сел с операциями сложения и умножения являются (числовыми) полями.

2. Множество целых чисел с операциями сложения и умножения не является полем, так как для всех целых чисел, отличающихся от 0 и 1, не выполняется свойство *M*5.

END

ПРИМЕР 2.10. Так как. поле должно содержать два единичных элемента: «0» относительно операции сложения и «1» относительно операции умножения, то наименьшее число элементов, образующих поле, равно двум. Легко установить, что эти два элемента должны удовлетворять приведенным ниже (рис. 2.1) правилам:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Рис. 2.1. Числовое двоичное поле

Рассмотренное поле называется числовым *двоичным* полем. Ниже мы будем рассматривать *двоичные* матрицы – матрицы, элементами которых являются элементы двоичного поля.

END

Поле, имеющее конечное число элементов, называется *конечным*; при этом число его элементов называется *порядком поля*; в противном случае поле называется *бесконечным* (счётным или несчётным). Будем обозначать порядок поля F как $|F|$.

Заметим, что «Кольцо» является более общим понятием, нежели понятие «Поле» в том смысле, что «Поле» является коммутативным «Кольцом» с единичным элементом по умножению, в котором каждый ненулевой элемент имеет об-

ратный элемент по умножению, а «Кольцо» «Полем» может не являться.

2.2. ОПИСАНИЕ ГРУППОВЫХ (n, k)-КОДОВ С ПОМОЩЬЮ ПОРОЖДАЮЩИХ МАТРИЦ. ПРЕОБРАЗОВАНИЕ ПОРОЖДАЮЩИХ МАТРИЦ. О ЧИСЛЕ РАЗЛИЧЫХ БАЗИСОВ $N_{(n)}$ В B^n. КОДИРОВАНИЕ СООБЩЕНИЙ

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

Всё ниже излагаемое, если не сказано противного, относится к двоичным кодам (компоненты векторов, элементы матриц, сомножители векторов и т.д. являются элементами двоичного числового поля).

Ранее, были определены *систематический код с проверкой на чётность и общий код с проверкой на чётность* (см. определения 1.9 и 1.10).

Как уже говорилось в первом разделе данной книги, систематический код с проверкой на чётность является частным случаем общего кода с проверкой на чётность.

n-мерное векторное пространство по отношению к операции сложения комбинаций согласно определению 2.2 является аддитивной абелевой группой; k-мерное векторное подпространство согласно определению 2.3 является подгруппой этой группы (см. табл. 2.1).

Так как всевозможные 2^k кодовые комбинации (n, k)-кода образуют *линейное k-мерное подпространство* линейного n-мерного векторного пространства, то этот код часто также называют *линейным* (n, k)*-кодом*.

Порождающие матрицы общего и систематического (n, k)-кодов с проверкой на чётность (1-62) и (1-63) соответственно имеют одну и ту же размерность $k \times n$, $n > k$, и один и

тот же ранг k; строки каждой из этих матриц образованы k линейно независимыми кодовыми комбинациями (векторами) (n, k)-кода, ею определяемого; эти кодовые комбинации образуют *базис* k-мерного линейного подпространства, являющегося *аддитивной абелевой группой*. Поэтому *двоичный линейный* (n, k)*-код*, определяемый порождающей матрицей $\boldsymbol{G}_{(n, k)}$, часто называют также *групповым* (n, k)*-кодом*. Следует заметить, что в недвоичном случае не всякий *групповой код* является *линейным кодом* [2.4, с. 16].

Согласно сказанному, можно говорить о разложении аддитивной абелевой группы – линейного векторного пространства B^n по подгруппе – групповому (n, k)-коду; подобное разложение играет большую роль при декодировании принятых комбинаций и лежит в его основе.

ПРЕОБРАЗОВАНИЕ ПОРОЖДАЮЩИХ МАТРИЦ

Два кода C_1 и C_2 называются *эквивалентными*, если кодовые слова одного кода, например C_2, получаются из кодовых слов другого кода, например C_1, некоторой *перестановкой символов одной и той же для всех кодовых слов*.

Так как при перестановке символов кодовых слов (*одной и той же для всех кодовых слов*) веса кодовых слов не меняются, то кодовые расстояния двух эквивалентных кодов C_1 и C_2 совпадают и, следовательно, обнаруживающая и исправляющая способности кодов также совпадают. Отсюда следует, что если одна порождающая матрица получена из другой перестановкой векторов-столбцов (кратко: столбцов) последней, то соответствующие этим матрицам коды *эквивалентны*.

