Таким образом, каждому конкретному (n, k)-коду, являющемуся k-мерным подпространством B^n, соответствует $N_{(k)}$ *различных базисов*, каждый из которых является k-набором ненулевых линейно независимых кодовых комбинаций в B^n.

Поэтому очевидно, что

$$N_{[1]} = N_{(n,\,k)} N_{(k)}$$

и, следовательно, число различных (n, k)-кодов в B^n

$$N_{(n,k)} = \frac{N_{[1]}}{N_{(k)}} = \frac{(2^n - 1)(2^n - 2)(2^n - 2^2) \ \ldots \ (2^n - 2^{k-1})}{(2^k - 1)(2^k - 2)(2^k - 2^2) \ \ldots \ (2^k - 2^{k-1})}. \quad (2\text{-}28)$$

END

ПРИМЕР 2.18. Ниже на рис. 2.7 приведены все 7 ($N_{(3,2)} = 7$) *возможных кодовых матриц* $\mathbf{C}_{(3,\,2)}$. *Сделаем важное замечание: эти семь приведенных матриц имеют* ***различные*** *множества строк - т.е. множества строк, отличающиеся хотя бы одним элементом-строкой*, таким образом, число $N_{(3,2)} = 7$ действительно определяет число всевозможных *различных* групповых (3, 2)-кодов.

Заметим, что (3, 2)-код, соответствующий седьмой матрице, считая слева направо и сверху вниз, имеет наибольшее значение $d_{\min} = 2$; остальные коды имеют $d_{\min} = 1$.

Первая, вторая и четвёртая матрицы имеют по нулевому столбцу. Таким образом, общетеоретическая формула (2-28) определяет $N_{(n,\,k)}$ – число всевозможных различных групповых (n, k)-кодов, включая коды, кодовые матрицы которых, а, следовательно, порождающие матрицы, вообще говоря, могут иметь нулевые столбцы. Однако нулевые столбцы в этих матрицах могут быть вычеркнуты, благодаря чему могут быть получены новые преобразованные коды без уменьшения $d_{\min}$; при этом скорость $R = k/n$ увеличится. Поэтому

порождающие и кодовые матрицы реально используемых для передачи сообщений кодов *не имеют нулевых столбцов.*

N1

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

N2

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

N3

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

N4

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

N5

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

N6

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

N7

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Рис. 2.7. Семь всевозможных (3, 2)-кодов

Каждому из кодов № 4, …, №7 может быть поставлена в соответствие *одна индивидуальная порождающая матрица в канонической форме* (каждая такая матрица приведена под соответствующей кодовой матрицей). Трём кодам – № 1, № 2 и № 3 не соответствует ни одной индивидуальной матрицы в канонической форме и, следовательно, эти коды являются *асистематическими.*

Таким образом, число различных систематических (3, 2)-кодов выражается соотношением

$$N^{cuc}_{(n,k)} = 2^{k(n-k)} = 2^2 = 4, \qquad (2\text{-}29)$$

коды № 4 – № 7, а число *асистематических кодов* – соотношением

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

$$= \frac{(2^n-1)(2^n-2)(2^n-2^2)\ \ldots\ (2^n-2^{k-1})}{(2^k-1)(2^k-2)(2^k-2^2)\ \ldots\ (2^k-2^{k-1})} - 2^{k(n-k)} = 7 - 4 = 3, \qquad (2\text{-}30)$$

коды № 1, № 2 и № 3 (см. задачи 2.8, 2.25, 2.26). Таким образом, доказано, что класс *асистематических кодов* ***не пуст***.

Половина кодовых слов кодов № 1 – № 6 имеют нечётный вес и половина – чётный; все кодовые комбинации кода № 7 имеют чётный вес.

END

ГРУППОВОЙ (n, k)-КОД И ЕГО КОРРЕКТИРУЮЩИЕ СВОЙСТВА

Следующая теорема упрощает определение корректирующих свойств групповых (n, k)-кодов.

ТЕОРЕМА 2.7. *Минимальное хэммингово расстояние группового (n, k)-кода равно минимальному весу его ненулевых кодовых комбинаций*

$$d_{\min} = \min_{i \mid w(\boldsymbol{v}_i)>0} w(\boldsymbol{v}_i). \qquad (2\text{-}31)$$

ДОКАЗАТЕЛЬСТВО. Действительно, так как $d(\boldsymbol{v}_s, \boldsymbol{v}_r) = w(\boldsymbol{v}_s+\boldsymbol{v}_r)$, $s \neq r$, то, из наличия группового свойства замкнутости следует, что $(\boldsymbol{v}_s+\boldsymbol{v}_r)$ есть также некоторая кодовая комбинация $\boldsymbol{v}_i \neq \boldsymbol{0}$ рассматриваемого группового (n, k)-кода. Поэтому $d(\boldsymbol{v}_s, \boldsymbol{v}_r) = w(\boldsymbol{v}_i)$,

$$\min_{s,r \mid s \neq r} d(\boldsymbol{v}_s, \boldsymbol{v}_r) = \min_{i \mid w(\boldsymbol{v}_i)>0} w(\boldsymbol{v}_i) \qquad (2\text{-}32)$$

и, следовательно,

$$d_{\min} = \min_{i \mid w(\boldsymbol{v}_i)>0} w(\boldsymbol{v}_i). \qquad (2\text{-}33)$$

ЧТД

Для определения $d_{\min}$, согласно доказанной теореме, необходим *тотальный перебор* весов кодовых комбинаций. Естественно, что возникает вопрос о существовании другого более эффективного метода определения $d_{\min}$. Несколько позже мы вернёмся к этому вопросу.

