Оглавление

[Введение 2](#_Toc417254377)

[Анализ методов передачи данных. 5](#_Toc417254378)

[Исследование существующих методов исправления ошибок 5](#_Toc417254379)

[Коды Соломона Рида 5](#_Toc417254380)

[Коды Боуза—Чоудхури—Хоквингема (БЧХ-коды) 7](#_Toc417254381)

[Разработка архитектуры и реализация протокола передачи данных с исправлением данных. 10](#_Toc417254382)

[Модель p a 10](#_Toc417254383)

[Модель ОПП. 10](#_Toc417254384)

[Выбор алгоритма декодирования кодов БЧХ. 12](#_Toc417254385)

[Выбор алгоритма кодирования БЧХ кодов 13](#_Toc417254386)

[Анализ результатов. 14](#_Toc417254387)

# Введение

**Каналом передачи информации (каналом связи)** называют совокупность устройств, обеспечивающих передачу сигналов с определёнными свойствами с одного пункта к другому. При построении системы канал, как правило, является заданным звеном, с которым источники и получатели должны быть согласованы посредством передатчиков и приёмников.

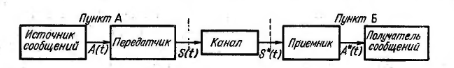


Рисунок Система передачи информации от одного источника к одному получателю по одному каналу

A(t) – сообщение поступающее от источника.

S(t) – сигнал полученный после преобразования сообщения A(t) передатчиком.

S\*(t) – сигнал полученный на выходе канала (выходной или принимаемый).

A\*(t) – сообщение преобразованное из сигнала S\*(t) приёмником.

Каналы связи характеризуются по различным признакам:

* По используемым линиям связи:
  + Кабельные;
  + Радиорелейные;
  + Тропосферные;
  + И др.
* По полосе частот сигнала в линии:
  + Тональные;
  + Высокочастотные;
  + Коротковолновые;
  + Световые;
  + И др.
* По техническому характеру сигналов и назначению систем связи:
  + Телефонные;
  + Звукового вещания;
  + Телевизионные;
  + Телеграфные;
  + Передачи цифровой информации;
  + И др.

При математическом описании каналы различают, в первую очередь, по типу множеств которым принадлежат входные и выходные сигналы (непрерывные и дискретные), и по характеру изменения этих сигналов во времени (каналы непрерывного и дискретного времени).

Среди непрерывных каналов непрерывного времени можно выделить два наиболее типичных:

1. Непосредственно линия связи, часто с усилительным или переприёмным (ретрансляционным) оборудованием. Такой канал входит в состав всех других каналов связи.
2. Отличается от первого наличием модуляционного и демодуляционного оборудования (часто многоступенного) и полосой пропускания. Примерами таких каналов могут служить телевизионные каналы, тракты систем высокочастотного телефонирования и т.п.

Дискретный канал чаще всего дискретен и по времени. Он состоит из непрерывного канала и подключенных к нему формирователя сигналов (дискретного модулятора) и решающего устройства. Последние и обуславливают дискретность множества входных и выходных элементарных сигналов. В идеальном случае эти два устройства действуют синхронно.

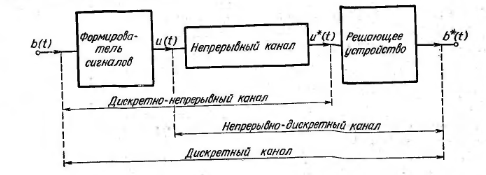


Рисунок Дискретный канал

Дискретный канал связи предназначен для передачи дискретных сигналов (символов). При передаче по такому каналу сообщение S(t) представляется некоторой последовательностью элементарных дискретных сообщений X(t), принадлежащих конечному множеству. В результате кодирования последовательность X(t) заменяется другой последовательностью Y(t), которая ставится в соответствие E(t). Последовательность Y(t) подаётся на вход дискретного канала.

