ПРИМЕРЫ НЕКОТОРЫХ СОВЕРШЕННЫХ КОДОВ

Двоичный код с многократной передачей символов или *двоичный код с повторением* нечётной длины $n = 2t+1$

В этом случае верхняя граница (2-63)

$$\frac{2^n}{|S_t^n(\mathbf{0})|} = \frac{2^{2t+1}}{\sum_{i=0}^{t} C_{2t+1}^i} = \frac{2^{2t+1}}{(1+1)^{2t}} = \frac{2^{2t+1}}{2^{2t}} = 2. \quad (2\text{-}65)$$

Полученный результат совпадает с числом кодовых слов $N = 2$ двоичного кода с многократной передачей символов. (см. табл. 1.1).

Код Хэмминга

Проверочная матрица кода Хэмминга состоит из r различных ненулевых строк и $2^r - 1$ различных ненулевых столбцов – двоичных ненулевых наборов длины r. Никакая совокупность из двух (и менее) столбцов этой проверочной матрицы не является линейно зависимой, но существуют линейно зависимые совокупности из трёх столбцов. Следовательно, минимальное хэммингово расстояние нулевого пространства этой матрицы $d_{\min} = 3 = 2t+1$; $t = 1$. Это нулевое пространство является кодом, исправляющим все одиночные ошибки. Очевидно, что

$$n = 2^r - 1; \quad (2\text{-}66)$$

$$k = 2^r - 1 - r. \quad (2\text{-}67)$$

В этом случае

$$\frac{2^n}{|S_t^n(\mathbf{0})|} = \frac{2^{2t+1}}{\sum_{i=0}^{t} C_n^i} = \frac{2^n}{\sum_{i=0}^{1} C_n^i} = \frac{2^n}{(1+n)} = 2^{n-r} = 2^k. \quad (2\text{-}68)$$

Полученный результат совпадает с числом кодовых слов $N = m(n, 2t+1) = 2^k$ (n, k)-кода Хэмминга.

По существу, речь здесь шла *о классе* конкретных кодов Хэмминга, каждый из которых определяется конкретным значением r.

Кроме приведенных выше совершенных кодов отметим также двоичный (23, 12)-код Голея, исправляющий трёхкратные ошибки, и троичный (11, 6)-код Голея, исправляющий двукратные ошибки.

Существуют также другие совершенные линейные и нелинейные коды [2.4, 2.5, 2.6].

2.5. ПРИНЦИПЫ ПОДСЧЁТА РАЗЛИЧНЫХ ОДНОРОДНЫХ ОБЪЕКТОВ, ОПИСЫВАЕМЫХ С ПОМОЩЬЮ МАТРИЦ. ОСНОВНЫЕ РЕЗУЛЬТАТЫ ПОДСЧЁТОВ

ПРИНЦИПЫ ПОДСЧЁТА РАЗЛИЧНЫХ ОДНОРОДНЫХ ОБЪЕКТОВ

Выше мы неоднократно подсчитывали число таких однородных различных объектов, как:

различных базисов линейного пространства заданной размерности,

различных линейных k-мерных подпространств пространства B^n и, в частности, групповых (n, k)-кодов,

различных систематических (n, k)-кодов,

различных асистематических групповых (n, k)-кодов

и т.д.

Необходимо ещё раз подчеркнуть, что в ряде случаев из соображений удобства мы описывали некоторые совокупности однородных элементов не путём их перечисления в фигурных скобках {…}, а путём записи совокупности элементов в виде матриц (например, кодовые матрицы; матрицы, содержащие базисы линейных пространств и их подпространств, и т.п.).

Типичными задачами при этом являются:

задачи упорядочения элементов некоторых совокупностей однородных элементов по некоторому критерию,

упорядочения подобных совокупностей однородных элементов одной и той же мощности по некоторому критерию,

«отлавливания» одинаковых совокупностей однородных элементов

и

исключение совокупностей одинаковых с ранее упорядоченными совокупностями, что предполагает в итоге получение *упорядоченного множества* ***различных*** *совокупностей однородных элементов.*

Легко понять, что применение матриц в случаях, когда необходимо рассмотреть значительные по мощности совокупности элементов, а число таких совокупностей может быть значительным (десятки и более), существенно упрощает решение сформулированных «типичных задач» и им подобных.

Какие приёмы здесь могут быть эффективно использованы? Элементы каждой из заданных совокупностей однородных элементов и сами совокупности могут быть упорядочены в соответствии с некоторым целесообразным критерием. Так, в частности, если рассмотреть совокупность заданных в матричной форме 28 базисов примера 2.15, то легко обнаружить, что каждой строке каждой матрицы было сопоставлено число, представляемое самой строкой, интерпретируемой как двоичная запись этого числа; строки каждой матрицы были упорядочены «сверху вниз» – «рост числа, представляемого строкой». При этом все матрицы оказалась взаимно однозначным способом занумерованными трёхзначными десятичными числами (124, 125, 126, …, 567), что, в свою очередь, позволило упорядочить матрицы «слева направо и сверху вниз» – «рост трёхзначного числа» и исключить случаи повторяющихся совокупностей однородных элементов, заданных с помощью матриц.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ПОДСЧЁТОВ

При подсчёте однородных объектов считалось

1. Два множества одинаковой мощности однородных элементов считаются различными, если они отличаются входящими в них элементами (хотя бы одним); при этом неважно, заданы ли множества с помощью фигурных скобок {…} или в матричном виде;

так, в частности, если две матрицы, представляющие два множества однородных элементов равны, то равны и представляемые ими множества, однако, если матрицы отличаются друг от друга, то представляемые ими множества могут как совпадать, так – и отличаться;

2. Две матрицы одной и той же размерности считаются различными, если они отличаются хотя бы одним элементом.