ОПИСАНИЕ ГРУППОВЫХ (n, k)-КОДОВ С ПОМОЩЬЮ ПРОВЕРОЧНЫХ МАТРИЦ

Мы уже знакомы с двумя возможными способами описания группового (n, k)-кода:

1) перечисление всех 2^k сообщений, подлежащих передаче, перечисление всех 2^k кодовых комбинаций и задание взаимно однозначного отображения между ними;

2) использование порождающей матрицы $\boldsymbol{G}_{(n,\,k)}$.

Естественен вопрос о существовании другого способа описания группового (n, k)-кода описания с помощью матрицы $\boldsymbol{H}_{(n,\,k)}$ и о его сравнительных характеристиках.

Оказывается, что существует ещё один способ описания группового (n, k)-кода с помощью *проверочной матрицы* $\boldsymbol{H}_{(n,\,k)}$, имеющей размерность $(n - k)\times n$.

Переходим к описанию *систематического (n, k)-кода с проверкой на чётность* с помощью матрицы $\boldsymbol{H}_{(n,\,k)}$. Поясним организацию структуры проверочной матрицы $\boldsymbol{H}_{(n,\,k)}$ систематического (n, k)-кода, порождающая матрица которого имеет каноническую форму: $\boldsymbol{G}_{(n,\,k)} = [\boldsymbol{I}_k\ \boldsymbol{R}_{k\times(n-k)}]$ и, следовательно,

первые k разрядов (позиций, знакомест) каждой кодовой комбинации являются *информационными*, а $r = (n - k)$ последних разрядов являются *проверочными*; символы (или элементы) кодовых комбинаций, в зависимости от занимаемых ими позиций, имеют *аналогичные* названия.

Матрица $\boldsymbol{H}_{(n,\,k)}$ состоит из $(n - k)$ строк, каждая из которых содержит закон формирования *одного* из $(n - k)$ проверочных элементов.

Единицы, стоящие в первых k позициях каждой конкретной строки $\boldsymbol{H}_{(n,\,k)}$, указывают местоположение информационных элементов любой кодовой комбинации, участвующих в формировании одного её проверочного элемента, местоположение которого указывается единственной единицей, стоящей в последних $(n - k)$ позициях этой же самой конкретной строки $\boldsymbol{H}_{(n,\,k)}$.

Так как в каждом из последних $(n - k)$ столбцах матрицы $\boldsymbol{H}_{(n,\,k)}$ имеется в точности по одной единице, и в последних $(n - k)$ позициях каждой строки $\boldsymbol{H}_{(n,\,k)}$ имеется в точности по одной единице, то ранг матрицы $\boldsymbol{H}_{(n,\,k)}$ равен $(n - k)$ и, следовательно, её строки, рассматриваемые как вектора, являются линейно независимыми векторами. Легко видеть, что, применяя элементарные операции *к строкам матрицы* $\boldsymbol{H}_{(n,\,k)}$, её всегда можно за конечное число шагов привести к *канонической форме*:

$$\boldsymbol{H}_{(n,k)} = \left[\boldsymbol{P}^{\mathrm{T}}_{k\times(n-k)} \boldsymbol{I}_{(n-k)} \right], \qquad (2\text{-}34)$$

где $\boldsymbol{P}^{\mathrm{T}}_{k\times(n-k)}$ – некоторая матрица (см. ниже), образованная первыми k позициями строк матрицы $\boldsymbol{H}_{(n,\,k)}$. Первые k позиций каждой конкретно рассматриваемой строки матрицы $\boldsymbol{H}_{(n,\,k)}$ содержат единицы, указывающие местоположение информационных элементов любой кодовой комбинации, участвующих в формировании одного проверочного элемента, местоположение которого указывается единственной единицей, стоящей в последних $(n - k)$ позициях каждой конкретно рассматриваемой строки $\boldsymbol{H}_{(n,\,k)}$.

Из (2-34) следует, что $\boldsymbol{H}_{(n,\,k)}$ может рассматриваться как *порождающая матрица* некоторого нового группового $(n, n - k)$-кода, имеющего $N_{(n,\,n-k)} = 2^{n-k}$ кодовых комбинаций; а $\boldsymbol{G}_{(n,\,k)}$ – как проверочная матрица этого нового кода. Этот новый групповой $(n, n - k)$-код называют *двойственным* или *дуальным* кодом к исходному групповому (n, k)-коду.

Согласно приведенному описанию структуры матрицы $\boldsymbol{H}_{(n,\,k)}$, можно утверждать, что каждая её строка и каждая строка порождающей матрицы $\boldsymbol{G}_{(n,\,k)}$, рассматриваемые как вектора, являются взаимно ортогональными; то же самое можно сказать и о любой ненулевой комбинации исходного (n, k)-кода и о любой ненулевой комбинации двойственного к нему $(n, n - k)$-кода – они взаимно ортогональны.

Часто двойственный к исходному (n, k)-коду групповой $(n, n - k)$-код называют *нулевым пространством* (n, k)-кода или порождающей матрицы $\boldsymbol{G}_{(n,\,k)}$.

Аналогично, групповой (n, k)-код является *двойственным* или *дуальным* к групповому $(n, n - k)$-коду и его (или матрицы $\boldsymbol{H}_{(n,\,k)}$) *нулевым пространством*.

В табл. 1.1 содержится простейший пример двух двоичных дуальных друг к другу групповых (n, k)- и $(n, n - k)$-кодов с проверкой на чётность:

код с многократной передачей символов (код с повторением) – (5, 1)-код;

код с однократной проверкой на чётность – (5, 4)-код.

ПРИМЕР 2.19. Рассмотрим матричное описание (5, 3)-кода и некоторых его свойств (рис. 2.8). По техническим причинам (свойства пакета Mathcad) обозначения на этом рисунке несколько отличаются от обозначений, введённых нами.

