

Лекция 2+. Контроль достоверности передачи

(Коды ЕСС)

Контроль достоверности передачи

Для повышения достоверности и качества передачи применяются:

- групповые методы защиты от ошибок,
- избыточное кодирование ,
- системы с обратной связью.

Из групповых методов получили широкое применение:

- мажоритарный метод, реализующий принцип Вердана,
- метод передач информационными блоками с количественной характеристикой блока.

Суть *мажоритарного метода* состоит в том, что каждое сообщение ограниченной длины передается несколько раз (чаще всего три раза), принимаемые сообщения запоминаются, а потом производится их поразрядное сравнение. Суждение о правильности передачи выносится по совпадению большинства из принятой информации методом «два из трех».

Например, кодовая комбинация 01101 при трехразовой передаче была частично искажена помехами, поэтому приемник принял такие комбинации: 10101, 01110, 01001.

В результате проверки по отдельности каждой позиции правильной считается комбинация 01101.

Контроль достоверности передачи

Существует три наиболее распространенных орудия борьбы с ошибками в процессе передачи данных:

- коды обнаружения ошибок (ECC);
- коды с коррекцией ошибок, называемые также схемами прямой коррекции ошибок (Forward Error Correction - FEC);
- протоколы с автоматическим запросом повторной передачи (Automatic Repeat Request - ARQ).

Рассмотрим основные механизмы обеспечения целостности передаваемой информации с помощью введения избыточности.



ECC (коды обнаружения ошибок);

- код Хэмминга,
- код Рида-Соломона.

FEC (Forward Error Correction - *прямая коррекция ошибок*) -

заблаговременное исправление ошибок, коррекция ошибок путем передачи избыточной информации, без требования повторной передачи.

FEC(*Forward Error Correction* -) — техника кодирования/декодирования, позволяющая исправлять ошибки методом упреждения. Применяется для исправления сбоев и ошибок при передаче данных путём передачи избыточной служебной информации, на основе которой может быть восстановлена первоначальное содержание посылки.

Передача блоками с количественной характеристикой

Передача блоками с количественной характеристикой предполагает передачу данных блоками с количественной характеристикой блока.

Таковыми характеристиками могут быть:


- число единиц или нулей в блоке,
- контрольная сумма передаваемых символов в блоке,
- остаток от деления контрольной суммы на постоянную величину и др.

На приемном пункте эта характеристика вновь подсчитывается и сравнивается с переданной по каналу связи. Если характеристики совпадают, считается, что блок не содержит ошибок. В противном случае на передающую сторону поступает сигнал с требованием повторной передачи блока. В современных телекоммуникационных вычислительных сетях такой метод получил самое широкое распространение.

Помехоустойчивое (избыточное) кодирование предполагает разработку и использование корректирующих (помехоустойчивых) кодов. Он применяется не только в телекоммуникационных сетях, но и в ЭВМ для защиты от ошибок при передаче информации между устройствами машины. Помехоустойчивое кодирование позволяет получить более высокие качественные показатели работы систем связи. Его основное назначение заключается в обеспечении малой вероятности искажений передаваемой информации, несмотря на присутствие помех или сбоев в работе сети.

К числу наиболее важных показателей корректирующих кодов относятся:

- *значность* кода n , или длина кодовой комбинации, включающей информационные символы (m) и проверочные, или контрольные, символы (k): $n = m + k$ (значения контрольных символов при кодировании определяются путем контроля на четность количества единиц в информационных разрядах кодовой комбинации. Значение контрольного символа равно 0, если количество единиц будет четным, и равно 1 при нечетном количестве единиц);
- *избыточность* кода ($K_{изб}$), выражаемая отношением числа контрольных символов в кодовой комбинации к значности кода: $K_{изб} = k / n$;
- *корректирующая способность* кода ($K_{кк}$), представляющая собой отношение числа кодовых комбинаций L , в которых ошибки были обнаружены и исправлены, к общему числу переданных кодовых комбинаций M в фиксированном объеме информации: $K_{кк} = L / M$.



