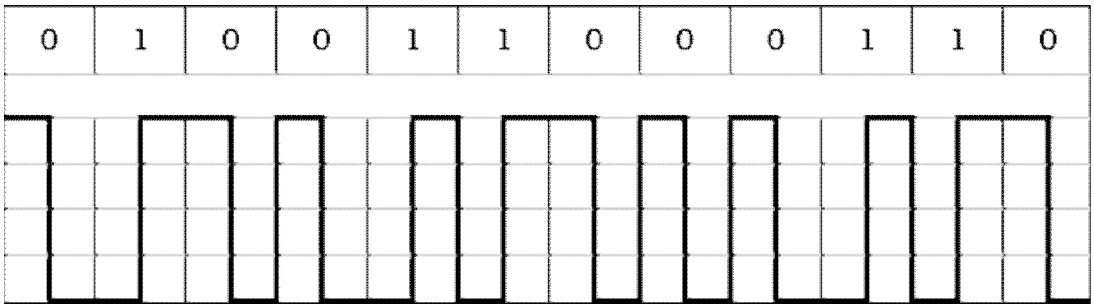


Рис. 2.4. Вид осциллограммы Кода Манчестер (внизу) в зависимости от вида передаваемой информации (вверху) [4]

Код Дифференциальный Манчестер (Differential Manchester encoding)

При дифференциальном манчестерском кодировании в течение битового интервала (времени передачи одного бита) уровень сигнала может меняться дважды. Обязательно происходит изменение уровня в середине интервала, этот перепад используется для синхронизации. Получается, что при передаче нуля в начале битового интервала происходит перепад уровней, а при передаче единицы такой перепад отсутствует.

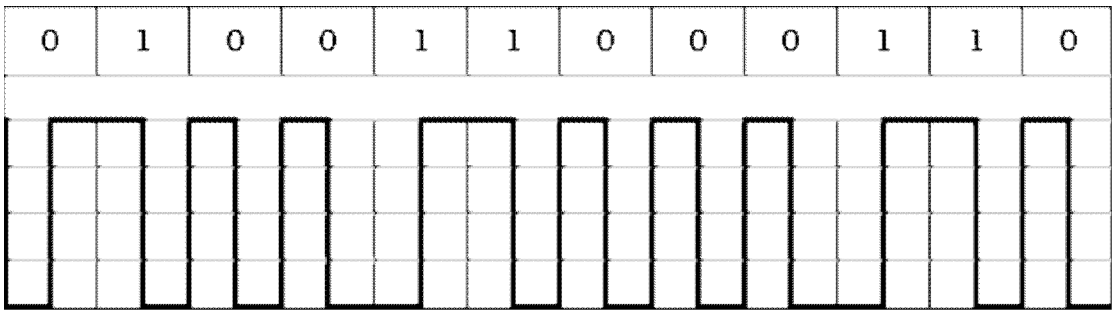


Рис. 2.5. Вид осциллограммы кода Дифференциальный Манчестер (снизу) в зависимости от вида передаваемой информации (сверху) [4]

Так как сигнал изменяется, по крайней мере, один раз за такт передачи одного бита данных, то манчестерский код обладает хорошими самосинхронизирующими свойствами. У манчестерского кода нет постоянной составляющей (меняется каждый такт), а основная гармоника в худшем случае (при передаче последовательности единиц или нулей) имеет частоту N Гц, а в лучшем случае (при передаче чередующихся единиц и нулей) - N/2 Гц, как и у NRZ.

Однако существуют и недостатки кода Манчестер: так, в среднем ширина спектра при манчестерском кодировании в два раза шире, чем при NRZ кодировании.

Выполнение лабораторных заданий

Задание 1. Исследование методов кодирования

Включить лабораторный стенд.

Подключить первый канал осциллографа к коаксиальному контакту X1 «Синхронизация» (5, рис. 2.1).

Подключить второй канал осциллографа к коаксиальному контакту X2 (12, рис. 2.1) выхода Передающего блока.

Установить режим синхронизации от первого канала осциллографа.

(***Примечание:*** В случае применения одноканального осциллографа, подключить вход внешней синхронизации осциллографа к контакту X1 «Синхронизация» (5, рис. 2.1), а канал входа осциллографа контакту X2 (12, рис. 2.1) выхода Передающего блока. Установить режим внешней синхронизации осциллографа. Далее нажав кнопку «#» клавиатуры (10, рис.2.1, вызвать меню настроек. Выбрать пункт «A: Синхронизация», затем последовательным нажатием кнопки «A» клавиатуры (10, рис. 2.1). Установить режим «Импульс», при котором синхронизация будет осуществляется импульсом, определяющего начало передачи выбранной восьмибитной комбинации.

Нажать кнопку Сброс (4, рис. 2.1) при этом произойдет обнуление всех оперативных триггеров кодирования.

Последовательно нажимая кнопку «Тип кодирования» (7, рис. 2.1), установить требуемый вид кодирования (в данном разделе работы исследуются коды NRZ, NRZI, Манчестер, Дифференциальный Манчестер).

С помощью клавиатуры (10, рис. 2.1) установить шестнадцатеричный код, подлежащий передаче (например, последнее число в номере зачетной книжки студента). Возможна также установка кода с помощью встроенного генератора случайных чисел. Для этого необходимо однократно нажать кнопку «Случайное число» (6, рис. 2.1).

На экране второго канала осциллографа наблюдать кодирующую последовательность, а на экране первого – синхронизирующие импульсы, совпадающие по времени с началом кодовой последовательности.

Наиболее характерные осциллограммы занести в отчет.

Задание 2. Исследование помехоустойчивости

Подключить первый канал осциллографа к коаксиальному контакту X1 (5, рис. 2.1) «Синхронизация».

Подключить второй контакт осциллографа к контакту X4 (15, рис 2.1).

Последовательно нажимая кнопку «Тип кодирования» (7, рис. 2.1), установить требуемый вид кодирования.

С помощью клавиатуры (10, рис. 2.1) или нажав кнопку «Случайное число» (6, рис. 2.1), установить комбинацию, подлежащую передаче.

Последовательно устанавливать регулятор «Уровень шума» (14, рис. 2.1) в положения рисок «1–9» шкалы лимба. В каждом положении регулятора выполнить действия:

1. Нажать кнопку «Сброс» (4, рис. 2.1), при этом обнулятся показания статистических счетчиков Блока индикации (18, рис. 2.1).

2. При необходимости, последовательным нажатием кнопки «Тип кодирования» (7, рис. 2.1), установить требуемый тип кода.

3. Нажать кнопку «Старт» (2, рис. 2.1) Передача в цикле, при этом на экране осциллографа можно наблюдать передаваемый код, искаженный шумом Источника помех. На экране «Блок индикации» (18, рис. 2.1) наблюдать увеличение показаний статистических счетчиков «Передано» байт, «Получено» байт, и счетчика количества «Ошибок» бит. (Следует обратить внимание, что счетчики «Передано » и принятых комбинаций отображают количество **байт** информации, а счетчик «Ошибок» – количество **бит).**

4. Набрав достаточный объем статистических данных (например 500 000 переданных байт), нажать кнопку «Стоп» (3, рис. 2.1). Показания счетчиков «Передано», «Получено» и «Ошибок» занести в таблицу.

В процессе выполнения лабораторных работ следует для каждого кода (NRZ, NRZI, Манчестер, Дифференциальный Манчестер) исследовать осциллограммы кодирования и занести в отчет графики помехоустойчивости.

На основании данных таблицы, построить кривую помехоустойчивости кода как зависимость $P_{ош}$ от h^2, при этом рекомендуется вероятность ошибок $P_{ош}$ откладывать в логарифмическом масштабе.

Таблица 2.1

Оценка помехоустойчивости кода.

Положение регулятора «Уровень шума»				
Объем переданной информации (Показания счетчика «Передано»), $M_{прд}$ байт				
Объем принятой информации (Показания счетчика «Принято»), $M_{прм}$ байт				
Количество битовых ошибок (Показания счетчика «Ошибок»), $m_{ош}$ бит				
Вероятность битовой ошибки $P_{ош}=(m_{ош} / 8 \cdot M_{прд})$.				
Эффективное напряжение сигнала U_s (показания индикатора S), В				
Эффективное напряжение шума U_n (показания индикатора N), В				
Отношение мощности сигнала к мощности шума $h^2=10\lg(U_s/U_n)^2$, дБ				

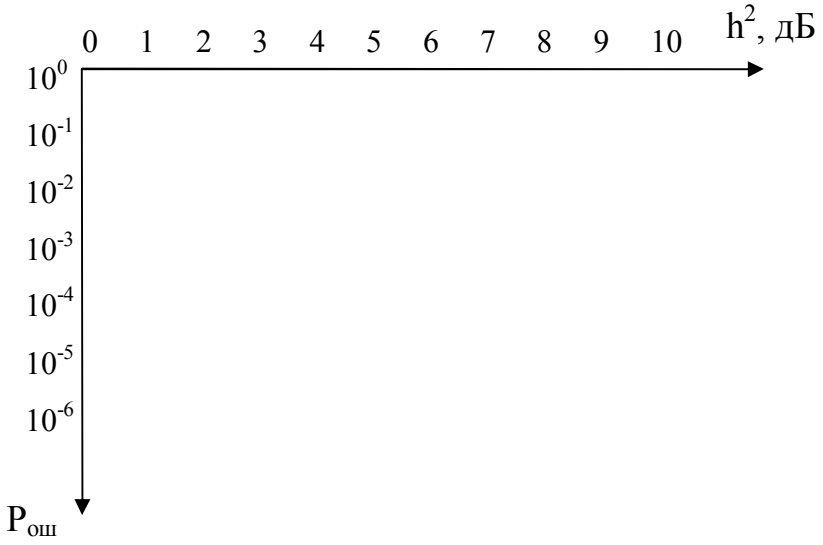


Рис. 2.6. Пример системы координат построения графиков помехоустойчивости кодов

Задание 3. Тренировка навыков «ручного декодирования» передаваемой кодовой комбинации

Нажав кнопку «#» клавиатуры (10, рис. 2.1) вызвать контекстное меню установки параметров. Нажать кнопку «C» клавиатуры (10, рис. 2.1), при этом будет активна меню строка «C: Запуск генератора случайного числа». Последовательно нажимая кнопку «C» клавиатуры (10 рис. 2.1) установить режим «Постоянно», при этом в каждом последующем цикле будет повторятся одно и тоже случайное число, сгенерированное в первом цикле.

Нажать кнопку «D» клавиатуры (10 рис. 2.1), при этом будет активна строка меню «D: режим отображения информации». Последовательно нажимая кнопку «D» клавиатуры (10, рис. 2.1) установить режим «Скрывать», при этом текущая кодовая комбинация не будет отображаться индикатором «Передаваемое число» (11, рис. 2.1).

Нажать кнопку «#» клавиатуры (10, рис. 2.1) и выйти из контекстного меню.

Затем, кратковременно нажать кнопку «Случайное число» (6, рис. 2.1), при этом будет проведена генерация случайного числа.

Нажать кнопку «Старт» (2, рис. 2.1) «Передача в цикле».

На экране осциллографа наблюдать кодированную последовательность. Занести осциллограмму в отчет. По осциллограмме «декодировать» передаваемую кодовую комбинацию.

Нажать кнопку «#» клавиатуры (10, рис. 2.1) и вызвать контекстное меню.

Нажать кнопку «D» клавиатуры (10, рис. 2.1), при этом будет активна строка меню «D: режим отображения информации». Последовательно нажимая кнопку «D» клавиатуры (10, рис. 2.1) установить режим «Отображать», при этом на Индикаторе «Передаваемое число» (11, рис. 2.1) будет индицироваться переданная комбинация. Убедиться в верности (или ошибочности) проведения операции ручного «декодирования».

Сделать соответствующие выводы и занести их в отчет.

2.3. Лабораторная работа «Исследование тринарных кодов RZ, AMI, HDB3, MLT-3, 4B/3T»

Необходимые теоретические сведения

Особенностью тринарного кодирования является то, что каждый бит комбинации передается сигналом с тремя уровнями напряжения, (а не двумя, как у бинарных кодов) вследствие чего реализуется более высокая скорость передачи.

Код RZ (**Return-to-zero**) (рус: «Со сбросом в ноль»). Относится к классу квазитроичных кодов, поскольку передаче логической «1» соответствует напряжение положительного потенциала «+U», а при передаче «0» – отрицательного «-U».

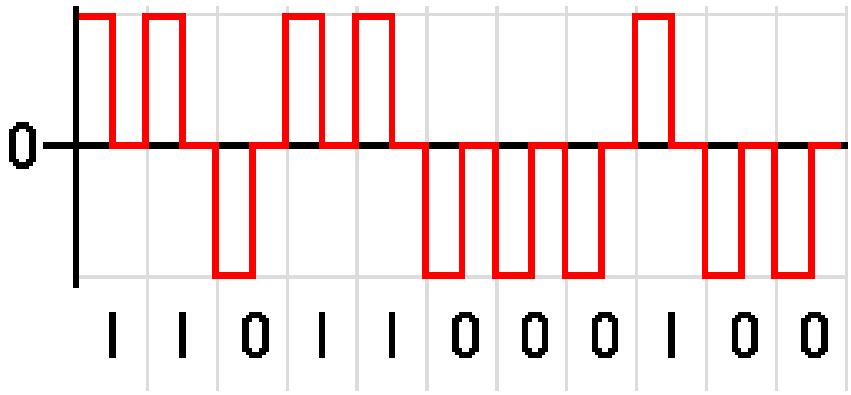


Рис. 2.7. Вид осциллограммы кода RZ (вверху) в зависимости от передаваемой информации (внизу) [3]

Код AMI реализует следующий алгоритм [4]:

– биты 0 представляются нулевым напряжением (0 В);

– биты 1 представляются поочерёдно значениями –U или +U (В).

AMI-код обладает хорошими синхронизирующими свойствами при передаче серий единиц и сравнительно прост в реализации. Недостатком кода является ограничение на плотность нулей в потоке данных, поскольку длинные последовательности нулей ведут к потере синхронизации.

Код HDB3 [5] является усовершенствованием AMI кода. Алгоритм аналогичен AMI за исключением кодирования последовательностей более четырех нулей, где каждые следующие четыре нуля заменяются последовательностью 000V, либо B00V. Где B – импульс по полярности противоположной предыдущему импульсу (отвечает правилу кодирования AMI), V (Violation) – импульс по полярности соответствующий предыдущему импульсу (нарушающий правило кодирования AMI). Выбор замены осуществляется таким образом, чтобы, во-первых, число импульсов B между двумя последовательно расположенными импульсами V было нечетным; и, во-вторых, чтобы полярности импульсов V чередовались.

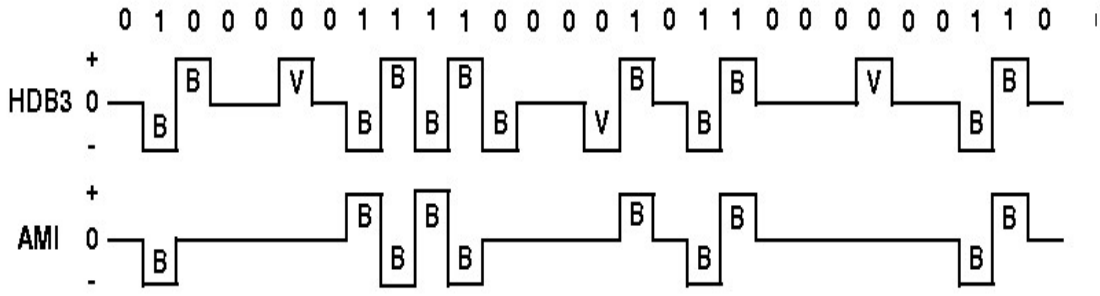


Рис. 2.8. Вид осциллограммы кода HDB3 и AMI в зависимости от передаваемой информации (сверху) [5]

Код MLT-3 (**Multi Level Transmission**) (многоуровневая передача) – метод кодирования, использующий три уровня сигнала. Метод основывается на циклическом переключении уровней -U, 0, +U. Единице соответствует переход с одного уровня сигнала на следующий. Так же как и в методе **NRZI** при передаче «нуля» сигнал не меняется.

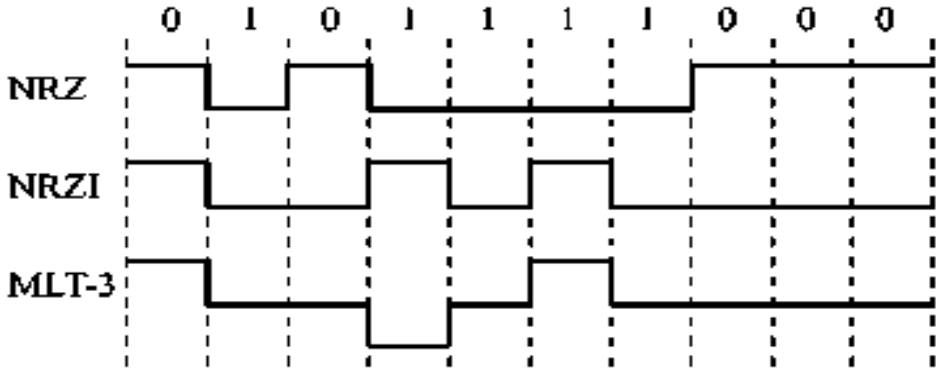


Рис. 2.9. Сравнение структуры кодов MLN3 с кодами NRZ и NRZI в зависимости от передаваемой информации (вверху) [6]

В случае наиболее частого переключения уровней (длинная последовательность единиц), для завершения цикла необходимо четыре перехода. Это позволяет вчетверо снизить частоту несущей относительно тактовой частоты, что делает MLT-3 удобным методом при использовании медных проводов в качестве среды передачи.

Код 4B/3T относятся к классу линейных кодов с изменением тактовой частоты, при этом группа из 4-х двоичных символов преобразуется в соответствующую группу из 3-х троичных символов, что обеспечивает необходимую избыточность и помехоустойчивость.

Три троичных символа дают 27 комбинаций, а четыре двоичных – 16. Поэтому для передачи многим двоичным комбинациям можно сопоставить по две троичных комбинации. Это делается для несбалансированных кодов, т.е. тех, в которых преобладают сигналы положительной или отрицательной полярности. Тогда второй код выбирается с обратной балансировкой, и их попеременная передача обеспечивает отсутствие постоянной составляющей в линии.

Таблица 2.2

Таблица кодирования линейного кода 4B/3T [6]

Двоичная комбинация	Троичная комбинация
0000	+ 0 +
0000	0 − 0
0001	0 − +
0010	+ − 0
0011	0 0 +
0011	− − 0
0100	− + 0
0101	0 + +
0000	+ 0 +
0000	0 − 0
0001	0 − +
0010	+ − 0
0011	0 0 +
0011	− − 0
0101	− 0 0
0110	− + +
0110	− − +
0111	− 0 +
1000	+ 0 0
1000	0 − −
1001	+ − +
1001	− − −
1010	+ + −
1011	+ 0 −
1100	+ + +
1100	− + −
1101	0 + 0
1101	− 0 −
1110	0 + −
1111	+ + 0
1111	0 0 −

Выполнение лабораторных заданий

Порядок исследования помехоустойчивости указанных методов кодирования в общем случае совпадает с порядком выполнения экспериментальных заданий предыдущей лабораторной работы. В качестве двузначной информационной комбинации рекомендуется выбрать две последние цифры номера зачетной книжки студента.

Задание 1. Исследование методов кодирования

В процессе выполнения заданий студенты должны осуществить исследование методов кодирования (см. «Задание 1» предыдущей лабораторной рабо-

ты). Результатом работы являются изучение осциллограмм исследуемых методов кодирования. В отчет следует занести осциллограммы кодированных сигналов.

Задание 2. Исследование помехоустойчивости

В процессе выполнения заданий студенты должны осуществить исследование помехоустойчивости кодированной последовательности (см. «Задание 2» предыдущей лабораторной работы). Результатом работы является построение экспериментальной таблицы помехоустойчивости кодирования (табл. 2.1) и график помехоустойчивости (рис. 2.6).

Задание 3. Тренировка навыков «ручного декодирования» передаваемой кодовой комбинации

В процессе выполнения заданий студенты должны осуществить декодирование исходной кодовой комбинации по осциллограмме кодированного сигнала (см. «Задание 3» предыдущей лабораторной работы). Результатом работы является осциллограммы кодированного сигнала и соответствующая ей декодированная двухзначная информационная комбинация.

По окончании выполнения лабораторных заданий обучающийся должен сделать соответствующие выводы и занести их в отчет.

2.4. Лабораторная работа «Исследование тетрадного кодирования 2B1Q»

Необходимые теоретические сведения [7]

Линейное кодирование **2B1Q** (***2 Binary 1 Quandary***) было разработано для использования в качестве протокола физического уровня в точке сопряжения UBRI-интерфейса сетей ISDN. Алгоритм 2B1Q представляет собой один из вариантов реализации амплитудно-импульсной модуляции с четырьмя уровнями выходного напряжения без возвращения к нулевому уровню (NRZ).

Таблица 2.3

Принцип тетрадного кодирования 2B1Q

Кодовая группа	Кодовый символ	Кодовое напряжение
00	-3	-2,5В
01	-1	-0.833В
10	+3	2.5В
11	+1	0.833В

Для формирования линейного кода, входной информационный поток делится на кодовые группы по два бита в каждой. В зависимости от комбинации значений битов кодовой группы, ей ставится в соответствие один из четырёх

кодовых символов, каждому из которых, в свою очередь, соответствует один из уровней напряжения.

Таким образом, закодированный в соответствии с правилами 2B1Q сигнал представляет собой последовательность скачкообразно изменяющихся напряжений с четырьмя возможными уровнями.

Поскольку в данном случае двум битам сигнала ставится в соответствие один кодовый символ, информационная скорость (data rate, скорость передачи данных) вдвое превышает символьную (symbol rate) - это означает, что модуляционная схема 2B1Q обеспечивает постоянную величину спектральной эффективности модулированного сигнала порядка 2бита/Гц.

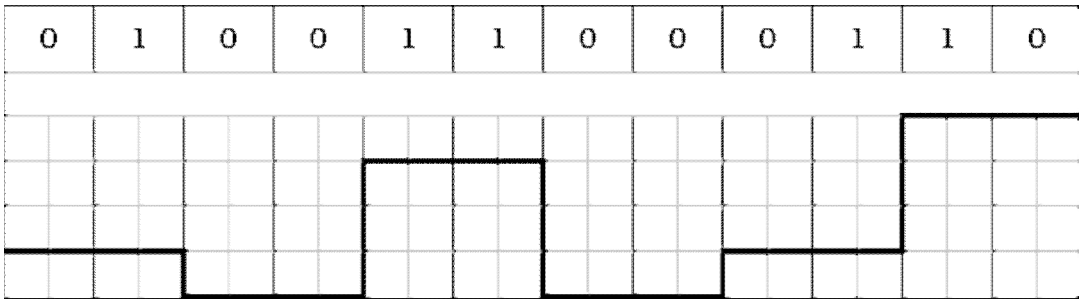


Рис. 2.10. Вид осциллограммы кода 2B1Q в зависимости от передаваемой информации (вверху) [3]

Алгоритм 2B1Q не обеспечивает поддержание баланса положительных и отрицательных импульсов выходного напряжения и, следовательно, входной код 2B1Q должен быть предварительно обработан специальными процедурами, которые должны обеспечить подавление постоянной составляющей.

Достоинство кода 2B1Q:

Сигнальная скорость у этого метода в два раза ниже, чем у кодов NRZ и AMI, а спектр сигнала в два раза уже. Следовательно, с помощью 2B1Q-кода можно по одной и той же линии передавать данные в два раза быстрее.