Здесь g – порождающая матрица, а h – проверочная матрица исследуемого (5, 3)-кода.

g - порождающая матрица; h - проверочная матрица (5, 3)-кода

$$n := 5 \qquad k := 3$$

$$g := \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \qquad h := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$s := g \cdot h^T \qquad p := 1..k \qquad q := 1..(n-k) \qquad c := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

$$s_{p,q} := mod(s_{p,q}, 2)$$

$$s = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad d := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

$$w := c \cdot h^T$$

$$z := 1..2^k \qquad e := 1..n$$

$$w_{z,e} := mod(w_{z,e}, 2)$$

$$x := c \cdot d^T$$

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

$$i := 1..2^k \qquad j := 1..2^{(n-k)}$$

$$x_{i,j} := mod(x_{i,j}, 2)$$

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

Рис. 2.8. (5, 3)-код и некоторые его свойства

Нулевая матрица $s = g \cdot h^T$ иллюстрирует свойство взаимной ортогональности векторов-строк порождающей матрицы g и векторов-строк проверочной матрицы h.

Кодовые матрицы c и d представляют два взаимно дуальных кода: (5, 3)-кода и (5, 2)-кода.

Нулевая матрица $w = c \cdot h^T$ иллюстрирует свойство взаимной ортогональности векторов-строк группового (5, 3)-кода и векторов-строк проверочной матрицы h.

Нулевая матрица $x = c \cdot d^T$ иллюстрирует свойство взаимной ортогональности векторов-строк двух взаимно дуальных кодов: (5, 3)-кода и (5, 2)-кода.

Необходимо обратить внимание на то обстоятельство, что два взаимно дуальных (5, 3)- и (5, 2)-кода (матрицы c и d) помимо *общего нулевого элемента* (0 0 0 0 0) имеют ещё один *общий ненулевой элемент* (1 0 1 1 1) – *кодовая комбинация чётного веса ортогональная сама себе*.

Отметим также, что (5, 3)-код имеет $d_{\min} = 2$, а минимальное хэммингово расстояние дуального к нему (5, 2)-кода $d^*_{min} = 3$. При этом минимальное число линейно зависимых столбцов матрицы $h = \boldsymbol{H}_{(5,\,3)}$ равно $d_{\min} = 2$ (например, столбцы первый и четвёртый; при этом любая совокупность столбцов, состоящая из $d_{\min} - 1 = 1$ столбца, является совокупностью линейно независимых столбцов); минимальное число линейно зависимых столбцов матрицы $g = \boldsymbol{G}_{(5,\,3)}$ равно $d^*_{\min} = 3$ (например, столбцы первый, второй и четвёртый; при этом любая совокупность столбцов, состоящая из $d^*_{\min} - 1 = 2$ столбцов, является совокупностью линейно независимых столбцов; см. теорему 2.9).

END

ТЕОРЕМА 2.8. *Пусть порождающая матрица некоторого группового (n, k)-кода задана в канонической форме*

$$\boldsymbol{G}_{(n,\,k)} = [\boldsymbol{I}_k\, \boldsymbol{R}_{k\times(n-k)}]. \qquad (2\text{-}35)$$

*Для того, чтобы матрица $\boldsymbol{H}_{(n,\,k)}$ являлась бы проверочной матрицей этого систематического (n, k)-кода в канонической форме, **необходимо и достаточно**, чтобы она имела вид:*

$$\boldsymbol{H}_{(n,\,k)} = [\boldsymbol{R}^{\mathrm{T}}{}_{k\times(n-k)}\, \boldsymbol{I}_{(n-k)}]. \qquad (2\text{-}36)$$

ДОКАЗАТЕЛЬСТВО.

ДОСТАТОЧНОСТЬ. Дано: $\boldsymbol{H}_{(n,\,k)}$ удовлетворяет соотношению (2-36). Требуется доказать, что в этом случае выполняется соотношение:

$$\boldsymbol{G}_{(n,\,k)}\boldsymbol{H}^{\mathrm{T}}{}_{(n,\,k)} = \boldsymbol{S}, \qquad (2\text{-}37)$$

где $\boldsymbol{S}$ – нулевая матрица размерности $k\times(n\text{-}k)$, и, следовательно, $\boldsymbol{H}_{(n,\,k)}$ является проверочной матрицей группового (n, k)-кода.

Подставим выражения для матриц $\boldsymbol{G}_{(n,\,k)}$ и $\boldsymbol{H}_{(n,\,k)}$ в канонической форме в левую часть (2-37):

$$[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]\begin{bmatrix}\boldsymbol{R}_{k\times(n-k)}\\ \boldsymbol{I}_{(n-k)}\end{bmatrix} =$$

$$= \begin{array}{|l|l|}\hline 1\,0\,0\,\ldots\,0\,r_{11}\,r_{12}\,\ldots\,r_{1(n-k)} & r_{11}\,r_{12}\,\ldots\,r_{1(n-k)}\\ 0\,1\,0\,\ldots\,0\,r_{21}\,r_{22}\,\ldots\,r_{2(n-k)} & r_{21}\,r_{22}\,\ldots\,r_{2(n-k)}\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\\ 0\,0\,0\,\ldots\,1\,r_{k1}\,r_{k2}\,\ldots\,r_{k(n-k)} & r_{k1}\,r_{k2}\,\ldots\,r_{k(n-k)}\\ \hline \end{array} = \begin{array}{|l|}\hline r_{11}\,r_{12}\,\ldots\,r_{1(n-k)}\\ r_{21}\,r_{22}\,\ldots\,r_{2(n-k)}\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ r_{k1}\,r_{k2}\,\ldots\,r_{k(n-k)}\\ 1\,0\,0\,0\,\ldots\,0\,0\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ 0\,0\,0\ldots\,0\,0\,0\,1\\ \hline \end{array} = \boldsymbol{Q}, \qquad (2\text{-}38)$$

где $\boldsymbol{Q}$ – *некоторая* матрица размерности $k\times(n - k)$. Необходимо доказать, что $\boldsymbol{Q} = \boldsymbol{S}$.