Основной характеристикой дискретного канала является вероятность того или иного изменения символа на данной позиции. Эта характеристика определяется теми изменениями, которые претерпевает символ при передаче по каналу:

* Смещение во времени;
* Отличие на некоторых позициях выходных символов от входных(аддитивные ошибки);
* Смещение номеров позиций выходной последовательности символов от позиций входной последовательности символов (ошибки синхронизации);
* Появление на некоторых ошибках символов стирания.

При действии рассмотренных факторов основная характеристика дискретного канала зависит от номера позиции, от значения, передаваемого и всех ранее переданных символов.

Поток ошибок представляет собой дискретный случайный процесс E. Каждая позиция E по определённому правилу складывается соответствующей позицией Y (сообщение на выходе).

Представляется логичным и достаточно удобным рассматривать поток ошибок дискретного канала связи как ступенчатый случайный процесс. Такой подход позволяет при исследовании каналов связи использовать многочисленные важные результаты, полученные для случайных процессов.

# Анализ методов передачи данных.

## Исследование существующих методов исправления ошибок

### Коды Соломона Рида

**Коды Рида — Соломона**  — недвоичные циклические коды, позволяющие исправлять ошибки в блоках данных. Элементами кодового вектора являются не биты, а группы битов (блоки).

Коды Рида — Соломона являются важным частным случаем БЧХ-кода, корни порождающего полинома которого лежат в том же поле, над которым строится код (m=1). Пусть \alpha — элемент поля \textstyle GF(q) порядка \textstyle n. Если \alpha —*примитивный* элемент, то его порядок равен q-1, то есть \alpha^{q-1}=1,\quad \alpha^i \neq 1, 0<i<q-1. Тогда нормированный полином g(x) минимальной степени над полем \textstyle GF(q), корнями которого являются d-1 подряд идущих степеней \alpha^{l_0}, \alpha^{l_0+1},...,\alpha^{l_0+d-2} элемента \alpha, является порождающим полиномом кода Рида — Соломона над полем \textstyle GF(q):

g(x) = (x - \alpha^{l_0})(x - \alpha^{l_0+1})\dots(x - \alpha^{l_0+d-2})

где l_0 — некоторое целое число (в том числе 0 и 1), с помощью которого иногда удается упростить кодер. Обычно полагается l_0 = 1. Степень многочлена \textstyle g(x) равна d-1.

Длина полученного кода n, минимальное расстояние d (минимальное расстояние d линейного кода является минимальным из всех расстояний Хемминга всех пар кодовых слов, см. Линейный код). Код содержит r=d-1=\deg (g(x)) проверочных символов, где \deg() обозначает степень полинома; число информационных символов k = n - r = n - d + 1. Таким образом \textstyle d = n - k + 1 и код Рида — Соломона является *разделимым кодом с максимальным расстоянием* (является оптимальным в смысле границы Синглтона).

Кодовый полином c(x) может быть получен из информационного полинома m(x), \deg m(x) \leqslant k-1, путем перемножения m(x) и g(x):

c(x) = m(x)g(x)

Код Рида — Соломона является одним из наиболее мощных кодов, исправляющих многократные пакеты ошибок. Применяется в каналах, где пакеты ошибок могут образовываться столь часто, что их уже нельзя исправлять с помощью кодов, исправляющих одиночные ошибки.

(q^m - 1,  q^m -2 - 2t)-код Рида — Соломона над полем \textstyle GF(q^m) с кодовым расстоянием d = 2t + 1 можно рассматривать как ((q^m - 1)m,(q^m -1 - 2t)m)-код над полем \textstyle GF(q), который может исправлять любую комбинацию ошибок, сосредоточенную в t или меньшем числе блоков из m символов. Наибольшее число блоков длины m, которые может затронуть пакет длины l_i, где l_i \leqslant mt_i - (m-1), не превосходит t_i, поэтому код, который может исправить t блоков ошибок, всегда может исправить и любую комбинацию из p пакетов общей длины l, если l+(m-1) \leqslant mt.