Недостаток метода 2B1Q:

Реализация этого метода требует более мощного передатчика и более сложного приемника, который должен различать четыре уровня.

Выполнение лабораторных заданий

Порядок исследования помехоустойчивости указанных методов кодирования в общем случае совпадает с порядком выполнения экспериментальных заданий первой лабораторной работы. В качестве двузначной информационной комбинации рекомендуется выбрать две последние цифры номера зачетной книжки студента.

Задание 1. Исследование методов кодирования

В процессе выполнения заданий студенты должны осуществить исследование методов кодирования. Результатом работы является изучение осциллограмм исследуемых методов кодирования. В отчет следует занести осциллограммы кодированных сигналов.

Задание 2. Исследование помехоустойчивости

В процессе выполнения заданий студенты должны осуществить исследование помехоустойчивости кодированной последовательности. Результатом работы является построение экспериментальной таблицы помехоустойчивости кодирования (табл. 2.1) и графика помехоустойчивости (рис. 2.6).

Задание 3. Тренировка навыков «ручного декодирования» передаваемой кодовой комбинации

В процессе выполнения заданий студенты должны осуществить декодирование исходной кодовой комбинации по осциллограмме кодированного сигнала. Результатом работы является осциллограмма кодированного сигнала и соответствующая ей декодированная двухзначная информационная комбинация.

По окончании выполнения лабораторных заданий обучающийся должен сделать соответствующие выводы и занести их в отчет.

2.5. Лабораторная работа «Исследование кодирования с использованием кодов замещения 4B/5B»

Необходимые теоретические сведения [7]

Протоколы, использующие код NRZ, чаще всего дополняют кодированием данных типа 4B/5B. В отличие от кодирования сигналов, обеспечивающего переход от импульсов к битам и наоборот, кодирование данных преобразует одну последовательность битов в другую.

В передатчике четырехбитовый информационный сигнал перекодируется в пятибитовый. Преобразованный сигнал имеет 16 значений для передачи информации и 16 избыточных значений. В приемнике из пятибитового сигнала выделяются информационные и служебные символы.

Достоинства кодирования 4B/5B:

– улучшение синхронизации за счет исключения последовательности из трех нулей и более;

– улучшение помехоустойчивости за счет возможности обнаружения ошибок в приемнике.

Недостаток кодирования 4B/5B:

– вследствие внесения избыточности (один избыточный бит на четыре информационных) снижается эффективность использования полосы частот на 25 %.

Таблица. 2.4

Таблица информационных кодов 4B/5B.

Исходный код 4B	Результирующий код 5B
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Выполнение лабораторных заданий

Порядок исследования помехоустойчивости указанных методов кодирования, в общем случае совпадает с порядком выполнения экспериментальных заданий первой лабораторной работ. В качестве двузначной информационной комбинации рекомендуется выбрать две последние цифры номера зачетной книжки студента.

Задание 1. Исследование методов кодирования

В процессе выполнения заданий студенты должны осуществить исследование методов кодирования. Результатом работы является изучение осциллограмм исследуемых методов кодирования. В отчет следует занести осциллограммы кодированных сигналов.

Задание 2. Исследование помехоустойчивости

В процессе выполнения заданий студенты должны осуществить исследование помехоустойчивости кодированной последовательности. Результатом работы является построение экспериментальной таблицы помехоустойчивости кодирования (табл. 2.1) и графика помехоустойчивости (рис. 2.6).

Задание 3. Тренировка навыков «ручного декодирования» передаваемой кодовой комбинации

В процессе выполнения заданий студенты должны осуществить декодирование исходной кодовой комбинации по осциллограмме кодированного сигнала. Результатом работы является осциллограммы кодированного сигнала и

соответствующая ей декодированная двухзначная информационная комбинация.

По окончании выполнения лабораторных заданий обучающийся должен сделать соответствующие выводы и занести их в отчет.

2.6. Лабораторная работа «Исследование особенностей передачи информации методом амплитудной модуляции»

Необходимые теоретические сведения

Сущность метода Амплитудной модуляции заключается в изменении амплитуды сигнала в зависимости от передаваемой информации. В случае использования бинарного кода, когда информация может принимать только два значения «0» или «1», корректно использовать термин «Амплитудная манипуляция». В иностранной литературе такой метод получил название ***«Amplitude Shift Keying» (ASK)*** – изменение сигнала, при котором скачкообразно меняется амплитуда несущего колебания.

На рис. 2.11 представлен процесс формирования Амплитудно-модулированного сигнала. В результате операции умножения двоичной информационной последовательности с сигналом гармонической несущей, формируется амплитудно-манипулированый сигнал, представляющий собой последовательность радиоимпульсов конгруэнтной с кодируемой информационной последовательностью. Представленные на рис. 2.11 сигналы относятся к классу сигналов с пассивной паузой и обладают относительно низкой (по сравнению с Частотной и Фазовой манипуляцией) помехоустойчивостью.

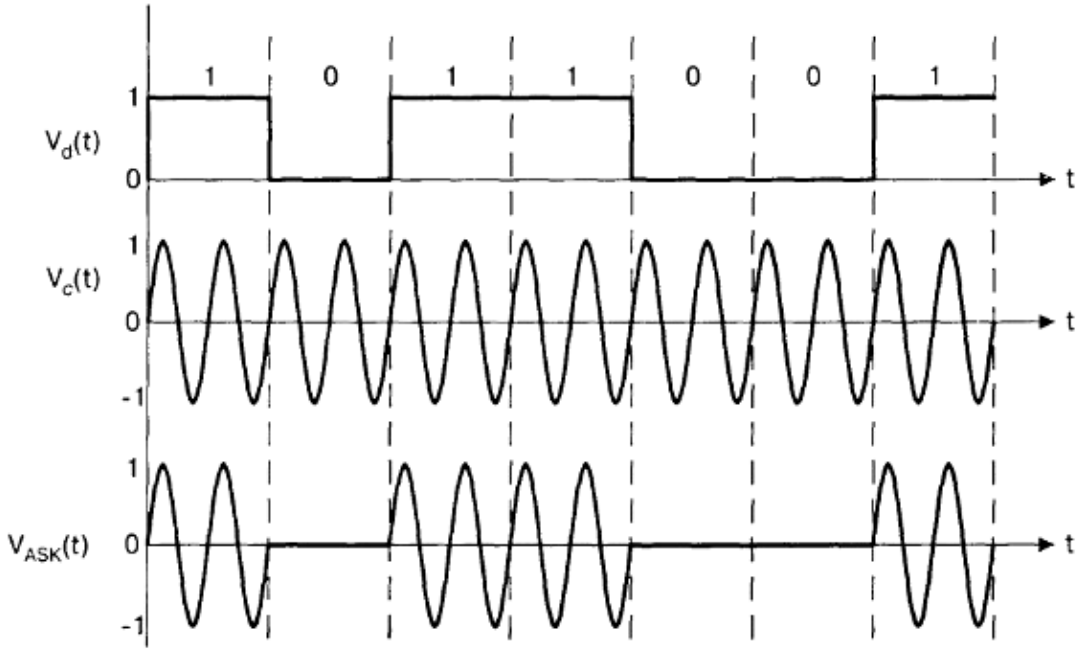


Рис. 2.11. Метод амплитудной модуляции [8]

Здесь $V_d(t)$ – кодирующая информационная последовательность, $V_c(t)$ – гармонический сигнал несущей частоты, $V_{ASK}(t)$ – амплитудно модулированный сигнал.

Выполнение лабораторных заданий

Порядок исследования помехоустойчивости указанных методов кодирования, в общем случае совпадает с порядком выполнения экспериментальных заданий первой лабораторной работы. В качестве двузначной информационной комбинации рекомендуется выбрать две последние цифры номера зачетной книжки студента.

Задание 1. Исследование методов кодирования

В процессе выполнения заданий студенты должны осуществить исследование методов кодирования. Результатом работы является изучение осциллограмм исследуемых методов кодирования. В отчет следует занести осциллограммы кодированных сигналов.

Задание 2. Исследование помехоустойчивости

В процессе выполнения заданий студенты должны осуществить исследование помехоустойчивости кодированной последовательности. Результатом работы является построение экспериментальной таблицы помехоустойчивости кодирования (табл. 2. 1) и графика помехоустойчивости (рис. 2.6).

Задание 3. Тренировка навыков «ручного декодирования» передаваемой кодовой комбинации

В процессе выполнения заданий студенты должны осуществить декодирование исходной кодовой комбинации по осциллограмме кодированного сигнала. Результатом работы является осциллограмма кодированного сигнала и соответствующая ей декодированная двухзначная информационная комбинация.

По окончании выполнения лабораторных заданий обучающийся должен сделать соответствующие выводы и занести их в отчет.

2.7. Лабораторная работа «Исследование особенностей передачи информации методом частотной модуляции»

Необходимые теоретические сведения

Метод частотной модуляции дискретным кодом заключается в изменении частоты несущей сигнала по закону двоичной информации при неизменной амплитуде сигнала. В этом и других дискретных методах, применяется термин «Частотная манипуляция» (англ. «**Frequency Shift Keying**» (**FSK**)). Принцип формирования Частотно манипулированного сигнала представлен на рис. 2.12.

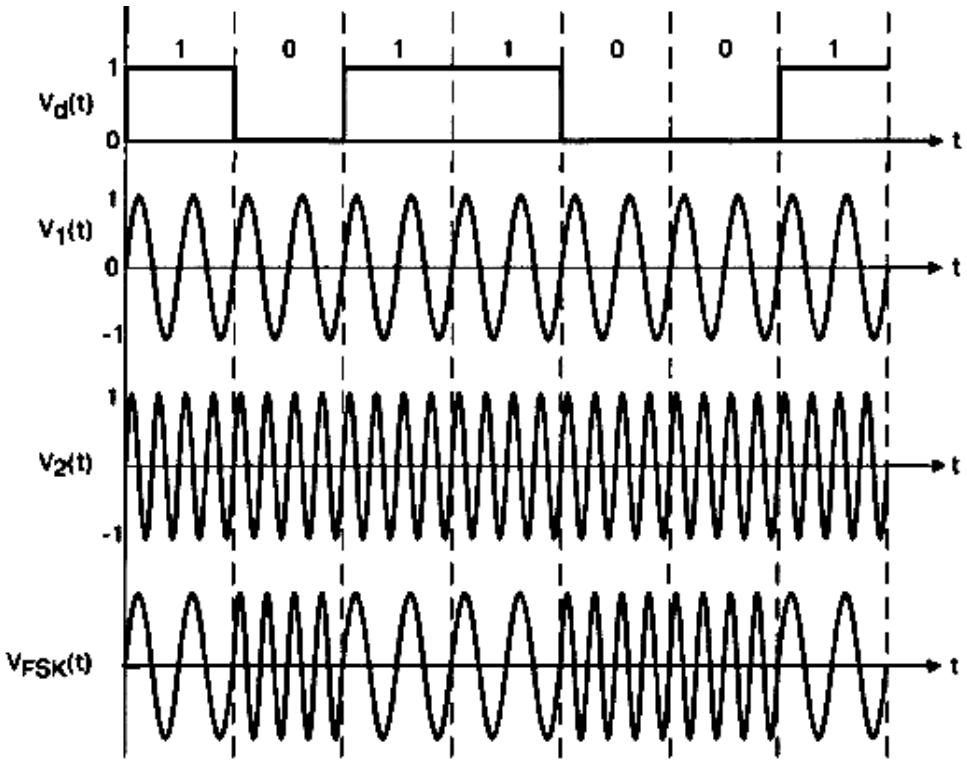


Рис. 2.12. Метод частотной модуляции [8]

Здесь $V_d(t)$ – кодирующая информационная последовательность, $V_1(t)$ – первая гармоническая несущая, $V_2(t)$ – вторая гармоническая несущая, $V_{FSK}(t)$ – частотно-манипулированный сигнал.

Согласно осциллограммам сигналов представленных на рис. 2.12, модулятор сигнала выполняет функции мультиплексора, последовательно подключая на выход гармонический сигнал первой несущей $V_1(t)$ при наличии на информационном входе модулятора логической «1», и гармонический сигнал второй несущей $V_2(t)$ при логическом «0».

Частотно манипулированный сигнал обладает большей помехоустойчивостью по сравнению с амплитудной манипуляцией. Это объясняется в первую очередь тем, что такой сигнал относится к классу сигналов с активной паузой, кроме того, сигналы с частотной манипуляцией образуют ортогональный базис ансамбля сигналов. В специальной литературе [9] отмечается, что подобные сигналы обладают (при прочих равных условиях) лучшей помехоустойчивостью по сражению с методом Амплитудной модуляции, но худшей по сравнению с Фазовой манипуляцией.

Выполнение лабораторных заданий

Порядок исследования помехоустойчивости указанных методов кодирования, в общем случае совпадает с порядком выполнения экспериментальных заданий первой лабораторной работ. В качестве двузначной информационной

комбинации рекомендуется выбрать две последние цифры номера зачетной книжки студента.

Задание 1. Исследование методов кодирования

В процессе выполнения заданий студенты должны осуществить исследование методов кодирования. Результатом работы является изучение осциллограмм исследуемых методов кодирования. В отчет следует занести осциллограммы кодированных сигналов.

Задание 2. Исследование помехоустойчивости

В процессе выполнения заданий студенты должны осуществить исследование помехоустойчивости кодированной последовательности. Результатом работы является построение экспериментальной таблицы помехоустойчивости кодирования (табл. 2.1) и графика помехоустойчивости (рис. 2.6).

Задание 3. Тренировка навыков «ручного декодирования» передаваемой кодовой комбинации

В процессе выполнения заданий студенты должны осуществить декодирование исходной кодовой комбинации по осциллограмме кодированного сигнала. Результатом работы является осциллограмма кодированного сигнала и соответствующая ей декодированная двухзначная информационная комбинация.

По окончании выполнения лабораторных заданий обучающийся должен сделать соответствующие выводы и занести их в отчет.

2.8. Лабораторная работа «Исследование особенностей передачи информации методом фазовой модуляции»

Необходимые теоретические сведения

Фазовая модуляция двоичным сигналом формирует последовательность непрерывных радиоимпульсов с отличающейся начальной фазой (0 , +π). В отечественной литературе такой дискретный метод модуляции фазы нашел название «Фазовая манипуляция». Метод формирования фазоманипулированных сигналов представлен на рис. 2.13.

Аппаратно метод манипуляции может быть реализован на базе линейного аналогового перемножителя, на первый вход которого подается непрерывный гармонический сигнал несущей, а на второй вход – управляющая двухполюсная кодирующая последовательность. В результате перемножения несущей с положительным импульсом кодирующей последовательности, формируется радиоимпульс, совпадающий по фазе с несущей. При умножении несущей на кодирующий импульс отрицательной полярности происходит «инверсия» несущей, в результате чего формируется радиоимпульс, сдвинутый по фазе относительно несущей на +π радиан.

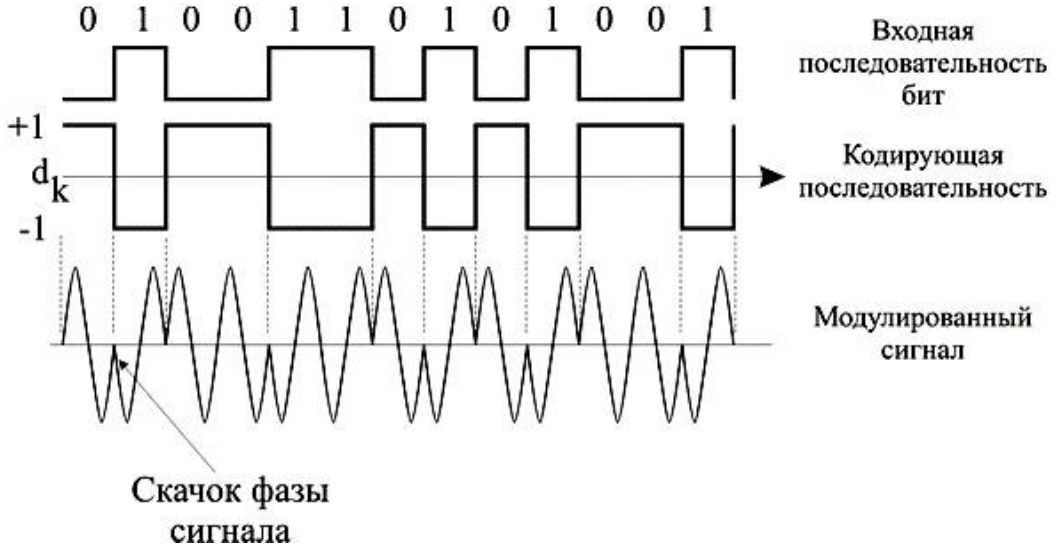


Рис. 2.13. Метод формирования фазоманипулированного (ФМ) сигнала [10]

Фазоманипулированный сигнал относится к классу сигналов с активной паузой и формирует ансамбль из двух противоположных сигналов. В специальной литературе [9] отмечается, что сигналы с фазовой манипуляцией обладают наилучшей помехоустойчивостью по сравнению с другими методами кодирования двоичной информации.

Выполнение лабораторных заданий

Порядок исследования помехоустойчивости указанных методов кодирования в общем случае совпадает с порядком выполнения экспериментальных заданий первой лабораторной работы. В качестве двузначной информационной комбинации рекомендуется выбрать две последние цифры номера зачетной книжки студента.

Задание 1. Исследование методов кодирования

В процессе выполнения заданий студенты должны осуществить исследование методов кодирования. Результатом работы являются изучение осциллограмм исследуемых методов кодирования. В отчет следует занести осциллограммы кодированных сигналов.

Задание 2. Исследование помехоустойчивости

В процессе выполнения заданий студенты должны осуществить исследование помехоустойчивости кодированной последовательности. Результатом работы является построение экспериментальной таблицы помехоустойчивости кодирования (табл. 2.1) и графика помехоустойчивости (рис. 2.6).

Задание 3. Тренировка навыков «ручного декодирования» передаваемой кодовой комбинации

В процессе выполнения заданий студенты должны осуществить декодирование исходной кодовой комбинации по осциллограмме кодированного сиг-

нала. Результатом работы является осциллограмма кодированного сигнала и соответствующая ей декодированная двухзначная информационная комбинация.

По окончании выполнения лабораторных заданий обучающийся должен сделать соответствующие выводы и занести их в отчет.

2.9. Лабораторная работа «Исследование особенностей квадратурной модуляции QAM»

Необходимые теоретические сведения [3]

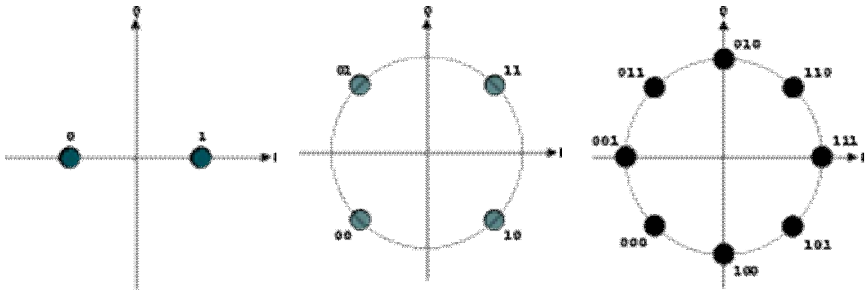
Квадратурная амплитудная модуляция относится к классу многопозиционных сигналов. Известно, что с увеличением объема ансамбля сигналов увеличивается количество информации (энтропия сообщения), переносимой каждым сигналом ансамбля. Так, классическая фазовая манипуляция (0, π) составляет ансамбль двух сигналов, таким образом, максимальное количество информации в расчете на один принятый сигнал составляет 1 бит (BPSK рис. 2.14, а). Объем ансамбля можно увеличить, например, снизив количество градаций фазы между сигналами ансамбля например до π/2 (QPSK рис. 2.14, б), где каждый сигнал потенциально может нести уже 2 бита информации, или же снизить количество градаций фазы до π/4 (8- PSK рис. 2.14, в), когда один принятый сигнал может нести до 3 бит информации. К сожалению, дальнейшее снижение градаций фазы между ансамблем сигнала приводит к резкому возрастанию взаимной корреляции и, как следствие, к снижению помехоустойчивости [9].

Одним из путей увеличения объема ансамбля сигналов является комбинация амплитудной и фазовой манипуляции, среди которых наибольшее распространение получила Квадратурная Амплитудная Модуляция (КАМ) или в иностранных источниках **QAM** (**Quadrature Amplitude Modulation***)*. При таком методе модуляции изменяется как фаза, так и амплитуда сигнала, что позволяет увеличить количество кодируемых бит и при этом существенно повысить помехоустойчивость. В настоящее время используются способы модуляции, в которых число кодируемых на одном бодовом интервале информационных бит может достигать 8...9, а число позиций сигнала в сигнальном пространстве – 256...512. Так на рис. 2.15 представлен вид «фазового созвездия» сигнала 16 КАМ.

Широкое распространение ансамблей QAM – сигналов в первую очередь зиждется на относительной простоте их генерации. Так, согласно [3] сигнал амплитудно – фазовой манипуляции можно формировать методов взвешенного суммирования (с переменными коэффициентами) суммы ортогональных гармонических сигналов:

$$S(t) = I(t)\cos(2\pi f_0 t) + Q(t)\sin(2\pi f_0 t),$$

где I(t) и Q(t) – сигналы весовых коэффициентов (информационные сигналы).



а) б) в)

Рис. 2.14. Методы многократной фазовой модуляции: а) Двоичная фазовая манипуляция (BPSK); б) Квадратурная фазовая манипуляция (QPSK); в) - Восьмеричная фазовая манипуляция (8-PSK) [3]

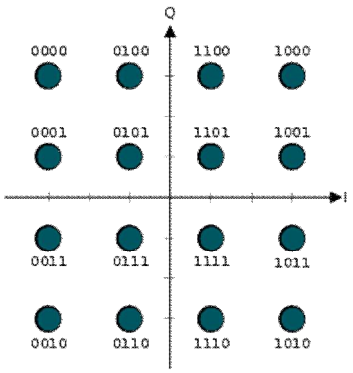


Рис. 2.15. Диаграмма структуры сигнала 16 QAM [3]

Выполнение лабораторных заданий

Порядок исследования помехоустойчивости указанных методов кодирования в общем случае совпадает с порядком выполнения экспериментальных заданий первой лабораторной работы. В качестве двузначной информационной комбинации рекомендуется выбрать две последние цифры номера зачетной книжки студента.

Задание 1. Исследование методов кодирования

В процессе выполнения заданий студенты должны осуществить исследование методов кодирования. Результатом работы являются изучение осциллограмм исследуемых методов кодирования. В отчет следует занести осциллограммы кодированных сигналов.

Задание 2. Исследование помехоустойчивости

В процессе выполнения заданий студенты должны осуществить исследование помехоустойчивости кодированной последовательности. Результатом работы является построение экспериментальной таблицы помехоустойчивости кодирования (табл. 2.1) и графика помехоустойчивости (рис. 2.6).

Задание 3. Тренировка навыков «ручного декодирования» передаваемой кодовой комбинации

В процессе выполнения заданий студенты должны осуществить декодирование исходной кодовой комбинации по осциллограмме кодированного сиг-

нала. Результатом работы является осциллограмма кодированного сигнала и соответствующая ей декодированная двухзначная информационная комбинация.

2.10. Лабораторная работа «Исследование помехоустойчивости РТС методом статистического моделирования»

Целью настоящей работы является:

1. Ознакомление с различными устройствами обнаружения и различения сигналов.

2. Изучение ансамблей сигналов: ортогональных, биортогональных, симплексных.

3. Освоение методики аналитического определения качественных показателей РТС.

4. Изучение метода статистического моделирования РТС, методов формирования на ЭЦВМ случайных чисел с нормальным и релеевским законом распределения.