Из (2-38) имеем

$$q_{i,j} = (r_{i,j} + r_{i,j}) \equiv 0, \mod 2, \qquad (2\text{-}39)$$
$$i = 1, 2, \ldots, k;\ \ j = 1, 2, \ldots, (n - k);$$

и, следовательно, $\boldsymbol{Q} = \boldsymbol{S}$.

НЕОБХОДИМОСТЬ. Дано: выполняется соотношение (2-37). Требуется доказать, что имеет место (2-36).

Пусть имеет место соотношение

$$\boldsymbol{H}_{(n,\,k)} = [\boldsymbol{P}^{\mathrm{T}}{}_{k\times(n-k)}\, \boldsymbol{I}_{(n-k)}], \qquad (2\text{-}40)$$

где $\boldsymbol{P}_{k\times(n-k)}$ – *некоторая* матрица размерности $k\times(n\text{-}k)$. Требуется доказать, что $\boldsymbol{P}_{k\times(n-k)} = \boldsymbol{R}_{k\times(n-k)}$.

Подставим выражения для матриц $\boldsymbol{G}_{(n,\,k)}$ и $\boldsymbol{H}_{(n,\,k)}$ из (2-35) и (2-40) в (2-37):

$$[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]\begin{bmatrix}\boldsymbol{P}_{k\times(n-k)}\\ \boldsymbol{I}_{(n-k)}\end{bmatrix} =$$

$$= \begin{array}{|l|l|}\hline 1\,0\,0\,\ldots\,0\,r_{11}\,r_{12}\,\ldots\,r_{1(n-k)} & p_{11}\,p_{12}\,\ldots\,p_{1(n-k)}\\ 0\,1\,0\,\ldots\,0\,r_{21}\,r_{22}\,\ldots\,r_{2(n-k)} & p_{21}\,p_{22}\,\ldots\,p_{2(n-k)}\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\\ 0\,0\,0\,\ldots\,1\,r_{k1}\,r_{k2}\,\ldots\,r_{k(n-k)} & p_{k1}\,p_{k2}\,\ldots\,p_{k(n-k)}\\ \hline \end{array} = \begin{array}{|l|}\hline p_{11}\,p_{12}\,\ldots\,p_{1(n-k)}\\ p_{21}\,p_{22}\,\ldots\,p_{2(n-k)}\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ p_{k1}\,p_{k2}\,\ldots\,p_{k(n-k)}\\ 1\,0\,0\,0\,\ldots\,0\,0\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ 0\,0\,0\,\ldots\,0\,0\,0\,1\\ \hline \end{array} = \boldsymbol{S}, \qquad (2\text{-}41)$$

Из (2-41) следует:

$$(p_{i,j} + r_{i,j}) = s_{i,j} \equiv 0, \mod 2, \qquad (2\text{-}42)$$
$$i = 1, 2, \ldots, k;\ \ j = 1, 2, \ldots, (n - k);$$

откуда вытекает:

$$p_{i,j} \equiv r_{i,j}, \mod 2, \qquad (2\text{-}43)$$
$$i = 1, 2, \ldots, k;\ \ j = 1, 2, \ldots, (n - k);$$

и, следовательно,

$$\boldsymbol{P}_{k\times(n-k)} = \boldsymbol{R}_{k\times(n-k)}. \qquad (2\text{-}44)$$

ЧТД

Доказанная теорема свидетельствует о том, что между матрицами $\boldsymbol{G}_{(n,\,k)}$ и $\boldsymbol{H}_{(n,\,k)}$ одного и того же систематического кода, заданными в канонической форме, существует взаимно однозначное соответствие и, следовательно, каждая из них исчерпывающим образом описывает два групповых взаимно дуальных кода с проверкой на чётность: (n, k)- и $(n, n - k)$-код.

Вернёмся к вопросу существования способа определения $d_{\min}$ группового (n, k)-кода с проверкой на чётность более эффективного по сравнению с тотальным перебором весов кодовых комбинаций. Ответ на этот вопрос даёт следующая теорема.

ТЕОРЕМА 2.9. *Минимальное хэммингово расстояние группового (n, k)-кода равно $d_{\min}$ тогда и только тогда, когда* ***любые*** *$(d_{\min} - 1)$ столбцов его проверочной матрицы $\boldsymbol{H}_{(n,\,k)}$ линейно независимы, но* ***некоторые*** *$d_{\min}$ столбцов линейно зависимы.*

ДОКАЗАТЕЛЬСТВО.

НЕОБХОДИМОСЬ. Дан групповой (n, k)-*код и* $\boldsymbol{H}_{(n,\,k)}$ – его *проверочная матрица; пусть* $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ – некоторая *ненулевая кодовая комбинация* группового (n, k)-кода, и $i_1, i_2, \ldots, i_w$ – номера её ненулевых компонент.