При несистематическом кодировании информационное слово умножается на некий неприводимый полином в поле Галуа. Полученное закодированное слово полностью отличается от исходного и для извлечения информационного слова нужно выполнить операцию декодирования и уже потом можно проверить данные на содержание ошибок. Такое кодирование требует большие затраты ресурсов только на извлечение информационных данных, при этом они могут быть без ошибок.

При систематическом кодировании к информационному блоку из k символов приписываются 2t проверочных символов, при вычислении каждого проверочного символа используются все k символов исходного блока. В этом случае нет затрат ресурсов при извлечении исходного блока, если информационное слово не содержит ошибок, но кодировщик/декодировщик должен выполнить k(n - k) операций сложения и умножения для генерации проверочных символов. Кроме того, так как все операции проводятся в поле Галуа, то сами операции кодирования/декодирования требуют много ресурсов и времени. Быстрый алгоритм декодирования, основанный на быстром преобразовании Фурье, выполняется за время порядка  O({ln( {n}) }^2).

При операции кодирования информационный полином умножается на порождающий многочлен. Умножение исходного слова S длины k на неприводимый полином при систематическом кодировании можно выполнить следующим образом:

* К исходному слову приписываются 2t нулей, получается полином \textstyle T = S x^{2t}.
* Этот полином делится на порождающий полином G, находится остаток R, \textstyle S x^{2t} = Q G + R, где Q — частное.
* Этот остаток и будет корректирующим кодом Рида — Соломона, он приписывается к исходному блоку символов. Полученное кодовое слово \textstyle C = S x^{2t} + R.

Кодировщик строится из сдвиговых регистров, сумматоров и умножителей. Сдвиговый регистр состоит из ячеек памяти, в каждой из которых находится один элемент поля Галуа.

Существует и другая **процедура** кодирования (более практичная и простая). Положим  a_{i} \in GF(q) , (i = 1,2,\ldots,k-1) , \alpha \in GF(q) - примитивный элемент поля GF(q), и пусть 
a = (a_0,a_1,\ldots,a_{k-1})
 - вектор информационных символов , а значит a(x) = a_0 + a_{1}x + \ldots + a_{k-1}x^{k-1} - информационный многочлен. Тогда вектор u = (a(1),a(\alpha),\ldots,a(\alpha^{q-2})) есть вектор кода Рида - Соломона , соответствующий информационному вектору a. Этот способ кодирования показывает , что для кода РС вообще не нужно знать порождающего многочлена и порождающей матрицы коды, достаточно знать разложение поля GF(q)по примитивному элементу \alpha и размерность кода k (длина кода в этом случае определяется как n = q - 1). Все дело в том, что за разностью n-k полностью скрывается порождающий многочлен g(x) и кодовое расстояние.

Декодировщик, работающий по авторегрессивному спектральному методу декодирования, последовательно выполняет следующие действия:

* Вычисляет синдром ошибки
* Строит полином ошибки
* Находит корни данного полинома
* Определяет характер ошибки
* Исправляет ошибки

### Коды Боуза—Чоудхури—Хоквингема (БЧХ-коды)

  БЧХ-код является циклическим кодом, который задается порождающим полиномом. Для его нахождения в случае БЧХ-кода необходимо заранее определить длину кода n  и требуемое минимальное расстояние d \leqslant n. Найти порождающий полином можно следующим образом.

