Занятие № 4. “Помехоустойчивое кодирование”

1. Принципы помехоустойчивого кодирования

Помехоустойчивое или избыточное кодирование применяется для обнаружения и (или) исправления ошибок, возникающих при передаче по дискретному каналу. Отличительное свойство помехоустойчивого кодирования состоит в том, что избыточность источника, образованного выходом кодера, больше, чем избыточность источника на входе кодера. Помехоустойчивое кодирование используется в различных системах связи, при хранении и передаче данных в сетях ЭВМ, в бытовой и профессиональной аудио- и видеотехнике, основанной на цифровой записи.

Классификация помехоустойчивого кодирования показана на рис.1 (возможен другой вариант).

Рис. 1. Классификация помехоустойчивого кодирования

Помехоустойчивые коды называют ***корректирующими.*** Помехоустойчивость кода основана на введении избыточности в передаваемый сигнал. Помехоустойчивый код отличается от обычного тем, что в канал передаются не все кодовые комбинации, которые можно сформировать. Из всего множества комбинаций выделяются так называемые разрешенные комбинации, которые выделяются по наличию определенных свойств. Только разрешенные кодовые комбинации передаются в канал связи. Остальные неиспользуемые кодовые комбинации называются ***запрещенными***. Передаче по каналу связи они не подлежат.

Для двоичного кода все множество кодовых комбинаций равно $N=2^n$, где n – число разрядов в кодовой комбинации. Это множество разбивается на два подмножества: разрешенных кодовых комбинаций и запрещенных. Эти подмножества известны как на передающей, так и на приемной сторонах.

Если в результате искажений передаваемых кодов комбинация перейдет в подмножество запрещенных комбинаций, то ошибка будет обнаружена. Коды, позволяющие только определить наличие ошибок, но не указывающие номер искаженных разрядов называют ***кодами с обнаружением ошибок.***

При необходимости исправления некоторых возникающих искажений поступают следующим образом. Все множество кодовых комбинаций N разбивают на $N_0<N$ непересекающихся подмножеств. Каждое из этих подмножеств, приписывается к одной из N_0 разрешенных комбинаций. Принцип исправления ошибок иллюстрируется на рис.2.

Если принятая комбинация A_j входит в подмножество N_{0j} ($A_j \in N_{0j}$), то принимается решение, что передана комбинация A_j. То есть, если принятая кодовая комбинация осталась в том же подмножестве, что и передаваемая, то прием будет без ошибки. Если

кодовая комбинация в результате искажений переходит в другое подмножество, то прием будет с ошибкой.

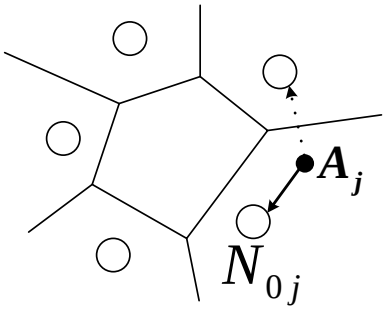

Рис. 2. Принцип исправления возникающих ошибок

Коды, которые не только обнаруживают ошибку, но и указывают номер искаженной позиции, называются ***кодами с исправлением ошибок***. При использовании помехоустойчивого кода в канале связи передаются только разрешенные кодовые комбинации. Если бы не было помех, то для передачи этих кодовых комбинаций потребовалось бы меньшее число разрядов n_0: $n_0 = \log_2 N_0 < n$.

Таким образом, обнаружение и исправление возникающих в каналах связи ошибок достигается за счет введения в передаваемые кодовые комбинации избыточных разрядов.

2. Обнаруживающая и исправляющая способность кодов

Рассмотрим возможность обнаружения и исправления ошибок на простейшем примере. Предположим, что информация передается одноразрядным двоичным кодом. То есть передается информация 0 или 1. Число возможных кодовых комбинаций $N_0=2^{n0}$, где $n_0=1$, $N_0=2^1=2$. В каждой кодовой комбинации добавим еще один разряд: $n= n_0+1=1+1=2$. Число кодовых комбинаций $N=2^n=2^2=4$. Эти комбинации составляют множество, состоящее из 00, 01, 10, 11. Это множество разделим на два подмножества разрешенных и запрещенных комбинаций. К числу разрешенных отнесем те комбинации, у которых сумма единиц всегда четная. Разрешенными выберем такие комбинации, которые отличаются друг от друга двумя разрядами – это 00 и 11. При таком выделении разрешенных комбинаций любая одиночная (или нечетная) ошибка будет изменять число единиц на нечетное. Принятая кодовая комбинация в этом случае переходит в подмножество запрещенных и ошибка будет обнаружена.