Подведём основные результаты применения изложенных принципов подсчёта однородных различных объектов применительно к изучению свойств групповых (n, k)-кодов с проверкой на чётность.

1) Число всех вершин куба B^n

$$|B^n| = 2^n.$$

2) Число всевозможных различных базисов в B^n

$$N_{(n)} = \frac{(2^n - 1)(2^n - 2)(2^n - 2^2)\cdot\ldots\cdot(2^n - 2^{n-1})}{n!},$$

число всевозможных различных базисов в B^k

$$N_{(k)} = \frac{(2^k - 1)(2^k - 2)(2^k - 2^2)\cdot\ldots\cdot(2^k - 2^{k-1})}{k!}.$$

3) Общее число всевозможных различных групповых (n, k)-кодов (систематических и асистематических) в B^n

$$N_{(n,k)} = \frac{(2^n - 1)(2^n - 2)(2^n - 2^2)\ \ldots\ (2^n - 2^{k-1})}{(2^k - 1)(2^k - 2)(2^k - 2^2)\ \ldots\ (2^k - 2^{k-1})}.$$

4) Число различных систематических (n, k)-кодов

$$N^{сис}_{(n,k)} = 2^{k(n-k)}.$$

5) Число различных асистематических (n, k)-кодов

$$N^{асис}_{(n,k)} = N_{(n,k)} - 2^{k\cdot(n-k)} =$$

$$= \frac{(2^n - 1)(2^n - 2)(2^n - 2^2)\ \ldots\ (2^n - 2^{k-1})}{(2^k - 1)(2^k - 2)(2^k - 2^2)\ \ldots\ (2^k - 2^{k-1})} - 2^{k(n-k)}.$$

6) Каждому конкретному систематическому (n, k)-коду из числа $N^{сис}_{(n,k)} = 2^{k(n-k)}$ взаимно однозначным образом соответствует одна конкретная порождающая матрица в канонической форме $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$.

Путём применения к конкретной порождающей матрице $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$ *элементарной операции перестановки строк* можно получить $(k! - 1)$ различных порождающих матриц типа $[\boldsymbol{I}_{[k]}\boldsymbol{R}_{[k\times(n-k)]}]$, имеющих условно каноническую форму, каждая из которых представляет один конкретный *условно систематический код первого типа*; при этом множество кодовых слов каждого из этих $(k! - 1)$ *условно систематических*

кодов совпадает с множеством кодовых слов систематического (n, k)-кода, определяемого матрицей $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$.

Путём применения к конкретной порождающей матрице $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$ *элементарной операции над строками* 2) *и возможно ещё элементарной операции* 1) можно получить некоторое конечное число конкретных порождающих матриц типа $[\mathcal{I}_{k\times k}\mathcal{R}_{k\times(n-k)}]$, каждая из которых представляет один конкретный *условно систематический код второго типа* (см. задачи 2.25 и 2.26).

Это, непростое на первый взгляд, рассуждение является следствием данных выше несколько путающих читателя, но являющихся уже классическими, определений 1.9 и 1.10 систематического и общего кодов с проверкой на чётность: указанные определения в качестве признаков определяемых кодов содержат *не только совокупность всех кодовых комбинаций определяемых кодов*, ***но также и*** *форму их представления*.

Действительно, можно было бы считать два (n, k)-кода, имеющих одни и те же параметры n и k, различными, если множества их кодовых комбинаций различны или, что – то же самое, если эти два кода являются различными k-мерными подпространствами; и, наоборот, два (n, k)-кода, имеющие одни и те же параметры n и k, можно было бы считать одним и тем же (n, k)-кодом, если они оба являются одним и тем же k-мерным подпространством. Однако сложившаяся практика задания (n, k)-кодов учитывает и форму их задания; так, например, два (n, k)-кода, являющиеся одним и тем же k-мерным подпространством, могу быть представлены двояким образом: один – с помощью матрицы $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$, а другой – с помощью матрицы $[\boldsymbol{I}_{[k]}\boldsymbol{R}_{[k\times(n-k)]}]$, полученной из указанной матрицы $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$ путём транспозиции строк последней; и при этом согласно определениям 1.9 и 1.10 речь уже идёт о двух различных кодах: систематическом и о несистематическом (общем коде).

7) Путём применения к порождающей матрице $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$ *элементарных операций* ***над строками и столбцами*** можно получить некоторое конечное число конкретных порождающих матриц типа $[\Xi_{k\times k}\,\boldsymbol{R}_{k\times(n-k)}]$, каждая из которых представляет один конкретный *асистематический код* (см. задачи 2.25 и 2.26).

8) Естественно, что аналогичные подсчёты могут быть выполнены применительно и к дуальному групповому $(n, n-k)$-коду.