5. Освоение методики определения основных качественных показателей РТС на ЭЦВМ.

При выполнении домашнего задания студенты знакомятся с различными устройствами оптимального приема сигналов и используемыми в них ансамблями сигналов, методом статистического моделирования РТС, рассчитывают помехоустойчивость РТС.

При выполнении статистического эксперимента рекомендуется использовать ПК вычислительной мощностью не ниже «Pentium 4».

Численное моделирование – сравнительно новое направление исследований в РТС. Оно применяется там, где аналитическое решение задачи из-за больших математических трудностей практически невозможно, а проведение экспериментальных исследований и натурных испытаний требует больших материальных затрат и немалого времени, или вообще невозможно. Численное моделирование позволяет при относительно небольших затратах времени и средств произвести испытание работы радиотехнической системы, не прибегая к использованию специальной аппаратуры. В статистических исследованиях численное моделирование на ПК незаменимо, так как статистические исследования требуют десятков и сотен тысяч испытаний, что с помощью, например натурных экспериментов, продлится в течении нескольких дней.

Применение вычислительной техники для численного моделирования позволяет сильно ускорить процесс вычислений, сократив его до десятков минут или, при решении наиболее сложных задач, до нескольких часов. Наибольшие затраты времени при этом приходятся на составление и отлаживание программ.

Метод статистического моделирования приемников обнаружения и различения сигналов

Любая сложная информационная система работает в условиях воздействия множества случайных факторов. При проведении аналитического исследования все их учесть не представляется возможным. Поэтому наряду с аналитическими исследованиями широко распространены методы исследования таких систем с помощью статистического моделирования на быстродействующем ПК.

В общем случае под статистическим моделированием понимается любая процедура, включающая искусственное формирование статистической выборки и ее обработку для приближенного решения различных физических и математических задач. Практическая реализация метода статистического моделирования стала возможной с появлением быстродействующих ПК.

Применительно к исследованию РТС реализация метода статистического моделирования на ЭВМ сводится к решению следующих задач:

- выбор алгоритма, имитирующего процесс функционирования исследуемой РТС;
- имитация выборок случайных сигналов на входе решающего устройства с заданными статистическими характеристиками;
- многократная реализация исследуемого алгоритма при воздействии выборок случайных сигналов;
- статистическая обработка полученных результатов, получение качественных показателей РТС.

Метод статистического моделирования на ПК является, вообще говоря, специальным образом построенным численным методом решения вероятностных задач. Однако, в отличие от обычных численных методов, при статистическом моделировании сохраняется логическая структура исследуемой системы, последовательность протекания во времени процессов ее функционирования, характер и состав информации о состояниях системы. С этой точки зрения существует некоторая аналогия между исследованиями системы методом статистического моделирования и методом натурного эксперимента.

Метод статистического моделирования основан на самых общих теоремах вероятности (теорема Чебышева, теорема Бернулли) и является универсальным методом исследования сложных систем. Если исследуемый процесс удается описать с помощью некоторой системы математических соотношений (формул, логических условий, операторов и т.д.), то статистическое моделирование этого процесса не представляет принципиальных трудностей и не налагает дополнительных ограничений на вышеуказанные соотношения.

Основное преимущество метода статистического моделирования – возможность решения задач очень высокой сложности, недоступных решению аналитическими методами. Необходимо также отметить удобство, быстроту и относительную дешевизну метода статистического моделирования, так как при этом методе не требуется создавать специальную аппаратуру.

Однако метод статистического моделирования обладает существенным недостатком, который состоит в том, что полученные решения носят частный характер, соответствующий фиксированному значению параметров и начальных условий. Это приводит к необходимости многократного моделирования даже для качественного анализа характеристик исследуемой системы в некотором диапазоне условий.

В данной лабораторной работе должна быть решена задача определения статистическим путем вероятности того или иного события. Если число положительных исходов при общем числе испытаний N равно n , то «вероятность» такого события $P^*=n / N$. При ограниченном значении N величина P^* (как и n) является случайной величиной, т.е. оценкой вероятности события P.

Чтобы дать представление о точности и надежности оценки P^*, в математической статистике пользуются так называемыми доверительными интервалами и доверительными вероятностями [9,10].

При выполнении заданий данной лабораторной работы для расчета объема выборки при моделировании можно воспользоваться следующим выражением

$$N = {4P(1-P)}/{\varepsilon^2} \quad , \qquad (7)$$

где $\boldsymbol{\varepsilon}$- заданная точность.

При расчетах N можно принять $\boldsymbol{\varepsilon}=0,1$, а в качестве P использовать наименьшее из значений P (или (1-P), если $P \approx 1$) при расчетах в домашнем задании.

Способы формирования случайных чисел, распределенных по нормальному и релеевскому законам

Получение случайных чисел с необходимым законом распределения – важная часть задачи статистического моделирования, так как от качества случайной последовательности зависят результаты всей работы.

Как правило, для получения последовательности случайных чисел с различными законами распределения используют последовательность чисел, распределенных по равномерному закону.

Существуют различные способы получения равномерно распределенных случайных чисел. Это выборка их из таблицы случайных, получение случайных чисел с помощью какого-либо физического генератора, генерация псевдослучайных чисел на ПК. Таблицы случайных чисел можно использовать лишь при ручном расчете. Физические датчики можно использовать при автоматизированном расчете, однако это требует применение дополнительной аппаратуры и не обеспечивает необходимого качества последовательности из-за неконтролируемого «дрейфа распределения» вырабатываемых физическим датчиком чисел. Поэтому чаще всего при статистическом моделировании используется метод генерации псевдослучайных чисел на ПК. Такие числа нельзя назвать случайными в полном смысле этого слова, так как при новом запуске программы

или достаточно продолжительном получении чисел последовательность повторяется. Метод генерации псевдослучайных чисел на ПК хорош тем, что для получения случайного числа ПК необходимо проделать несколько простейших операций и скорость генерации числа сравнима со скоростью работы вычислительной машины. Кроме того возможность повторения последовательности позволяет использовать программу генерации чисел для решения сходных задач, при этом качество последовательности достаточно проверить только один раз.

Имея в распоряжении равномерно распределенные числа, можно получить случайные величины с заданным законом распределения. Известно, что, если случайная величина x имеет плотность распределения $w(x)$, то распределение случайной величины

$$y = \int_{-\infty}^{x} w(x)dx \qquad (8)$$

является равномерным в интервале (0, 1). Как видно из этого соотношения, для получения числа x_i , распределенную по закону $w(x)$, надо получить число y_i из множества равномерно распределенных чисел и найти величину x_i из решения уравнения

$$y_i = \int_{-\infty}^{x_i} w(x)dx \; . \qquad (9)$$

Например, для получения случайных чисел x_i, распределенных по закону Рэлея из (6) получаем

$$x_i = \sigma\sqrt{2\ln(1-y_i)} \; . \qquad (10)$$

Часто интеграл типа (6) взять не удается. Тогда поступают по-другому. Например, для получения чисел x_i , распределенных по нормальному закону, можно просуммировать n чисел с равномерными законами

$$x_i = \sum_{j=1}^{n} y_j \; , \quad \text{где } n \geq 10. \qquad (11)$$

Математическое ожидание и дисперсия полученной величины равны

$$M[x] = \frac{n}{2} \; ; \quad \sigma_x^2 = \frac{n}{12} \; . \qquad (12)$$

Если случайные числа g_i должны иметь нормальное распределение с $M[g]=a$ и $\sigma_g^2=\sigma^2$, то полученное выше число x_i надо преобразовать следующим образом:

$$g_i = \frac{\left(x_i - \frac{n}{2}\right)\sigma}{\frac{n}{2}\sqrt{3}} + a \; . \qquad (13)$$

Получив нормальные числа, можно по ним сформировать релеевские и квазирелеевские числа (см. выше).

Все современные математические пакеты для ПК имеют встроенные датчики нормальных чисел.

Пример статистического моделирования РТС на ПК

Хорошей иллюстрацией сказанному выше является пример моделирования корреляционного обнаружителя полностью известного сигнала. Известно [5] , что при действии на его вход белого нормального шума со спектральной плотностью N_0 напряжение на выходе коррелятора $Z_1(T)$ является нормальной случайной величиной с дисперсией $\sigma^2=N_0E/2$, где E – энергия сигнала. При наличии полезного сигнала на входе математическое ожидание величины $Z(T)$ равно E (т.е. отношение с/ш на выходе равно $q^2=E^2/\sigma^2=2\ E/N_0$) , а при отсутствии равно нулю. Если для простоты принять $\sigma=1$, то $E=q$, а относительный порог в решающем устройстве будет численно равен z_0 .

Для нахождения статистическим путем вероятности ложной тревоги $P_л$ надо сформировать N выборок нормальных чисел с нулевым средним и σ = 1 и сравнить их с порогом z_0 . Очевидно, что $P_л \approx N_Л / N$, где $N_л$ – число превышений порога.

На практике часто надо обеспечить значение $P_л<10^{-10}$. Провести эксперимент при таком условии оказывается весьма затруднительно. Поэтому при известных статистических характеристиках помехи целесообразно находить значение $P_л$ аналитическим путем.

В рассматриваемом случае

$$P_л = 0{,}5\left[1-\Phi_0(z_0)\right] = 0{,}5\left[1-erf\left(z_0/\sqrt{2}\right)\right], \qquad (14)$$

где $$\Phi_0(x)=\frac{2}{\sqrt{2\pi}}\int_0^x e^{-\frac{t^2}{2}}dt ,$$

erf(x) – функция ошибок, содержащаяся в перечне встроенных функций во всех современных математических пакетах для ПК.

Рассчитав значение z_0 по заданному значению $P_л$, можно статистическим путем определить вероятность правильного обнаружения сигнала P_o . Для этого с порогом z_0 надо сравнить N нормально распределенных чисел с математическим ожиданием q. Если число превышений порога - N_0, то $P_o \approx N_0 / N$.

Листинг программы для нахождения значений $P_л$ и P_o , выполненный в среде Mathcad 12, при $N=10^5$ приведен в приложении.

Домашнее задание и указания по его выполнению

1. Изобразить функциональную схему оптимального корреляционного обнаружителя сигнала с неизвестной начальной фазой. Рассчитать значение относительного порога в приемнике для значений вероятности ложной тревоги

$P_л=10^{-2}$, 10^{-3}, 10^{-4}. Рассчитать и построить семейство характеристик обнаружения $P_0=P_0(q)$ (где $q^2=2E/N_0$, где Е- энергия сигнала, N_0- спектральная плотность шума) при действии на входе приемника белого нормального шума для q=0,1,…,8. Расчет значений P_0 производить с точностью до четырех знаков после запятой.

2. Изобразить функциональные схемы оптимальных корреляционного и фильтрового устройств когерентного и некогерентного приема двоичных сигналов. Записать выражения для определения уровня полезных сигналов и дисперсий шума на выходе корреляторов (согласованных фильтров) приемников и выражение для вероятностей ошибочного приема равномощных противоположных и ортогональных сигналов. Построить кривые потенциально помехоустойчивости $P_{ош}=P_{ош}(h)$ $(h^2=E/N_0)$ для случая когерентного приема сигналов при $h=0; 0,2…4$.

3. Изобразить функциональные схемы устройств оптимального приема двоичных сигналов с относительной фазовой манипуляцией (ОФМ) по методам сравнения полярностей и сравнения фаз. Объяснить принципы их работы. Изобразить на одном рисунке временные диаграммы радиосигналов при фазовой манипуляции (ФМ) и при ОФМ для последовательности передаваемых информационных символов длительности Т 011001. Рассчитать и построить кривые потенциальной помехоустойчивости $P_к=P_к\ (h)$ и $P_{нк}=P_{нк}\ (h)$ для указанных методов приема при $h=0; 0,2…4$.

4. В соответствии с методом статистического моделирования разработать программы для исследования помехоустойчивости оптимальных приемников, виды которых указаны в лабораторном задании. Определить объем выборочных значений N, необходимый для проведения экспериментов на ПК.

Для выполнения п.п. 1, 2 следует изучить разделы «Обнаружение сигналов» и «Различение сигналов» [15, с. 38-47; с. 60-71] , а п. 3 – [16, с. 293-296; 301-306]. Расчет значений Q- функции Маркума [15] можно производить на ПК. Используемый в [15] интеграл вероятности $Ф(x)$ может быть выражен через специальную математическую функцию – функцию ошибок $erf(x)$

$$\Phi(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}e^{-\frac{t^2}{2}}dx, \qquad \Phi(x)=0{,}5\left[1+erf\left(\frac{x}{\sqrt{2}}\right)\right].$$

Эта функция входит в перечень встроенных функций во всех современных математических пакетах для ПК.

При выполнении следует иметь в виду следующее.

Максимальная помехоустойчивость при передаче двоичной информации достигается при противоположных сигналах, получаемых путем фазовой манипуляции несущей частоты на 0, π. Спектр таких сигналов, как известно, не содержит составляющей с несущей частотой, поэтому по принимаемому сигналу нельзя определить начальную фазу последней, необходимой для создания копии передаваемого сигнала в корреляционном приемнике (импульсов синхронизации в фильтровой схеме) и реализации когерентного приема. Поэтому для

обеспечения фазовой синхронизации приемника принимают дополнительные меры (например, по каналу связи передают специальный пилот-сигнал). Однако это приводит обычно к значительному усложнению системы.

Указанный недостаток был устранен радикальным образом, когда вместо классической ФМ Петровичем Н.Т. была предложена ОФМ [17]. При ОФМ передаваемая информация заложена не в самом значении фазы данного элемента сигнала, соответствующего символу сообщения, как при ФМ, а в разности фаз данного элемента и предыдущего. При двоичной ОФМ эта разность может принимать, например, значения 0 и π . Для передачи символа «1» посылается элемент сигнала, фаза которого совпадает с фазой предыдущего элемента, а для передачи символа «0» - элемент, фаза которого противоположна фазе предыдущего элемента. Первый элемент (в начале сеанса связи) при ОФМ информации не несет, а служит опорным для второго уже информационного элемента.

Прием сигналов ОФМ можно осуществить как когерентным, так и некогерентным методом.

Простейшей схемой при когерентном методе является схема сравнения полярностей (рис. 2.16).

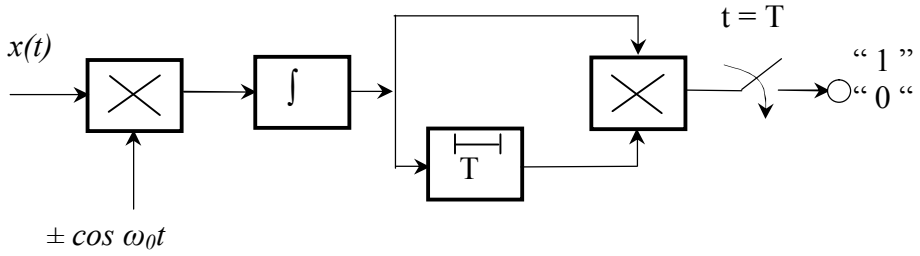


Рис. 2.16

Опорное напряжение $\cos\omega_0 t\,(-\cos\omega_0 t)$ (с равной вероятностью) может быть создано по принимаемому сигналу с помощью одной из схем: Пистелькорса, Костаса, Сифорова.

Нетрудно убедится, что в случае перескока фазы опорного сигнала на противоположную (вероятность этого события обычно мала), будет ошибочно принят лишь один информационный символ. В случае, если помеха изменит полярность напряжения на выходе интегратора, ошибочно принимается не только символ, соответствующий этому элементу, но и последующий, т.е. происходит сдваивание ошибок.

Поэтому вероятность ошибок при когерентном приеме P_k равна

$$P_k = 2P_{фм}\left(1 - P_{фм}\right), \qquad (15)$$

где $P_{фм}$ – вероятность ошибки при ФМ (при противоположных сигналах).

При некогерентном методе приема ОФМ сигналов опорное напряжение вообще не требуется. Простейшей схемой оптимального приема в этом случае является схема сравнения фаз (рис. 2.17) [6].

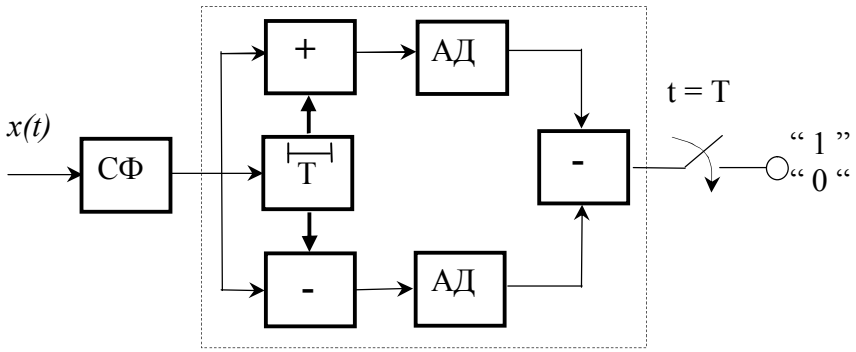


Рис. 2.17

На схеме рис. 2.17 блок СФ представляет собой фильтр, согласованный с одним элементом сигнала длительности T ; АД – амплитудный детектор. Часть схемы, обведенная пунктиром создает напряжение, являющееся функцией разности фаз соседних элементов сигнала φ . Если детекторы квадратичные, то - пропорциональное $\cos\varphi$.

Вероятность ошибки при некогерентном приеме $P_{нк}$ незначительно отличается от случая когерентного приема при ФМ и равна

$$P_{нк} = 0{,}5\exp\left(-h^2\right). \qquad (16)$$

Для выполнения необходимо изучить метод статистического моделирования РТС и методы формирования случайных чисел на ПК, приведенные в приложении и в [18] , а также математический пакет Mathcad 12.

При исследовании обнаружителя с двумя квадратурными каналами следует иметь ввиду следующее.

При действии на его вход белого нормального шума и полезного сигнала с неизвестной начальной фазой β напряжения на выходах каналов $Z_1(T)$ и $Z_2(T)$ являются нормальными, взаимно независимыми случайными величинами с одинаковыми дисперсиями $\sigma^2 = N_0E/2$ и математическими ожиданиями $E\cdot\cos\beta$ и $E\cdot\sin\beta$ [15]. Корень квадратный из суммы квадратов этих величин (т.е. напряжение Z на входе порогового устройства) при любом значении β , в том числе и при $\beta=0$, подчиняется квазирелеевскому закону. Причем при $\beta=0$ напряжение полезного сигнала на выходе одного из каналов численно равно E и отношение с/ш $q^2=E^2/\sigma^2 =2E/N_0$. Если полезный сигнал на входе обнаружителя отсутствует ($E=0$) , то напряжение на его выходе подчиняется релеевскому закону [15].

При статистическом моделировании удобно приять $\sigma=1$. Тогда $E=q$, а относительный порог в решающем устройстве (пороговом устройстве) Z_0/σ будет численно равен Z_0.

Сформировав N выборок квазирелеевских случайных чисел можно определить вероятность правильного обнаружения сигнала P_o для заданных значений $P_л$. Значение N взять здесь (и др. п.п. задания) 10^5.

В схеме сравнения фаз (рис. 2.17) амплитуда напряжения полезного сигнала и дисперсия шума на выходе СФ , соответственно равны U_m и σ^2. При передаче по каналу связи символа «1» (начальные фазы двух смежных элементов

сигнала одинаковы) на выходе сумматора они равны $2U_m$ и $2\sigma^2$, а на выходе вычитающего устройства – 0 и $2\sigma^2$. При этом распределение напряжения на выходе линейно детектора АД верхнего канала U_1 при $t=T$ подчиняется квазирелеевскому закону, а нижнего U_2 – релеевскому закону. Формирование таким образом распределенных чисел можно осуществлять, как и прежде, используя нормальные числа

$$U_1 = \left[(x_1 + x_2 + 2U_m)^2 + (y_1 + y_2)^2\right]^{1/2},$$
$$U_2 = \left[(x_1 - x_2)^2 + (y_1 - y_2)^2\right]^{1/2}. \qquad (17)$$

где x_1 и y_1 – нормальные числа с нулевыми средними и дисперсиями σ^2 , соответствующие первому из сравниваемых по фазе элементов сигнала; x_2 и y_2 – соответствующие второму элементу.

Следует иметь ввиду, что кривые помехоустойчивости для СПИ изображается в координатах $(P;h)$, где $h^2 = 0{,}5q^2 = E/N_0$. Если принять $\sigma = 1$, то при этом $h = U_m/\sqrt{2}\sigma$, а $U_m = \sqrt{2}\,h$.

Вероятность ошибочного приема символов «1» и «0» при ОФМ одинаковы, поэтому эксперимент удобно производить для случая передачи сообщения, состоящего из последовательности одних символов «1».

Лабораторное задание и методические указания по его выполнению

Включить ПК и активизировать математический пакет Mathcad 12.

Провести эксперименты по статистическому моделированию:

1. Оптимального приемника обнаружения с двумя квадратурными каналами при значениях q , $P_л$ и порога Z_0 , указанных в п.1 домашнего задания. Полученные значения P_0 свести в таблицу и построить графически кривые характеристик обнаружения.

2. Когерентных корреляционных приемников противоположных и ортогональных сигналов. Значения отношения с/ш h взять из п.2 домашнего задания. Данные моделирования включить в таблицу и по ним построить кривые потенциальной помехоустойчивости.

3. Некогерентного приемника ОФМ сигналов (прием по методу сравнения фаз) для тех же значений h , что и в п. 2 при линейных детекторах в каналах схемы. Полученные данные свести в таблицу и построить кривые помехоустойчивости. Используя данные п. 2 , на том же графике отобразить кривую помехоустойчивости для случая приема ОФМ сигналов по методу сравнения полярностей.

Содержание отчета

Отчет о проделанной работе должен содержать:

1. Результаты выполнения домашнего задания.

2. Данные статистического моделирования и их сопоставление с расчетными данными, необходимые рисунки, таблицы и графики.

3. Краткие выводы по всем этапам исследований.

Контрольные вопросы

1. В каких случаях для обнаружения сигналов используется приемник с двумя квадратурными каналами?

2. Зависят ли от начальной фазы полезного сигнала напряжения на выходах корреляторов и на общем выходе квадратурного приемника?

3. По какому закону распределены напряжения на выходах корреляторов и на общем выходе квадратурного приемника при действии на его входе нормального белого шума при наличии и отсутствии сигнала?

4. Какие значения имеют напряжения полезного сигнала и дисперсий шума на выходе корреляторов в квадратурной схеме?

5. Какой вид имеют фильтровые схемы обнаружителей полностью известного сигнала и со случайной начальной фазой?

6. Чем отличаются функциональные схемы оптимальных приемников различения и обнаружения сигнала?

7. Отличаются ли между собой сигналы при ОФМ и классической ФМ при передаче двоичной информации?

8. Какой вид имеют функциональные схемы приема ОФМ сигналов по методам сравнения фаз и полярностей?

9. Отличаются ли по помехоустойчивости сигналы с ОФМ и ФМ?

10. Как зависит выходное напряжение в схеме сравнения фаз от разности фаз смежных элементов сигнала?

11. Какие методы используются для формирования случайных нормальных и релеевских чисел на ПК? По какому закону распределена сумма квадратов независимых нормальных чисел с нулевым и ненулевым математическими ожиданиями?

12. В чем состоит сущность метода статистического моделирования при исследовании помехоустойчивости РТС?

13. Из каких соображений выбирается количество испытаний при статистическом эксперименте?

3. НЕОБХОДИМЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ. КОДОВЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ И КОДИРОВАНИЕ В ШИРОКОПОЛОСНЫХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

К сигналам, применяемым в системах связи со свободным доступом [22], предъявляются три основных требования: простота формирования с возможностью перестройки, хорошие корреляционные характеристики, большой объем ансамбля сигналов. В качестве корреляционных характеристик часто используют уровни боковых выбросов корреляционных функций (КФ). Целесообразно использовать такие двоичные последовательности (для формирования фазоманипулированных сложных сигналов), КФ которых имеют минимальные боковые выбросы. Такие сигналы называются квазиортогональными. Среди квазиортогональных сигналов наибольшее применение нашли М-последовательности [22]. Они имеют хорошие корреляциионные характеристики, их просто формировать с помощью регистра сдвига с m разрядами, охваченного обратными связями через сумматор по модулю 2 (линейная обратная связь). Но у них недостаточно большой объем ансамбля. Для увеличения объема ансамбля используются составные двоичные последовательности, образованные, например, путем суммирования по модулю 2 двух или трех М-последовательностей, а такте их различных сдвигов. В результате получаются последовательности Голда и Касами. Эти последовательности и устройства их формирования, их корреляционные характеристики достаточно подробно описаны в литературе, в частности, в учебном пособии [22].

В последнее время внимание специалистов привлекли ГМВ последовательности, которые существуют только для длины, содержащей в качестве множителя 2^k-1 (k - целое положительное число). Их периодическая автокорреляционная функция (АКФ) двухуровневая, как и у М-последовательности. Но они имеют значительно больший объем ансамбля. ГМВ последовательности описаны только в научных статьях. В этом раздела описаны ГМВ последовательности: принципы их построения на основе матричного представления М-последовательностей, структурные схемы их формирования. Здесь же рассмотрены коды Рида-Соломона, которые формируются схемами, подобными схемам формирования ГМВ последовательностей.

3.1. ГМВ последовательности

3.1.1. Матричное представление м-последовательностей

К ГМВ последовательностям можно придти, представляя М-последовательности в матричном виде.

Длину некоторых М-последовательностей

$$N = 2^m - 1 \qquad (18)$$

можно представить в виде произведения чисел, одно из которых имеет вид $2^{m_1}-1$ при m_1 - целом, положительном:

$$N = A \cdot (2^{m_1} - 1). \qquad (19)$$

Элементы таких последовательностей могут быть распределены в матрице с А строками 2^k-1 столбцами. Строками этой матрицы будут либо последовательности из одних нулей, либо М-последовательности длины

$$N_1 = 2^{m_1} - 1. \qquad (20)$$

При этом во всех ненулевых строках стоят одинаковые М-последовательности, в общем случае с различными сдвигами. Последовательность, стоящую в строках, будем называть короткой ПСП.

Например, последовательность длины $N = 63 = 9 \cdot 7$ с номером 31:

000001111110101011001101110110100100111000101111001010001100001

можно представить матрицей, размещая ее элементы сначала в первый столбец, потом во второй и т.д.:

$$\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array} \qquad (21)$$

В строках этой матрицы стоят циклические сдвиги М-последовательности длины $N_1 = 7$:

1 0 0 1 0 1 1.

За нулевой сдвиг последовательности берется так называемый характеристический сдвиг. Таблица номеров характеристических сдвигов относительно сдвига с начальным блоком 0...01 (m_1-1 нулей) приведена в приложении 1.

Матрицу (21) можно заменить последовательностью номеров сдвигов короткой ПСП для всех строк, обозначая положение нулевой строки звездочкой (*) :

[*, 5, 3, 5, 6, 3, 3, 2, 5] .

Эту последовательность можно назвать вектором-строкой (вектором-столбцом). Мы назовем ее матрицей сдвигов. М-последовательности длины N отличаются друг от друга матрицами сдвигов. При этом для нескольких М-последовательностей короткие ПСП могут быть одинаковыми. Короткая М-последовательность длины $N_1 = 7$ с номером 1, которая стоит в строках матрицы (21) последовательности длины $N = 63$ с номером 31, будет также образовы-

вать матрицы М-последовательностей с номерами 5 и 13. Их матрицы сдвигов будут соответственно:

ПСП №5 [*, 6, 5, 5, 3, 0, 3, 4, 6],
ПСП №13 [*, 1, 2, 5, 4, 1, 3, 1, 1] .

Остальные М-последовательности длины $N = 63$ с номерами 1, 11, 23 в строках матрицы имеют последовательность с номером 3 1110100 длины $N_1 = 7$. Их матрицы сдвигов будут следующими:

ПСП №1 [*, 3, 6, 5, 5, 2, 3, 5, 3] ,
ПСП №11 [*, 0, 0, 5, 0, 4, 3, 6, 0] ,
ПСП №23 [*, 2, 4, 5, 1, 5, 3, 3, 2] .

Две последовательности номеров 1 - 11- 23 и 31 - 5 - 13 являются ветвями децимации с индексом $q_1 = 11$; вторая ветвь получена из первой путем децимации по индексу $q_2 = 31$. Напомним, что операция децимации состоит в следующем. М-последовательность №11 можно получить из М-последовательности №1, выбирая каждый 11-й ее элемент, индекс децимации равен 11. М-последовательность № 23 можно получить из М-последовательности №1 путем децимации по индексу 23, Первая ветвь 1 - 11 - 23 характеризуется индексом децимации $q_1 = 11$. Это означает, что М-последовательность №23 можно получить из М-последовательности №11 децимацией по индексу $q_1 = 11$, М-последовательность №1 из М-последовательности № 23 децимацией по тому же индексу $q_1 = 11$. Ветвь замкнута, ее можно назвать q-ветвью с указанием индекса децимации q. Для каждой длины можно составить различные ветви для различных значений индексов децимации. Например, для той же длины $N = 63$ М-последовательности могут образовать q-ветвь ($q = 5$) 1 - 5 - 11 - 31 - 23 - 13. Можно указать и другие q-ветви. Нас интересуют такие q-ветви, чтобы М-последовательности, принадлежащие одной ветви, имели одинаковые короткие ПСП в строках при их представлении в виде матрицы. Это будет в том случае, если индекс децимации q_2 равен 2^k по модулю N_1. Выбранные две ветви с $q_1 = 11$ удовлетворяют этому условию: $11 = 4$ по модулю 7. Напоминаем, что вычисление числа a по модулю b сводится к определению остатка от деления a на b). Индекс децимации q_2 между ветвями может дать номер короткой ПСП. Если известен номер P_1 короткой ПСП первой ветви, то номер P_2 короткой ПСП второй ветви получают вычислением по модулю N_1 произведения $P_1 \cdot q_2$. Результат может быть равен P_2 или $P_2 \cdot 2^k$ (k- целое, положительное число). В приведенном примере $q_2 = 31$ или $P_2 = 3$ по модулю 7.

3.1.2. Получение ГМВ последовательностей на основе матричного представления М-последовательностей

Если в строки матрицы для *i*-й М-последовательности подставить другую короткую М-последовательность, то полученная ПСП будет иметь такую же периодическую автокорреляционную функцию, как и М-последовательность, т.е. центральный пик, равный N, и боковые выбросы уровня -1. Кроме М-последовательности в строки может быть поставлена любая другая ПСП длины N_1 с двухуровневой АКФ, с боковыми выбросами -1. В частности, можно использовать последовательности Лежандра. Это приводит к увеличению объема ансамбля ПСП. Вновь полученные ПСП называются ГМВ последовательностями. Они имеют объем ансамбля

$$V_1 = \varphi(m) \cdot n(m_1), \qquad (22)$$

где $\varphi(m)$- число М-последовательностей длины, определяемой формулой (18); $n(m_1)$- число коротких ПСП длины N_1 с двух уровневой АКФ (N_1 , -1). Объем ансамбля возрастает в число раз, равное числу $n(m_1)$ для коротких ПСП:

$$n(m_1) = \begin{cases} \varphi(m_1) & \text{для } N_1 = 7, 15 \\ \varphi(m_1) - 2 & \text{для } N_1 \neq 7 \end{cases} \qquad (23)$$

В формуле (23) $\varphi(m)$ - число М-последовательностей длины N_1. Здесь учитывалось, что для N_1 = 7 последовательности Лежандра совпадают с М-последовательностями той же длины, для N_1 = 15 последовательности Лежандра не существуют, а для других значений N_1, выражаемых простым числом, существуют только две последовательности Лежандра.

3.1.3. Устройства формирования ГМВ последовательностей

В устройстве, формирующем ГМВ последовательности, используются ПЗУ и генератор q-ичной М-последовательности, $q = 2^{m_1}$, m_1- целое положительное число, которое делит m. Схема генератора ГМВ последовательности представлена на рис. 3.1.

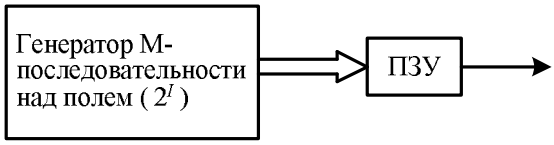


Рис. 3.1. Генератор ГМВ последовательности

Длина q-ичной М-последовательности

$$N = q^{m/m_1} - 1 \qquad (24)$$

совпадает с длиной двоичной М-последовательности. Чтобы в этом убедиться, подставим в (24) $q = 2^{m_1}$:

$$N = (2^{m_1})^{m/m_1} - 1 = 2^m - 1.$$

Характеристический полином двоичной М-последовательности имеет степень m. Для q-ичной М-последовательности также можно найти характеристический полином, его степень равна m/m_1. Элементы q-ичной М-последовательности и коэффициенты ее характеристического полинома степени m/m_1 являются элементами конечного поля, которое обозначается $GF(q)$. В этом случае говорят об М-последовательности и о полиноме над полем $GF(q)$. При $q = 2^{m_1}$ элементы поля $GF(q) = GF(2^{m_1})$ могут быть представлены в виде полинома над полем $GF(2)$ - коэффициенты в таком полиноме принимают только два значения 0 или 1. Степень полинома не превышает m_1-1. Полиномы над $GF(2)$ могут быть представлены в двоичном виде: m_1-разрядными двоичными комбинациями, символами которых являются коэффициенты 0 или 1 при соответствующей степени переменной в полиноме.

В схеме генератора (рис. 3.1) генератор М- последовательности над полем $GF(2^{m_1})$ выдает элементы в двоичном виде. Элементы в q-ичной М-последовательности являются адресными сигналами для ПЗУ. В ПЗУ записана двоичная последовательность длины N_1, имеющая двухуровневую АКФ.

Основной задачей при синтезе генератора ГМВ последовательности является определение характеристического полинома над полем $GF(2^{m_1})$ степени $k = m/m_1$.

3.1.4. Определение характеристического полинома степени m/m_1 над полем $GF(2^{m1})$

Элементы q-ичной М-последовательности и коэффициенты ее характеристического полинома являются элементами поля $GF(q)$ (последовательность и полином над полем $GF(q)$). Элементы этого поля не являются корнями характеристического полинома. Его корнями будут элементы поля $GF(q^k)$, для которого поле $GF(q)$ является подполем. Если в поле $GF(q^k)$, выбрать элемент α, который является корнем характеристического полинома, то элементы $\alpha^q, \alpha^{q_1}, ..., \alpha^{q_{k-1}}$ также будут корнями

этого полинома. Тогда характеристический полином q-ичной М-последовательности можно определить по формуле (25)

$$h(x) = (x+\alpha)(x+\alpha^q)...(x+\alpha^{q^{K-1}}). \qquad (25)$$

После перемножения получим коэффициенты в виде α^i и $\alpha^{i_1} + ...\alpha^{i_0}$. Эти коэффициенты надо выразить через элементы подполя $GF(q)$. Для этого в поле $GF(q^k)$ выбираем примитивный полином, одним из корней которого является α.

Поясним методику определения характеристического полинома на примере ПСП длины $N = 15,\ m = 4$. Значение $m_1 = 2$, тогда $K = m/m_1 = 2$ и $q = 2^m = 4$. Корнями характеристического полинома 4-ичной М-последовательности будут элементы поля $GF(q^k) = GF(4^2) = GF(2^4)$ α и α^4. Характеристический полином записывается в виде:

$$h(x) = (x+\alpha)(x+\alpha^4) = x^2 + x(\alpha+\alpha^4) + \alpha^5. \qquad (26)$$

Коэффициенты этого полинома должны быть элементами подполя $GF(4)$. Если рассматривать $GF(4)$ как поле, то его элементами будут $0,1,\beta,\beta^2$. Примитивный полином этого поля единственный $x^2 + x + 1$. Элемент β является корнем этого полинома, т.е. $\beta^2 + \beta + 1 = 0$. Отсюда можно получить период элемента β, значение которого совпадает с минимальным ε, для которого $\beta^\varepsilon = 1$. Запишем последовательные степени элемента β (мультипликативную группу, образованную элементом β): β, $\beta^2 = \beta + 1$, $\beta^3 = \beta^2 + \beta = 1$. Следовательно, элемент β имеет период, равный 3.

Если поле $GF(4)$ рассматривать как подполе $GF(4^2)$, то его элементы следует выразить через элементы поля $GF(4^2)$. Для этого среди элементов поля $GF(4^2)$ следует найти такой элемент, который образует мультипликативную группу периода 3, такого же как и у элемента β. Период элемента α^l поля $GF(p)$ определяется как $p/2$, если l делит p. Элементом поля $GF(4^2)$, имеющим период 3, является α^5. Он образует мультипликативную подгруппу $\alpha^5;\ \alpha^{10};\ \alpha^{15} = 1$ (последнее равенство обусловлено тем, что элемент α является примитивным, т.е. его период является максимальным и равным 15). Тогда элементы подполя $GF(4)$ обозначаются следующим образом:

$$(0, 1, \alpha^5, \alpha^{10},). \qquad (27)$$

Чтобы выразить коэффициент полинома (27) через элементы подполя $GF(4)$, надо задать примитивный полином в поле $GF(4^2) = GF(2^4)$, корнем

которого будет элемент α. Для длины ПСП 15, т.е. поля $GF(2^4)$, имеется два примитивных полинома:

$$x^4 + x + 1 \text{ и } x^4 + x^3 + 1. \qquad (28)$$

Если α является корнем первого полинома, то $\alpha^4 + \alpha + 1 = 0$ и $\alpha^4 + \alpha = 1$. Характеристический полином 4-ичной М- последовательности имеет вид

$$h(x) = x^2 + x + \alpha^3. \qquad (29)$$

Если α является корнем второго полинома, то $\alpha^4 + \alpha^3 + 1 = 0$, $\alpha^4 + \alpha = \alpha^3$ и $h(x) = x^2 + \alpha^5 x + \alpha^5$.

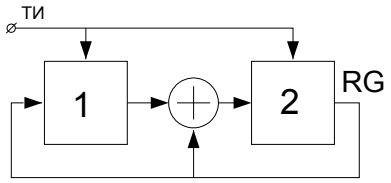
Эти два полинома определяют две различные 4-ичные М-последовательности длины 15. В связи с тем, что других примитивных полиномов в поле $GF(2^4)$ не существует, 4-ичных М-последовательностей длины 15 будет только две.

При построении генератора $q-$ичной М-последовательности следует выбрать базис представления $q-$ичных элементов. Базис должен содержать K элементов подполя $GF(q)$. Для рассматриваемого примера выбираем степенной базис $1, \beta$ или $1, \alpha^5$. Тогда элемент γ подполя $GF(4)$ можно представить в виде

$$\gamma = \gamma_0 + \gamma_1 \alpha^5. \qquad (30)$$

В генераторе $q-$ичной М-последовательности $q-$ичные элементы должны умножаться на α^5. В результате умножения может получиться какая то степень элемента α^5 которую надо опять представить с помощью степенного базиса $1, \alpha^5$. Для получения представления элементов подполя $GF(4)$ через степенной базис можно использовать генератор двоичной М-последовательности со встроенными сумматорами по модулю два [22], построенный в соответствии с характеристическим полиномом степени m_1. Для длины $N = 15$ генератор М-последовательности строится в соответствии с характеристическим полиномом $x^2 + x + 1$.

Схема этого генератора представлена на рис. 3.2. Генератор формирует двоичную М-последовательность длины 3. При начальной установке 1 0 он формирует последовательные степени элемента β, т.е. их двоичные представления. В соответствии с этой схемой α^{10} может быть представлено через степенной базис в $\alpha^{10} = 1 + \alpha^5$.



$\beta^0 = 1 \quad 1 \quad 0$

$\beta^1 = \alpha^5 \quad 0 \quad 1$

$\beta^2 = \alpha^{10} \quad 1 \quad 1 \quad \alpha^{10} = 1 + \alpha^5$

Рис. 3.2. Схема генератора М-последовательности со встроенными сумматорами, а также представление степеней в степенном базисе

Рассмотрим пример посложнее: М-последовательность имеет длину $N = 63 = 9 \cdot 7 = 2^6 - 1$. $m = 6$; выбираем $m_1 = 3$, $k = 2$. В этом случае степень характеристического полинома равна 2, а элементы последовательности и коэффициенты характеристического полинома будут элементами поля $GF(2^3)$, которое является подполем $GF(2^6)$. Определим общий вид характеристического полинома, корнями которого являются элементы α, α^8,

$$h(x) = (x + \alpha)(x + \alpha^8) = x^2 + x(\alpha + \alpha^8) + \alpha^9. \qquad (31)$$

Примитивный элемент β поля $GF(2^3)$ имеет период 7. Среди элементов поля $GF(2^6)$ следует выбрать элемент, имеющий такой же период. Таким элементом будет α^9, его период равен 63/9=7. Коэффициент $(\alpha + \alpha^8)$ в полиноме (31) надо выразить через степени элемента $\beta = \alpha^9$. Для этого следует задать примитивный полином в поле $GF(2^6)$. В этом поле примитивных полиномов 6, выбираем полином $x^6 + x + 1$, имеющий номер 1. Элемент α является корнем этого полинома, т.е. $\alpha^6 + \alpha + 1 = 0$ или $1 + \alpha = \alpha^6$. Используя эти соотношения, определим:

$$\alpha + \alpha^8 = \alpha(1 + \alpha^7) = \alpha(\alpha + \alpha^6 + \alpha^7) = \alpha^2(1 + \alpha^5 + \alpha^6) =$$
$$= \alpha^2(\alpha + \alpha^5) = \alpha^3(1 + \alpha^4) = \alpha^3(\alpha^6)^4 = \alpha^{27}$$

Полученный результат подставим в (31), получим полином

$$h(x) = x^2 + x\alpha^{27} + \alpha^9. \qquad (32)$$

М-последовательность, сформированная в соответствии с этим полиномом, имеет символы, являющиеся элементами подполя

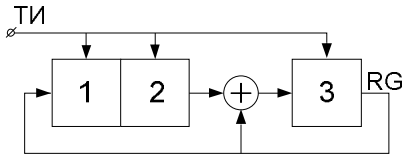
$GF(2^3) = (1, \alpha^9, \alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54})$. В качестве степенного базиса выбираем элементы $1, \alpha^9, \alpha^{18}$, т.е. 0,1 и 2-ю степени элемента $\beta = \alpha^9$.

Для представления элементов поля $GF(2^3)$ через степенной базис $1, \beta, \beta^2$ надо задать примитивный полином поля $GF(2^3)$. Для этого поля существуют два полинома:

$$x^3 + x + 1 \quad \text{и} \quad x^3 + x^2 + 1.$$

Следует выбрать тот полином, который является характеристическим полиномом короткой ПСП при матричном разложении двоичной М-последовательности длины 63. Номер М-последовательности определяется номером выбранного примитивного полинома в поле $GF(2^6)$. Из этого следует, что для М- последовательности с номером N характеристический полином короткой ПСП будет $x^3 + x^2 + 1$. (двоичное представление 1101). На рис. 3.3. представлена схема генератора, построенного в соответствии с этим полиномом, который дает представление в степенном базисе последовательных степеней элемента $\beta = \alpha^9$: элемент α^{36}, например, можно выразить через базисные элементы

$\alpha^{36} = 1 + \alpha^9 + \alpha^{18}$.



$\beta^0 = 1$	1	0	0	
$\beta^1 = \alpha^9$	0	1	0	
$\beta^2 = \alpha^{18}$	0	0	1	
$\beta^3 = \alpha^{27}$	1	0	1	$\alpha^{27} = 1 + \alpha^{18}$
$\beta^4 = \alpha^{36}$	1	1	1	$\alpha^{36} = 1 + \alpha^9 + \alpha^{18}$
$\beta^5 = \alpha^{45}$	1	1	0	$\alpha^{45} = 1 + \alpha^9$
$\beta^6 = \alpha^{54}$	0	1	1	$\alpha^{54} = \alpha^9 + \alpha^{18}$

Рис. 3.3. Схема генератора со встроенными сумматорами по модулю два для характеристического полинома $x^3 + x^2 + 1$, а также представление степеней элемента β через степенной базис

Подобным образом вычисляются характеристические полиномы других $q-$ичных М-последовательностей длины 63, а также для других длин. Укажем на особенности вычисления характеристического полинома для $N = 511$. В этом случае $511 = 2^9 - 1$ и $m = 9$, $m_1 = 3$ и K=3. Как и в случае длины 63, формируем М-последовательность над полем $GF(2^3)$. Но характеристический полином этой последовательности будет иметь третью степень, так как K=3. Характеристический полином имеет три корня: $\alpha, \alpha^8, \alpha^{64}$.

$$(x) = (x+\alpha)(x+\alpha^8)(x+\alpha^{64}) =$$
$$= x^3 + x^2(\alpha^{64} + \alpha^8 + \alpha) + x(\alpha^{19} + \alpha^{72} + \alpha^9) + \alpha^{72} \qquad (33)$$

Среди элементов поля $GF(2^9)$ выберем элемент, который имеет период, равный 7- периоду примитивного элемента β поля $GF(2^9)$, для рассматриваемой длины 7=511/73. Следовательно, элемент α^{73} имеет период, равный 7. Полагаем $\beta = \alpha^{73}$.

Для примитивного полинома, выбранного в поле $GF(2^9)$, необходимо выразить через степени элемента $\beta = \alpha^{73}$ следующие суммы:

$\alpha^{64} + \alpha^8 + \alpha$; $\alpha^{72} + \alpha^{63} + \alpha^9$.

Это очень трудоемкая и длительная процедура, но ее можно облегчить с помощью специальной программы на ЭВМ. Последовательные степени элемента β в поле $GF(2^3)$ уже вычислялись при рассмотрении М-последовательностей длины. Здесь следует иметь в виду, что $\beta = \alpha^{73}$.

Характеристические полиномы для $q-$ичных М-последовательностей длины $q^k - 1$ вычислены для длин 63,255,511,1023 и сведены в таблицы [22] .

3.1.5. Генератор М-последовательности над полем GF(2^{m1})

Генератор М- последовательности над полем $GF(2^{m1})$ строится в соответствии с характеристическим полиномом. Степень характеристического полинома определяет число ячеек регистра, каждая из которых является m_1-разрядной.

Рассмотрим схему генератора, формирующего М-последовательность длины $N = 15$ над полем $GF(2^2)$ в соответствии с характеристическим полиномом $x^2 + x + \alpha^5$. Схема 2^{m_1}-ичного генератора со встроенными сумматорами по модулю 2 (рис. 3.4) строится так же, как и схема двоичного, но в отличии от него наличие ненулевого коэффициента при соответствующей степени x означает не только наличие сумматора по модулю два после соответствующей ячейки регистра и связи этого сумматора с последним разрядом регистра, но и умножение в этой связи на какую-то степень примитивного элемента α.