Пусть ~\alpha — примитивный элемент поля ~GF(q^m) (то есть \alpha^{q^m-1}=1, \alpha^i \neq 1, i< q^m-1), пусть ~\beta=\alpha^s , — элемент поля ~GF(q^m) порядка ~n, \quad s = (q^m-1) / n . Тогда нормированный полином g(x) минимальной степени над полем GF(q), корнями которого являются ~d-1 подряд идущих степеней ~\beta^{l_0}, \beta^{l_0+1},\ldots,\beta^{l_0+d-2}элемента ~\beta для некоторого целого ~l_0 (в том числе 0 и 1), является порождающим полиномом БЧХ-кода над полем ~GF(q) с длиной n и минимальный расстоянием ~d_0 \geqslant d. Поясним почему у получившегося кода будут именно такие характеристики (длина кода ~n , минимальное расстояние ~d_0). Действительно, как показано в [1] , длина БЧХ кода равна порядку элемента ~\beta, если ~d>2 и равна порядку элемента ~\beta^{l_0}, если ~d=2, тогда, так как случай ~d=2нам не интересен (такой код не может исправлять ошибки, только обнаруживать), то длина кода будет равна порядку элемента ~\beta ,то есть равна ~n. Минимальное расстояние ~d_0 может быть больше ~d, когда корнями минимальных функций(стр.83[2]) от элементов ~\beta^{l_0}, \beta^{l_0+1},\ldots,\beta^{l_0+d-2} будут элементы расширяющие последовательность, то есть элементы ~\beta^{l_0+d-1},\beta^{l_0+d},\ldots,\beta^{l_0+d_0 - 2}.

Число проверочных символов r равно степени g(x), число информационных символов k=n-r, величина dназывается *конструктивным расстоянием* БЧХ-кода. Если n=q^m-1, то код называется *примитивным*, иначе *не примитивным*.

Так же, как и для циклического кода, кодовый полином c(x) может быть получен из информационного полинома m(x), степени не больше k-1, путём перемножения m(x) и g(x):

c(x)=m(x)g(x).

Для нахождения порождающего полинома необходимо выполнить несколько этапов:

* выбрать q, то есть поле GF(q), над которым будет построен код;
* выбрать длину n кода из условия n=(q^m-1)/s, где m,s — целые положительные числа;
* задать величину d конструктивного расстояния;

1) построить циклотомические классы элемента \beta=\alpha^s поля GF(q^m) над полем GF(q), где \alpha — примитивный элемент GF(q^m);

2) поскольку каждому такому циклотомическому классу соответствует неприводимый полином над GF(q), корнями которого являются элементы этого и только этого класса, со степенью равной количеству элементов в классе, то выбрать \beta^{l_0}, \beta^{l_0+1},\ldots, \beta^{l_0+d-2} таким образом, чтобы суммарная длина циклотомических классов была минимальна; это делается для того, чтобы при заданных характеристиках кода ~n и ~d минимизировать количество проверочных символов ~k;

3) вычислить порождающий полином g(x)=f_1(x)f_2(x)\ldots f_h(x), где f_i(x) — полином, соответствующий i-ому циклотомическому классу; или вычислить g(x), как НОК минимальных функций от элементов \beta^{l_0}, \beta^{l_0+1},\ldots,\beta^{l_0+d-2} .

При несистематическом кодировании кодовое слово получается в виде произведения информационного полинома на порождающий

c(x)=m(x)g(x).

Оно может быть реализовано при помощи перемножения полиномов.

При систематическом кодировании кодовое слово формируется в виде информационного подблока и проверочного c(x) = [s(x)\;m(x)]

Пусть информационное слово образует старшие степени кодового слова, тогда

c(x)=x^rm(x) + s(x),r=n-k

Тогда из условия c(x)=x^rm(x) + s(x)=0\mod g(x), следует

s(x)=-x^r m(x)\mod g(x)

Главной идеей в декодировании БЧХ кодов является использование элементов конечного поля для нумерации позиций кодового слова (или, эквивалентно, в порядке коэффициентов ассоциированного многочлена).

Основные методы декодирования кодов БЧХ:

* **Евклидов алгоритм** (ЕА). Из-за высокой регулярности структуры этого алгоритма его широко используют для аппаратной реализации декодеров БЧХ и кодов Рида-Соломона.

В основе этого метода лежит широко известный алгоритм Евклида по нахождению наибольшего общего делителя двух чисел (НОД), только в данном случае ищем НОК не двух чисел, а двух полиномов.