Если в кодовую комбинацию ввести количество дополнительных разрядов, то можно не только обнаруживать, но и исправлять ошибки. Если разрешенные комбинации определить таким образом, что любые из них отличаются друг от друга не менее чем тремя разрядами, то одиночная ошибка может быть исправлена. Возможность исправления одиночной ошибки в этом случае связана с тем, что ошибочная комбинация будет отличаться от истинной только одним разрядом и останется в области, относящейся к передаваемой разрешенной комбинации.

Рассмотрим сказанное на геометрической модели трехразрядного двоичного кода при помощи которого можно получить $2^3=8$ комбинаций. А именно: 000, 001, 010, 011, 100, 101, 110, 111. Каждую новую комбинацию можно представить точкой в трехмерном пространстве (рис. 3).

Для исправления одиночной ошибки разобьем все множества комбинаций на две области, и будем передавать только две кодовые комбинации 111 и 000. Эти комбинации отличаются друг от друга тремя разрядами. Любая одиночная ошибка оставляет кодовую комбинацию в области, относящейся к передаваемой комбинации. Так, при искажении одного разряда в комбинации 000 она превратится в 001, или в 100, или в 010. Все эти

комбинации находятся в той же области, что и комбинация 000.

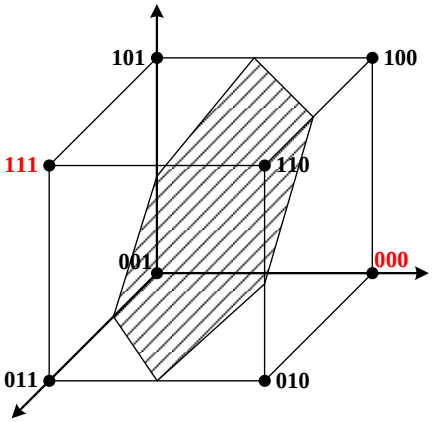

Рис. 3. Геометрическая модель помехоустойчивого кода

Рассмотренные примеры показывают, что для обнаружения одиночных ошибок кодовые комбинации должны различаться не менее чем двумя разрядами. Для исправления одиночной ошибки кодовые комбинации должны различаться не менее чем тремя разрядами. Это различие именуют кодовым (Хэминговым) расстоянием. Под ***кодовым расстоянием*** понимают минимальное число позиций, на которых символы данной кодовой комбинации отличаются от символов другой кодовой комбинации. Например, для показанных на рис. 4 комбинаций кодовое расстояние d равно 3.

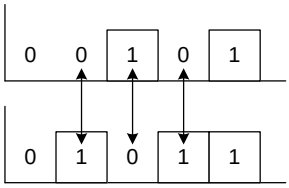

Рис. 4. Кодовое расстояние между двумя кодовыми комбинациями

В общем случае кодовое расстояние между комбинациями выражается формулой:

$$d(a,b)=\sum_{i=0}^{n}(a_i \oplus b_i), \qquad (1)$$

где $\oplus$ – операция сложения по модулю два;

$\boldsymbol{a=(a_0,a_1,...,a_{n-1})}$;

$\boldsymbol{b=(b_0,b_1,...,b_{n-1})}$.

Пользуясь расстоянием Хэмминга как метрикой в множестве кодовых слов можно выделить зоны исправления и обнаружения ошибок.

Утверждение. Если код используется только для обнаружения ошибок, то, чтобы обнаружить в кодовом слове произвольную комбинацию из ***s*** ошибок, необходимо и достаточно, чтобы расстояние Хэмминга для любых двух разрешенных кодовых слов было на **1** больше, чем ***s*** (количество обнаруживаемых ошибок): $d_{\min}(a,b)=s+1$

В соответствии с утверждением в данном примере могут быть обнаружены ошибки кратные ***s*=1** и ***s*=2**. При ***s*=3** передаваемая кодовая комбинация переходит в другую разрешенную комбинацию. Ошибка не обнаруживается.

Утверждение. Если код используется только для исправления ошибок, то, чтобы исправить ***t*** ошибок необходимо и достаточно, чтобы $d_{\min}(a,b)=2t+1$.

Утверждение. Для того, чтобы исправить t и обнаружить s ошибок в кодовом слове, необходимо и достаточно, чтобы $d_{\min}(a,b)=2t+s+1$.

Таким образом, правильный выбор разрешенных и запрещенных кодовых комбинаций передаваемого сообщения позволяет сформировать помехоустойчивый код с обнаружением и исправлением ошибок.