Выбор корректирующего кода для его использования в данной компьютерной сети зависит от требований по достоверности передачи информации. Для правильного выбора кода необходимы статистические данные о закономерностях появления ошибок, их характере, численности и распределении во времени. Например, корректирующий код, обнаруживающий и исправляющий одиночные ошибки, эффективен лишь при условии, что ошибки статистически независимы, а вероятность их появления не превышает некоторой величины. Он оказывается непригодным, если ошибки появляются группами. При выборе кода надо стремиться, чтобы он имел меньшую избыточность. Чем больше коэффициент $K_{\text{изб}}$, тем менее эффективно используется пропускная способность канала связи и больше затрачивается времени на передачу информации, но зато выше помехоустойчивость системы.

Коррекция ошибок (код исправления ошибок).


(Error Correcting Code – ECC)

Этот метод включает определение ошибки не только в одиночном разряде, но и двух, трех и четырех разрядах. Кроме того, ЕСС может также исправлять ошибку в одиночном разряде.

Во время считывания результат ЕСС-слова сравнивается с рассчитанным, подобно тому, как происходит в описанных выше методах проверки контрольных сумм. Основное различие состоит в том, что в проверке четности каждый бит связан с одним байтом, в то время как ЕСС-слово связано с совокупностью байт. Если четность корректна, то для всех групп, то это свидетельствует об отсутствии ошибок. Если одна одно или более значение четности для переданного блока не верно, генерируется уникальный код, называемый синдромом, по которому можно идентифицировать переданный с ошибкой бит.

Виды ЕСС:

- код Хэмминга,
- код Рида-Соломона




Введем основные понятия из области корректирующих кодов.

Количество единиц в двоичной кодовой комбинации называется ее кодовым весом W . Например, если $X = 1,1010_2$, то $W = 3$.

Количество разрядов d , в которых не совпадают двоичные цифры в двух кодовых комбинациях, называется расстоянием между этими комбинациями. Оно обычно определяется методом поразрядного сложения по модулю два (исключающее ИЛИ) с последующим вычислением веса суммы:

$$X_1 = 1,010, \quad X_2 = 0,1011, \quad C = X_1 \oplus X_2 = 1,001, \quad W = 2, \quad d = 2.$$

Минимальным кодовым расстоянием d_{min} называется самое малое кодовое расстояние, возможное между двумя любыми кодовыми комбинациями из рассматриваемых множеств. В обычном двоичном коде n -разрядных чисел возможны кодовые расстояния от 1 до n , т. е. здесь $d_{min} = 1$.



В общем случае, когда в кодовой комбинации могут появляться ошибки любой кратности $i \leq n$ (одиночная, двойная, тройная и т. д.), для обнаружения некоторой ошибки требуется корректирующий код с минимальным расстоянием $d_{min} = i + 1$.

Следовательно, обнаружение одиночной ошибки можно обеспечить ценой минимальной избыточности – добавлением к слову всего одного контрольного разряда (контроль четности). Возникновение одиночной ошибки (или же ошибки с нечетным изменением количества разрядов) приводит к нарушению нечетности веса всей комбинации.

Таким образом, избыточность кодовой комбинации на один разряд позволяет обнаруживать все нечетные групповые ошибки и, как частный случай, одиночную ошибку.


Идея (двоичного) кода с **исправлением одиночной ошибки** состоит в следующем. Пусть исходный (незащищенный) код имеет m двоичных разрядов. Выберем $n > m$ так, чтобы

$$\frac{2^n}{n+1} \geq 2^m$$

- . Полученный защищенный код будет иметь $k = n - m$ контрольных разрядов, причем


$$2^k \geq m + k + 1 = n + 1$$

- . Каждому из n разрядов присваивается номер от 1 до n . Далее для любого значения защищенного (n -разрядного) кода составляется k контрольных сумм S_1, S_2, \dots, S_k по модулю 2 значений специально выбранных разрядов этого кода. Для S_i выбираются разряды, для которых двоичные коды номеров имеют в i -м разряде единицу. Для суммы S_1 это будут, очевидно, разряды с номерами 1, 3, 5, 7, ..., для суммы S_2 – разряды с номерами 2, 3, 6, 7, 10, 11, ... и т. д.