Рассмотрим следующие элементарные операции преобразования матриц:

а) обмен местами (транспозиция или перестановка) двух векторов-строк (кратко: строк) или двух столбцов;

б) умножение произвольной строки или произвольного столбца на произвольное не равное нулю число;

в) прибавление к одной строке или к одному столбцу *другой* строки или *другого* столбца, умноженных на некоторое не равное нулю число.

ЗАМЕЧАНИЕ 2.1. В случае двоичных кодов:

вектор-сумма некоторого числа двоичных векторов-строк или векторов-столбцов является двоичным вектором и определяется путём сравнения результирующих чисел – компонент вектора-суммы (с 0 или 1) по mod 2.

В п. б) произвольное не равное нулю число – единица.

Число перечисленных выше элементарных операций можно уменьшить до:

1) обмена местами (транспозиции) двух строк или двух столбцов;

2) прибавления к одной строке или к одному столбцу *другой* строки или *другого* столбца соответственно.

END

В дальнейшем при применении элементарных операций к двоичным матрицам и ссылках на свойства элементарных операций мы будем *иметь в виду свойства*, приведенные в замечании 2.1.

Очевидно, что применение перечисленных элементарных операций 1) и 2) к строкам или к столбцам матрицы ранга k приводит в общем случае к новой матрице с тем же рангом k [2.9, с.75 – 76].

Так как множество кодовых комбинаций группового (n, k)-кода, порождаемого матрицей $\boldsymbol{G}_{(n,k)}$, является аддитивной абелевой группой, то применение перечисленных выше элементарных операций *к строкам порождающей матрицы* $\boldsymbol{G}_{(n, k)}$ ранга k приводит в общем случае к новой порождающей матрице с тем же рангом k, порождающей *то же самое под-*

пространство, что и матрица $\boldsymbol{G}_{(n,\,k)}$; причём в случае применения только транспозиции строк *сохраняется* и *базис* подпространства, образуемый строками порождающей матрицы.

Так как множество кодовых комбинаций группового $(n,\ n-k)$-кода, порождаемого матрицей $\boldsymbol{H}_{(n,\,k)}$, является аддитивной абелевой группой, то применение перечисленных выше элементарных операций *к строкам проверочной матрицы* $\boldsymbol{H}_{(n,\,k)}$ ранга $n-k$ приводит в общем случае к новой порождающей матрице с тем же рангом $n-k$, порождающей *то же самое* подпространство, что и матрица $\boldsymbol{H}_{(n,\,k)}$; причём в случае применения только транспозиции строк *сохраняется* и *базис* подпространства, образуемый строками порождающей матрицы.

ПРИМЕР 2.11. На рис. 2.2 в пункте a) приведены исходная порождающая матрица группового $(n,\ k)$-кода C $\boldsymbol{G}_{(n,\,k)}$ размерности $k \times n$ ($k = 2$, $n = 4$) и соответствующая ей (т.е. представляющая тот же самый групповой $(n,\ k)$-код C) кодовая матрица $\boldsymbol{C}_{(n,\,k)}$.

Пункт b) носит вспомогательный характер: приведенные здесь различные пары ненулевых кодовых комбинаций используются в пункте c) для образования порождающих матриц (2), (3), …, (6) из матрицы (1) путём применения элементарных операций к строкам матриц.

Совокупность двух линейно независимых ненулевых кодовых комбинаций-строк порождающей матрицы $\boldsymbol{G}_{(4,\,2)}$ является базисом k-мерного подпространства B^k (пространства B^n), являющегося кодом C. Кодовые комбинации $\boldsymbol{x}_i$, $i = 1, 2, 3, 4$; кода C получаются как линейные комбинации базисных кодовых комбинаций:

$$\boldsymbol{x}_i = \lambda_{i1}\cdot(1100) + \lambda_{i2}\cdot(0111), \qquad (2\text{-}11)$$

где $i = 1, 2, 3, 4$; $\lambda_{i1}, \lambda_{i2} \in \{1, 0\}$; очевидно, что в этом случае $N = 2^k = 2^2 = 4$.

