Лекция 2
ЭЛЕМЕНТЫ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ
Канальный кодер (блок помехоустойчивого кодирования)

Цифровые данные, подлежащие передаче через канал связи, представляют собой последовательность нулей и единиц. Поскольку в процессе передаче данных через канал в них всегда появляются ошибки, то задачей блока помехоустойчивого кодирования является добавление к исходным информационным символам некоторого количества дополнительных символов с таким расчетом, чтобы с их помощью на приемном конце можно было обнаружить и по возможности исправить возникшие ошибки.

Создание помехоустойчивых кодов основано на том, что непрерывная последовательность двоичных символов делится на k-разрядные комбинации (**информационные слова**) и к каждой такой комбинации добавляется еще r дополнительных символов, рассчитанных по определенному закону. Полученное **кодовое слово** будет содержать k+r=n символов. Поскольку символы двоичные, то общее число возможных k-разрядных комбинаций (информационных слов) равно 2^k, а общее число n-разрядных комбинаций равно 2^n. Однако среди всех 2^n таких комбинаций кодовыми словами будут являться только 2^k слов, а остальные 2^n-2^k n-разрядных слов таковыми являться не будут. Следовательно, если на приемном конце вместо кодового слова будет прията n-разрядная комбинация, не принадлежащая к числу кодовых слов, то это однозначно укажет на присутствие в данном слове ошибки.

Пусть информационные слова состоят только из двух символов (k = 2) 00, 01, 10 и 11. Можно закодировать их путем добавления еще одного двоичного символа (r=1), вычисленного с таким расчетом, чтобы общее число единиц в полученном 3-разрядном кодовом слове (n = 3) было четным. Получим:

$$00 \rightarrow 000,$$
$$01 \rightarrow 011,$$
$$10 \rightarrow 101,$$
$$11 \rightarrow 110.$$

Таким образом, число двухразрядных информационных слов равно $2^2 = 4$. Число полученных 3-разрядных кодовых слов также равно 4. Оставшиеся $2^3 - 2^2 = 4$ трехразрядные комбинации 001, 010, 100, 111 кодовыми словами являться не будут

Здесь следует обратить внимание на то, что каждое из четырех кодовых слов отличается от других кодовых слов не менее чем в двух символах. Эта величина является одной из важнейших характеристик кода и называется **минимальным кодовым расстоянием**. Определение минимального кодового расстояния вытекает из определения так называемого расстояния Хэмминга: ***расстоянием по Хэммингу между двумя последовательностями x и y длины n называется число позиций в которых они различаются.*** Расстояние по Хэммингу обозначается через $d(\mathbf{x},\mathbf{y})$ или просто d.

Минимальное расстояние кода равно наименьшему из всех расстояний по Хэммингу между различными парами кодовых слов и обозначается как d_{min}. Между разными кодовыми словами одного кода, тем не менее, могут быть различные кодовые расстояния.

Возникновение одиночной ошибки приводит к тому, что кодовое слово преобразуется в одну из 3-разрядных комбинаций, не принадлежащих к числу кодовых слов, что и позволяет установить факт наличия ошибки. В данном простейшем коде с помощью каждого из четырех кодовых слов можно передать два бита информации. Платой за возможность обнаружения одной ошибки является введение для образования каждого кодового слова третьего двоичного символа. При возникновении же двух ошибок одно кодовое слово может перейти в другое, и ошибки на приемной стороне не будут замечены. Поэтому использовать данный код для обнаружения двух ошибок нельзя.

Для того чтобы помехоустойчивый код мог обнаружить t_o ошибок, должно выполняться соотношение

$$d_{мин} \geq t_0 + 1 \qquad (1)$$

В рассмотренном примере $d_{мин}$=2, поэтому t_o=1 и код может обнаружить одну ошибку.

Однако, данный код исправлять ошибки не способен, то есть по принятому запрещенному кодовому слову невозможно определить действительно переданное.