3. Блочные помехоустойчивые коды

Разделимые коды обычно обозначают как (***n, k***) - коды. Здесь ***n*** – количество элементов в кодовой комбинации, ***k*** – число информационных элементов.

Общепринятым методом задания (*n, k*) кодов является представление набора используемых кодовых комбинаций в виде матрицы, имеющей ***n*** столбцов и ***k*** строк. Такую матрицу называют ***порождающей матрицей***. Обозначается порождающая матрица – $G_{n\times k}$.

Путем элементарных преобразований (перестановкой строк; заменой строки суммой данной строки с любой другой строкой, перестановкой столбцов) порождающая матрица может быть преобразована к канонической форме:

$$G_{n\times k} = \left| I_{k\times k} \_ h_{r\times k} \right|, \qquad (2)$$

где $\left| I_{k\times k} \right|$ – единичная матрица размерностью $k \times k$;

$\left| h_{r\times k} \right|$ – матрица размерностью $r \times k$;

$r = n - k$ – число проверочных элементов.

Важным подмножеством групповых кодов являются коды Хэмминга.

Коды Хэмминга – это (n, k) коды, длина которых равна $n = 2^r - 1$.

Примеры кодов Хэмминга: (7,4); (15,11) и т.д. Для данных кодов $d_{\min} = 3$.

Код Хэмминга (7,4) как правило задается порождающей матрицей, причем эта матрица может быть приведена к каноническому виду:

$$G_{7\times 4} = \begin{vmatrix} 1000\_011 \\ 0100\_101 \\ 0010\_110 \\ 0001\_111 \\ I_{4\times 4} \_ h_{3\times 4} \end{vmatrix}. \qquad (3)$$

Построение подматрицы $\left| \boldsymbol{h_{r\times k}} \right|$ производится следующим образом: в столбик записывается двоичное представление чисел от **0** до ***n*** разрядами ***r***, после этого вычеркиваются строки с количеством единиц меньше двух, из оставшихся строк составляется подматрица $\left| \boldsymbol{h_{r\times k}} \right|$.

Алгоритм кодирования кодом Хэмминга

Пусть задано информационное слово $C = (b_0 b_1 b_2 b_3) = (0010)$, которое нужно закодировать кодом Хэмминга (7,4). Код Хэмминга (7,4) задан порождающей матрицей вида (3).

Комбинация на выходе кодера получается из соотношения:

$$C' = C \cdot G_{7\times 4} = (b_0 b_1 b_2 b_3) \cdot \begin{vmatrix} 1000\_011 \\ 0100\_101 \\ 0010\_110 \\ 0001\_111 \end{vmatrix} = (b_0 b_1 b_2 b_3 \_ a_0 a_1 a_2).$$

Проверочные символы для кода Хэмминга (7,4) формируются в соответствии с приведенными выражениями:

$$a_0 = b_1 \oplus b_2 \oplus b_3 = 0 \oplus 1 \oplus 0 = 1,$$

$$a_1 = b_0 \oplus b_2 \oplus b_3 = 1 \oplus 1 \oplus 0 = 0,$$

$$a_2 = b_0 \oplus b_1 \oplus b_3 = 1 \oplus 0 \oplus 0 = 1.$$

При записи кодовой комбинации на выходе кодера первые ***k*** символов кода называются информационными, остальные $\boldsymbol{r = n - k}$ – проверочными.

На выходе кодера получим кодовую комбинацию:

$$C' = (b_0 b_1 b_2 b_3 \_ a_0 a_1 a_2) = (0010\_101).$$

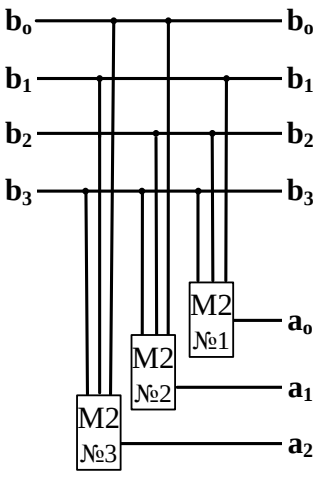

Рис. 2. Схема кодера Хэмминга (7,4)

Структурная схема кодера для кода Хэмминга (7,4) приведена на рис. 2.

Задача декодирования состоит в том, чтобы принятому кодовому слову поставить в соответствие кодовое слово из числа разрешённых. Используя принцип максимального правдоподобия, в соответствие ставится такое разрешённое слово, которое минимально отличается от принятого.

Алгоритмы декодирования можно задавать таблично. Однако гораздо удобнее знание математической структуры кода, что может облегчить реализацию операций кодирования и декодирования.