Пункт d) иллюстрирует *некоторую* последовательность преобразований порождающих матриц *одного и того же кода* C с помощью элементарных операций преобразования: 1c+2c (к первой строке преобразуемой матрицы прибавляется её вторая строка) или 2c+1c (ко второй строке преобразуемой матрицы прибавляется её первая строка).

a) Порождающая матрица и порождаемый ею код C:

$$\boldsymbol{G}_{(4,2)} := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \qquad \boldsymbol{C}_{(4,2)} := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

b) Всевозможные различные пары ненулевых кодовых комбинац

{(1100), (0111)}; {(1100), (1011)}; {(0111), (1011)}

c) Всевозможные порождающие матрицы кода C $\boldsymbol{G}_{(4,2)}$:

(1) $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ (2) $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$ (3) $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$

(4) $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$ (5) $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$ (6) $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$

Рис. 2.2 a, b, c. Преобразование порождающих матриц группового (4, 2)-кода с помощью применения элментарных операций к строкам матриц

d) Преобразование матриц с помощью однократных элементарных операций (движение по часовой стрелке)

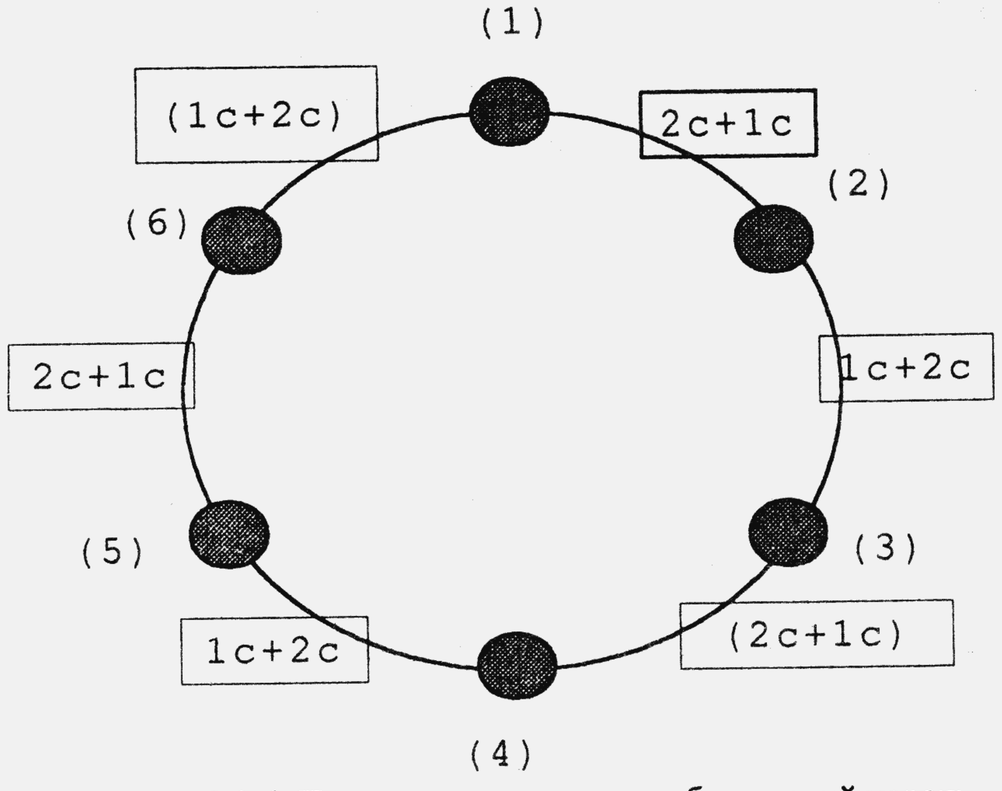

Рис. 2.2 d. Последовательность преобразований порождающих матриц одного и того же (4, 2)-кода

END

Применение перечисленных выше элементарных операций *к столбцам порождающей матрицы* ранга k приводит в общем случае к новой порождающей матрице *с тем же рангом* k, которая может порождать как *тот же самый*, так и *другой* (n, k)-код, корректирующие свойства которого могут отличаться от свойств исходного кода. Только лишь перестановка столбцов не изменяет весов строк порождающей матрицы; поэтому новые коды, полученные таким путём, являются *эквивалентными*.

Аналогичные замечания можно сделать относительно применения элементарных операций *к столбцам проверочной матрицы* относительно порождаемого ею дуального кода (см. ниже).