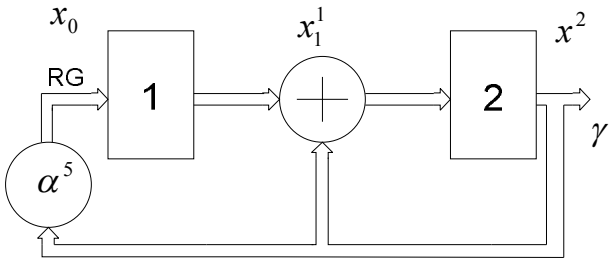


Рис. 3.4. Структурная схема генератора со встроенными сумматорами по модулю два для характеристического полинома $x^2 + x + \alpha^5$

На входе первой ячейки регистра коэффициент умножения равен коэффициенту при x^0 в характеристическом полиноме. Выход второй ячейки подается на сумматор, стоящий после первой ячейки, с предварительным умножением на коэффициент при x^1 в характеристическом полиноме. Здесь следует заметить, что ячейки регистра являются двухразрядными. Запись элементов в них осуществляется с использованием степенного базиса $1, \alpha^5$.

Рассмотрим построение функциональной схемы с учетом выбранного базиса. Выход последней ячейки регистра обозначим

$$\gamma = \gamma_0 + \gamma_1 \alpha^5 . \qquad (34)$$

Значение γ_0 записывается в первом разряде, а значение γ_1 во втором разряде.

Умножение на α^5, которое производится перед подачей сигнала на вход первой ячейки регистра, можно представить следующим образом:

$$\gamma\alpha^5 = (\gamma_0 + \gamma_1 \alpha^5) \cdot \alpha^5 = \gamma_0 \alpha^5 + \gamma_1 \alpha^{10} . \qquad (35)$$

Это выражение также нужно представить в степенном базисе. Для этого обратимся к схеме рис. 3.2, который дает $\alpha^{10} = 1 + \alpha^5$.

Тогда

$$\gamma\alpha^5 = \gamma_0 \alpha^5 + \gamma_1 (1 + \alpha^5) = \gamma_1 + \alpha^5 (\gamma_0 + \gamma_1) . \qquad (36)$$

Выражение (36) означает, что умножение на α^5 эквивалентно подаче на вход первого разряда первой ячейки регистра выхода γ_1 второго разряда второй ячейки, а на вход второго разряда-суммы выходов $\gamma_0 + \gamma_1$ первого и второго разрядов второй ячейки. В соответствии с этим структурная схема генератора М- последовательности длины 15 над полем $GF(2^2)$ может иметь вид, представленный на рис. 3.5.

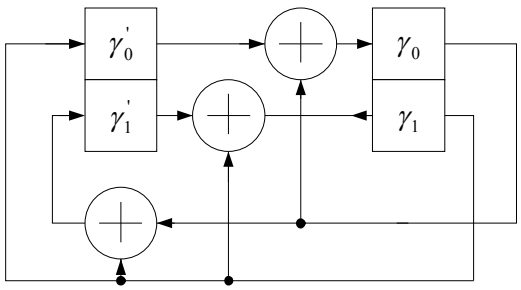


Рис. 3.5. Структурная схема генератора М-последовательности длины 15 над полем $GF(2^2)$

В табл. 3.1 представлены состояния ячеек регистров этой схемы. Двухразрядным выходом генератора может быть 1-й или 2-й разряды регистра 7. Получили последовательность длины 15, состоящую из двухразрядных элементов.

Теперь рассмотрим методику построения генератора М-последовательности длины 511 над полем $GF(2^3)$. Например из таблицы полиномов [22] выбираем последовательность с номером 239, которая имеет характеристический полином $x^3 + \alpha^{38}x^2 + \alpha^{73}$.

Таблица 3.1

Состояние ячеек регистров в схеме рис. 3.6

	Такты																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	14	16	…
γ_0'	0	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	…
γ_1'	1	1	0	0	0	1	0	0	1	1	0	1	0	1	1	1	…
γ_0	0	0	1	1	0	1	0	1	1	1	1	0	0	0	1	0	…
γ_1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	…

Генератор содержит три ячейки трехразрядных регистров. Структурная схема генератора представлена на рис. 3.6.

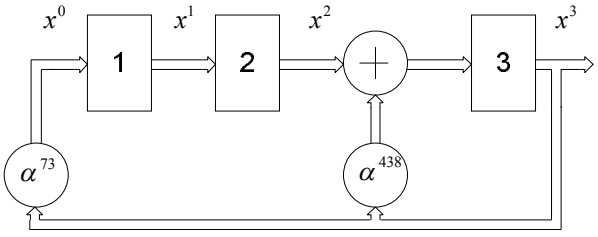


Рис. 3.6. Структурная схема генератора М-последовательности длины 511 над полем $GF(2^3)$

В характеристическом полиноме коэффициент при x^1 равен 0, поэтому сумматор по модулю два после первой ячейки регистра отсутствует.

Для построения функциональной схемы генератора надо определить два произведения: $\gamma\alpha^{438}$ и $\gamma\alpha^{73}$.

Здесь надо воспользоваться представлением степеней элемента β поля $GF(2^3)$ через степенной базис при примитивном полиноме $x^3 + x + 1$ (двоичное представление (1011)), учитывая, что $\beta = \alpha^{73}$:

$$\gamma\alpha^{73} = (\gamma_0 + \gamma_1\alpha^{73} + \gamma_2\alpha^{146})\alpha^{73} = \\ = \gamma_0\alpha^{73} + \gamma_1\alpha^{146} + \gamma_2\alpha^{219}. \quad (37)$$

В соответствии с таблицей полиномов [22] для М-последовательности с номером 239

$$\alpha^{219} = 1 + \alpha^{146}.$$

Тогда

$$\gamma\alpha^{73} = \gamma_0\alpha^{73} + \gamma_1\alpha^{146} + \gamma_2(1 + \alpha^{146}) = \\ = \gamma_2 + \gamma_0\alpha^{73} + (\gamma_1 + \gamma_2)\alpha^{146}. \quad (38)$$

Следовательно, умножение γ на α^{73} эквивалентно подаче на вход первого разряда γ_2, второго разряда γ_0, третьего разряда $(\gamma_1 + \gamma_2)$.

Теперь определим $\gamma\alpha^{438}$:

$$\gamma\alpha^{438} = (\gamma_0 + \gamma_1\alpha^{73} + \gamma_2\alpha^{148})\alpha^{438} = \gamma_0\alpha^{438} + \gamma_1\alpha^{314} + \gamma_1\alpha^{73} \\ = \gamma_1 + \gamma_2\alpha^{73} + \gamma_0(\alpha^{73} + \alpha^{145}) = \gamma_1 + (\gamma_0 + \gamma_2)\alpha^{73} + \gamma_0\alpha^{145}. \quad (39)$$

Умножение на $\gamma\alpha^{438}$ можно заменить подачей на вход первого разряда γ_1, второго разряда $(\gamma_0 + \gamma_2)$, третьего - γ_0.

В соответствии с полученными выражениями (38), (39) структурная схема будет иметь вид, представленный на рис. 3.4.

В табл. 3.2 приведены состояния разрядов регистров в течение первых нескольких тактов.

Таблица 3.2

Состояние ячеек регистров в схеме рис. 3.1.7

Разряды регистра	Такты					
	1	2	3	4	5	…
γ_0''	0	1	1	1	0	…
γ_1''	0	0	0	1	0	…
γ_2''	1	1	0	0	0	…
γ_0'	0	0	1	1	1	…
γ_1'	0	0	0	0	1	…
γ_2'	1	1	1	0	0	…
γ_0	0	0	1	0	1	…
γ_1	0	1	1	0	0	…
γ_2	1	1	1	0	0	…

Генератор формирует М-последовательность длины 511, символами которой являются трехразрядные элементы

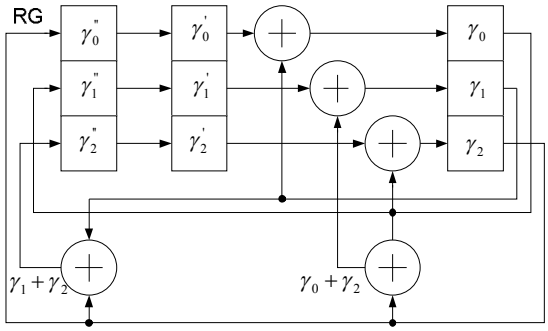


Рис. 3.7. Функциональная схема генератора М-последовательности длины 511 над полем $GF(2^3)$

3.1.6. Коды Рида-Соломона

Коды Рида-Соломона (РС-коды) - это q-ичные коды (кодовые символы принимают q различных значений), причем длина n кода жестко связана с q: $n = q - 1$. Например, РС код (63,55) использует 2^6-ичные символы, длина кода 63, информационных символов 55. Число разрешенных кодовых комбинаций огромно $(2^6)^{55} = 2^{310}$. Каждый информационный символ несет $\log_2 q = 6$ бит информации, следовательно, каждая кодовая комбинация несет $55 \cdot 6 = 330$ бит информации.

Порождающий полином РС кода определяется при заданных q и ρ_u-числе исправляемых ошибок или кодовом расстоянии $\alpha = 2\rho_u + 1$:

$$g(x) = (x - \alpha^{m_0})(x - \alpha^{m_0+1})...(x - \alpha^{m_0+2\rho_u-1}).$$

То есть корнями порождающего полинома являются элементы $\alpha^{m_0}, \alpha^{m_0+1}, \alpha^{m_0+2\rho_u-1}$ поля $GF(q)$. Степень порождающего полинома равна $2\rho_u$, такое же число проверочных символов в кодовой комбинации. Если известно обозначение кода (n,k), то сразу можно оценить корректирующие способности кода. Например, код (63,55) имеет 63-55=8 проверочных символов, следовательно, этот код исправляет все ошибки кратности, не превышающей 4. Кодовое расстояние на единицу больше числа проверочных символов и для кода (63,55) равно 9.

По методике определения порождающего полинома коды РС очень похожи на коды БЧХ. Отличие от них состоит в том, что для кодов БЧХ порождающий полином определяется как наименьшее общее кратное произведения полиномов, корнями которых являются элементы $\alpha^{m_0}, \alpha^{m_0+1}, \alpha^{m_0+2\rho_u-1}$, а для кодов РС - само произведение. Кроме того, коды БЧХ

обычно двоичные (могут быть и q-ичными), а коды РС - обычно q-ичные. Однако коды РС можно перевести в двоичные, при этом кодовое расстояние не уменьшается, но не обязательно получается циклические коды.

Если $q = 2^m$, то говорят о коде РС над полем $GF(2^m)$, то есть его кодовыми символами являются элементы этого поля. В этом случае в выражении (40) используется операция сложения по модулю два. Коэффициенты порождающего полинома также будут элементами поля $GF(2^m)$.

Рассмотрим код РС (7,3). Символами этого кода являются элементы поля $GF(8) = GF(2^3)$. Число проверочных символов $r = 7 - 3 = 4$. Следовательно, кратность исправляемой ошибки $\rho_u = 2$, кодовое расстояние равно 5. Число разрешенных кодовых комбинаций равно $2^9 = 512$. Порождающий полином имеет степень $r = 4$. Определим порождающий полином при $m_0 = 1$:

$$g(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4). \qquad (40)$$

После проведения умножения в (40) получим:

$$g(x) = (x^2 + x(\alpha + \alpha^2) + \alpha^3)(x^2 + x(\alpha^3 + \alpha^4) + \alpha^7). \qquad (41)$$

При проведении операции умножения и сложения с элементами поля $GF(2^m)$ следует выбрать примитивный полином степени m. Для поля $GF(2^3)$ выберем полином $x^3 + x + 1$- это примитивный полином над полем $GF(2)$. Корнем этого полинома является элемент α, следовательно, $\alpha^3 + \alpha + 1 = 0$ и для последовательных степеней элемента α можно записать выражения, приведенные в табл. 3.3. Тогда

$$\begin{aligned} &\alpha + \alpha^2 = \alpha^4, \quad \alpha^3 = 1, \\ &\alpha^3 + \alpha^4 = \alpha^3(1 + \alpha) = \alpha^6. \end{aligned} \qquad (42)$$

Продолжаем преобразования порождающего полинома

$$\begin{aligned} &g(x) = (x^2 + \alpha^4 x + \alpha^3)(x^2 + \alpha^6 x + 1) = \\ &= x^4 + x^3(\alpha^6 + \alpha^4) + x^2 + x(\alpha^4 + \alpha^2) + \alpha^3 = \\ &= x^4 + (\alpha + 1)x^3 + x^2 + \alpha x + (\alpha + 1) = \\ &= x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3. \end{aligned} \qquad (43)$$

Кодирующее устройство содержит четыре трехразрядных ячейки регистра сдвига. На схеме не показаны ключи, которые необходимо использовать для получения систематического кода, обращается внимание только на связи регистра с сумматором по модулю два. На вход сумматора подаются 2^3-ичные символы информации. Элемент γ, записанный в какую-то

ячейку регистра, можно с помощью степенного базиса $1,\alpha,\alpha^2$ записать в виде $\gamma = \gamma_0 + \gamma_1\alpha + \gamma_2\alpha^2$.

Таблица 3.3

Полиномиальное и двоичное представления степеней элемента α - корня примитивного полинома $x^3 + x + 1$ в поле $GF(2^3)$

α^i	Полиномиальное представление	Двоичное представление
α^0	1	001
α^1	α	010
α^2	α^2	100
α^3	$\alpha + 1$	011
α^4	$\alpha^2 + \alpha$	110
α^5	$\alpha^2 + \alpha + 1$	111
α^6	$\alpha^2 + 1$	101

В соответствии с полученным полиномом можно построить кодирующее устройство, структурная схема которого представлена на рис. 3.8.

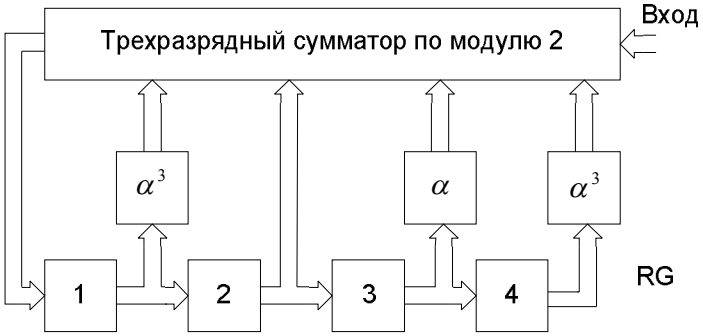


Рис. 3.8. Кодирующий регистр РС кода

Коэффициенты $\gamma_0,\gamma_1,\gamma_2$ являются элементами поля $GF(2)$ и принимают значения 0 или 1. В первом разряде регистра содержится значение γ_0, во втором разряде - значение γ_1, в третьем - γ_2. Рассмотрим, что означает умножение элемента γ на α^3 и α.

$$\begin{aligned}\gamma\alpha &= (\gamma_0 + \gamma_1\alpha + \gamma_2\alpha^2)\alpha = \gamma_0\alpha + \gamma_1\alpha^2 + \gamma_2\alpha^3 = \\ &= \gamma_0\alpha + \gamma_1\alpha^2 + \gamma_2(1+\alpha) = \gamma_2 + \alpha(\gamma_0 + \gamma_2) + \gamma_1\alpha^2.\end{aligned} \qquad (44)$$

Это выражение определяет связи третьей ячейки регистра сдвига с сумматором по модулю два. На первый разряд сумматора подается выход γ_2 третьего разряда третьей ячейки, на вход второго разряда сумматора - сумма $(\gamma_0 + \gamma_2)$ выходов первого и третьего разрядов, а на третий разряд сумматора подается выход γ_1 второго разряда третьей ячейки регистра.

$$\begin{aligned}\gamma\alpha^3 &= (\gamma_0 + \gamma_1\alpha + \gamma_2\alpha^2)\alpha^3 = \gamma_0\alpha^3 + \gamma_1\alpha^4 + \gamma_2\alpha^5 = \\ &= \gamma_0(1+\alpha) + \gamma_1(\alpha + \alpha^2) + \gamma_2(1+\alpha+\alpha^2) = \\ &= (\gamma_0 + \gamma_2) + \alpha(\gamma_0 + \gamma_1 + \gamma_2) + \alpha^2(\gamma_1 + \gamma_2).\end{aligned} \qquad (45)$$

Это выражение определяет связи первой и четвертой ячеек регистра сдвига с сумматором: на вход первого разряда сумматора подается сумма $(\gamma_0 + \gamma_2)$ выходов первого и третьего разрядов ячейки регистра, на вход второго разряда сумматора подается сумма $(\gamma_0 + \gamma_1 + \gamma_2)$ выходов всех трех разрядов, а на вход третьего разряда сумматора - сумма $(\gamma_1 + \gamma_2)$ выходов второго и третьего разрядов ячейки регистра.

С учетом выражений (44) и (45) схему кодирующего устройства РС кода (7.3) можно представить в виде, приведенном на рис. 3.9.

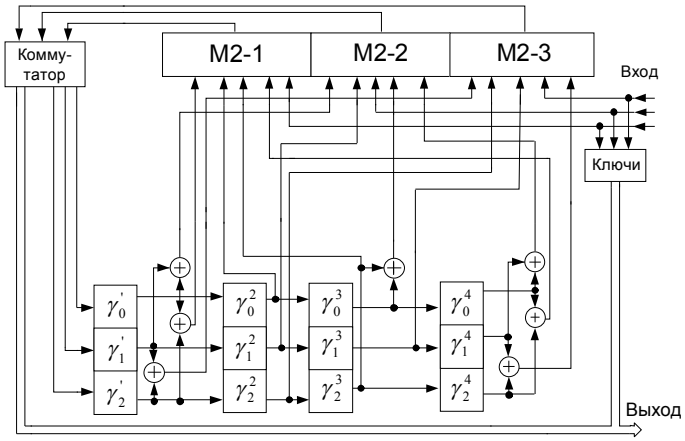


Рис. 3.9. Кодирующее устройство РС кода

Порождающий полином запишем в виде q-ичного представления:

$$g(x) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3 \rightarrow 1\alpha^3 1\alpha\alpha^3. \qquad (46)$$

Двоичное представление получим, если элементы q-ичного представления заменить их двоичным представлением в соответствии с табл. 3.3:

$$g(x) = 1\alpha^3 1\alpha\alpha^3 \rightarrow 1011001010011. \qquad (47)$$

Двоичное представление запишем в виде полинома. Получим порождающий полином кода РС над полем $GF(2)$

$$g(x) = x^{12} + x^{10} + x^8 + x^6 + x^4 + x + 1. \qquad (48)$$

В соответствии с этим полиномом кодирующее устройство строится на 12-разрядном регистре сдвига так же, как и для любого двоичного циклического кода. Длина n_2 двоичного РС кода и число k_2 информационных символов определяются по формулам:

$$n_2 = n \log q, \qquad k_2 = k \log q.$$

В рассматриваемом примере q-ичный РС код преобразуется в двоичный код (21,9), кодовое расстояние двоичного кода больше или равно пяти.

3.1.7. Порядок определения порождающего полинома РС-кода и составления структурной схемы кодирующего устройства

1. Для заданного кода (n,k,d) определить поле $GF(q)$, $q = n-1$, элементы которого являются кодовыми символами.

2. Определить число проверочных символов

$$r = n - k, \qquad (49)$$

то есть степень порождающего полинома, число его корней.

3. Записать порождающий полином в виде произведения двучленов в соответствии с формулой (30), положив $m_0 = 0$ или 1. В формуле (30) в двучленах используется операция суммирования по модулю два, если выбранное поле имеет характеристику 2, то есть $q = 2^k$, k- целое, положительное число.

4. Выбрать примитивный полином поля $GF(q)$, обратившись к приложению учебного пособия [22]. Записать степенное, полиномиальное и двоичное представления примитивного элемента аналогично тому, как это сделано в табл. 3.3.

5. Преобразовать выражение для порождающего полинома, чтобы его коэффициенты были степенями α примитивного полинома $GF(q)$. Сначала надо перемножить двучлены, затем преобразовать коэффициенты с использованием матрицы, полученной в предыдущем пункте.

6. Начертить структурную схему связей регистра с сумматором аналогично тому, как это сделано на рис. 3.8 для кода (7,3).

7. Выбрать базис, с его помощью записать элемент γ поля $GF(q)$.

8. Провести умножение элемента γ на коэффициенты порождающего полинома, отличные от 0 или 1. Результат перемножения представить в выбранном базисе.

9. Нарисовать структурную схему кодирующего устройства с учетом результатов, полученных в предыдущем пункте. Схема должна иметь вид, аналогичный представленному на рис. 3.9.

10. Указать информационные характеристики кода и его корректирующие способности.

3.2. Элементы теорий конечных полей

В структуре псевдослучайных последовательностей существуют особые закономерности, которые вытекают из их построения на основе конечных полей или их групп. Конечными полями являются множества номеров элементов псевдослучайной последовательности, а саму двоичную псевдослучайную последовательность можно рассматривать как полученную в результате сопоставления 0 или 1 элементам с определенными номерами.

В этой главе дается краткое математическое введение в теорию конечных полей и групп. Изложение ведется описательно, со множеством примеров, доказательства основных положений опущены. Автор пытается изложить материал так, чтобы он был понятен для инженеров-радистов, не знакомых с теорией конечных полей. В главе вводятся понятия конечных полей - расширенных и простых, мультипликативных и аддитивных групп, первообразного и примитивного элементов, а также смежных и сопряженных классов.

3.2.1. Конечные поля

Классическое определение поля [13]:

Поле - это множество элементов, на которых заданы операции умножения и сложения, удовлетворяющие законам замкнутости, ассоциативности, коммутативности и дистрибутивности.

Поясним эти законы, обозначив элементы поля через a, b и c, знаки умножения и сложения - общим знаком композиции *.

Замкнутость: если $a \in M$ и $b \in M$, то существует единственный элемент $c \in M$: $c=a*b$. Из этого следует, что среди элементов поля должен быть единичный элемент e, такой, что $a*e=a$, а также наличие обратного элемента $\bar{a} \in M$ такого, что $a*\bar{a}=e$.

Ассоциативность: $(a*b)*c = a*(b*c)$.

Коммутативность: $a*b=b*a$.

Дистрибутивность: $a\cdot(b+c)=a\cdot b+a\cdot c$.

При рассмотрении полей применительно к псевдослучайным последовательностям будем иметь дело со множествами чисел, для которых безусловно выполняются законы ассоциативности, коммутативности и дистрибутивности. В этом случае остается проверять только закон замкнутости, выполнение которого сводится к наличию единичного e и обратных элементов (по умножению $\bar{a}=-a^{-1}$, по сложению $\bar{a}=-a$). Поэтому в нашем случае определение поля упрощается.

Поле - это множество элементов, для которых заданы операции сложения и умножения, обязательно имеется единичный элемент, и для каждого элемента (кроме нулевого) среди элементов поля имеется обратный элемент.

Задание операций сложения и умножения означает, что если элементы a и b принадлежат полю G ($a \in G$ и $b \in G$), то $a+b \in G$ и $a \cdot b \in G$. Единичный элемент e определяется выражением $a*e=a$, где композиция * означает сложение или умножение. Единичный элемент относительно операции умножения есть «1», а относительно операции сложения – «0». Понятие обратного элемента $\bar{a}$ вытекает из равенства $a*\bar{a}=e$. О нем есть смысл говорить относительно операции умножения $a \cdot \bar{a} = 1$, то есть $\bar{a}=-a^{-1}$. Относительно операции сложения обратным элементом $\bar{a}$ является элемент $-a$, что вытекает из равенства $a+\bar{a}=0$ (0 - единичный элемент относительно сложения).

Примерами полей являются:

- поле действительных чисел Q,
- поле рациональных чисел R,
- поле комплексных чисел C.

Они содержат 0 и 1 - единичные элементы соответственно по сложению и умножению, сумма и произведение любых двух элементов любого из этих полей также принадлежит этому полю, и каждый элемент имеет обратный.

Особую важность для теории кодирования и псевдослучайных последовательностей имеют конечные поля.