Необходимо отметить, что операция декодирования, не есть операция, обратная операции кодирования. Это операция оценки принятого сообщения и принятия наиболее достоверного решения относительно того, какое из возможных сообщений было передано.

Различают синдромное и мажоритарное декодирование.

Синдромом называется кодовая комбинация размерностью $\boldsymbol{r = n - k}$, равная произведению принятого кодового слова на транспонированную проверочную матрицу.

Если кодовое слово будет принято без искажений, то синдром будет равен нулю, т.е. $\boldsymbol{S = 000}$. Если же какой-либо символ будет принят с искажением, то синдром совпадает со столбцом проверочной матрицы и укажет на номер разряда (символа в кодовом слове), который принят с ошибкой.

Для исправления ошибки нужно к символу разряда в котором произошла ошибка прибавить единицу по модулю два.

Под мажоритарными групповыми кодами принято понимать такие групповыми коды, которые позволяют при декодировании использовать принцип решения по большинству (мажоритарный принцип).

При декодировании кодом Хэмминга используется синдромное декодирование.

Для порождающей матрицы вида (3), проверочная матрица имеет канонический вид:

$$H = \begin{vmatrix} 0111\_100 \\ 1011\_010 \\ 1101\_001 \\ h^{\mathrm{T}}{}_{k\times r} \_\_ I_{r\times r} \end{vmatrix}. \qquad (4)$$

Проверочная матрица $\boldsymbol{H}$ состоит из 2-х подматриц:

$\boldsymbol{h^{\mathrm{T}}{}_{k\times r}}$ – транспонированной матрицы, определяемой из порождающей матрицы;

$\boldsymbol{I_{r\times r}}$ – единичной матрицы размерностью $\boldsymbol{r \times r}$.

Свойство проверочной матрицы: произведение закодированного слова (разрешенной кодовой комбинации) на транспонированную проверочную матрицу равно нуль-вектору:

$$(b_0, b_1, b_2, ..., b_{k-1}, a_0, a_1, ..., a_{r-1}) \cdot H^T = (0,0,...,0_{r-1}).$$

Проверочная и порождающая матрицы связаны выражением:

$$G_{k\times n} \cdot H^T_{n\times k} = 0.$$

В обобщенном виде, алгоритм исправления ошибок включает в себя три этапа: вычисление синдрома; синтез вектора ошибок; исправление ошибки.

Рассмотрим этапы более подробно.

Вычисление синдрома.

Для кода Хэмминга (7,4) синдромом будет 3-х разрядная кодовая комбинация:

$$S = C'' \cdot H^T = (b_0 b_1 b_2 b_3 \_ a_0 a_1 a_2) \cdot \begin{vmatrix} 011 \\ 101 \\ 110 \\ 111 \\ 100 \\ 010 \\ 001 \end{vmatrix} = (S_0 S_1 S_2),$$

где $C'' = (b_0 b_1 b_2 b_3 \_ a_0 a_1 a_2)$ – принятое сообщение;

$\boldsymbol{H^T}$ – транспонированная проверочная матрица.

Согласно правилу умножения вектора на матрицу элементы синдрома будут определяться выражениями:

$$S_0 = b_1 \oplus b_2 \oplus b_3 \oplus a_0, \qquad S_1 = b_0 \oplus b_2 \oplus b_3 \oplus a_1, S_2 = b_0 \oplus b_1 \oplus b_3 \oplus a_2.$$

Если кодовое слово будет принято без искажений, то синдром будет равен нулю, т.е. $S = 000$.

Если же какой-либо символ будет принят с искажением, то синдром укажет на номер элемента в кодовом слове, который принят ошибочно.

Вектор ошибок это кодовая комбинация, которая ставится в соответствие синдрому и содержит единицу в том разряде, где произошла ошибка, и нули во всех остальных разрядах. Составим таблицу соответствия синдрома и вектора ошибок:

Таблица 1

Таблица соответствия вектора ошибки синдрому сообщения

Синдром			***Вектор ошибок***			
$\boldsymbol{S_0}$	$\boldsymbol{S_1}$	$\boldsymbol{S_2}$	$\boldsymbol{e_0}$	$\boldsymbol{e_1}$	$\boldsymbol{e_2}$	$\boldsymbol{e_3}$
0	0	0	0	0	0	0
0	1	1	1	0	0	0
1	0	1	0	1	0	0
1	1	0	0	0	1	0
1	1	1	0	0	0	1

На основании данной таблицы получим элементы вектора ошибок:

$$e_0 = \bar{S}_0 S_1 S_2, \quad e_1 = S_0 \bar{S}_1 S_2, \quad e_2 = S_0 S_1 \bar{S}_2, \quad e_3 = S_0 S_1 S_2.$$

Например, с ошибкой был принят символ $\boldsymbol{b_2}$, в этом случае синдром будет равен $S = 110$, а это третий столбец в проверочной матрице, которому соответствует вектор ошибок $e = 0010$.