Если взять за основу приведенные выше восемь трехсимвольных комбинаций, то с их помощью можно создать код, исправляющий одну ошибку. Однако для этого в качестве информационных слов надо взять всего один символ 1 и 0, а два других символа использовать как k дополнительных. Тогда кодовыми словами будут только комбинации 000 и 111, а все остальные комбинации уже не будут принадлежать коду. В этом случае комбинации 001, 010, 100 , которые отличаются только на один символ от первого кодового слова - 000, будут однозначно идентифицироваться с ним, а комбинации 011, 110, 101, отличающиеся на один символ от второго кодового слова - отождествляться, соответственно, с кодовым словом 111.

С помощью каждого из двух кодовых слов в данном случае можно передать всего один бит информации. Возможность исправления одной ошибки потребовала введения в кодовые слова двух дополнительных двоичных символов на один информационный. При этом избыточность составит 200%. Если кодовому слову 000 поставить в соответствие информационный символ 0, а кодовому слову 111 – символ 1, то получим так называемый код с повторениями, в котором информационные символы повторяются в кодовых словах определенное количество раз.

Для того, чтобы помехоустойчивый код мог исправлять $t_и$ ошибок, величину минимального кодового расстояния $d_{мин}$ следует выбирать из соотношения:

$$d_{мин} \geq 2t_и + 1 \qquad (2)$$

В рассмотренном случае $d_{мин}$ = 3, поэтому $t_и$ = 1 и код может исправить одну ошибку. Если требуется исправить $t_и$ = 2 ошибки, то по формуле (2) $d_{мин} \geq 5$, и в коде с повторениями информационные символы в кодовых словах нужно повторять по 5 раз и т. д. При этом соответственно возрастает и избыточность кода, что является крайне невыгодным.

Табличные методы декодирования

Рассмотрим код, кодовые слова которого состоят из 5 двоичных символов. Из всех 5-разрядных наборов символов выберем в качестве кодовых слов наборы 00000, 00111, 11100, 11011. Минимальное кодовое расстояние в данном случае $d_{мин}$=3, хотя между первым и последним кодовыми словами расстояние d=4.

Составим таблицу (табл.1), в которой под каждым кодовым словом выпишем 5-разрядные наборы, отличающиеся от кодового слова на один символ (содержащие одну ошибку), а ниже – слова с двумя ошибками.

Алгоритм декодирования заключается в следующем. Определяется колонка, в которой расположено принятое кодовое слово. При наличии в принятом кодовом слове одной ошибки, оно будет находиться в одной из колонок в средней части таблицы. В этом случае действительно переданным считается то кодовое слово, которое стоит в первой строке данной колонки.

Если принятое кодовое слово содержит две ошибки, то оно будет находиться в нижней части таблицы и установить однозначное соответствие между принятым и переданным кодовыми словами будет невозможно. Например, принято кодовое слово 10001, содержащее две ошибки и отличающееся на два символа от разрешенных кодовых слов 00000 и 11011. В данном случае невозможно определить, какое из разрешенных кодовых слов было на самом деле передано. Таким образом данный код, может исправлять одну ошибку и обнаруживать две, как и следует из формул (1), (2) при $d_{мин}$ = 3.

В рассмотренном примере длина кодовых слов равна пяти двоичным символам. Общее количество 5-разрядных слов

$N_{общ} = 2^5 = 32,$

	00000	00111	11100	11011
1 ошибка	10000 01000 00100 00010 00001	10111 01111 00011 00101 00110	01100 10100 11000 11110 11101	01011 10011 11111 11001 11010
2 ошибки	10001 10010	10110 10101	01101 01110	01010 01001

поэтому не составляет труда составить таблицу, состоящую из 32 5-разрядных слов. Однако в настоящее время применяются коды, в которых кодовые слова содержат по 300 и более двоичных символов. Общее количество кодовых комбинаций, содержащих по 300 двоичных символов в каждой, равно

$$N_{общ} = 2^{300} \approx 2 \bullet 10^{90} .$$

Применение табличных методов для декодирования таких кодов потребовало бы составления чрезвычайно громоздких таблиц, требующих больших объемов памяти. Реализация таких устройств представляется нецелесообразной. Поэтому теория помехоустойчивого кодирования с самого начала развивалась по другому пути, основанному на использовании алгебраических структур, называемых группами, кольцами и полями.