Конечное поле - поле, содержащее конечное число элементов. Конечные поля называются полями Галуа по имени их первого исследователя Эвариста Галуа.

Число элементов в поле называется его *порядком*. Приведенные выше в качестве примера поля действительных, рациональных и комплексных чисел имеют бесконечный порядок. Число элементов любого поля Галуа (его порядок) есть степень p^m некоторого натурального простого числа p, являющегося *характеристикой* этого поля. Для любого натурального простого числа p и любого натурального m существует поле из p^m элементов. Его обозначают $GF(p^m)$. Поле $GF(p^m)$ содержит в качестве подполя $GF(p^n)$ в том и только в том случае, если m делится на n, что обозначается $n \mid m$ – n делит m.

Пример 1. В поле $GF(2^4)$ существуют два подполя GF(2) и $GF(2^2)$.

В любом поле $GF(p^m)$ содержится подполе GF(p), *называемое простым полем характеристики* p (p - *простое число*).

Поле $GF(p^m)$ называется *расширением* простого поля GF(P), так как расширенное поле - это поле, содержащее данное поле в качестве подполя.

Так, в соответствии с примером 1.1 поле $GF(2^4)$ можно рассматривать как расширение полей GF(2) или $GF(2^2)$. Из этих двух полей первое является простым полем характеристики 2, а второе, в свою очередь, может рассматриваться как расширение простого поля GF(2).

Элементами простого поля являются целые числа по модулю простого числа p.

Здесь надо пояснить, как вычисляется число по модулю и что такое вычеты. Для этого надо использовать теорию сравнения целых чисел [22].

Сравнение целых чисел a и b по модулю k (k - любое целое положительное число) записывается в виде $a \equiv b (mod\ k)$, оно эквивалентно равенству $a-b=r \cdot k$, то есть b можно рассматривать как остаток от деления a на модуль k (r - целое число). Так

$2=0\ mod\ 2$, $15=5\ mod\ 10$, $23=2\ mod\ 7$, $-2=5\ mod\ 7$, $-23=2\ mod\ 7$.

Все целые числа a такие, что $a \equiv b (mod\ k)$ при фиксированном b образуют класс чисел по модулю k, который обозначается, через $\{ b \}$ или $b (mod\ k)$. Всем числам этого класса соответствует один и тот же остаток b, и можно получить все числа класса (их количество бесконечно), если в формуле $b+r \cdot k$ заставить r пробегать все целые числа (положительные и отрицательные). Соответственно k различным значениям b имеем k классов чисел по модулю k.

Рассмотрим случай k=3. Имеем три класса чисел по модулю 3:

{ 0 } = {…-9, -6, -3, 0, 3, 6,…}, { 1 } = {-8, -5, -2, 1, 4, 7,…},

{ 2 } = {…-7, -4, -1, 2, 5, 8,…}.

Любое число класса называется *вычетом* по модулю k по отношению ко всем числам этого класса. Из свойств сравнений известно, что если $x \equiv a (mod\ k)$, а $y \equiv b (mod\ k)$, то $x+y \equiv a+b (mod\ k)$, $x \cdot y \equiv a \cdot b (mod\ k)$. Тем самым определены операции сложения и умножения классов вычетов по модулю k :

$\{ a \}+\{ b \}=\{ a+b \}$, $\{ a \} \cdot \{ b \}=\{ a \cdot b \}$.

Взяв от каждого класса по вычету, получим полную систему вычетов. Чаще всего в *качестве представителей классов вычетов берут наименьшие неотрицательные вычеты* 0,1, ...,(k-1). Полная система вычетов по модулю простого числа p (k=p) удовлетворяет всем законам поля, и поэтому можно утверждать, что простое поле характеристики p *изоморфно* (*Изоморфизм - соответствие между объектами, в данном случае между полями, выражающее в некотором смысле тождество их строения*) полю вычетов по модулю p. Приведенная выше полная система вычетов по модулю 3 дает простое поле GF(3) =(0, 1, 2) характеристики 3.

Пример 2. Представить классы вычетов по модулю чисел 7 и 10. Показать, что полная система вычетов по модулю 7 (7-простое число) является полем, а по модулю 10 - нет (10=5·2 - не является простым числом).

Классы вычетов по модулю простого числа 7:

{ 0 } = {-14, -7, 0, 7, 14, …}, { 1 } = {-13, -6, 1, 8, 15, …},

{ 2 } = {-12, -5, 2, 9, 16, …}, { 3 } = {-11, -4, 3, 10, 17, …},

{ 4 } = {-10, -3, 4, 11, 18, …}, { 5 } = {-9, -2, 5, 12, 19, …},

{ 6 } = {-8, -1, 6, 13, 20, …}.

Полная система вычетов 0, 1, 2, 3, 4, 5, 6. Проверим, выполняются ли для этого множества законы поля. Среди элементов этого множества имеются элементы 1 и 0 - единичные элементы относительно операций соответственно умножения и сложения. Любая сумма и произведение элементов приводят к элементам того же множества. Приведем некоторые примеры:

3+4 = 7 =0(*mod* 7), 5+6 = 11 = 4(*mod* 7), 6+6 = 12 = 5(*mod* 7),
3+6 = 9 =2(*mod* 7);
3·4 = 12 = 5(*mod* 7), 5·6 = 30 = 2(*mod* 7), 6·6 = 36 = 1(*mod* 7),
3·6 = 18 =4(*mod* 7), 4·2=1(*mod* 7).

Напоминаем, что определение числа по какому-то модулю - это определение остатка от деления числа на этот модуль.

Вычисление обратного элемента следует проводить по формуле $\bar{a}=1/a=(1+r\cdot k)/a$, в которой учитывается, что число 1 может быть представителем любого числа $1+r\cdot k$ класса вычетов {1}. Тогда $\overline{1}=1,\ \overline{2}=2,\ \overline{3}=3,\ \overline{4}=4,\ \overline{5}=5,\ \overline{6}=6$, то есть все элементы, кроме 0, имеют обратные элементы. Все это позволяет назвать полную систему вычетов 0, 1, 2, 3, 4, 5, 6 по модулю 7 полным конечным полем характеристики 7: GF(7)=(0, 1, 2, 3, 4, 5, 6).

Рассмотрим полную систему вычетов по модулю 10:
{ 0 } = {-20, -10, 0, 10, 20, …}, { 1 } = {-19, -9, 1, 11, 21, …},
{ 2 } = {-18, -8, 2, 12, 22, …}, { 3 } = {-17, -7, 3, 13, 23, …},
{ 4 } = {-16, -6, 4, 13, 24, …}, { 5 } = {-15, -5, 5, 15, 25, …},
{ 6 } = {-14, -4, 6, 16, 26, …}, { 7 } = {-13, -3, 7, 17, 27, …},
{ 8 } = {-12, -2, 8, 18, 28, …}, { 9 } = {-11, -1, 9, 19, 29, …}.

В качестве представителей классов вычетов возьмем, как и в предыдущем случае, наименьшие положительные значения вычетов 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Это множество элементов уже не будет полем. Хотя в результате сложения и умножения по модулю 10 любых элементов получатся элементы, принадлежащие этому же множеству, обратные элементы по умножению будут иметь не все элементы, отличные от 0. Так, например, элементы 2, 4, 5 не будут иметь обратных элементов, так как ни при каком r не делится $(1+10\cdot r)$ на 2, 4 и 5.

Для любого натурального простого p и любого натурального m существует единственное с точностью до изоморфизма поле из p^m элементов. Для определения элементов расширенного поля $GF(p^m)$ используются полиномы переменной x степени не выше m-1 с коэффициентами из поля GF(p). Число слагаемых в каждом полиноме равно m (переменная x в степенях от 0 до m-1), коэффициенты при x могут принимать одно из p значений. Следовательно, такие полиномы определят все p^m элементов расширенного поля.

Приведем пример расширения $GF(2^3)$ степени 3 простого поля GF(2). Элементами поля GF(2) будут 0 и 1. Эти элементы будут элементами и поля $GF(2^3)$. Кроме того, его элементами также будут все возможные полиномы степени не выше 2. Таким образом, поле GF (2^3) будет содержать элементы: 0, 1, x, $1+x$, $1+x+x^2$, $1+x^2$, $x+x^2$, x^2. Мы задали множество из 2^3 элементов. Но пока это множество еще не является полем, так как не определены между его элементами операции сложения и умножения. Для этого надо задать полином степени m (в нашем случае m=3), по модулю которого будут проводиться вычисления при сложении и умножении. По аналогии с простым полем Галуа GF(p), элементами которого является полная система вычетов по модулю числа p, элемента-

ми расширения GF(p^m) степени m простого поля GF(p) является полная система вычетов по модулю полинома степени m, неприводимого над полем GF(p).

Полином P(x) *степени* $m \geq 1$ *с коэффициентами из поля* GF(p) *неприводим над полем* GF(p), *если он не может быть представлен в виде произведения полиномов меньшей степени над полем* GF(p).

Поясним понятие вычетов по модулю какого-то полинома.

Сравнение полиномов A (x) и B(x) по модулю P(x)

$$A(x) \equiv B(x) (mod\ P(x)) \qquad (50)$$

эквивалентно равенству A(x)-B(x)=K(x)P(x) для некоторого полинома K(x). Все операции с коэффициентами при x в одинаковых степенях проводятся по модулю p - характеристики простого поля GF(p), элементы которого используются в качестве коэффициентов в полиномах, B(x) - это остаток от деления полинома A(x) на полином P(x). Все полиномы A(x) над полем GF(p), которые при делении на P(x) дают один и тот же остаток, образуют класс вычетов полиномов по модулю P(x). Обычно в качестве представителя класса вычетов по модулю полинома берется полином наименьшей степени R(x) , класс вычетов обозначается {R(x)} или R(x) (*mod* P(x)).

В соответствии со свойством сравнений, если

$A(x) \equiv R_1(x) (mod\ P(x))$ и $B(x) \equiv R_2(x) (mod\ P(x))$, то

$A(x)+B(x) \equiv R_1(x)+R_2(x) (mod\ P(x))$ и $A(x) \cdot B(x) \equiv R_1(x) \cdot R_2(x) (mod\ P(x))$.

Тем самым определены операции сложения и умножения классов вычетов по модулю полинома P(x):

$\{ R_1(x) \}+\{ R_2(x) \}=\{ R_1(x)+R_2(x) \}$,

$\{ R_1(x) \} \cdot \{ R_2(x) \}=\{ R_1(x) \cdot R_2(x) \}$.

Если полином P(x) *является неприводимым над полем* GF(p), *то полная система вычетов по модулю этого полинома образует конечное поле* GF(p^m), m *- степень полинома* P(x).

Для определения поля GF(2^3) зададим операции сложения и умножения по неприводимому полиному x^3+x+1. Кстати, для m=3 существует еще один неприводимый полином x^3+x^2+1, а два других возможных полиномов 3-ей степени не являются неприводимыми $x^3+x^2+x+1=(x+1)(x^2+1)$, $x^3+1=(x+1)^3$, так как они могут быть представлены в виде произведения полиномов меньшей степени.

Таблица 3.4

Сложение в поле GF(2^3) по модулю полинома x^3+x+1

+	1	x	$1+x$	x^2	$1+x^2$	$1+x+x^2$	$x+x^2$
1	0	$1+x$	x	$1+x^2$	x^2	$x+x^2$	$1+x+x^2$
x	$1+x$	0	1	$x+x^2$	$1+x+x^2$	$1+x^2$	x^2
$1+x$	x	1	0	$1+x+x^2$	$x+x^2$	x^2	$1+x^2$
x^2	$1+x^2$	$x+x^2$	$1+x+x^2$	0	1	$1+x$	X
$1+x^2$	x^2	$1+x+x^2$	$x+x^2$	1	0	x	$1+x$
$1+x+x^2$	$x+x^2$	$1+x^2$	x^2	$1+x$	x	0	1
$x+x^2$	$1+x+x^2$	x^2	$1+x^2$	x	$1+x$	1	0

Таблица 3.5

Умножение в поле $GF(2^3)$ по модулю полинома x^3+x+1

•	1	x	$1+x$	x^2	$1+x^2$	$1+x+x^2$	$x+x^2$
1	1	x	$1+x$	x^2	$1+x^2$	$1+x+x^2$	$x+x^2$
x	x	x^2	$x+x^2$	$1+x$	1	$1+x^2$	$1+x+x^2$
$1+x$	$1+x$	$x+x^2$	$1+x^2$	$1+x+x^2$	x^2	x	1
x^2	x^2	$1+x$	$1+x+x^2$	$x+x^2$	x	1	x^2+1
$1+x^2$	$1+x^2$	1	x^2	x	$1+x+x^2$	$x+x^2$	$1+x$
$1+x+x^2$	$1+x+x^2$	$1+x^2$	x	1	$x+x^2$	$1+x$	x^2
$x+x^2$	$x+x^2$	$1+x+x^2$	1	$1+x^2$	$1+x$	x^2	x

Из таблиц 3.4 и 3.5 видно, что умножение и сложение элементов поля приводит к элементам этого поля, то есть в поле $GF(2^3)$ заданы операции умножения и сложения. В табл. 3.4 и 3.5 элемент 0 не приводится, так как операции с ним однозначно определены как $A(x)+0=A(x)$ и $A(x)\cdot 0=0$ и не зависят от вида неприводимого полинома.

При смене полинома изменится только таблица умножения. Например, для неприводимого полинома x^3+x^2+1 умножение элементов $GF(2^3)$ даст результаты: $(1+x)\cdot x^2=1$, $(1+x^2)\cdot(1+x)=x$, $(1+x^2)\cdot(1+x^2)=x^2+x$. Поясним подробнее процесс умножения полиномов по модулю какого-то полинома:
$(1+x+x^2)\cdot(x+x^2)=x+x^2+x^3+x^2+x^3+x^4=x+x^4$. Здесь мы провели сложение по модулю p=2 коэффициентов при одинаковых степенях x.

Теперь надо определить остаток от деления на неприводимый полином.

$$\begin{array}{r|l} x^4+x & x^3+x+1 \\ +\ x^4+x^2+x & x \\ \hline x^2 & \end{array} \qquad \begin{array}{r|l} x^4+x & x^3+x^2+1 \\ +x^4+x^3+x & x+1 \\ \hline x^3 & \\ +x^3+x^2+1 & \\ \hline x^2+1 & \end{array}$$

Деление проводится как деление обычных многочленов, но вычитание коэффициентов при x в одинаковых степенях должно проводиться по модулю простого числа p. В рассматриваемом случае p=2, при использовании этого модуля операции сложения и вычитания эквивалентны 1+1=0(*mod* 2), 1-1=0, 0+1=1, 0-1=p-1=2-1=1(*mod* 2) - в последнем выражении 0 заменяется на p=2, так как p=0(*mod* p). При определении остатка при делении вычитание заменено суммированием по модулю два. Следовательно,

$$(1+x+x^2)\cdot(x+x^2)=x^2(mod(x^3+x+1))=(1+x^2)(mod(x^3+x^2+1)).$$

Остаток от деления можно определить и по-другому. Из этого следует, что полином $B(x)=A(x)-K(x)\cdot P(x)$, где $A(x)$ - исходный полином, степень которого выше степени $B(x)$,

$P(x)$ - полином, по модулю которого вычисляется $A(x)$,

$K(x)$ - какой-то полином.

Если используют полиномы над полем GF(2), то есть коэффициенты при переменных являются элементами 0 и 1 этого поля и сложение их проводится по модулю два, то можно записать:

$B(x)=A(x)+K(x)\cdot P(x)$.

Для вычисления полинома $B(x)$, являющегося вычетом по модулю $P(x)$ полинома $A(x)$, надо к $A(x)$ прибавить полином $P(x)$, умноженный на какой-то полином $K(x)$, который, выбирается так, чтобы степень $B(x)$ была меньше степени полинома $P(x)$. Например, преобразование полинома x^4+x можно провести следующим образом:

$$x^4+x=x^4+x+x(x^3+x+1)=x^2(mod(x^3+x+1)),$$
$$x^4+x=x^4+x+x(x^3+x^2+1)=x^3+(x^3+x^2+1)=x^2+1(mod(x^3+x^2+1)).$$

Если степень исходного полинома высокая, то обычно понижают ее постепенно, как это сделано в последнем примере.

При оперировании с полиномами над простым полем характеристики p для упрощения вычислений можно использовать соотношение $(a+b)^p=a^p+b^p$, которое удовлетворяется при любом числе слагаемых $(\Sigma a_k)^p = \Sigma a_k^p$. Поэтому при составлении табл. 3.5 (p=2) можно сразу написать для произведения $(1+x+x^2)\cdot(1+x+x^2)=1+x^2+x^4$ и далее понижать степень, как было указано выше.

Число элементов конечного поля является степенью его характеристики p *и не может быть равно другому числу. Следовательно, поля* $GF(p^m)$ *исчерпывают все возможные поля. При* $m=1$ *получаем простое поле* GF(p).

3.2.2. Мультипликативная структура конечных полей

Сначала введем понятие группы.

Группа - это множество элементов, для которых задана ассоциативная операция, имеется единичный элемент и для каждого элемента имеется обратный элемент. *Если в группе определена операция сложения, то группа называется аддитивной. Если задано умножение - то мультипликативной*. Группа, имеющая конечное число элементов, называется *конечной*. Она обозначается как $G(a, b, c,...)$. Число элементов в группе называется ее *порядком*.

В конечном поле можно выделить аддитивную и мультипликативную группы.

Все элементы любого конечного поля образуют аддитивную группу. Порядок аддитивной группы совпадает с порядком поля. Мультипликативная группа включает все элементы поля, кроме нулевого, поэтому ее порядок на I меньше порядка поля.

Наиболее интересна мультипликативная группа поля. Перейдем к ее рассмотрению.

Определение операции умножения на элементах поля означает, что если $a\in GF(q)$, то это поле должно содержать и $a\cdot a=a^2$, $a^2\cdot a=a^3$ и так далее. Иначе, по-

ле должно содержать все степени любого своего элемента. Должен существовать такой наименьший положительный показатель степени ε, что $a^{\varepsilon}=1$, тогда $a^{\varepsilon+k}=a^k$ и ε называется *периодом* элемента a. Все элементы a^k, $k=\overline{0,\varepsilon-1}$, различны. Так как порядок мультипликативной группы поля GF(q) равен q-1, то максимально возможный период элемента поля

$$\varepsilon_{max}=q\text{-}1. \qquad (51)$$

Если известен период ε произвольного элемента a поля GF(q), то можно определить период элемента a^k, он будет равен $\varepsilon/(\varepsilon,k)$, где (ε,k) - наименьший общий делитель чисел ε и k. Период ε любого ненулевого элемента поля GF(q) всегда делит порядок мультипликативной группы поля q-1: ε/q.

Элемент a, имеющий максимально возможный период $\varepsilon_{max}=q$-1, называется *первообразным элементом поля* GF(q). Обозначим его через α. Степени α^0, $\alpha^1,\ldots, \alpha^{q-2}$ различны и пробегают все ненулевые элементы поля GF(q). Поэтому первообразный элемент является образующим элементом мультипликативной группы G поля GF(q):

$$G=\{\alpha^0,\alpha^1,\ldots,\alpha^{q-2}\},$$

$$GF(q)=\{0,\alpha^0,\alpha^1,\ldots,\alpha^{q-2}\}.$$

Все k-е степени первообразного элемента α^k также являются первообразными элементами этого поля, если k и q-1 взаимно простые числа, то есть, $(k,q\text{-}1)=1$. Число чисел, взаимно простых с q-1 и не превосходящих q-1, определяется функцией Эйлера $\varphi(q\text{-}1)$. Следовательно, *в поле* GF(q) *имеется* $\varphi(q\text{-}1)$ *первообразных элементов.*

Элемент поля, мультипликативно обратный первообразному, тоже является первообразным.

Пример 3. Определить периоды элементов поля GF(7) и найти его первообразные элементы.

Поле GF(7)={ 0, 1, 2, 3, 4, 5, 6 } имеет мультипликативную группу G={ 1, 2, 3, 4, 5, 6 } порядка 6. Элементы этой группы могут иметь максимальный период $\varepsilon_{max}=6$, а также меньшие периоды $\varepsilon=1, 2, 3$. Число элементов максимального периода, т.е. первообразных элементов, определяется функцией Эйлера $\varphi(6)=2$. Для определения периодов элементов поля составим табл. 3.6.

Таблица 3.6

Степени элементов a

a	$\{a^k, k=0,1,\ldots\}$	ε
1	1, 1, …	1
2	1, 2, 4, 1, …	3
3	1, 3, 2, 6, 4, 5, 1, …	6
4	1, 4, 2, 1, …	3
5	1, 5, 4, 6, 2, 3, 1, …	6
6	1, 6, 1, …	2

Из таблицы видно, что первообразными элементами являются элемент 3 и обратный ему 5, имеющие максимальный период 6, совпадающий с порядком мультипликативной группы поля GF(7). Степени этих элементов пробегают все элементы мультипликативной группы, но в различной последовательности. Обращаем внимание на то, что период ε=3 также имеют два элемента: 2 и обратный ему 4 (см. пример 2). Периоды 1 и 2 имеют соответственно элементы 1 и 6, так как число чисел, взаимно простых с 1 и 2, равно 1.

В расширении любой степени m GF(p^m) любого простого поля GF(p) все p^m-1 элементов, отличных от 0, образуют циклическую мультипликативную группу, ее порядок p^m-1: все элементы этой группы можно представить как различные степени первообразного элемента, или, как его еще называют, примитивного корня α. Степени α^k, (k,p^m-1)=1, также являются первообразными элементами расширенного поля GF(p^m), их число равно φ(p^m-1). Таким образом, *для любого расширенного поля* GF(p^m) *существуют* φ(p^m-1) *первообразных элементов.*

Пример 4. Найти период элемента x поля GF(2^3) с неприводимым полиномом x^3+x+1 (все возможные элементы мультипликативной группы этого поля приведены в первой строке табл. 3.1 и 3.2).

Запишем последовательные степени x и найдем их вычеты по модулю полинома x^3+x+1: x^0, x, x^2, $x^3=x+1$, $x^4=x^2+x$, $x^5=x^2+x+1$, $x^6=x^2+1$, $x^7=1$. Видим, что период элемента x равен $\varepsilon_{max}=7$. Степени x^k, $k=\overline{1,6}$, пробегают все отличные от 0 элементы поля, следовательно, x является первообразным элементом поля. Показатели степени k первообразного элемента x, $k=\overline{1,6}$, все являются взаимно простыми с периодом мультипликативной группы 7, поэтому все степени x^k, $k=\overline{1,6}$ являются первообразными элементами поля GF(2^3). Всего имеется φ(2^3-1)=φ(7)=6 первообразных элементов.

Рассмотрим пример определения первообразных элементов расширенного поля

Пример 5. Определить первообразные элементы (примитивные корни) расширенного поля GF(2^4) с неприводимым полиномом x^4+x+1.

Запишем последовательные степени x и найдем их вычеты по модулю полинома x^4+x+1 (табл.3.2.4). Число первообразных элементов φ(15)=8. Элемент x является первообразным элементом расширенного поля GF(2^4), так как его период равен p^m-1=15. Первообразными элементами также являются x^2, $x^4=x+1$, $x^7= x^3+x+1$, $x^8=x^2+1$, $x^{11}=x^3+ x^2+x$, $x^{13}=x^3+x^2+1$, $x^{14}=x^3+1$, так как эти показатели степеней x не имеют общих делителей с 15. Образующим элементом мультипликативной группы расширенного поля GF(2^4) может быть любой из приведенных первообразных элементов.

Но 3, 5, 6, 9, 10, 12-я степени первообразных элементов будут иметь меньший период и не будут первообразными элементами расширенного поля GF(2^4): 3, 6, 9 и 12-я степени любого первообразного элемента будут иметь период 15/3 =5, а 5 и 10-я - 15/5=3. Первообразные элементы расширенного поля обозначаются через α.