Исправить ошибку довольно легко, для этого нужно произвести поразрядное сложение по модулю два принятого кодового слова и синтезированного вектора ошибок.

Пример.

Пусть принята кодовая комбинация $C'' = 1010\_101$ без ошибки.

Произведем вычисление синдрома:

$$S_0 = b_1 \oplus b_2 \oplus b_3 \oplus a_0 = 0 \oplus 1 \oplus 0 \oplus 1 = 0,$$

$$S_1 = b_0 \oplus b_2 \oplus b_3 \oplus a_1 = 1 \oplus 1 \oplus 0 \oplus 0 = 0,$$

$$S_2 = b_0 \oplus b_1 \oplus b_3 \oplus a_2 = 1 \oplus 0 \oplus 0 \oplus 1 = 0.$$

Т.к. полученный синдром является нулевым, то ошибки нет и можно сразу записать итоговую кодовую комбинацию: $C = 1010$.

Пример.

Введем в принятую кодовую комбинацию, ошибку во втором разряде, т.е. $C'' = 1110\_101$.

Произведем вычисление синдрома:

$$S_0 = b_1 \oplus b_2 \oplus b_3 \oplus a_0 = 1 \oplus 1 \oplus 0 \oplus 1 = 1,$$
$$S_1 = b_0 \oplus b_2 \oplus b_3 \oplus a_1 = 1 \oplus 1 \oplus 0 \oplus 0 = 0,$$
$$S_2 = b_0 \oplus b_1 \oplus b_3 \oplus a_2 = 1 \oplus 1 \oplus 0 \oplus 1 = 1.$$

Полученному синдрому $S = 101$, соответствует второй столбец проверочной матрицы, в таблице соответствия (табл. 2.1) это третья строка следовательно вектор ошибок примет вид $e = 0100$.

Запишем процесс исправления ошибки:

$C'' = 1110$ – информационные символы принятой кодовой комбинации,

$\oplus$

$e = 0100$ – вектор ошибок,

$C = 1010$ – исправленная информационная кодовая комбинация.

Схема декодера для выбранного кода Хэмминга (рис. 3) строится по известной проверочной матрице $\boldsymbol{H}$ с использованием метода синдромного декодирования.

В состав структурной схемы декодера кода Хэмминга (7,4) входят:

блок вычисления синдрома;

формирователь вектора ошибок;

выходные сумматоры по модулю два, в которых происходит процесс исправления ошибок.

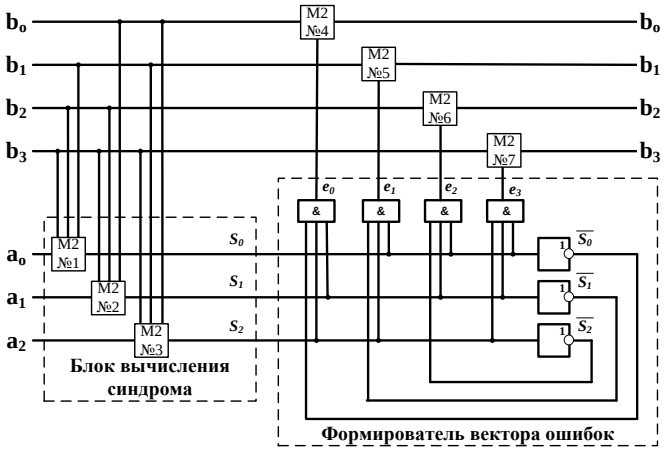

Рис. 3. Схема декодера Хэмминга (7,4)

Таким образом, как следует из материалов занятия:

1. Помехоустойчивость корректирующих кодов основана на введении избыточности в передаваемый сигнал. Из множества всех кодовых комбинаций в канал связи передаются только некоторые – разрешенные комбинации. Ошибка обнаруживается, если принятая комбинация кода отличается от разрешенных. Помехоустойчивые коды могут не только обнаруживать ошибки, но и исправлять их.

2. Кроме длины кодовой комбинации *n*, для характеристики помехоустойчивых кодов пользуются кодовым расстоянием *d*. Кодовое расстояние определяет насколько различаются кодовые комбинации между собой. С увеличением кодового расстояния корректирующие возможности помехоустойчивого кода расширяются. Однако, для этого необходимо увеличивать число избыточных разрядов кода.