При любом исходном коде контрольные разряды могут быть выбраны так, чтобы все контрольные суммы были равны нулю. Проверочный (двоичный) код $S = S_k \dots S_1$ при этом будет нулевым. При таком условии защищенный код называется *правильным*. При возникновении одиночной ошибки в этом коде в любом (безразлично, основном или контрольном) разряде проверочный код будет отличен от нуля. При этом в силу способа выбора контрольных сумм значение проверочного кода S будет представлять собой двоичный код номера разряда защищенного кода, в котором возникла ошибка. Для исправления этой ошибки достаточно изменить значение указанного разряда на противоположное.

Примером корректирующих кодов являются код Хемминга и код Рида-Соломона.



Код, в котором в качестве контрольных берут разряды $1, 2, 4, \dots, 2^n$, называется *кодом Хемминга*. Код Хемминга может либо исправлять одиночные ошибки (при гипотезе, что ошибки более высокой кратности невозможны), либо обнаруживать любые ошибки, не кратные трем. Тройные ошибки считаются маловероятными, и поэтому иногда говорят, что *код Хэмминга позволяет обнаруживать одиночные и двойные ошибки*.

Покажем на примере, как ликвидируется одиночная ошибка с помощью кода Хемминга при передаче четырехразрядного двоичного слова $X = 0110$ ($m = 4$).

Построение кода выполняется в три этапа:

1а Вычислим необходимый размер (n) разрядной сетки защищенного слова и количество контрольных разрядов (k). Минимальное значение n , при котором выполняется неравенство

$$\frac{2^n}{n+1} \geq 2^m = 2^8$$

равно 7, $k = 7 - 4 = 3$.

2 Определим номера контрольных разрядов в защищенном слове: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$.

3 Построим защищенное слово в 7-разрядной сетке. Для этого запишем исходное слово в порядке следования его разрядов, пропуская места контрольных разрядов:

1	2	3	4	5	6	7
001	010	011	100	101	110	100
		0		1	1	0

Определим значения защищенных разрядов исходя из равенства сумм S_i нулю. В сумму S_1 должны войти значения разрядов, расположенных на нечетных местах $(1, 3, 5, 7) = (001, 011, 101, 111)$, Чтобы сумма S_1 была равна нулю, входящий в нее 1-й контрольный разряд должен быть равен 1,

Аналогично отыскиваются и другие контрольные разряды.

В S_2 войдут разряды $(2, 3, 6, 7) = (010, 011, 110, 111)$,

В S_3 войдут разряды $(4, 5, 6, 7) = (100, 101, 110, 111)$,

По результатам вычисления контрольных разрядов и значениям разрядов передаваемого слова строим защищенное слово:

1	1	0	0	1	1	0
---	---	---	---	---	---	---

В месте приема переданного слова снова вычисляются контрольные суммы S_1 , S_2 , S_3 , но уже при известных значениях заштрихованных контрольных разрядов. При равенстве всех сумм нулю считается, что передача произошла правильно. Предположим, что в процессе передачи произошло искажение только одного разряда (не важно какого: контрольного или основного). Например, предположим, что неправильно передан 6-й разряд. Это означает, что вместо 1 в 6-й разряде появился 0. Тогда после вычисления контрольных сумм получим: $S_1 = 0$, $S_2 = 1$, $S_3 = 1$. Располагаем эти суммы в порядке убывания их номеров и получаем $S = S_1 S_2 S_3 = 011$. Это двоичное число соответствует номеру 6. Тогда можно автоматически исправить ошибку в 6-м разряде, заменив пришедший 0 на 1. После исправления ошибки контрольные биты отбрасываются.