Таблица 3.7

x^k и их вычеты по модулю полинома x^4+x+1

x^k	$x^k(mod(x^4+x+1))$
x^0	1
x^1	x
x^2	x^2
x^3	x^3
x^4	$x+1$
x^5	x^2+x
x^6	x^3+x^2
x^7	x^3+x+1
x^8	x^2+1
x^9	x^3+x
x^{10}	x^2+x+1
x^{11}	x^3+x^2+x
x^{12}	x^3+x^2+x+1
x^{13}	x^3+x^2+1
x^{14}	x^3+1
x^{15}	1

Если в табл. 3.7 заменить x на α, то эта таблица будет верна для любого первообразного элемента, определенного выше: x^2, x^4, x^7, x^8, x^{11}, x^{13}, x^{14}.

В мультипликативной группе можно выделить подгруппы, если в группе имеются элементы, период которых меньше ε_{max}. Подгруппа ***g*** *- это часть группы, которая обладает свойствами группы, то есть в ней определена ассоциативная групповая операция, имеется единичный элемент и для каждого элемента обратный.*

Например, для расширенного поля GF(2^4) , элементы которого приведены в табл.1.4., подгруппами могут быть множества элементов: $x^0=1$, $x^5=x^2+x$, $x^{10}=x^2+x+1$ (период 3) и $x^0=1$, x^3, $x^6=x^3+x^2$, $x^9=x^3+x$ (период 5).

Пример 6. Определить все подгруппы мультипликативной группы, поля GF(7).

Воспользуемся результатами примера 3. Образующими элементами мультипликативных подгрупп могут быть 1, 2, 4, 6. Эти элементы имеют период, меньший $\varepsilon_{max}=6$. Подгруппы с образующими 2 и 4 имеют одни и те же элементы. Таким образом, в мультипликативной группе поля GF(2^3) можно выделить 3 мультипликативные подгруппы:

$g_1=\{ 1 \}$, $g_2=\{ 1, 2, 4 \}$, $g_3=\{ 1, 6 \}$.

Здесь следует заметить, что мультипликативная группа поля GF(2^3), рассмотренная в примере 1.4, не имеет подгрупп, так как все ее элементы имеют максимальный период, являются первообразными элементами.

Введем понятие смежных классов. Пусть G={ a_1, a_2,…} - мультипликативная группа и g={ g_1, g_2,… } - ее подгруппа. Тогда *множество элементов вида* $a \cdot g_i$, где g_i принимает значения из g и a - фиксированный элемент G, называется *смежным классом по* g *и обозначается* ag. Из определения следует, что смежный класс по g и подгруппа g содержат одинаковое число элементов. Кроме того, *если у двух классов оказался общий элемент, то они совпадают*. Элемент a_k, принадлежащий смежному классу a_kg называется образующим элементом этого смежного класса. В качестве образующего может быть выбран любой элемент смежного класса.

Группу G можно представить как объединение непересекающихся смежных классов

$$G=\{a_1 g\}+\{a_2 g\}+\ldots+\{a_k g\}. \qquad (52)$$

Здесь символ сложения следует рассматривать как символ объединения. Представление (1.3) называется разложением группы на смежные классы.

Пример 7. Представить разложение на смежные классы мультипликативной группы поля GF(7).

Из решения примера 1.6 можно взять подгруппы { 1, 6 } и { 1, 2, 4 }, по которым можно разложить мультипликативную группу на смежные классы. Первую подгруппу, состоящую из одного элемента { 1 }, брать нет смысла, так как смежные классы будут состоять из одного элемента.

Следует пояснить образование смежных классов (образующим элементом является 1). При определении других смежных классов в качестве образующих элементов выбирают элементы поля, которые не входят ни в один из уже определенных смежных классов.

Рассмотрим смежные классы по подгруппе g={ 1, 6 }. Одним из смежных классов является подгруппа { 1.6 } (её элементы умножены на 1 - первый элемент мультипликативной группы). Второй смежный класс получим умножением элементов подгруппы { 1, 6 } на 2 - второй элемент группы: { 2·1, 2·6 }={ 2, 5 }, Третий смежный класс получим умножением элементов подгруппы {1,6} на 3 – третий элемент группы: { 3·1, 3·6 }={ 3,4 }. Дальнейшее умножение на элементы группы 4, 5, 6 проводить не будем, так как эти элементы уже входят в определенные смежные классы. Таким образом получим смежные классы по подгруппе { 1, 6 }: { 1, 6 }, { 2, 5 }, { 3, 4 }. Тогда мультипликативную группу G={ 1, 2, 3, 4, 5, 6 } можно представить в виде

G={ 1, 6 }+{ 2, 5 }+{ 3, 4 }.

Рассмотрим подгруппу {1, 2, 4 }, смежные классы по этой подгруппе { l, 2, 4 } и { 3, 6, 5 }. Следовательно, G(1, 2, 3, 4, 5, 6)={ 1, 2, 4 }+{ 3, 6, 5 }.

Пример 8. Представить разложение на смежные классы мультипликативной группы расширенного поля GF(2^4) с неприводимым полиномом x^4+x+1.

Элементы мультипликативной группы расширенного поля GF(2^4) будем представлять степенями первообразного элемента α. Мультипликативную группу поля можно представить в виде степеней α^0, α^1, α^2, α^3, α^4, α^5, α^6, α^7, α^8, α^9, α^{10}, α^{11}, α^{12}, α^{13}, α^{14}.

Порядок мультипликативной группы 15. Подгруппы могут иметь порядок 3 или 5. Выберем подгруппу порядка 5: α^0, α^3, α^6, α^9, α^{12}. В табл.3.8 приведены смежные классы мультипликативной группы поля GF(2^4) по рассматриваемой подгруппе (элементы поля представлены степенями примитивного элемента α^k, а также вычетами по модулю неприводимого полинома x^4+x+1.

Таблица 3.8

Смежные классы расширенного поля GF(2^4)

Подгруппа	1	α^3	α^6	α^9	α^{12}
	α	α^4	α^7	α^{10}	α^{13}
	α^2	α^5	α^8	α^{11}	α^{14}
Подгруппа	1	α^3	$\alpha^3+\alpha^2$	$\alpha^3+\alpha$	$\alpha^3+\alpha^2+\alpha+1$
	α	$\alpha+1$	$\alpha^3+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+1$
	α^2	$\alpha^2+\alpha$	α^2+1	$\alpha^3+\alpha^2+\alpha$	α^3+1

3.2.3. Алгебраическая структура полей Галуа

Будем рассматривать расширенные поля Галуа, элементы которых представляются алгебраическими выражениями. Различные представления элементов поля Галуа приведены в табл. 3.9 для частного случая GF(2^4) с неприводимым полиномом x^4+x+1.

Как было определено в примере 5, элементы мультипликативной группы поля GF(2^4) имеют периоды: 15, 5 и 3. В общем случае любой элемент α мультипликативной группы поля GF(p^m), имеющий период ε, удовлетворяет сравнению

$$\alpha^{\varepsilon}\equiv 1 \qquad (53)$$

Первообразный элемент α имеет максимальный период $\varepsilon=p^m-1$ и, следовательно,

$$\alpha^{p^m-1}\equiv 1 . \qquad (54)$$

Остальные элементы расширенного поля Галуа имеют периоды ε, которые делят период первообразного элемента $\varepsilon/(p^m-1)$.

Если обозначить $(p^m-1)/\varepsilon=k$, то, возведя в k-ю степень обе части сравнения (54), получим

$$\alpha^{\varepsilon\cdot k}=\alpha^{p-1}\equiv 1. \qquad (55)$$

Из (54) и (55) следует, что любой элемент мультипликативной группы расширенного поля Галуа удовлетворяет уравнению

$$x^{p^m-1}-1=0 , \qquad (56)$$

а все элементы поля (включая нулевой) - уравнению

$$x^{p^m}-x=0 . \qquad (57)$$

С другой стороны, известно, что полином $x^{p^m}-x$ можно представить в виде произведения неприводимых полиномов, то есть таких, которые не представляются в виде произведения полиномов меньшей степени над простым полем GF(p), для которых элементы поля GF(p) не являются корнями. Однако в расширенном поле GF(p^m) неприводимые над полем GF(p) полиномы уже имеют корни, то есть могут обращаться в 0.

Таблица 3.9

Различные представления элементов поля GF(2^4)

Номер элемента, k	Представление степенью, α^{k-1}	Представление в виде полинома		Псевдослучайная последовательность
		степени < 4	двоичного	
0				
1	α^0	1	0001	0
2	α^1	α	0010	0
3	α^2	α^2	0100	0
4	α^3	α^3	1000	1
5	α^4	$\alpha+1$	0011	0
6	α^5	$\alpha^2+\alpha$	0110	0
7	α^6	$\alpha^3+\alpha^2$	1100	1
8	α^7	$\alpha^3+\alpha+1$	1011	1
9	α^8	$\alpha^2+\alpha$	0101	0
10	α^9	$\alpha^3+\alpha$	1010	1
11	α^{10}	$\alpha^2+\alpha+1$	0111	0
12	α^{11}	$\alpha^3+\alpha^2+\alpha$	1110	1
13	α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111	1
14	α^{13}	$\alpha^3+\alpha^2+1$	1101	1
15	α^{14}	α^3+1	1001	1
16	α^{15}	1	0001	0

Какие-то k элементов расширенного поля GF(p^m) *будут корнями только одного неприводимого над полем* GF(p) *полинома степени k, при этом k должно делить m. Если* α *является корнем неприводимого полинома k -й степени, то остальными* (k-1) *корнями будут*

$$\alpha^{p}, \alpha^{p^2}, \ldots, \alpha^{p^{k-1}}. \qquad (58)$$

Элементы (58) называются *p-сопряженными* с α.

Неприводимые полиномы степени m, которые делят $x^{p^{m-1}}-1$, но не делят никакой двучлен меньшей степени, называются примитивными полиномами. Корни именно этих полиномов имеют максимальный период p^m-1 и называются *примитивными элементами*. По-другому примитивный элемент называют *примитивным корнем*, так как он определяется как корень степени p^m-1 из 1 (в соответствии с формулой (58)). Число примитивных элементов определяется

функцией Эйлера $\varphi(p^m-1)$, а число примитивных полиномов в m раз меньше - $\varphi(p^m-1)/m$, так как каждый примитивный полином имеет m различных корней. В разложении полинома $x^{p^m-1}-1$ на множители могут встречаться и другие полиномы степени m, но они не будут примитивными, хотя и будут неприводимыми над полем GF(p). В разложении могут встречаться неприводимые полиномы любой степени k, которая делит m: $k \mid m$. Сумма степеней всех полиномов должна равняться p^m-1. Например, для поля $GF(2^4)$

$$x^{16}+x=x\cdot(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x+1)(x^4+x^3+1).$$

Все полиномы в этом разложении являются неприводимыми над полем GF(2), но только два последних являются примитивными в поле $GF(2^4)$. Полином $x^4+x^3+x^2+x+1$ не является примитивным, так как делит без остатка x^5+1: $(x^5+1)/(x^4+x^3+x^2+x+1)=x+1$. Степени полиномов могут быть 1, 2 и 4, так как они должны делить m=4.

В общем случае корни полинома степени k будут иметь период, который определяется как наименьшее значение степени n, при которой двучлен x^n-1 *делится на этот полином без остатка.* Так, полином $x+1$ делит $x+1$, следовательно, период элемента, являющегося корнем полинома $x+1=0$, равен 1. Полином x^2+x+1 делит без остатка x^3+1, следовательно, его корни имеют период 3, а корни полинома $x^4+x^3+x^2+x+1$ имеют период 5. Примитивные полиномы x^4+x+1 и x^4+x^3+1 делят без остатка только $x^{15}+1$, их корни имеют максимальный период 15.

Элементы поля, являющиеся корнями одного полинома, называются сопряженными. Все элементы поля можно распределить на классы эквивалентности (сопряженности), в каждом классе объединяются сопряженные элементы. Классы сопряженности обозначим через A_i , где индекс i определяется показателем степени примитивного элемента, входящего в этот класс. Например, для поля $GF(2^4)$ будут следующие классы сопряженности:

$$A_0(\alpha^0),\ A_1(\alpha^1, \alpha^2, \alpha^4, \alpha^8),\ A_7(\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}),$$

$$A_3(\alpha^3, \alpha^6, \alpha^{12}, \alpha^9),\ A_5(\alpha^5, \alpha^{10}).$$

Рассмотрим подробнее объединение элементов мультипликативной группы поля $GF(2^4)$ в классы сопряженности.

Пример 9. Определить классы сопряженных элементов мультипликативной группы поля $GF(2^4)$.

Обозначим, как и прежде, через α какой-то *первообразный элемент поля* $GF(2^4)$*, который теперь будем называть примитивным*. Предположим: α является корнем примитивного полинома x^4+x+1.

Корнями этого же полинома так же будут α^2, α^4, α^8, всего 4 корня. Второй примитивный полином является обратным первому, то есть коэффициенты при x^i в первом полиноме будут коэффициентами при x^{m-i} во втором, обратном, полиноме. Корнями второго полинома будут элементы мультипликативной

группы, обратные корням первого полинома, то есть α^{14}, α^{13}, α^{11}, α^{7}. Напомним, что в мультипликативной группе обратный элемент $\bar{a}=a^{-1}$, так, если $a=\alpha^2$, то $\bar{a}=\alpha^{-2}=\alpha^{15-2}=\alpha^{13}$. Осталось определить корни не примитивных полиномов. Полином $x+1$ будет иметь корнем элемент $\alpha^0=1$, а полином x^2+x+1 элемент периода 3, Используя результаты решения примера 1.5, получим корни этого полинома α^5 и α^{10}. Из того же примера можно получить корни полинома $x^4+x^3+x^2+x+1$ (период этих элементов 5): α^3, α^6, α^9, α^{12} . Таким образом, для мультипликативной группы поля GF(2^4) имеем классы сопряженности A_0, A_1, A_7, A_3, A_5, которые были указаны выше. В классах сопряженности элементы могут быть представлены и полиномами степени ниже $m=4$, а также двоичными полиномами. Эти представления элементов поля GF(2^4) можно взять из табл. 3.9. Классы сопряженных элементов тогда будут представлены следующим образом:

$$A_0(1),\ A_1(\alpha,\ \alpha^2,\ \alpha+1,\ \alpha^2+1),\ A_7(\alpha^3+\alpha^2,\ \alpha^3+1,\ \alpha^3+\alpha^2+1,\ \alpha^3+\alpha^2+\alpha),$$

$$A_3(\alpha^3,\ \alpha^3+\alpha^2,\ \alpha^3+\alpha^2+\alpha+1,\ \alpha^2+1),\ A_5(\alpha^2+\alpha,\ \alpha^2+\alpha+1)$$

или

$A_0(1)$, $A_1(0010,0100,0011,0101)$, $A_7(1011,1001,1101,1110)$,
$A_3(1000,1100,1111,0101)$, $A_5(0110,0111)$.

Выводы по разделу.

1. Поле - это множество элементов, для которых заданы ассоциативные, дистрибутивные, коммутативные операции сложения и умножения, обязательно имеется единичный элемент и для каждого элемента, кроме нулевого, обратный. Число элементов поля называется порядком. Поле с конечным числом элементов называется конечным. Порядок конечного поля является степенью его характеристики p (p – простое число) и не может быть равно другому числу. Поля GF(p^m) исчерпывают все возможные поля.

2. Элементами простого поля GF(p) являются целые числа по модулю простого числа p. Элементами расширенного поля GF(p^m) степени m являются полиномы степени не выше m, являющиеся вычетами по модулю неприводимого над полем GF(p) полинома.

3. Группа - это множество элементов, для которых задана одна ассоциативная операция, имеется единичный элемент и для каждого элемента обратный. В конечном поле можно выделить аддитивную и мультипликативную группы. Порядок аддитивной группы (число ее элементов) совпадает с порядком поля, а мультипликативной - на 1 меньше. Все элементы мультипликативной группы можно представить степенями какого-то элемента. Этот элемент поля называется первообразным. В группе можно выделить подгруппу, все элементы которой можно представить степенями элемента, образующего подгруппу (он не является первообразным элементом). Порядок подгруппы делит порядок группы. Все элементы группы могут быть распределены на смежные классы по какой-то подгруппе, элементами которых является результат умножения элементов подгруппы на элементы группы.

4. В расширенном поле существует конечное число неприводимых полиномов, часть из которых является примитивными. Первообразный элемент расширенного поля является корнем какого-то примитивного полинома и называется примитивным элементом. Все элементы мультипликативной группы расширенного поля можно распределить на классы сопряженных элементов; элементы, принадлежащие одному классу, являются корнями одного неприводимого полинома.

3.2.4. Задания для самопроверки

1. Записать конечные поля характеристик p=3, 5, 7. Для каждого из этих полей:

а) записать аддитивную и мультипликативную группы, указать их порядок;

б) записать таблицу степеней элементов мультипликативной группы, определить порядок каждого элемента;

в) определить образующие элементы мультипликативных подгрупп, определить их порядок, записать подгруппы мультипликативной группы;

г) определить смежные классы мультипликативной группы по каждой подгруппе, представить мультипликативную группу как объединение непересекающихся смежных классов.

2. Для расширенных полей $GF(2^3)$, $GF(2^4)$, $GF(2^5)$ определить число примитивных элементов (с использованием функции Эйлера) и степени неприводимых полиномов.

3.В поле $GF(2^3)$ для примитивного полинома x^3+x+1 составить таблицу последовательных степеней примитивного элемента α в виде: степеней примитивного элемента α^i , i=0,7, полиномов степени, меньшей 3 (использовать, что α является корнем примитивного полинома $\alpha^3+\alpha+1=0$), двоичных полиномов.

3.3. Поля Галуа и псевдослучайные последовательности

Псевдослучайные двоичные последовательности можно рассматривать как результат сопоставления элементов конечных полей (простого GF(p) или расширенного $GF(p^m)$) с элементами 1 или 0 конечного двоичного поля GF(2). При этом одно значение 1 или 0 присваивается элементам, номера которых составляют целый класс или целую группу. Такое отображение элементов одного поля (GF(p) или $GF(p^m)$) в элементы другого поля GF(2) называется *гомоморфизмом*.

Рассматривая псевдослучайные последовательности как сигналы для РТС передачи информации, следует отметить их важнейшую характеристику - корреляционные функции. В этой главе приводятся корреляционные свойства двоичных последовательностей, необходимые и достаточные условия для получения одноуровневой корреляционной функции с заданным значением выбросов.

Приводится правило гомоморфного отображения для получения последовательностей Лежандра и М-последовательностей, а также структурные схемы устройств их формирования.

В этой главе рассматривается изоморфное отображение последовательностей, когда порядок поля не меняется, а меняется нумерация элементов поля. Изоморфным отображением является децимация, заключающаяся в построении новой последовательности путем выбора $q \cdot i$-х элементов исходной последовательности, i=1, 2, …N-1, q – целое число. Рассмотрены децимации последовательностей Лежандра и М- последовательностей, определены номера сдвигов результирующей ПСП. Определен характер изменения корреляционных функций и спектра при децимациях любых последовательностей.

3.3.1. Псевдослучайные двоичные последовательности и их корреляционные свойства

В радиотехнических системах часто используются сигналы, для формирования которых применяются псевдослучайные последовательности, В этом случае основными характеристиками сигналов являются их корреляционные свойства. Оказывается, на основе конечных полей можно синтезировать псевдослучайные последовательности, которые обладают хорошими корреляционными свойствами. Здесь ограничимся рассмотрением так называемых фазоманипулированных сигналов, когда в соответствии с символами псевдослучайной двоичной последовательности (ПСП) изменяется фаза гармонической несущей сигнала, принимая два значения: 0 или π. Огибающая корреляционной функции фазоманипулированного сигнала совпадает с корреляционной функцией (КФ) ПСП. Элементами ПСП в этом случае должны быть +1 и -1. ПСП именно с такими элементами нас будут интересовать. Но для простоты записи элементы ПСП будем обозначать 1 и 0.

Построение ПСП с элементами +1 и -1 на основе конечных полей Галуа сводится к *гомоморфному отображению группы поля* GF(p) *или* GF(p^m) *в группу* (+1, -1). Отображение G→H элементов группы G на элементы группы H называется гомоморфным, если из $g_1 \rightarrow h_1$ и $g_2 \rightarrow h_2$ следует, что $g_1 * g_2 \rightarrow h_1 * h_2$ (* обозначает групповую операцию). Иными словами, при гомоморфизме соотношения между элементами сохраняются. *В общем случае гомоморфное отображение сопровождается укрупнением элементов: в один элемент группы* H *отображаются целые классы, подгруппы или другие множества элементов группы* G. Гомоморфное отображение, которое не сопровождается укрупнением элементов, называется изоморфным. *Изоморфизм сводится к изменению порядка следования элементов конечного поля, к перенумерации его элементов. Порядок поля не меняется*.

Прежде, чем рассмотреть различные характеры гомоморфных отображений при синтезе ПСП, приведем некоторые свойства периодических автокорреляционных функций двоичных фазоманипулированных сигналов.

Обозначим k-й элемент ПСП через μ_k, k=0,1,…N-1, N - длина последовательности, число элементов в ней. Тогда автокорреляционная функция, которую далее будем называть корреляционной, определяется выражением

$$R(l) = \sum_{k=0}^{N-1} \mu_k \cdot \mu_{k+l} \ , \qquad (59)$$

где l означает сдвиг одной копии ПСП относительно другой при вычислении КФ. Значение l выражается целым числом.

КФ R(l) можно определить, не вычисляя произведение элементов в соответствии с формулой (59). Если используются двоичные ПСП, то для заданного l достаточно определить в двух копиях ПСП число A элементов одного знака (произведение этих элементов равно 1) и число D элементов различных знаков (их произведение равно -1). Здесь следует еще раз обратить внимание на то, что хотя ПСП записываются элементами 1 и 0, но под 0 подразумевается -1, что и учитывается при вычислении произведения элементов с разными и одинаковыми знаками: (-1)·(+1)=-1 и (-1)·(-1)=1 (а не 0). Тогда

$$R(l)=A–D=2A–N=N–2D. \qquad (60)$$

В этой формуле учитывалось, что A+D=N.

Формулу (60) рекомендуется использовать при вычислении КФ на ЭВМ, так как операции сравнения на ЭВМ выполняются значительно быстрее, чем умножение. Можно представить и еще одну формулу для вычисления КФ

$$R(l)=N–4(K^{+} - \lambda), \qquad (61)$$

в которой K^{+} - число единиц в последовательности, а λ - число произведений вида (1,·1) в формуле (59) для заданного l.

Приведем некоторые свойства периодических КФ псевдослучайных последовательностей, представленных элементами (1,-1).

1. Разность N-R(l) всегда делится на 4, то есть N-R(l)≡0(*mod* 4). Максимальное значение КФ будет при l=0: R(0)=N, а возможные боковые уровни КФ могут принимать дискретный ряд значений с интервалом 4. Это свойство можно использовать для проверки правильности вычисления периодических КФ.

2. Нижняя оценка максимальных боковых выбросов. Минимальное значение максимальных (по модулю) боковых выбросов определяется соотношениями

$$R_{max} \geq \begin{cases} 0 \text{ при } N \equiv 0(mod\ 4), \\ 1 \text{ при } N \equiv 1(mod\ 4), \\ 2 \text{ при } N \equiv 2(mod\ 4), \\ -1 \text{ при } N \equiv 3(mod\ 4), \end{cases} \qquad (62)$$

Пример 1. Определить возможные уровни КФ последовательностей длины N= 4, 10, 11, 13.