2.Введение в алгебру конечных полей

Совокупность вещественных чисел образует известное множество математических объектов, которые можно складывать, вычитать, умножать и делить. Комплексные числа также образуют множество математических объектов, которые можно складывать, вычитать, умножать и делить. Обе эти арифметические системы общеизвестны и являются основой всех инженерных дисциплин. В теории помехоустойчивого кодирования используются менее известные арифметические системы, которые, тем не менее, очень полезны для создания и исследования кодов, контролирующих ошибки. Такие арифметические системы состоят из множеств математических объектов и операций над элементами этих множеств. Операции над этими множествами, хотя и называются «сложением», «вычитанием», «умножением» и «делением», не обязательно являются теми же операциями, что известны из элементарной арифметики. Дадим несколько неформальных определений.

Группой называется множество математических объектов, для которых определена одна основная операция – сложение, и операция, ей обратная – вычитание (аддитивная группа). Группой также может быть множество, в котором определено умножение (основная операция) и деление (обратная операция). Такая группа называется мультипликативной.

Кольцо – это множество математических объектов, для которых определены две основные операции – сложение и умножение, и операция, обратная первой из них – вычитание.

Поле – это множество математических объектов, для которых определены две основные операции – сложение и умножение, и для каждой из них обратные операции – вычитание и деление.

Рассмотрим эти множества более подробно.

2.1.Группа

Определение G.1. ***Группой G называется совокупность объектов или элементов, для которых определена некоторая операция и выполняются четыре аксиомы G.1-G.4.***

Пусть a, b, c, …, - элементы группы. Операция – это однозначная функция двух переменных, которая может быть обозначена как f(a,b) = c, но обычно ее записывают в виде a + b = c или ab = c и называют сложением или умножением, даже если она не является арифметическим сложением или арифметическим умножением обычных чисел.

Аксиома G.1 ***(замкнутость). Операция может быть применена к любым двум элементам группы, и в результате операции получится третий элемент группы.***

Аксиома G.2 ***(ассоциативный закон). Для любых трех элементов a, b и c группы (a+b)+c = a+(b+c), если операция записана как сложение, или a(bc) = (ab)c, если операция записана как умножение.***

Ассоциативный закон означает, что порядок выполнения операций несущественен, и поэтому скобки не являются необходимыми.

Аксиома G.3. ***Существует единичный элемент.***

Если операция называется сложением, то она обозначается символом «+» (даже если она не является обычным сложением), а единичный элемент называется нулем, обозначается как 0 и определяется из уравнения 0+a = a+0 = a, которое должно выполняться для любого элемента группы. Если операция называется умножением, то она обозначается символом «·» (даже если она не является обычным умножением), а единичный элемент называется единицей, обозначается как 1 и определяется из уравнения 1·a =a·1 = a. Иногда знак «·» все же опускается, и умножение записывается просто ab=c.

Аксиома G.4. ***Каждый элемент группы обладает обратным элементом.***

Если операция называется сложением, то обратный элемент, соответствующий элементу a, обозначается через –a и определяется как решение уравнения a+(-a)=(-a)+a=0. Если операция называется умножением, то обратный элемент обозначается как a^{-1} и определяется уравнением $aa^{-1} = a^{-1}a = 1$.

Кроме перечисленных аксиом, элементы группы могут удовлетворять коммутативному закону, т.е. для них может выполняться равенство $a + b = b + a$ или, если операция называется умножением, равенство $ab = ba$. В этом случае группа называется **абелевой** или **коммутативной**.

Кроме аксиом, для элементов группы справедлива еще и теорема, которую примем без доказательства.

Теорема G.1. ***Группа обладает единственным единичным элементом, и каждый элемент группы имеет единственный обратный элемент.***

Совокупность всех действительных чисел является группой относительно операции обычного сложения. Совокупность всех положительных и отрицательных чисел с нулем также является группой относительно сложения. Совокупность всех действительных чисел без нуля является группой относительно обычного умножения. Все эти группы являются абелевыми.