Очевидно, что согласно определению проверочной матрицы $\boldsymbol{H}_{(n,\,k)}$ должно выполняться соотношение

$$[v_1\, v_2 \ldots v_n]\cdot\boldsymbol{H}^{\mathrm{T}}{}_{(n,\,k)} = \sum_{j=1}^{w} v_{i_j}\cdot\boldsymbol{h}_{i_j} = \boldsymbol{S}, \qquad (2\text{-}45)$$

где $\boldsymbol{S} = [0 \ \ldots \ 0]$ – нулевая матрица-строка размерности $1\times(n - k)$, называемая *синдромом*; $\boldsymbol{h}_i$, $i = 1, 2, \ldots, n$, – столбцы $\boldsymbol{H}_{(n,\,k)}$.

Если w – *минимальный вес ненулевой кодовой комбинации* рассматриваемого (n, k)-кода, то, согласно (2-45), $d_{\min} = w$ и $d_{\min}$ *равно минимальному числу линейно зависимых столбцов его проверочной матрицы* $\boldsymbol{H}_{(n,\,k)}$. При этом любая совокупность из $(d_{\min} - 1)$ или из меньшего числа столбцов является совокупностью *линейно независимых* столбцов, так как в противном случае существовал бы ненулевой кодовый вектор рассматриваемого кода, вес которого был бы меньше w.

ДОСТАТОЧНОСТЬ. Дан групповой (n, k)-*код и* $\boldsymbol{H}_{(n,\,k)}$ – его *проверочная матрица*. Предположим, что w столбцов проверочной матрицы $\boldsymbol{H}_{(n,\,k)}$ с номерами $i_1, i_2, \ldots, i_w$ линейно зависимы, но любая совокупность из меньшего числа столбцов $\boldsymbol{H}_{(n,\,k)}$ является линейно независимой. При этом согласно определению линейной зависимости существует совокупность ненулевых чисел $\{a_j\}$, $1 \le j \le w$, – элементов двоичного числового поля, для которых выполняется соотношение

$$\sum_{j=1}^{w} a_j\boldsymbol{h}_{i_j} = \boldsymbol{0}, \qquad (2\text{-}46)$$

где $\boldsymbol{0}$ – нуль-вектор. Пусть $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ – комбинация, компоненты которой с номерами i_j, $1 \le j \le w$, равны a_j, а другие равны 0. Тогда согласно (2-46)

$$[v_1\, v_2 \ldots v_n]\cdot\boldsymbol{H}^{\mathrm{T}}{}_{(n,\,k)} = \sum_{j=1}^{w} v_{i_j}\cdot\boldsymbol{h}_{i_j} = \sum_{j=1}^{w} a_j\cdot\boldsymbol{h}_{i_j} = \boldsymbol{0}, \qquad (2\text{-}47)$$

и, следовательно, $\boldsymbol{v}$ является *кодовой комбинацией минимального веса* w, который равен минимальному хэммингову расстоянию кода $d_{\min}$, так как, согласно предположению, любая совокупность из числа столбцов меньшего w является *линейно независимой.*

ЧТД

Так как ранг $\boldsymbol{H}_{(n,\,k)}$ равен $(n-k)$, то $(d_{\min}-1) \le (n-k)$ и, следовательно,

$$d_{\min} \le n - k + 1. \qquad (2\text{-}48)$$

Пример 2.19 иллюстрирует только что доказанную теорему.

2.4. НЕКОТОРЫЕ ОЦЕНКИ d_{min} ГРУППОВОГО (n, k)-КОДА. ЭЛЕМЕНТАРНЫЕ ОЦЕНКИ СВЕРХУ И СНИЗУ МАКСИМАЛЬНОЙ МОЩНОСТИ $m(n, 2t+1)$ $<n, 2t+1>$-КОДА. НЕКОТОРЫЕ СОВЕРШЕННЫЕ КОДЫ

Неравенство (2-48) является оценкой сверху минимального хэммингова расстояния кода группового (n, k)-кода и, несмотря на его большое теоретическое значение, оно всё же не даёт исчерпывающей информации об области возможных значений d_{min}.

Групповой (n, k)-код, для которого соотношение (2-48) выполняется со знаком равенства, называется *разделимым кодом с достижимым максимальным расстоянием* (см. БЧХ-коды и коды Рида-Соломона).

ВЕРХНЯЯ ГРАНИЦА ПЛОТКИНА ДЛЯ d_{min}

Из (2-48) при больших n ($n>>1$) можно получить оценку сверху d_{min} – так называемую верхнюю границу Плоткина (рис. 2.9):

$$k/n = R1(x) = 1 - 4x, \text{ где } x = d_{min}/(2n). \qquad (2\text{-}48а)$$

ВЕРХНЯЯ ГРАНИЦА ХЭММИНГА ДЛЯ d_{min}

Верхняя граница Хэмминга для d_{min} даётся также следующей теоремой.

ТЕОРЕМА 2.10. *Для любого двоичного блокового (n, k)-кода с минимальным хэмминговым весом $(2t+1)$ или больше число проверочных символов*

$$r = n - k \geq ld[\sum_{i=0}^{t} C_n^i], \qquad (2\text{-}49)$$

или

$$1 - \frac{k}{n} = 1 - R \geq \frac{1}{n} ld[\sum_{i=0}^{t} C_n^i]. \qquad (2\text{-}50)$$

ДОКАЗАТЕЛЬСТВО. Групповой (n, k)-код имеет 2^k кодовых комбинаций и при разложении группы по подгруппе порождает 2^{n-k} смежных классов. Если код способен исправлять t- и менее кратные ошибки, то все комбинации ненулевого веса t и менее должны быть образующими смежных классов. Следовательно, число комбинаций веса t и менее не должно превосходить числа смежных классов:

$$1 + C_n^1 + C_n^2 + \ldots + C_n^t = \sum_{i=0}^{t} C_n^i \leq 2^{n-k}. \qquad (2\text{-}51)$$

Беря логарифм от обеих частей неравенства (2-51), получим (2-49).