ПСП длины 4 может иметь только 3 уровня КФ; 4, 0 и -4. ПСП длины 10 может иметь КФ с уровнями: 10, 6, 2, -2, -6, -10. ПСП длины 11 может иметь КФ с уровнями: 11, 7, 3, -1, -5, -9, а длины 13: 13, 9, 5, 1, -3, -7, -11.

Для рассмотрения 3-го свойства надо ввести следующие понятия.

Периодическая КФ называется *одноуровневой*, если R(*l*), *l*≠0, принимает *одно и только одно значение*. Если R(*l*), *l*≠0, принимает *два различных значения*, то периодическая КФ называется *двухуровневой.* Аналогичным образом определяются многоуровневые КФ.

3. Необходимым условием получения одноуровневой КФ является

$$K^+(K^+-1)\equiv 0(mod(N-1)) \qquad (63)$$

То есть произведение $K^+(K^+-1)$ должно делиться без остатка на (N-1). Частное от деления и будет равно λ (целое число), которое входит в формулу (61):

$$\lambda=K^+(K^+-1)/(N-1) \qquad (64)$$

Решая совместно уравнения, можно определить число единиц в ПСП, при котором ее корреляционная функция будет одноуровневой с минимально возможными уровнями выбросов, определяемыми (61). Результаты расчетов, а также примеры приведены в табл.3.3.1.

В таблице приведено число единиц K^+ в ПСП, при котором *возможно* получение одноуровневых КФ с минимальными боковыми выбросами, определяемыми выражением (59). К сожалению, это только *необходимые* условия, и не все последовательности, приведенные в таблице в качестве примеров, будут иметь одноуровневые КФ.

Таблица 3.10

Длина N ПСП и число единиц K^+ в ней, необходимые для получения одноуроневой КФ с минимальным выбросом

R	N	K^+	Доп. усл.	Примеры (N, K^+)
-1	$4k+3$	$(N\pm1)/2$	k- любое	(7, 4), (7, 3), (11, 6), (11, 5), (19, 10), (19, 9), (23, 12), (23, 12)
1	$(k^2+1)/2$	$(k\pm1)^2/4=N(1\pm k)/2$	$k=1(mod\ 2)$	(13, 9), (13, 4), (25, 16), (25, 9), (41, 25),(41, 16), (61, 36), (61, 25), (85, 49), (85, 36), (145, 81), (145, 64), (181, 100), (181, 81)
0	$4k^2$	$k\ (2k\pm1)=N/2\pm k$	k-любое $k>0$	(4, 3), (4, 1), (16, 10), (16, 6), (36, 21), (36, 15), (64, 36), (64, 28), (100, 55), (100, 45)
2	$2(2k^2+1)/3$	$N/2\pm k$	$k\neq0(mod\ 3)$ $k>1$	(22, 15), (22, 17), (6, 1), (6, 1), (34, 22), (34, 21), (66, 40), (66, 26), (86, 59), (86, 27), (134, 77), (134, 57), (162, 103), (162, 59)

Достаточным условием получения одноуровневых КФ является существование разностного множества D(N, K^+, λ), при этом λ зависит от значений N и K^+ и определяется формулой (2.6). Разностное множество определяет номера позиций в ПСП, на которых стоят 1. Разностное множество D(N, K^+,λ) содержит числа от 1 до N-1 (всего K^+ чисел), такие, что разности между ними (по модулю N) принимают каждое из значений 1, 2,..., (N-1) ровно λ раз. Верно и обрат-

ное утверждение: если получена ПСП с одноуровневой КФ (не обязательно с минимальным значением R_{max} ()), то позиции единичных элементов составляют разностное множество $D(N,K^+,\lambda)$ при λ, удовлетворяющем условию (61).

Существуют также разностные множества, которые соответствуют ПСП с двухуровневыми КФ. Подробнее с известными разностными множествами можно познакомиться в работах [22,23].

Двоичные последовательности с минимальными боковыми выбросами КФ можно построить на основе конечных полей. К таким последовательностям относятся М-последовательности длины $N=2^m-1$, последовательности Лежандра, длина которых равна простому числу N=p. Длина М-последовательностей может быть представлена в виде $N=2^m-1=2^m-2^2+3=2^4(2^{2m-2-1})+3\equiv 3(mod\ 4)$ и в соответствии с (59) боковой выброс КФ может иметь значение -1. Последовательности Лежандра имеют длину $N\equiv 3(mod\ 4)$ либо $N\equiv 1(mod\ 4)$. В первом случае они также будут иметь одноуровневые КФ с $R(l)=-1$, $l\neq 0$. Во втором случае одноуровневой КФ получить нельзя, так как число 1 в последовательности Лежандра равно $K^+=(N\pm 1)/2$, то есть не соответствует числу K^+, приведенному в табл.1.7. В этом случае получаются двухуровневые КФ с выбросами 1 и -3, Причем половина боковых выбросов будет иметь уровень 1, а другая половина -3. Это следует из того, что при таких значениях числа K^+ расчеты по формуле (63) дадут значение λ, равное нецелому числу, дробная часть его равна 0,5. Поэтому половина значений может быть равна целой части числа, полученного по формуле (63), а половина - на 1 больше. На рис. 3.10 представлены корреляционные функции М-последовательности длины 15 (а), последовательностей Лежандра длины 11 и 13 (соответственно б и в).

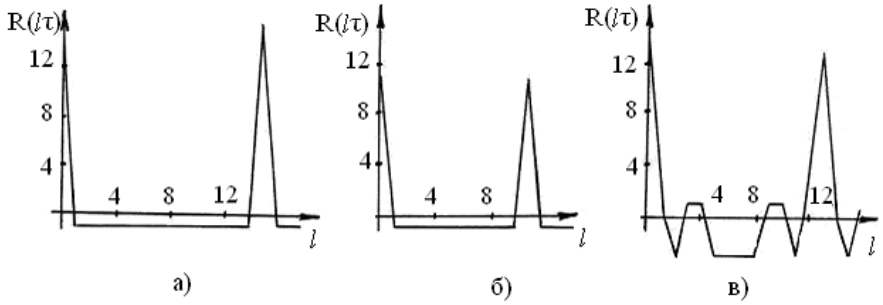


Рис. 3.10. Корреляционные функции М-последовательности длины 15 (а), последовательностей Лежандра длины 11 (б) и 13 (в)

3.3.2. Последовательности Лежандра

Эти последовательности называют последовательностями квадратичных вычетов. Число элементов в последовательности равно простому числу, они строятся на основе простого поля GF(p). Как было указано выше, все ненулевые элементы простого поля составляют мультипликативную группу и могут быть представлены как степени первообразного элемента θ. Для каждого простого p существует $\varphi(p-1)$ первообразных элементов.

В мультипликативной группе простого поля можно выделить подгруппу,

образующим элементом которой будет θ^2. Элементами этой подгруппы будут все четные степени первообразного элемента $\{ \theta^0, \theta^2, \theta^4, \theta^6,\ldots\}=\{\theta^{2k}\}$, k=0, 1, ...(p-3)/2.. Покажем, что $\{\theta^{2k}\}$ является подгруппой. Подгруппа должна обладать всеми свойствами группы: иметь единичный элемент (θ^0); каждый элемент должен иметь обратный, принадлежащий этой же подгруппе; на элементах подгруппы должна быть определена групповая операция (умножение). Покажем, что обратный к элементу θ^{2k} является квадратичным вычетом, то есть представляется четной степенью первообразного элемента θ: $\overline{\theta^{2k}} = \theta^{-2k} = \theta^{p-1-2k}$. Здесь учитывалось, что первообразный элемент имеет период (p-1) и θ^{p-1}. Значение (p-1-2k) всегда четно, так как (p-1) четно. Следовательно, $\overline{\theta^{2k}}$ - квадратичный вычет, то есть принадлежит подгруппе $\{\theta^{2k}\}$. Произведение любых элементов подгруппы дает элемент, принадлежащий подгруппе $\theta^{2k}\cdot\theta^{2l}=\theta^{2(k+l)}$, показатель степени 2($k$+$l$) всегда четен, поэтому $\theta^{2(k+l)}$ принадлежит подгруппе $\{\theta^{2k}\}$. Все нечетные степени первообразного элемента составляют смежный класс по подгруппе $\{\theta^{2k}\}$ с образующим элементом: каждый элемент смежного класса может быть получен умножением на θ элементов подгруппы $\{\theta^{2k}\}$.

Синтез последовательностей Лежандра сводится к гомоморфному отображению мультипликативной группы простого поля GF(p) в мультипликативную группу {-1, 1}. При этом отображении все элементы одного смежного класса переходят в один элемент. Схематично это можно представить следующим образом:

$\{\theta^{2k}\}\rightarrow 1$, $\{\theta^{2k+1}\}\rightarrow -1$.

Образом класса $\{\theta^{2k}\}$ является 1, а -1 – образом класса $\{\theta^{2k+1}\}$. Соответственно классы $\{\theta^{2k}\}$ и $\{\theta^{2k+1}\}$ являются прообразами элементов 1 и -1.

При гомоморфном отображении групп нулевой элемент поля не определен. Ему можно поставить в соответствие -1 или 1. Число элементов мультипликативной группы равно p-1 или через длину ПСП N-1. Следовательно, подгруппа квадратичных вычетов даст (N-1)/2 единичных элементов в ПСП. Если нулевому элементу поля GF(p) будет присвоена 1, то число единиц в ПСП увеличится на 1. Поэтому число единиц в последовательностях Лежандра, как было указано выше, определяется выражением

$$K^{+}=(N\pm 1)/2.$$

В дальнейшем элемент -1 будет обозначен 0.

Пример 2. Построить последовательность Лежандра для N=7. Последовательность Лежандра длины N=7 строим на основе простого конечного поля GF(7), первообразным элементом которого, как следует из табл.2.2, является θ=3. Представим ненулевые элементы этого поля, то есть его мультипликативную группу, степенями первообразного элемента: $1=3^0$, $2=3^2$, $3=3^1$, $4=3^4$, $5=3^5$, $6=3^3$. Напоминаем, что все операции в этом поле проводятся по модулю N=7. Квадратичными вычетами, то есть четными степенями первообразного элемента, являются элементы: $2=3^2$, $4=3^4$, $1=3^0$. Следовательно, 1, 2 и 4-й элементы ПСП будут представляться 1, а 3, 5 и 6-й -1, для простоты записи -1 заменим на

0. Нулевому элементу присваиваем 0. Получим последовательность 0110100. Если нулевому элементу присвоить 1, то получим ПСП 1110100. Обе полученные последовательности будут иметь одноуровневые КФ с выбросом -1.

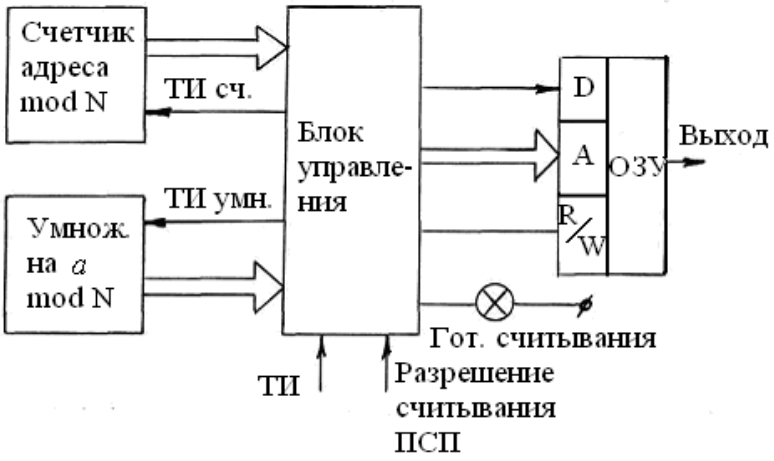


Рис. 3.11. Генератор последовательностей Лежандра

Подгруппу квадратичных вычетов $\{\theta^{2k}\}$ можно рассматривать как подгруппу с образующим элементом θ^{2k}. В качестве образующего элемента a этой подгруппы могут быть использованы любые четные степени первообразного элемента $a=\theta^t$, t – четно, но при условии, что наибольший общий делитель $(t,N-1)=2$. Тогда при использовании этих элементов в качестве образующих получим подгруппу периода (p-1)/2, то есть всю подгруппу квадратичных вычетов. Если среди четных степеней θ^t, $t\equiv 0$ (*mod* 2), найдется *хотя бы один элемент, а меньший* θ *или* θ^2*, то его целесообразно использовать в качестве образующего элемента мультипликативной подгруппы квадратичных вычетов*. Все единичные элементы, кроме, возможного, одного, который может занимать нулевую позицию, располагаются на позициях, номерами которых являются результаты вычисления по модулю N степеней этого образующего элемента.

Пример 3. Определить образующий элемент для подгруппы квадратичных вычетов GF(7). Первообразная элемента $\theta=3$ (табл.3.2.)

Воспользуемся результатами решения примера 2. Элементы 1, 2 и 4 составляют подгруппу квадратичных вычетов 2=32, 4=34, 1=30. Показатели степени элементов 2 и 4 (соответственно 2 и 4) будут иметь наибольший общий делитель с N-1=6, равный 2. Поэтому элементы 2 и 4 образуют подгруппу периода 3: $2^0=1$, $2^1=2$, $2^2=4$, $2^3=1$; $4^0=1$, $4^1=4$, $4^2=2$, $4^3=1$. Оба эти элемента могут быть выбраны в качестве образующего подгруппы квадратичных вычетов. Выбираем наименьший из них $a=2$.

По таблицам первообразных элементов и их степеней, приведенным в [9], найдены наименьшие образующие элементы подгруппы квадратичных вычетов, которые приведены в 3-м столбце табл.3.2 (p=N). Использование образующего элемента мультипликативной подгруппы квадратичных вычетов $a<\theta$ или θ^2 по-

зволяет построить довольно простое устройство формирования последовательностей Лежандра, которое должно содержать ОЗУ, устройство умножения на *a*, выход которого является адресом ячейки ОЗУ, в которую записывается 1. Схема устройства формирования последовательностей Лежандра представлена на рис.3.10.

Перед началом работы ОЗУ обнуляется (по нулевому адресу может быть записана «1»). Блок умножения на *a* по модулю N формирует адреса, которые соответствуют номерам единичных позиций в ПСП. По этим адресам в ОЗУ записываются 1. После записи (N-1)/2 единиц ОЗУ будет содержать последовательность Лежандра, При подаче сигнала разрешения считывания счетчик адресов формирует последовательные адреса считывания элементов ПСП из ОЗУ, и на выходе устройства формируется последовательность Лежандра.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Теория передачи сигналов / А.Г. Зюко, Д.Д. Кловский, М.В. Назаров, Л.М. Финк. - М.: Связь, 1980. 420 с.

2. Радиосистемы передачи информации/ И.М. Тепляков, Б.В. Рощин, А.И. Фомин, В.А. Вейцель. - М.: Радио и связь, 1982. 264 с.

3. Non-return-to-zero [Электронный ресурс]. Режим доступа: http://en.wikipedia.org / wiki/Non-return-to-zero(дата обращения 23.02.2021)

4. Воловодов А.А. От тактовой частоты до информационной магистрали [Электронный ресурс]. Режим доступа: http://www.ecolan.ru /imp_info/introduction/magest (дата обращения 23.02.2021)

5. Кодирование HDB3 и AMI [Электронный ресурс]. Режим доступа: http://wiki.metrotek.spb.ru/wiki/CV_HDB3 _&_AMI (дата обращения 23.02.2021)

6. Определение локальных сетей и их топология [Электронный ресурс]. Режим доступа: http://lib.znate.ru/docs/index-61151.html page=8 (дата обращения 23.02.2021)

7. Энциклопедия сетевых протоколов [Электронный ресурс]. Режим доступа: http://www.protocols.ru/modules. php?name=News&file=article&sid=73 (дата обращения 23.02. 2021)

8. Амплитудная манипуляция [Электронный ресурс]. Режим доступа: http://www.kipis.ru/info/index.php?ELEMENT_ ID=41016 (дата обращения 23.02.2021)

9. Финк Л.М. Теория передачи дискретных сообщений [Электронный ресурс]. Режим доступа: http://log-in.ru/books/ fink-l-m-teoriya-peredachi-diskretnykh-soobsheniiy-1-fink-l-m-tek hnicheskie (дата обращения 23.02.2021)

10. Анатомия беспроводных сетей [Электронный ресурс]. Режим доступа: http://compress.ru/article.aspx?id=11265& part=31ext1 (дата обращения 23.02.2021)

11. Варакин Л.Е. Теория систем сигналов/ Л.Е. Варакин. -М.: Сов. Радио, 1978. 303 с.

12. Радиосистемы передачи информации/ И.М. Тепляков, Б.В. Рощин, А.И. Фомин, В.А. Вейцель. / -М.: Радио и связь, 1982. 264 с.

13. Бессарабова А.А. Разделение каналов по форме в широкополосных системах передачи информации: учеб. пособие/ А.А. Бессарабова, В.Д. Бенедиктов./ Воронеж: ВПИ, 1984. 80 с.

14. Многоканальная система связи. Патент РФ № 2103827 (автор В.И.Ледовских).

15. Радиотехнические системы / Ю.Л. Гришин, В.П. Игнатов и др.; под ред. Ю.М. Казаринова. – М.: Высш. шк. , 1990.

16. Финк Л.М. Теория передачи дискретных сообщений./Л.М. Финк. – М.: Сов. Радио 1970.

17. Петрович Н.Т. Передача дискретной информации в каналах с фазовой манипуляцией./ Н.Т. Петрович. – М.: Сов. Радио 1965.

18. Кузьмин С.З. Цифровая обработка радиолокационной информации / С.З. Кузьмин. – М.: Сов. Радио, 1967.

19. Вентцель Е.С. Теория вероятностей / Е.С. Венцель. – М.: Физматгиз, 1962.

20. Пустыльник Е.И. Статистические методы анализа и обработки наблюдений / Е.И. Пустыльник. – М.: Физматгиз, 1968.

21. Бессарабова А.А., Системы передачи информации с кодовым разделением каналов: учеб. пособие. / А.А. Бессарабова, В.И. Ледовских / Воронеж. гос. техн. ун-т, 2006. 181 с.

22. Бессарабова А.А. Псевдослучайные двоичные последовательности: учеб. пособие / А.А. Бессарабова, В.И. Ледовских / Воронеж. гос. техн. ун-т, 2006. 129 с.

ПРИЛОЖЕНИЕ

Листинг программы статистического моделирования помехоустойчивости системы связи в среде Mathcad

$i := 0 \ldots 10 \quad v_i := 2 + 0.2 \cdot i$

Задание порогов решающего устройства v_i

$$PL_i := 0.5 \cdot \left(1 - erf\left(\frac{v_i}{\sqrt{2}}\right)\right)$$

Вероятности ложной тревоги при разных значениях v_i

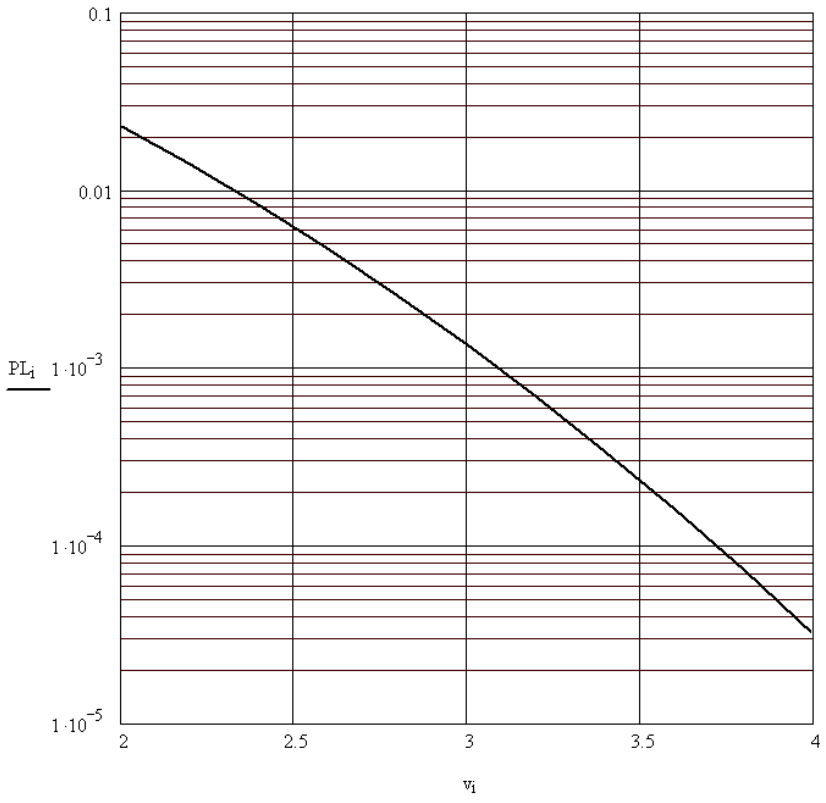


Рис. П1

$N := 10^5 \quad j := 0 \ldots 12 \quad q_i := 2 + 0.5 \cdot j$

Число испытаний и задание значений отношений с/ш

$x_j := rnorm(N, 0, 1) + q_j$

Задание вектора с разными элементами (векторами)

$y := (x > 3.7)$

Сравнение с порогом, равным 3.7

$n_j := \sum y_j$

Количество превышений порога в каждом элементе

$$PO_j := \frac{n_j}{N}$$

Вероятности правильного обнаружения для различных q_i

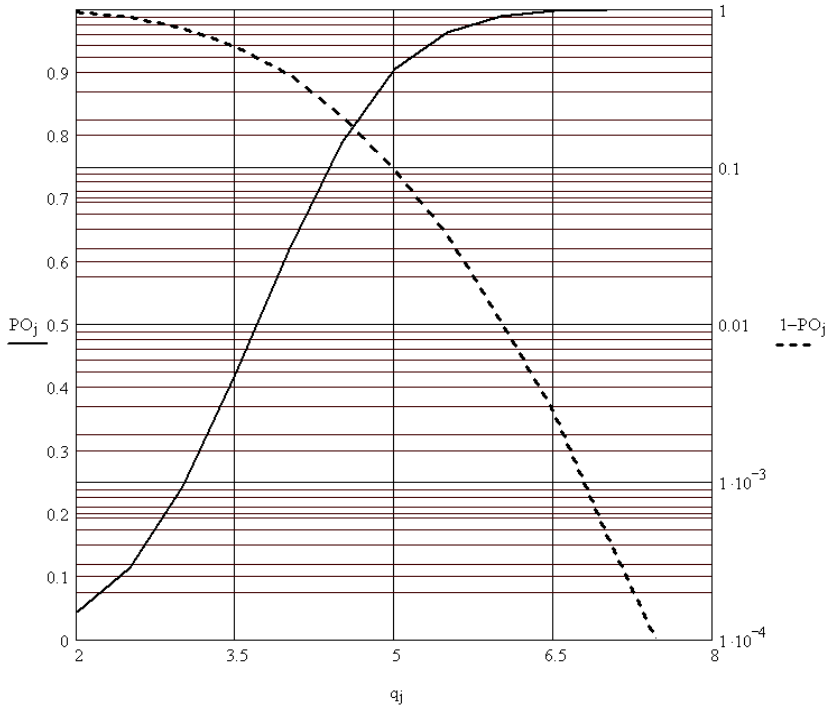


Рис. П2

ОГЛАВЛЕНИЕ

Учебное издание

Володько Александр Владиславович

СТАТИСТИЧЕСКАЯ ТЕОРИЯ СИСТЕМ

Практикум

В авторской редакции

Компьютерный набор А. В. Володько

Подписано к изданию 15.12.2021.
Объем данных 1,5 Мб.

ФГБОУ ВО «Воронежский государственный технический университет»
394006 Воронеж, ул. 20-летия Октября, 84