2.2.Кольцо

Определение R.1. ***Кольцом R называется совокупность объектов или элементов, для которой определены две операции. Одна из них называется сложением и***

обозначается как a+b, а другая называется умножением и обозначается как a·b (ab), даже если эти операции не являются обычными операциями сложения и умножения чисел. Для того чтобы ***R*** было кольцом, должны выполняться следующие аксиомы:

Аксиома R.1. ***Множество R является абелевой группой относительно операции сложения, т.е. аддитивной абелевой группой.***

Аксиома R.2. ***(замкнутость). Для любых двух элементов a и b из множества R определено произведение ab, результат которого также является элементом R.***

Аксиома R.3. ***(ассоциативный закон). Для любых трех элементов a, b и c из множества R a(bc) = (ab)c.***

Аксиома R.4. ***(дистрибутивный закон). Для любых трех элементов a, b и c из множества R справедливы равенства a(b+c) = ab+ac и (b+c)a = ba+ca.***

Сложение в кольце всегда коммутативно, а умножение – не всегда. ***Поэтому кольцо называется коммутативным, если коммутативна операция умножения, т.е. если для любых двух элементов a и b из R выполняется равенство ab = ba.***

Примем без доказательства следующую теорему, которая справедлива для любого кольца.

Теорема R.1. ***В любом кольце для любых элементов a и b справедливы соотношения a0 = 0a = 0 и a(-b) = (-a)b = -(ab).***

Операция сложения в кольце имеет единичный элемент, называемый нулем. Операция умножения не обязательно имеет единичный элемент, но если он есть, то является единственным. Кольцо, обладающее единственным единичным элементом относительно умножения, называется **кольцом с единицей**. Этот единичный элемент называется единицей и обозначается символом 1. Тогда для всех ***a*** из ***R*** имеет место равенство ***1a = a1 = a***.

Относительно операции сложения каждый элемент кольца имеет обратный элемент. Относительно операции умножения элемент, обратный данному элементу, не обязательно существует, но в кольце с единицей обратные элементы могут существовать. Это означает, что для данного элемента ***a*** может существовать элемент ***b***, такой, что ***ab = 1***. Если это так, то ***b*** называется **правым обратным** к элементу ***a***. Аналогично, если существует элемент ***c***, такой, что ***ca = 1***, то ***c*** называется **левым обратным** к элементу ***a.***

Теорема R.2. ***В кольце с единицей единица единственна. Если элемент a имеет как правый обратный b, так и левый обратный c, то элемент a называется обратимым, причем обратный ему элемент является единственным и обозначается через*** a^{-1}***. При этом*** $(a^{-1})^{-1} = a$.

Все действительные числа образуют кольцо относительно обычных операций сложения и умножения. Все положительные и отрицательные числа и нуль также образуют кольцо относительно обычных операций сложения и умножения. Оба эти кольца коммутативны.

2.3.Поле

Определение F.1. ***Полем называется коммутативное кольцо с единичным элементом относительно умножения (единичный мультипликативный элемент кольца), в котором каждый ненулевой элемент имеет мультипликативный обратный элемент (т.е. обратный по умножению).***

Некоммутативное кольцо, в котором у каждого ненулевого элемента есть обратный, называют **кольцом с делением**, или **телом**.

Определение F.2. ***Полем называется множество с двумя определенными в нем операциями – сложением и умножением, причем для этого множества справедливы следующие аксиомы.***

Аксиома F.1. ***Множество образует абелеву группу по сложению.***

Аксиома F.2. ***Поле замкнуто относительно умножения, и множество ненулевых элементов образует абелеву группу по умножению***.

Аксиома F.3. ***Закон дистрибутивности:***

(a + b)c = ac + bc для любых a, b, c из поля.

Единичный элемент относительно сложения принято обозначать через ***0*** и называть нулем, аддитивный обратный элементу a элемент – через ***–a***; единичный элемент относительно умножения обозначать через ***1*** и называть единицей, мультипликативный обратный к элементу a элемент – через a^{-1}. Под вычитанием ***(a-b)*** понимается ***a+(-b)***; под делением ***(a/b)*** понимается ab^{-1}.