ЧТД

В приложении А [2.2] приведены формулы, удобные для оценки сумм вида $\sum_{i=0}^{t} C_n^i$ (см. также [2.16]). При больших n с помощью этих формул из (2-50) можно получить оценку сверху d_{min} – так называемую верхнюю границу Хэмминга (рис. 2.9):

$$k/n = R2(x) = 1 - H(x), \text{ где } x = d_{min}/(2n), \qquad (2\text{-}51а)$$

$H = H(x)$ – энтропийная функция.

НИЖНЯЯ ГРАНИЦА ВАРШАМОВА-ГИЛБЕРТА ДЛЯ d_{min}

Нижняя граница Варшамова-Гилберта для d_{min} даётся следующей теоремой [2.2, с. 101].

ТЕОРЕМА 2.11. *Существует* (n, k)*-код с минимальным хэмминговым расстоянием* $d_{\min}$, *удовлетворяющим неравенству*:

$$\sum_{i=0}^{d_{min}-2} C_n^i \geq 2^{n-k} . \qquad (2\text{-}52)$$

ДОКАЗАТЕЛЬСТВО. Согласно ранее доказанной теореме 2.9 проверочная матрица $\boldsymbol{H}_{(n,\,k)}$ группового (n, k)-кода с минимальным хэмминговым расстоянием $d_{\min}$ имеет следующие свойства: ***любые*** $(d_{\min} - 1)$ или меньшее число её столбцов линейно независимы, но ***некоторые*** $d_{\min}$ столбцов линейно зависимы. Основываясь на этом результате, можно построить групповой (n, k)-код с минимальным хэмминговым расстоянием $d_{\min}$ следующим способом:

в качестве первого столбца проверочной матрицы выберем любой двоичный ненулевой набор длины r;

в качестве второго столбца проверочной матрицы выберем любой двоичный ненулевой набор длины r, не пропорциональный первому набору;

в качестве третьего столбца проверочной матрицы выберем любой двоичный ненулевой набор длины r, не являющийся линейной комбинацией первых двух наборов;

.....

в качестве i-го столбца проверочной матрицы выберем любой двоичный ненулевой набор длины r, не являющийся линейной комбинацией любой совокупности из $(d_{\min} - 2)$ или из меньшего числа столбцов из ранее присоединённых $(i - 1)$ столбцов.

Такой способ построения проверочной матрицы гарантирует, что никакая линейная комбинация из $d_{\min} - 1$ или меньшего числа столбцов проверочной матрицы не обращается в нуль.

Очередной столбец может быть присоединён к создаваемой проверочной матрице только в том случае, если совокупность всех различных линейных комбинаций из $d_{\min} - 2$ или меньшего числа ранее созданных столбцов матрицы не

исчерпывает всех наборов длины r. В наихудшем возможном случае все такие линейные комбинации будут различными.

Предположим, что $(j - 1)$ – общее число уже присоединённых к создаваемой матрице столбцов.

Число всевозможных различных линейных комбинаций из $d_{\min} - 2$ или из меньшего числа столбцов, выбранных из общего числа уже присоединённых к создаваемой матрице $j - 1$ столбцов, равно

$$C_{j-1}^1 + C_{j-1}^2 + C_{j-1}^3 + \ldots + C_{j-1}^{d_{min}-2} . \qquad (2\text{-}53)$$

Если это число меньше $(2^r - 1)$ – общего числа различных ненулевых наборов длины r, то наверняка найдётся ещё один j-й ненулевой набор длины r, который может быть присоединён к создаваемой проверочной матрице.

Таким образом, если

$$k = j - r \geq 1 \qquad (2\text{-}54)$$

и

$$C_{j-1}^1 + C_{j-1}^2 + C_{j-1}^3 + \ldots + C_{j-1}^{d_{min}-2} < 2^r - 1 , \qquad (2\text{-}54а)$$

то существует (j, k)-код с длиной кодовых комбинаций j, числом проверочных символов не более r, числом информационных символов не менее $k = j - r$ и с минимальным хэмминговым расстоянием $d_{\min}$. Этот код является нулевым пространством матрицы размерности $r \times j$, которая была образована приведенным способом последовательного присоединения ненулевых наборов длины r.

Предположим теперь, что n – максимальное значение j, для которого выполняется соотношение (2-54а). Тогда существует (n, k)-код с минимальным хэмминговым расстоянием $d_{\min}$, который удовлетворяет неравенству

$$\sum_{i=1}^{d_{min}-2} C_n^i \geq 2^r - 1 . \qquad (2\text{-}55)$$

или, что то же самое, неравенству

$$\sum_{i=0}^{d_{min}-2} C_n^i \geq 2^r = 2^{n-k} . \qquad (2\text{-}56)$$

Выражение (2-56) и является искомой нижней границей минимального хэммингова расстояния $d_{\min}$.