Код Хемминга

В коде Хемминга вводится понятие *кодového расстояния* d (расстояния между двумя кодами), равного числу разрядов с неодинаковыми значениями. Возможности исправления ошибок связаны с минимальным кодовым расстоянием d_{min} . Исправляются ошибки кратности $r = \lfloor (d_{min}-1)/2 \rfloor$ и обнаруживаются ошибки кратности $d_{min}-1$ (здесь $\lfloor \rfloor$ означает “целая часть”). Так, при контроле на нечетность $d_{min} = 2$ и обнаруживаются одиночные ошибки. В коде Хемминга $d_{min} = 3$. Дополнительно к информационным разрядам вводится $L = \log_2 K$ избыточных контролирующих разрядов, где K - число информационных разрядов, L округляется до ближайшего большего целого значения. L -разрядный контролирующий код есть инвертированный результат поразрядного сложения (т.е. сложения по модулю 2) номеров тех информационных разрядов, значения которых равны 1.

Определяется четность или нечетность целого блока символов. Каждый бит четности вычисляется для определенной комбинации бит данных.

Коррекция ошибок (код исправления ошибок).

Пример 1. Пусть имеем основной код 100110, т.е. $K = 6$. Следовательно, $L = 3$ и дополнительный код равен $010 \# 011 \# 110 = 111$, где $\#$ - символ операции поразрядного сложения, и после инвертирования имеем 000. Теперь вместе с основным кодом будет передан и дополнительный. На приемном конце вновь рассчитывается дополнительный код и сравнивается с переданным. Фиксируется код сравнения (поразрядная операция отрицания равнозначности), и если он отличен от нуля, то его значение есть номер ошибочно принятого разряда основного кода. Так, если принят код 100010, то рассчитанный в приемнике дополнительный код равен инверсии от $010 \# 110 = 100$, т.е. 011, что означает ошибку в 3-м разряде.


Коды Рида-Соломона

Коды Рида – Соломона позволяют исправлять ошибки в блоках данных. Элементами кодового вектора являются не биты, а группы битов (блоки, в частности, байты)ю

Кодирование информационного блока может быть выполнено разными способами, при этом исходный блок будет либо дополнен некоторым проверочным блоком, либо перекодирован, из которого затем получаются полученный информационный и проверочный блоки.

Декодировщик последовательно вычисляет синдромы ошибок, строит соответствующий полином ошибок и находит корни данного полинома (они определяют положение искаженных символов в кодовом слове), по которым определяет характер ошибок и исправляет их.

Устранение ошибок с помощью корректирующих кодов (такое управление называют Forward Error Control) реализуют в симплексных каналах связи. В дуплексных каналах достаточно применения кодов, обнаруживающих ошибки (Feedback or Backward Error Control), так как сигнализация об ошибке вызывает повторную передачу от источника. Это основные методы, используемые в информационных сетях.



В кодах Рида-Соломона сообщение представляется в виде набора символов некоторого алфавита, в качестве которого используются элементы поля Галуа. *Поле Галуа* является конечным полем (обычно обозначается $GF(N)$, где N – размерность поля, равная количеству его элементов). Арифметические действия над элементами конечного поля дают результат, который также является элементом этого поля.

Количество чисел в поле должно являться простым числом в любой натуральной степени, однако в случае простых кодов Рида-Соломона размерность поля – простое число в степени 1. Например, для поля Галуа размерности 7, т. е. $GF(7)$, все математические операции будут происходить с числами 0, 1, 2, 3, 4, 5, 6.

Сложение, вычитание, умножение и деление в полях Галуа выполняется по модулю N .

Примеры: $4 + 5 = 9 \bmod 7 = 2$.

$$3 - 5 \bmod 7 = 5;$$

$$3 \cdot 5 \bmod 7 = 1;$$

$$2^4 \bmod 7 = 2;$$

$$5 : 6 \bmod 7 = 2 \text{ (верно, т. к. } 6 \cdot 2 \bmod 7 = 5);$$

Полезное свойство обнаруживается в полях Галуа при возведении в степень. Можно заметить, что значения степеней чисел 3 либо 5 в выбранном поле Галуа $GF(7)$ это все элементы текущего поля Галуа кроме 0.