**Прямое решение** (алгоритм Питерсона — Горенстейна — Цирлера, ПГЦ). Исторически это первый метод декодирования, найденный Питерсоном для двоичного случая (q=2), затем Горенстейном и Цирлером для общего случая. Этот алгоритм находит коэффициенты *многочлена локаторов ошибок* прямым решением соответствующей системы линейных уравнений. В действительности, так как сложность этого алгоритма растет как куб минимального расстояния ~d, прямой алгоритм может быть использован только для малых значений ~d.

* **Алгоритм Берлекемпа-Мэсси** (BMA). Алгоритм поиска кратчайшего регистра сдвига с линейной обратной связью для поданной на вход бинарной последовательности. Также алгоритм позволяет найти минимальный многочлен поданной на вход линейной рекуррентной последовательности над произвольным полем.

# Разработка архитектуры и реализация протокола передачи данных с исправлением данных.

## Модель p a

Основным понятием, положенным в основу данной модели является плотность ошибка порядка t. Это неслучайная функция от n и t , где - среднее число ошибок на блоке длинной n с t или большим количеством ошибок. Значение плотности порядка t подчиняется следующему условию . Значения функции v(t,n) не убывают с ростом t, то есть

, если выполняются условия больше p хотя бы в несколько раз. Параметр носит название показателя группирования ошибок, подчиняется условию . При получаем канал с независимыми ошибками, а при получаем канал с “жестким” пакетированием ошибок.

На практике применяют данное соотношение для задания модели (p, a). Параметр p – характеризует вероятность ошибки символа и рассчитывается по формуле ФОРМУЛА. Параметр а – находят из уравнения .

Достоинством применение данной модели для исследования каналов связи является то, что учитывается пакетирования ошибок, возможность единообразно описать разные типы каналов передачи данных. Так для кабельных каналов значение максимально (>0.5), а для радиоканалов применяют значение в промежутке от 0.3 до 0.45. У данного способа моделирования каналов связи есть недостаток, заключающийся в неполноте и вопрос модели на уровне блоков.

## Модель ОПП.

Наблюдаемое пакетирование ошибок в каналах связи при предположении о пуассоновском характере потока можно объяснить, если считать параметр  не константой, а случайной величиной или процессом. Получающийся путем рандомизации  новый случайный процесс называют обобщенным пуассоновским . Будем считать  случайной величиной, закон распределения которой известен . Тогда канал задается как поток ошибок первым способом:



Поскольку вид и параметры закона распределения для реальных каналов обычно неизвестны, указанной выше формулой воспользоваться не удается.

По экспериментальным данным относительно легко можно найти закон распределения интервалов между ошибками – функцию Пальма-Хинчина , которая полностью определяет ОПП (второй способ здания потока).

Справедлива формула:

,

где - параметр потока,

 и 

 - вероятность отсутствия ошибок за время .

Таким образом, для ОПП, зная функцию распределения интервалов между ошибками или , вычисляются вероятности , т.е. приходим к конструктивному заданию потока первым способом.

Для моделирования будем считать распределение интервалов заданное обобщенной гиперболой:

, .

Исследование записей потоков ошибок в телефонных каналах показало, что такая ситуация наблюдается довольно часто.

Тогда для параметра потока тогда получается

.

 и

.

Для расчетов вероятностей наиболее удобна рекуррентная формула:

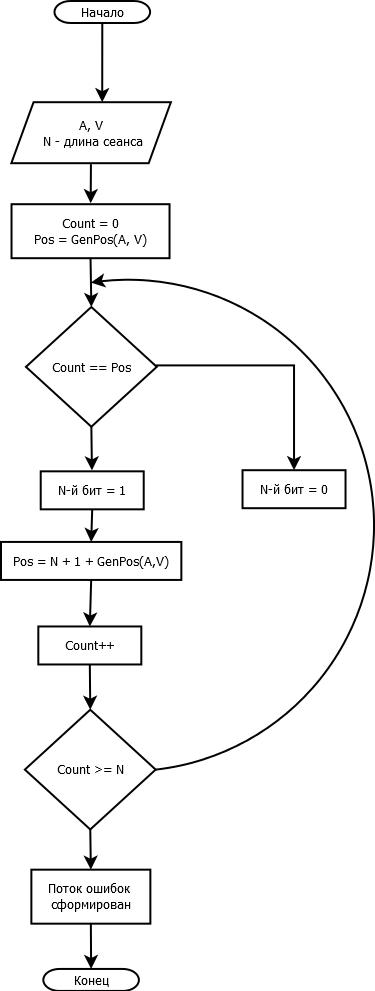


.