ЧТД

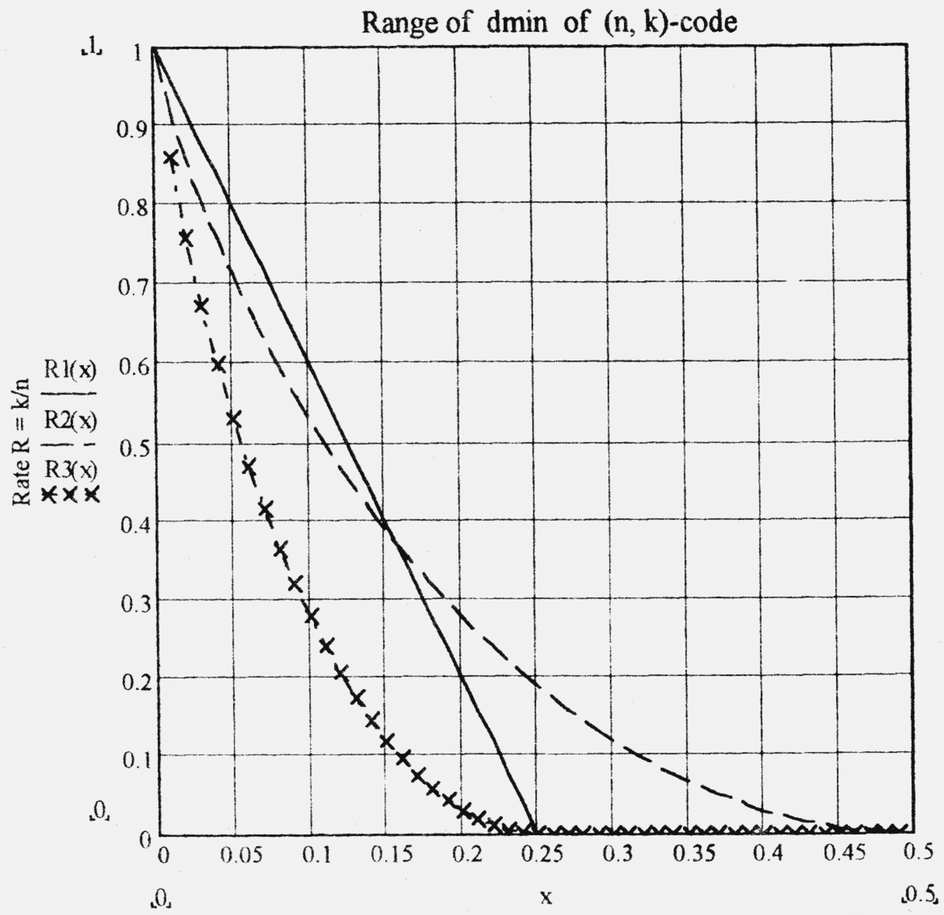

Рис. 2.9. Границы для $d_{\min}$ (n>>1); x= $d_{\min}/(2n)$:

$R1(x) = (1 - 4x)$ – верхняя граница Плоткина;

$R2(x) = (1 - H(x))$ – верхняя граница Хэмминга;

$$R3(x) = \begin{cases} (1 - H(2x)), & H'(2x) \geq 0, \\ 0, & H'(2x) < 0. \end{cases}$$

– нижняя граница Варшамова-Гилберта

Для больших n и $d_{\min}$ с помощью соотношений из приложения А [2.2] можно получить асимптотическую оценку $d_{\min}$:

$$n - k \leq H((d_{\min} - 2)/n), \qquad (2\text{-}57)$$

где $H = H(x)$ – энтропийная функция.

Пренебрегая в (2-57) числом 2, получим нижнюю оценку Варшамова-Гилберта минимального хэммингова расстояния $d_{\min}$ в форме (рис. 2.9):

$$R3(x) = \begin{cases} (1 - H(2x)), & H'(2x) \geq 0, \\ 0, & H'(2x) < 0, \end{cases} \qquad (2\text{-}58)$$

где $x = d_{\min}/(2n)$.

ВСЕВОЗМОЖНЫЕ СИСТЕМАТИЧЕСКИЕ (5, 2)-КОДЫ

ПРИМЕР 2.20. В табл. 2.6, приведены некоторые характеристики систематических (5, 2)-кодов (см. решение задачи 1.12).

Для иллюстрации теоремы 2.9 рассмотрим вопросы:

1) чему равно $N_{(5,\ 2)}$ - число различных всевозможных *систематических* (5, 2)-кодов;

2) каковы возможные значения минимального хэммингова расстояния $d_{\min}$ различных систематических (5, 2)- кодов;

3) чему равно число различных систематических (5, 2)-кодов, обладающих одним и тем же значением $d_{\min}$;

4) как для рассматриваемых кодов набирать конкретную проверочную матрицу из $2^r = 8$ всевозможных различных столбцов длины $r = 3$?

Таблица 2.6

(5, 2)-коды	Двоичные пятизначные групповые (5, 2)-коды;	L=2; N_0=32; n=5; k=2; r=3	N=4, d_{min}=1,2,3 R = 2/5= =0.40
$G_{(5,2)} = [I_2 R_{2\times 3}]$, $H_{(5,2)} = \begin{bmatrix} R^{T}_{2\times 3} I_3 \end{bmatrix}$			

Ответы на поставленные вопросы.

1. Число всевозможных систематических (5, 2)-кодов

$$N_{(5,\,2)} = 2^{k(n-k)} = 2^{2\cdot 3} = 2^6 = 64$$

(см. Приложение 5.1).

2. Из рассмотрения табл. 2.7 следует, что различные значения d_{min} всевозможных систематических (5, 2)-кодов образуют множество {1, 2, 3};

15 систематических (5, 2)-кодов имеют $d_{min} = 1$,

37 систематических (5, 2)-кодов имеют $d_{min} = 2$ и

12 систематических (5, 2)-кодов имеют $d_{min} = 3$.

3. Табл. 2.7 содержит номера систематических (5, 2)-кодов, имеющих конкретные значения d_{min}.

Для уяснения деталей доказательства теоремы 2.10, полезно рассмотреть обширный иллюстрационный материал примера 2.19 (см. также Приложение 5.1).