2.6. ДЕКОДИРОВАНИЕ ПРИНЯТЫХ СООБЩЕНИЙ В СЛУЧАЕ ГРУППОВОГО (n, k)-КОДА ПРИМЕНИТЕЛЬНО К ДСК

СТАНДАРТНОЕ РАСПОЛОЖЕНИЕ И СИНДРОМНОЕ ДЕКОДИРОВАНИЕ

На вход кодера ДСК последовательно во времени поступают *равновероятные* сообщения $\boldsymbol{v}_i$, $i \in \{1, 2, \ldots, 2^k\}$; *на выходе кодера* ДСК, в соответствии с выражением (2-25), появляются кодовые комбинации $\boldsymbol{x}_i = \boldsymbol{y}_i$, $i \in \{1, 2, \ldots, 2^k\}$ группового (n, k)-кода C, поступающие затем *на вход* ДСК; а *на выходе* ДСК принимаются комбинация $\boldsymbol{y}_j$, $j \in \{1, 2, \ldots, 2^n\}$, поступающая далее *на вход декодера* ДСК (рис. 2.10а). Предположим, что $\boldsymbol{v}_1$ и $\boldsymbol{x}_1$ – нулевые вектора. Спрашивается, каким образом следует декодировать принятую комбинацию в переданную кодовую комбинацию?

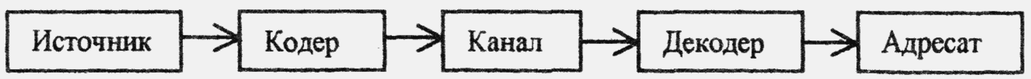

Рис. 2.10а. Система передачи сообщений

Ответ на поставленный вопрос предполагает: 1) указание критерия оптимальности декодирования и 2) указание алгоритма декодирования.

В качестве критерия оптимальности укажем критерий максимума средней вероятности правильного декодирования, а в качестве алгоритма декодирования укажем *алгоритм синдромного декодирования*.

Ниже мы изложим процедуру построения таблицы, которая применительно к групповым (n, k)-кодам называется «стандартным расположением» и может быть использована как таблица декодирования (см. «Таблица декодирования», подраздел 1.5; «Разложение группы по подгруппе», подраздел 2.1) [2.1, 2.2, 2.3].

ПРИМЕР 2.22

ОБОБЩЁННЫЙ ДСК

Согласно определению ДСК вероятности *искажения шумом* передаваемых по нему символов 1 и 0 равны одной и той же величине $e \geq 0$, которая удовлетворяет неравенствам:

$$1\text{-}e > e \qquad (2\text{-}68а)$$

(см. [2.2, с. 17]) и, следовательно,

$$0 \leq e < 0.5. \qquad (2\text{-}68б)$$

Заметим, что при стремлении мощности шума в канале к нулю вероятность $e \to 0$, а при неограниченном росте мощности шума в канале $e \to 0.5$. Конечно же, речь здесь идёт только о модели канала, не всегда адекватно отражающей свойства реальных каналов.

Мы обобщим это определение, включив в него также *инвертирующий* ДСК (рис. 2.10 b), для которого тоже потребуем выполнение условия (2-68а), а следовательно, и (2-68б).

Пусть при подаче на вход двоичного канала символов 1 или 0 и при $e \to 0$ с вероятностью 1 (эта единица стоит в индексе *условного обозначения* выходного символа канала) на его выходе получаются соответственно символы 1_1 (*условное*

обозначение выходного символа канала при поступлении на его вход символа 1) или 0_1 (*условное обозначение* выходного символа канала при поступлении на его вход символа 0); вообще говоря, при этом возможны два вида соответствия:

1) $1_1 = 1$ и $0_1 = 0$

или

2) $1_1 = 0$ и $0_1 = 1$.

ДСК Инвертирующий ДСК

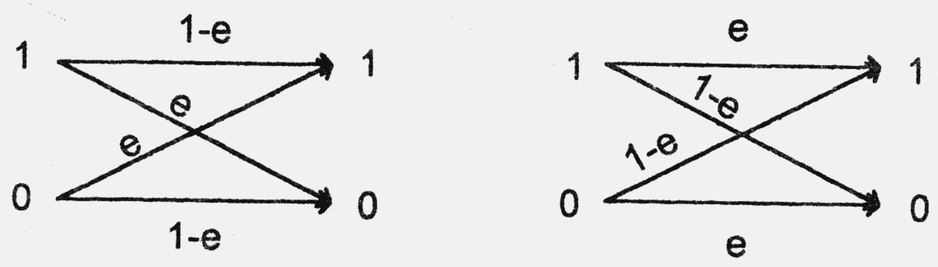

Рис. 2.10 b. ДСК и инвертирующий ДСК

В зависимости от вида соответствия 1) или 2) мы будем различать два канала:

соответствие 1): ДСК (*прямой или не инвертирующий*)

и

соответствие 2): *инвертирующий* ДСК (см. рис. 2.10 b).

Пусть p – некоторая переменная, удовлетворяющая неравенствам: $0 \le p \le 1$. Введём функцию (рис. 2.10 c):

$$e = e(p) = \begin{cases} p, & 0 \le p < 0.5, \\ 1 - p, & 0.5 \le p \le 1. \end{cases} \qquad \text{(2-68в)}$$

Используя введённые переменную p и функцию $e = e(p)$, можно оба канала – ДСК и инвертирующий ДСК – свести к одному каналу – *обобщённому* ДСК (рис. 2.10 d).