Например:

$$3^0 = 1, 3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1.$$

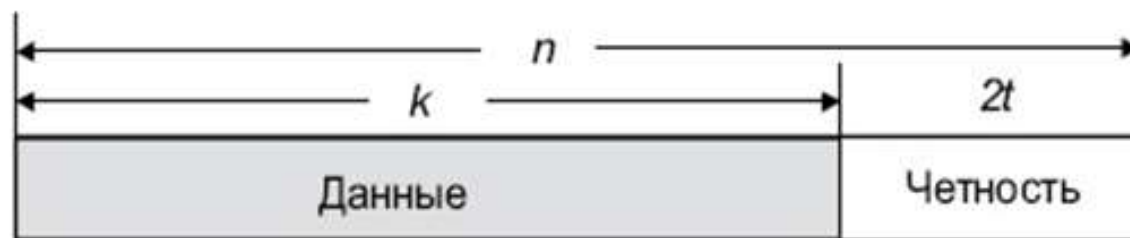
$$5^0 = 1, 5^1 = 5, 5^2 = 4, 5^3 = 6, 5^4 = 2, 5^5 = 3, 5^6 = 1.$$

Такие числа называются *примитивными элементами*. В кодах Рида-

Соломона обычно используется самый большой примитивный элемент выбранного поля Галуа. Для $GF(7)$ он равен 5.

Структура кода Рида-Соломона

Данные обрабатываются порциями по t бит, которые принято называть символами. Как правило, порция представляет собой байт, то есть $t = 8$. При построении кода Рида-Соломона задается пара чисел n, k , где n – общее количество символов (длина блока), а k – количество информационных символов, остальные $n - k$ символов представляют собой избыточный код, предназначенный для восстановления ошибок. Такой код будет иметь расстояние Хэмминга $D = n - k + 1$



В соответствии с теорией кодирования, код, имеющий расстояние Хемминга $D = 2t + 1$, позволяет восстанавливать t ошибок. Таким образом, если в кодовое слово случайно внести $t = (n - k) : 2$ ошибок (т.е. просто произвольно заменить значения t символов любыми значениями), то окажется возможным обнаружить и исправить эти ошибки.


Пусть $t = 1$, $m = 8$. Длина блока равна $n = 2^8 - 1 = 255$ символов или 2040 бит. Длина контрольной части – 2 символа или 16 бит. Код обнаруживает любой пакет ошибок, длина которого не более 16 бит, и исправляет ошибки в пределах одного байта.

Исходное сообщение при кодировании Рида-Соломона представляется полиномом $p(x)$ степени $k - 1$, имеющем k коэффициентов.

Порождающий многочлен Рида-Соломона $g(x)$ строится следующим образом:

$$g(x) = (x + a^1)(x + a^2) \dots (x + a^{D-1}),$$

где a – это примитивный элемент.



В несистематическом коде закодированное сообщение $C(x)$ получается как произведение исходного сообщения на порождающий многочлен:

$$C(x) = p(x) \cdot g(x).$$


Систематический код строится аналогично CRC ($p(x)$ сдвигается на k коэффициентов влево, а затем прибавляется остаток от его деления на $g(x)$):

$$C(x) = p(x) \cdot x^{n-k} + p(x) \cdot x^{n-k} \bmod g(x).$$

Пример: Пусть нам нужно передать кодовое слово $X = (3, 1)$ с возможностью исправить две ошибки ($k = 2, t = 2$). Для этого нужно взять $2t = 4$ избыточных символа. Полученное значение $X = (3, 1, 0, 0, 0, 0)$ в виде полинома имеет вид $X = 3 \cdot x^0 + 1 \cdot x^1 + 0 \cdot x^2 + \dots = 3 + x$. В поле Галуа $GF(7)$ с примитивным элементом 5 получаем код $c(4, 1, 0, 2, 5, 6)$, где $c_i = C(z^i) = 3 + 1 \cdot z^i$. Например, $c_2 = C(z^2) = 3 + 1 \cdot z^2 = 0$.

Закодированное сообщение $C(x)$ без остатка делится на порождающий многочлен $g(x)$:

$$C(x) \bmod g(x) = 0.$$



В случае, если закодированное сообщение будет изменено, то это равенство окажется нарушенным.