Таким образом, очевидно, что подтверждаются данные в начале темы нестрогие определения, т.е. абелева группа – это множество, в котором можно складывать и вычитать; кольцо – это множество, в котором можно складывать, вычитать и умножать и, наконец, самой сильной алгебраической структурой является поле, то есть множество, в котором можно складывать, вычитать, умножать и делить.

Примерами полей могут служить:

- множество вещественных чисел;
- множество комплексных чисел;
- множество рациональных чисел.

Все эти поля содержат бесконечное множество элементов. Нам же в рассматриваемом случае интересны поля, содержащие конечное число элементов. Поле с ***q*** элементами, если оно существует, называется **конечным полем** или **полем Галуа** и обозначается через ***GF(q)***.

Что представляет собой наименьшее поле? Очевидно, что оно обязательно должно содержать нулевой элемент и единичный элемент. Оказывается, что этих двух элементов уже вполне достаточно, чтобы образовать поле. Обозначим нулевой элемент через ***0***, а единичный через ***1*** и определим операции сложения и умножения равенствами:

$$0 + 0 = 0, \quad 0 \cdot 0 = 0,$$
$$0 + 1 = 1, \quad 0 \cdot 1 = 0,$$
$$1 + 0 = 1, \quad 1 \cdot 0 = 0,$$
$$1 + 1 = 0, \quad 1 \cdot 1 = 1.$$

Определенные таким образом сложение и умножение называются **сложением по модулю *2*** и **умножением по модулю *2***. Очевидно, что из равенства $1 + 1 = 0$ следует, что $-1 = 1$, а из равенства $1 \cdot 1 = 1$ – что $1^{-1} = 1$. Алфавит из двух символов ***0*** и ***1*** вместе со сложением по модулю ***2*** и умножением по модулю ***2*** называется **двоичным полем** и обозначается, как говорилось ранее, через ***GF(2)***.

Можно показать, что для любого числа ***q***, являющегося степенью простого числа, существует поле, содержащее ***q*** элементов. Однако, следует отметить, что это утверждение, чаще всего, не относится к совокупности целых чисел по модулю ***q***. В то же время поле с ***p*** элементами можно получить, рассмотрев совокупность целых чисел по модулю ***p***, ***если p является простым числом***. То есть совокупность целых чисел по модулю ***q*** образует поле только в том случае, если ***q*** – простое число. ***Или – поле, содержащее $q = p^m$ элементов (m>1), не может быть образовано из совокупности целых чисел по модулю q***.

Пример 1. Поле ***GF(3).*** Правила сложения и умножения.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Пример 2. Поле $GF(2^2)$**.** Правила сложения и умножения.

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

×	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

В первом примере поле ***GF(3)*** является совокупностью целых чисел по модулю 3, а во втором примере поле ***GF(2^2)*** не является совокупностью целых чисел по модулю $2^2 = 4$.

Еще один пример поля ***GF(2^2),*** которое в отличие от поля в примере 2, содержит целые числа ***{0,1,2,3},*** но операции сложения и умножения в нем не являются сложением и умножением по модулю ***4***.

Пример 3. Поле ***GF(4) = {0,1,2,3}.*** Правила сложения и умножения.

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

В приведенных примерах отметим, что в поле ***GF(4)*** из примера 3 содержится поле ***GF(2),*** поскольку в поле ***GF(4)*** два элемента 0 и 1 складываются и умножаются точно так же, как они складываются и умножаются в поле ***GF(2)***. В то же время поле ***GF(2)*** не содержится в поле ***GF(3)*** из примера 1.

Определение F.3. ***Пусть F – некоторое поле. Подмножество F' в F называется*** **подполем*****, если оно само является полем относительно наследуемых из F операций сложения и умножения. В этом случае исходное поле F называется*** **расширением поля *F'*.**

Поле обладает всеми свойствами кольца, а также важным дополнительным свойством – в нем всегда возможно сокращение. Сокращение представляет собой слабую форму деления и означает, что если $ab = ac$, то $b = c$.