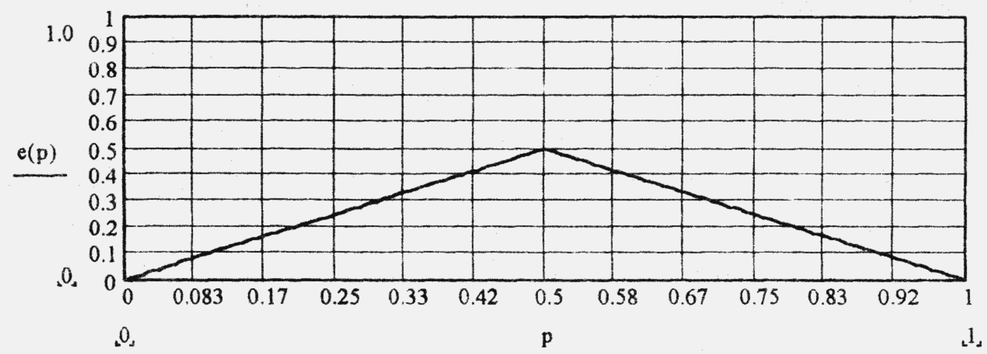

Рис. 2.10 c. Зависимость $e = e(p)$

В дальнейшем, под аббревиатурой ДСК без уточнений, будет подразумеваться ДСК (*прямой или неинвертирующий*).

Настоящий пример является ответом на сформулированный на с. 119 в [2.13] вопрос о канале, рассмотренном в задаче 6.9 из [2.13], в которой, таким образом, речь шла об *обобщённом* ДСК.

Обобщённый ДСК

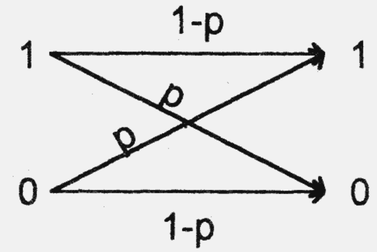

Рис. 2.10 d. Обобщённый ДСК, характеризуемый параметром p

END

! Рассмотренная трактовка функционирования ДСК носит принципиальный характер. Несколько иная трактовка функционирования ДСК при $0 \le p \le 1$ даётся в [2.19] на с. 337:

«Наибольшее значение (равное L) эта функция (*т.е. пропускная способность канала* – В.В.П.) принимает при $p =$

0 (т.е. при отсутствии помех) и при $p = 1$ (т.е. в случае помех, переводящих каждый передаваемый сигнал A_1 в A_2, а каждый сигнал A_2 – в A_1; ясно, что такие помехи нисколько не мешают понять, какой именно сигнал был передан)».

На самом же деле при $p = 1$ «помехи» *отсутствуют*, а преобразование передаваемого символа каналом в принимаемый – инверсия носит *не случайный, а детерминированный характер* и именно поэтому в канале отсутствует рассеяние информации.

↵

При построении стандартного расположения для группового (n, k)-кода применительно к ДСК следует учитывать, что *наиболее вероятными* ошибками в нём являются *низкократные* ошибки.

Стандартное расположение для группового (n, k)-кода строится следующим образом.

Пусть $\boldsymbol{x}_j$, $j = 1, 2, \ldots, 2^k$, – кодовые комбинации группового (n, k)-кода. Введём дополнительные обозначения для комбинаций, получаемых на выходе ДСК (т.е. для кодовых и запрещённых комбинаций).

Пусть $\boldsymbol{e}_1$ – нулевой вектор ошибки и $\boldsymbol{x}_1$ – нулевой кодовый вектор: $\boldsymbol{e}_1 = \boldsymbol{x}_1 = \mathbf{0}$.

В качестве *первой* строки такой таблицы выпишем последовательно слева направо все кодовые комбинации группового (n, k)-кода с нулевой кодовой комбинацией $\boldsymbol{x}_1$, слева для которых введём дополнительные обозначения:

$$\boldsymbol{y}_{1j} = \boldsymbol{x}_j + \boldsymbol{e}_1 = \boldsymbol{x}_j, \quad j = 1, 2, \ldots, 2^k. \qquad (2\text{-}68г)$$

Затем одна из комбинаций из B^n, не вошедших в ранее выписанную первую строку таблицы, *которую наиболее вероятно получить на выходе рассматриваемого ДСК при передаче по нему нулевой кодовой комбинации* $\boldsymbol{x}_1$ и которую мы обозначим, например, как $\boldsymbol{e}_2$, помещается в качестве первого – самого левого элемента *второй строки* под нулевым элементом $\boldsymbol{x}_1$ первой строки; далее *вторая строка* таблицы заполняется так, чтобы под каждой кодовой комбинацией $\boldsymbol{x}_j$ помещалась бы запрещённая комбинация

$$\boldsymbol{y}_{2j} = \boldsymbol{x}_j + \boldsymbol{e}_2, \quad j = 1, 2, \ldots, 2^k. \qquad (2\text{-}68д)$$

Аналогично строится третья, четвёртая и т.д.,

……

строка таблицы и, наконец, последняя 2^{n-k}-я строка таблицы:

$$\boldsymbol{y}_{2^{n-k}j} = \boldsymbol{x}_j + \boldsymbol{e}_{2^{n-k}}, \quad j = 1, 2, \ldots, 2^k. \qquad (2\text{-}68е)$$

После выписывания последней строки таблицы *все элементы* B^n оказываются помещёнными в таблицу – стандартное расположение, имеющую 2^k столбцов, 2^{n-k} строк и, следовательно, $2^k \cdot 2^{n-k} = |B^n| = 2^n$ элементов; причём каждый элемент B^n встречается в таблице *один и только один раз*.