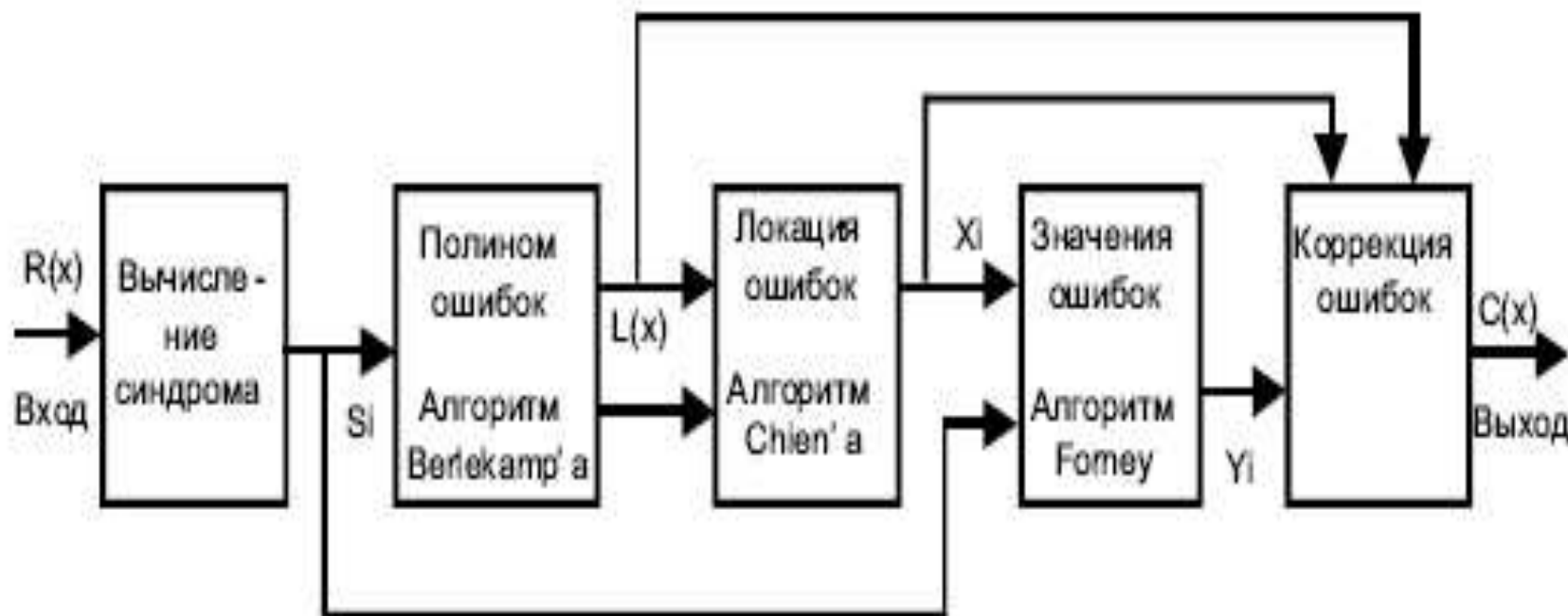
Декодировщик последовательно вычисляет синдромы ошибок, строит соответствующий полином ошибок и находит корни данного полинома (они указывают положение искаженных символов в кодовом слове), по которым определяет характер ошибок и исправляет их.

Устранение ошибок с помощью корректирующих кодов (такое управление называют *Forward Error Control*) реализуют в симплексных каналах связи. В дуплексных каналах достаточно применения кодов, обнаруживающих ошибки (*Feedback or Backward Error Control*), так как сигнализация об ошибке вызывает повторную передачу от источника.

. Схема коррекции ошибок Рида-Соломона



Схема работы с кодами Рида-Соломона



- $r(x)$ – Полученное кодовое слово
- S_i – Синдромы
- $L(x)$ – Полином локации ошибок
- X_i – Положения ошибок
- Y_i – Значения ошибок
- $c(x)$ – Восстановленное кодовое слово
- v – Число ошибок