Таблица2.7

d_{min}	Номера (5, 2)-кодов	Общее число (5, 2)-кодов
1	1, 2, 3, 4, 5, 6, 7, 8, 9, 17, 25, 33, 41, 49, 57	15
2	10, 11, 12, 13, 14, 15, 16, 18, 19, 20, 21, 22, 23, 24, 26, 27, 28, 29, 34, 35, 36, 37, 38, 39, 40, 42, 43, 45, 46, 50, 51, 53, 55, 58, 59, 61, 64	37
3	30, 31, 32, 44, 47, 48, 52, 54, 56, 60, 62, 63	12

$$\boldsymbol{H}_{0(5,2)} := \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Рис. 2. 10 «Исходная» матрица $H_{0(5,\,2)}$

4. Считая справа налево, занумеруем столбцы «исходной» матрицы $\boldsymbol{H}_{0(5,\ 2)}$ (рис. 2.10) целыми положительными числами 1, 2, …, 11. При этом первые три столбца образуют единичную матрицу $\boldsymbol{I}_3$. Из этих 11 столбцов способом, изложенным в доказательстве теоремы 2.9, для любого из возможных значений d_{min} можно набрать любую проверочную матрицу $\boldsymbol{H}_{(5,\ 2)}$ из 64 матриц, приведенных в Приложении 5.1; при этом в качестве первых трёх столбцов следует каждый раз выбирать столбцы с номерами 1, 2 и 3.

Интересно также на основе приведенного в данном примере материала рассмотреть вопрос существования взаимосвязи между наличием нулевых и единичных столбцов в проверочной матрице систематического (5, 2)-кода с кодовым расстоянием d_{min}.

END

ЭЛЕМЕНТАРНЫЕ ОЦЕНКИ СВЕРХУ И СНИЗУ МАКСИМАЛЬНОЙ МОЩНОСТИ $m(n, 2t+1)$ $<n, 2t+1>$-КОДА

Мы завершим данный подраздел примером, в котором рассмотрим получение элементарных оценок сверху и снизу $m(n,\ 2t+1)$ – максимальной мощности $<n,\ 2t+1>$-кода, где $d_{min} = 2t+1$.

Актуальность постановки этого вопроса очевидна, так как ответ на него позволит охарактеризовать предельно возможные свойства $<n,\ 2t+1>$-кода исправлять все ошибки

кратности $q \le t$ и при этом передавать требуемое число сообщений $N \le m(n, 2t+1)$.

ПРИМЕР 2.21.

Оценка сверху. Окружим каждую кодовую комбинацию $<n, 2t+1>$-кода шаром радиуса t; очевидно, что эти шары с центрами – кодовыми комбинациями не *пересекаются* и поэтому число двоичных комбинаций длины n – элементов B^n, содержащихся во всех таких шарах, будет удовлетворять условию (см. задачу 1.2)

$$m(n, 2t+1)\,|\,S_t^n(\mathbf{0})\,| \le 2^n, \qquad (2\text{-}59)$$

так как возможно не все элементы B^n принадлежат шарам и, следовательно,

$$m(n, 2t+1) \le \frac{2^n}{|\,S_t^n(\mathbf{0})\,|} = \frac{2^n}{\sum_{i=0}^{t} C_n^i}. \qquad (2\text{-}60)$$

Соотношение (2-60) называется *верхней границей Хэмминга* или *границей сферической упаковки*. Коды, для которых в (2-59) имеет место знак равенства, называются *совершенными* или *плотно упакованными*.

Оценка снизу. Окружим каждую *кодовую комбинацию* $<n, 2t+1>$-кода шаром радиуса $2t$. Очевидно, что шары радиуса $2t$ с центрами – кодовыми комбинациями *пересекаются*.

Так как рассматривается *максимальный* код, то любая двоичная комбинация длины n – элемент B^n, принадлежит хотя бы одному такому шару. В противном случае, если бы нашлась хотя бы одна комбинация длины n, не принадлежащая ни одному шару, то её можно было бы назначить ещё одной кодовой комбинацией, присоединив к рассматриваемому коду и, следовательно, вопреки исходным данным рассматриваемый код был бы не максимальным, т.е. объединение всех шаров есть B^n. Поэтому справедливо соотношение

$$m(n, 2t+1)\,|\,S_{2t}^n(\mathbf{0})\,| \ge 2^n, \qquad (2\text{-}61)$$

так как многие из двоичных комбинаций принадлежат нескольким шарам и, следовательно, учитываются в (2-61) несколько раз. Из (2-60) и (2-61) следует:

$$\frac{2^n}{|\,S_{2t}^n(\mathbf{0})\,|} \le m(n, 2t+1) \le \frac{2^n}{|\,S_t^n(\mathbf{0})\,|}. \qquad (2\text{-}62)$$

На основании выражения (2-62) запишем соотношение, являющееся критерием принадлежности $<n, 2t+1>$-кода к классу совершенных или плотно упакованных кодов:

$$m(n, 2t+1) = \frac{2^n}{|\,S_t^n(\mathbf{0})\,|}. \qquad (2\text{-}63)$$

Соотношение (2-63) объясняет термин «плотно упакованный код» – т.е. код, множество кодовых комбинаций которого с окружающими их взаимно непересекающимися шарами радиуса t целиком заполняют множество B^n.

Из (2-63) следует, что для существования максимального совершенного кода мощности $m(n, 2t+1)$ *необходимо*, чтобы $|\,S_t^n(\mathbf{0})\,|$ было бы целочисленной степенью двойки:

$$|\,S_t^n(\mathbf{0})\,| = 2^s, \qquad (2\text{-}64)$$

где целое s удовлетворяет неравенствам: $0 < s < n$. Очевидно, что если это условие не выполняется, то совершенный код мощности $m(n, 2t+1)$ не существует.

Из (2-63) следует: класс совершенных кодов является подклассом максимальных кодов

END

Ниже приведены примеры плотно упакованных кодов [2.1 - 2.5, 2.20].