Таким образом, все вектора из B^n в итоге получили единообразное обозначение $\boldsymbol{y}_{ij}$, $i = 1, 2, \ldots, 2^{n-k}$; $j = 1, 2, \ldots, 2^k$.

Из изложенного способа построения стандартного расположения в случае ДСК следует, что вес лидера любого смежного класса равен *минимальному весу* из множества весов всех комбинаций соответствующего ему смежного класса (т.е. вес лидера не больше веса никакой другой комбинации из соответствующего ему смежного класса), а вектора ошибок $\boldsymbol{e}_i$, $i = 1, 2, \ldots, 2^{n-k}$, находящиеся в первом столбце стандартного расположения, оказываются упорядоченными в соответствии с *законом не убывания* их веса с ростом i, считая сверху вниз.

Таблица 2. 8

$x_1+e_1=y_{11}=$ $=e_1=00000$	$x_2+e_1=y_{12}=$ $=01011$	$x_3+e_1=y_{13}=$ $=10110$	$x_4+e_1=y_{14}=$ $=11101$
$x_1+e_2=y_{21}=$ $=e_2=00001$	$x_2+e_2=y_{22}=$ 01010	$x_3+e_2=y_{23}$ 10111	$x_4+e_2=y_{24}=$ 11100
$x_1+e_3=y_{31}=$ $=e_3=00010$	$x_2+e_3=y_{32}=$ $=01001$	$x_3+e_3=y_{33}=$ 10100	$x_4+e_3=y_{34}=$ 11111
$x_1+e_4=y_{41}=$ $=e_4=00100$	$x_2+e_4=y_{42}=$ $=01111$	$x_3+e_4=y_{43}=$ 10010	$x_4+e_4=y_{44}=$ 11001
$x_1+e_5=y_{51}=$ $=e_5=01000$	$x_2+e_5=y_{52}=$ $=00011$	$x_3+e_5=y_{53}=$ 11110	$x_4+e_5=y_{54}=$ 10101
$x_1+e_6=y_{61}=$ $=e_6=10000$	$x_2+e_6=y_{62}=$ $=11011$	$x_3+e_6=y_{63}=$ 00110	$x_4+e_6=y_{64}=$ 01101
$x_1+e_7=y_{71}=$ $=e_7=11000$	$x_2+e_7=y_{72}=$ $=10011$	$x_3+e_7=y_{73}=$ $=01110$	$x_4+e_7=y_{74}=$ $=00101$
$x_1+e_8=y_{81}=$ $=e_8=01100$	$x_2+e_8=y_{82}=$ $=00111$	$x_3+e_8=y_{83}=$ $=11010$	$x_{14}+e_8=y_{84}=$ $=10001$

В качестве примера приведём табл. 2.8, являющуюся *стандартным расположением* для группового (5, 2)-кода с $d_{\min} = 3$ (см. пример 2.19, код (52)). В методических целях в табл. 2.8 помимо собственно кодовых комбинаций помещены дополнительные сведения, которые отсутствуют в окончательном варианте этого же самого стандартного расположения – в табл. 2.9.

Поясним ещё раз структуру стандартного расположения на примере таблицы 2.8:

первая, считая сверху вниз, строка содержит *все* 2^k кодовые комбинации группового (n, k)-кода;

первый, считая слева направо, столбец содержит 2^{n-k} векторов ошибок – только *одну* кодовую комбинацию – нулевую и все остальные – *запрещённые комбинации*;

ячейки таблицы, не входящие в первую строку, содержат только *запрещённые комбинации*;

в верхнем левом углу таблицы расположен элемент $e_1 = x_1 = \mathbf{0}$.

Таблица 2. 9

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

Конкретное стандартное расположение для заданного конкретного группового (5, 2)-кода {00000, 01011, 10110, 11101} строится следующим образом. Для единообразия элементы построенной таблицы обозначим как y_{ij}, $i = 1, 2, \ldots, 2^3$; $j = 1, 2, 3, 2^2$.

Согласно ранее сказанному, построенная табл. 2.9 является разложением аддитивной абелевой группы B^n по подгруппе – групповому (5, 2)-коду; подобное разложение играет большую роль при синдромном декодировании принятых комбинаций и лежит в его основе. Очевидно, что строки табл. 2.9 являются смежными классами разложения, а самые левые элементы каждой строки – образующими элементами или лидерами смежных классов. Легко убедится, что лидер любого смежного класса имеет минимальный вес среди всех комбинаций соответствующего ему смежного класса, а вес векторов e_i с ростом i монотонно не убывает.