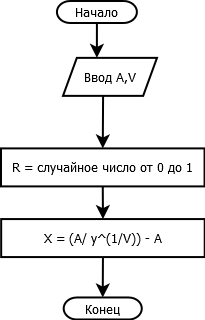
Неизвестные параметры  и  легко находятся, например, методом моментов, поскольку обобщенная гипербола для интервалов между ошибками приводит к гамма-распределению параметра .

К недостаткам этой модели можно отнести более трудоемкие формулы для расчета, чем у модели ДСК и тот факт, что не все каналы имеют обобщенную гиперболу в качестве закона распределения между ошибочных интервалов.

Генерация потока ошибок для модели на основе ОПП осуществляется по следующему алгоритму:



**Рисунок . Алгоритм генерации потока ошибок**

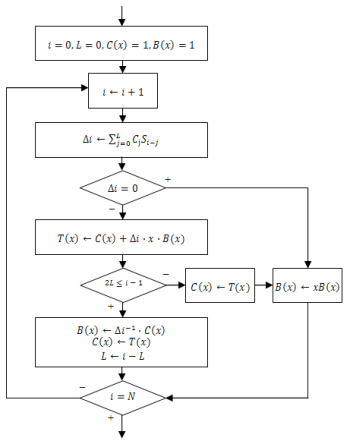


**Рисунок . Алгоритм функции генерации позиции ошибки в потоке битов.**

## Выбор алгоритма декодирования кодов БЧХ.

Из существующих методов декодирования кодов БЧХ был выбран ВМА. По числу операций в конечном поле этот алгоритм обладает высокой эффективностью.

* Задать требуемую последовательность битов ~s_0, s_1, ..., s_{n-1}.
* Создать массивы ~b, ~t, ~c длины ~n, задать начальные значения b_0 \leftarrow 1, c_0 \leftarrow 1, N \leftarrow 0, L \leftarrow 0, m \leftarrow -1.
* Пока ~N < n:
  1. Вычислить d \leftarrow s_N \oplus c_1s_{N-1} \oplus c_2s_{N-2} \oplus ... \oplus c_Ls_{N-L}.
  2. Если ~d=0, то текущая функция генерирует выбранный участок ~s_{N-L}, s_{N-L+1}, ..., s_N последовательности; оставить функцию прежней.
  3. Если ~d \not = 0:
     + Сохранить копию массива ~c в ~t.
     + Вычислить новые значения ~c_{N-m} \leftarrow c_{N-m} \oplus b_0, c_{N-m+1} \leftarrow c_{N-m+1} \oplus b_1, ..., c_{n-1} \leftarrow c_{n-1} \oplus b_{n-N+m-1}.
     + Если 2L \leqslant N, установить значения L \leftarrow N+1-L, m \leftarrow N и скопировать ~t в ~b.
  4. N \leftarrow N+1.
* В результате массив ~c — функция обратной связи, то есть c_Ls_i \oplus c_{L-1}s_{i+1} \oplus c_{L-2}s_{i+2} \oplus ... \oplus c_0s_{i+L} = 0 для любых ~i.



**Рисунок . Блок-схема алгоритма Берлекэмпа — Мэсси**

## Выбор алгоритма кодирования БЧХ кодов

Для реализации кодирования было выбрано несистематическое кодирование. Данный метод кодирования позволяет реализовать модель наиболее простым способом.

# Анализ результатов.