ДЕКОДИРОВАНИЕ С ПОМОЩЬЮ СТАНДАРТНОГО РАСПОЛОЖЕНИЯ

Если на вход канала поступил вектор $\boldsymbol{x}$, а на выходе канала был принят вектор $\boldsymbol{y}$, то *вектор ошибки* $\boldsymbol{e} = \boldsymbol{y} + \boldsymbol{x}$.

ТЕОРЕМА 2.12. *Если в качестве таблицы декодирования для группового* (n, k)*-кода используется его стандартное расположение, то по полученному вектору* $\boldsymbol{y}$ *переданный кодовый вектор* $\boldsymbol{x}$ *будет декодирован правильно в том и только в том случае, если вектор ошибки* $\boldsymbol{e} = \boldsymbol{y} + \boldsymbol{x}$ *является лидером смежного класса, которому принадлежит* $\boldsymbol{y}$.

ДОКАЗАТЕЛЬСТВО.

ДОСТАТОЧНОСТЬ. Пусть при передаче кодового вектора $\boldsymbol{x}$ был получен вектор $\boldsymbol{y}$ и реализовался некоторый вектор ошибки $\boldsymbol{e}_i = \boldsymbol{y} + \boldsymbol{x}$, совпадающий с лидером смежного класса, которому принадлежит $\boldsymbol{y}$. Требуется доказать, что в этом случае декодирование с помощью стандартного расположения, используемого в качестве таблицы декодирования, будет правильным.

В этом случае вектор $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}_i$ должен находится в i-м смежном классе стандартного расположения под кодовым словом $\boldsymbol{x}$ и, следовательно, будет декодирован правильно в $\boldsymbol{x}$ с помощью стандартного расположения, используемого в качестве таблицы декодирования.

НЕОБХОДИМОСТЬ. Пусть при передаче кодового вектора $\boldsymbol{x}$ был получен вектор $\boldsymbol{y}$ и реализовался некоторый вектор ошибки $\boldsymbol{e}_i = \boldsymbol{y} + \boldsymbol{x}$, не совпадающий с $\boldsymbol{e}_s$ – лидером смежного класса, которому принадлежит $\boldsymbol{y}$: $\boldsymbol{e}_i \neq \boldsymbol{e}_s$. Требуется доказать, что в этом случае принятый вектор $\boldsymbol{y}$ не может быть декодирован правильно с помощью стандартного расположения, используемого в качестве таблицы декодирования.

Так как согласно сделанному допущению $\boldsymbol{e}_i \neq \boldsymbol{e}_s$, то $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}_i \neq \boldsymbol{x} + \boldsymbol{e}_s$, и, следовательно, правильное декодирование

вектора $\boldsymbol{y}$ с помощью стандартного расположения, используемого в качестве таблицы декодирования, невозможно.

ЧТД

Как уже говорилось, групповой (n, k)-код может быть задан либо порождающей матрицей $\boldsymbol{G}_{(n,\,k)}$, либо проверочной матрицей $\boldsymbol{H}_{(n,\,k)}$. Будем далее считать, что обе эти матрицы имеют каноническую форму. Если полученный на выходе канала вектор $\boldsymbol{y}$ является кодовым или не кодовым вектором, то синдромом этого вектора называется соответственно нулевой или не нулевой вектор или матрица-строка $\boldsymbol{S}$ размерности $1\times(n-k)$

$$\boldsymbol{y}\boldsymbol{H}^{\mathrm{T}}_{(n,k)} = \boldsymbol{S}; \qquad (2\text{-}69)$$

каждая компонента вектора $\boldsymbol{S}$ *соответствует проверке на ортогональность* вектора $\boldsymbol{y}$ некоторому вектору-столбцу матрицы $\boldsymbol{H}^{\mathrm{T}}_{(n,k)}$ или соответствующему вектору-строке матрицы $\boldsymbol{H}_{(n,\,k)}$; причём, если проверка удовлетворяется, то соответствующая компонента $\boldsymbol{S}$ равна нулю, если же проверка не удовлетворяется, то эта компонента $\boldsymbol{S}$ не равна нулю.

ТЕОРЕМА 2.13. *Два вектора* $\boldsymbol{y}_1$ и $\boldsymbol{y}_2$ *принадлежат одному и тому же смежному классу стандартного расположения тогда и только тогда, когда их синдромы равны.*

ДОКАЗАТЕЛЬСТВО.

ДОСТАТОЧНОСТЬ. Предположим, что синдромы векторов $\boldsymbol{y}_1$ и $\boldsymbol{y}_2$ равны:

$$\boldsymbol{y}_1\,\boldsymbol{H}^{\mathrm{T}}_{(n,k)} = \boldsymbol{y}_2\,\boldsymbol{H}^{\mathrm{T}}_{(n,k)}\,. \qquad (2\text{-}70)$$

Требуется доказать, что оба эти вектора принадлежат одному и тому же смежному классу стандартного расположения.

Из (2-70) следует

$$(\boldsymbol{y}_1 - \boldsymbol{y}_2)\boldsymbol{H}^{\mathrm{T}}_{(n,k)} = \boldsymbol{0} \qquad (2\text{-}71)$$

и, следовательно, (y_1 - y_2) является *кодовым вектором*. Поэтому, согласно теореме 2.2, y_1 и y_2 принадлежат одному и тому же смежному классу.

НЕОБХОДИМОСТЬ. Пусть векторы y_1 и y_2 принадлежат одному и тому же смежному классу стандартного расположения. Требуется доказать, что синдромы векторов y_1 и y_2 равны: $y_1 H^{T}_{(n,k)} = y_2 H^{T}_{(n,k)}$.

Так как векторы y_1 и y_2 принадлежат одному и тому же смежному классу стандартного расположения, то, согласно теореме 2.2, (y_1 - y_2) является *кодовым вектором* и, следовательно, его синдром равен нулю: $(y_1 - y_2)H^{T}_{(n,k)} = \mathbf{0}$, откуда следует:

$$y_1 H^{T}_{(n,k)} = y_2 H^{T}_{(n,k)} . \qquad (2\text{-}71а)$$

ЧТД

1) Из способа построения стандартного расположения группового (n, k)-кода следует, что оно имеет 2^{n-k} различных смежных классов и столько же *различных лидеров смежных классов* e_i, $i = 1, 2, \ldots, 2^{n-k}$. Каждый синдром $S = S(y)$ является двоичной кодовой комбинацией длины $n - k$ и, следовательно, число всевозможных различных синдромов равно 2^{n-k}. Таким образом, с учётом доказанной теоремы 2.13, можно утверждать, что каждому смежному классу, а следовательно, и его лидеру соответствует свой индивидуальный синдром.

2) С другой стороны теорема 2.13 фактически также утверждает, что синдром S=$S(y)$ принятого вектора y *однозначно определяет* ***смежный класс***, которому принадлежит y, а следовательно, *однозначно определяет* и ***лидера*** этого смежного класса, являющегося одним из представителей смежного класса; т.е. каждому конкретному синдрому S соответствует свой индивидуальный смежный класс и его лидер.

Из 1) и 2) вытекает, что существует взаимно однозначное соответствие:

$$S(y_{i\,j}) \Leftrightarrow e_i, \; i = 1, 2, \ldots, 2^{n-k}. \qquad (2\text{-}71б)$$

Синдром S некоторого конкретного смежного класса, определённый, например, по его лидеру, соответствует всем представителям этого смежного класса и, следовательно, не определяет однозначно его представителей; однако S однозначно определяет сам смежный класс и, следовательно, его лидера.

Рассмотрим вопрос декодирования принятых комбинаций с помощью стандартного расположения. Как уже отмечалось, стандартное расположение может быть использовано в *качестве таблицы декодирования*. Однако оно может быть положено также в основу *синдромного декодирования*.

При синдромном декодировании некоторого полученного на выходе ДСК вектора y выполняются следующие операции:

сначала в соответствии с выражением (2-69) определяется соответствующий ему *однозначным образом* синдром $S = S(y)$ (теорема 2.12);

затем по найденному синдрому S с помощью *взаимно однозначного соответствия* (2-71б) определяется лидер e смежного класса, к которому принадлежит полученный вектор y (и лидер e);

и, наконец, определяется переданный кодовый вектор:

$$x = y + e. \qquad (2\text{-}72)$$

Табл. 2.10 иллюстрирует сказанное применительно к групповому (5, 2)-коду.

ПРИМЕР 2.23

Ниже, на рис. 2.11 приведена написанная в пакете Mathcad программа декодирования принятой комбинации y и результат её декодирования в кодовую комбинацию x для группового (5, 2)-кода, имеющего $d_{min} = 3$, стандартное расположение, приведенное в табл. 2.10, и используемого с ДСК.

Таблица 2.10

00000 ***S***=000	01011	10110	11101
00001 ***S***=001	01010	10111	11100
00010 ***S***=010	01001	10100	11111
00100 ***S***=100	01111	10010	11001
01000 ***S***=011	00011	11110	10101
10000 ***S***=110	11011	00110	01101
11000 ***S***=101	10011	01110	00101
01100 ***S***=111	00111	11010	10001

РАБОТА ПРОГРАММЫ СИНДРОМНОГО ДЕКОДИРОВАНИЯ ДЛЯ (5-2)-КОДА ПРИ y = (0 1 1 0 1)

Приведенная ниже на рис. 2.11 программа иллюстрирует процесс синдромного декодирования принятой *запрещённой* комбинации y = (0 1 1 0 1) в переданную *кодовую* комбинацию x = (1 1 1 0 1) искажённую ошибкой, описываемой вектором e = (1 0 0 0 0):

$$(0\ 1\ 1\ 0\ 1) = (1\ 1\ 1\ 0\ 1) \oplus (1\ 0\ 0\ 0\ 0).$$

Заметим, что не все ошибки веса 2 (и более) исправляются с помощью рассмотренной только что программы синдромного декодирования, так как рассматриваемый групповой (5, 2)-код гарантийно исправляет лишь однократные ошибки e, в то время как $w(e_7)=w(e_8)=2 > 1$ (см. табл. 2.8, 2.10).

Принятая комбинация:

$y := (0\ 1\ 1\ 0\ 1)$

$$H := \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$S(y) := y \cdot H^T$

$S := S(y) \qquad i := 1..3$

$S_{1,i} := \mathrm{mod}(S_{1,i}, 2)$

$$G := \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$e(S) := \begin{cases} (0\ 0\ 0\ 0\ 0) \text{ if } S = (0\ 0\ 0) \\ (0\ 0\ 0\ 0\ 1) \text{ if } S = (0\ 0\ 1) \\ (0\ 0\ 0\ 1\ 0) \text{ if } S = (0\ 1\ 0) \\ (0\ 0\ 1\ 0\ 0) \text{ if } S = (1\ 0\ 0) \\ (0\ 1\ 0\ 0\ 0) \text{ if } S = (0\ 1\ 1) \\ (1\ 0\ 0\ 0\ 0) \text{ if } S = (1\ 1\ 0) \\ (1\ 1\ 0\ 0\ 0) \text{ if } S = (1\ 0\ 1) \\ (0\ 1\ 1\ 0\ 0) \text{ if } S = (1\ 1\ 1) \end{cases}$$

$S = (1\ 1\ 0)$

$Sr := G \cdot H^T$

$i := 1..2 \qquad j := 1..3$

$Sr_{i,j} := \mathrm{mod}(Sr_{i,j}, 2)$

$$Sr = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$e(S) = (1\ 0\ 0\ 0\ 0) \qquad x := y + e(S) \qquad j := 1..5$

$x_{1,j} := \mathrm{mod}(x_{1,j}, 2)$

Результат декодирования:

$x = (1\ 1\ 1\ 0\ 1)$

Рис. 2.11. Программа декодирования

Программа в рассматриваемом случае безупречно отработала заложенный в неё алгоритм декодирования:

она правильно определила по принятой комбинации y = (01101) синдром S = (110);

правильно определила по синдрому лидера смежного класса e_6 =(10000), которому принадлежит принятая комбинация y;

и, согласно заложенному в неё алгоритму декодирования,

правильно нашла результат декодирования – кодовую комбинацию $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{e}_6 = =(11101)$,

что с *наибольшей вероятностью* соответствует действительности (см. табл. 2.10).

END

ПРИМЕР 2.24. Допустим, что на вход ДСК поступила *кодовая комбинация* $\boldsymbol{x} = (10110)$, а в канале имела место ошибка $\boldsymbol{e} = (01001)$ веса $w(\boldsymbol{e}) = 2$. Согласно ниже приведенной распечатке результата работы уже упоминавшейся программы полученная на выходе ДСК комбинация (11111) будет неправильно декодирована в не передававшуюся комбинацию (11101).

Очевидно, что описанный только что пример неправильного декодирования не противоречит излагаемой концепции синдромного декодирования, так как приведенный случай ошибочного декодирования при возникновении *двукратной* ошибки $\boldsymbol{e} = (01001)$ реализуется существенно реже по сравнению со случаем возникновения *однократной* ошибки $\boldsymbol{e} = (00010)$ – лидера смежного класса, которому принадлежит принятая комбинация (11111), если только учесть соотношение вероятностей возникновения *однократных* и *двукратных* ошибок (предполагается, что вероятность искажения двоичных символов в ДСК $p_0 << 1$). Поэтому в подавляющем большинстве случаев описанное *синдромное декодирование* конкретной принятой комбинации (11111) окажется *правильным.*

Следует также отметить, что на приёмном конце канала неизвестен вектор двукратной ошибки $\boldsymbol{e} = (01001)$, в действительности возникшей в канале вследствие действия в нём шума, а известна лишь принятая комбинация (11111); этих же данных достаточно только для осуществления синдромного декодирования, но не достаточно для осуществления правильного декодирования в случае двукратной ошибки в рассматриваемом примере.

Теорема 2.12 объясняет эту ситуацию. Вопреки условию этой теоремы имевшая место в ДСК *двукратная* ошибка $\boldsymbol{e} = (01001)$, реально имевшая место в канале, не равна лидеру (00010) смежного класса, которому принадлежит принятая комбинация $\boldsymbol{y} = (11111)$.

Однако, если в ДСК имела, например, место *двукратная* ошибка (11000), то в соответствии с теоремой 2.12 любая принятая комбинация $\boldsymbol{y}$ из седьмого (считая сверху вниз) смежного класса с помощью синдромного метода декодирования будет декодирована правильно.

Аналогично, если в канале имела место *двукратная* ошибка (01100), то в соответствии с теоремой 2.12 любая принятая комбинация $\boldsymbol{y}$ из восьмого (считая сверху вниз) смежного класса с помощью синдромного метода декодирования также будет декодирована правильно.

На рис. 2.12 приведена программа декодирования принятой комбинации, содержащей двукратную ошибку.

РАБОТА ПРОГРАММЫ СИНДРОМНОГО ДЕКОДИРОВАНИЯ ДЛЯ (5-2)-КОДА ПРИ $\boldsymbol{y}$ = (1 1 1 1 1)

При $i \le I_m \le 2^{n-k}$, где

$$I_m = \sum_{j=1}^{t} C_n^j , \qquad (2\text{-}72a)$$

$t = \left]\frac{d_{\min} - 1}{2}\right[$, обеспечено гарантированное исправление ошибок, определяемых векторами $\boldsymbol{e}_i$. I_m делит множество векторов ошибок стандартного расположения на два подмножества, первое из которых (считая сверху вниз) соответствует гарантийно исправляемым ошибкам. Использование I_m даёт воз-