ПРИМЕР 2.12

$$\boldsymbol{G}_{(4,2)} := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \quad \boldsymbol{G}_{(4,2)} := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\boldsymbol{C}_{(4,2)} := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \boldsymbol{C}_{(4,2)} := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\boldsymbol{G}_{(4,2)} := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \quad \boldsymbol{G}_{(4,2)} := \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\boldsymbol{C}_{(4,2)} := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \boldsymbol{C}_{(4,2)} := \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Рис. 2.3. Преобразование заданной порождающей матрицы (4, 2)-кода путём перестановки её столбцов

На рис. 2.3, считая слева направо и сверху вниз, приведены четыре порождающие матрицы $\boldsymbol{G}_{(4,\,2)}$ – исходная – первая, и полученные из неё перестановкой её столбцов вто-

рая (перестановка первого и второго столбцов первой матрицы), третья (перестановка второго и четвёртого столбцов первой матрицы) и четвёртая (перестановка второго и третьего столбцов первой матрицы). Под каждой из порождающих матриц приведены соответствующие им кодовые матрицы $\boldsymbol{C}_{(4,\,2)}$.

Множества кодовых слов – строк первой и второй, считая слева направо и сверху вниз, кодовых матриц $\boldsymbol{C}_{(4,\,2)}$ совпадают; а различные между собою множества кодовых слов – строк третьей и четвёртой кодовых матриц $\boldsymbol{C}_{(4,\,2)}$ отличаются от одного и того же множества кодовых слов – строк первой и второй матриц $\boldsymbol{C}_{(4,\,2)}$.

END

ОПРЕДЕЛЕНИЕ 2.7. *Будем говорить, что двоичная порождающая матрица размерности $k \times n$ ($k < n$) имеет* ***каноническую форму****, если при $1 \le i \le k$ и $1 \le j \le k$ её элементы*

$$g_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \ne j, \end{cases} \qquad (2\text{-}12)$$

а при $1 \le i \le k$ и $k + 1 \le j \le n$ множество двоичных чисел $\{g_{ij}\}$ является произвольным.

END

С учётом определения 2.7 порождающую матрицу систематического кода с проверкой на чётность *в канонической форме* можно представить в виде

$$\boldsymbol{G}_{(n,\,k)} = [\boldsymbol{I}_k \boldsymbol{R}_{k\times(n-k)}], \qquad (2\text{-}12\text{а})$$

где единичная матрица $\boldsymbol{I}_k$ и $\boldsymbol{R}_{k\times(n-k)}$ – подматрицы матрицы $\boldsymbol{G}_{(n,\,k)}$.

ЗАМЕЧАНИЕ 2.2. В некоторых литературных источниках порождающая матрица в канонической форме записывается так:

$$\boldsymbol{G}_{(n,\,k)} = [\boldsymbol{R}_{k\times(n-k)} \boldsymbol{I}_k]. \qquad (2\text{-}12\text{б})$$

Вообще говоря, какой из видов записи (2-12а) или (2-12б) выбрать не имеет принципиального значения, важно лишь то, чтобы в последующих построениях использовался только один вполне определённый вид записи; в данной книге выбран вид (2-12а) и, следовательно, вид записи (2-12б) не является канонической формой.

END

ТЕОРЕМА 2.6. *Всякая двоичная порождающая матрица группового (n, k)-кода, заданная в произвольной не канонической форме, путём применения элементарных операций может быть приведена к* ***любой*** *из $2^{k(n-k)}$ возможных различных порождающих матриц, имеющих каноническую форму.*

Иначе говоря,

1° *любая двоичная матрица путём применения элементарных операций может быть приведена к* ***некоторой*** *матрице, имеющей каноническую форму;*

2° *полученная в п.* 1° ***некоторая*** *матрица, имеющая каноническую форму, путём применения элементарных операций к столбцам матрицы может быть преобразована в* ***любую*** *из остальных $2^{k(n-k)} - 1$ возможных порождающих матриц, имеющих также каноническую форму.*

ДОКАЗАТЕЛЬСТВО.

Предположим, что задана матрица $\boldsymbol{G}$ размерности $k \times n$, не имеющая канонической формы; требуется преобразовать её к некоторой матрице, имеющей каноническую форму: $[\boldsymbol{I}_k \boldsymbol{R}_{k\times(n-k)}]$.

Пункт 1°. В произвольной i-й строке, $i = 1, 2, \ldots, k$ матрицы $\boldsymbol{G}$ найдётся по меньшей мере одна единица, так как строки матрицы $\boldsymbol{G}$ линейно независимы. Предположим, что первый отличный от нуля элемент – единица находится в j-м столбце: $g_{ij} = 1$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, n$.

К каждой m-й строке, $m \neq i$, для которой $g_{mj} = 1$, прибавим i-ю строку. В результате в j-м столбце i-я строка будет содержать единицу, а все остальные строки – нули.

Заметим, что как только в каком-либо j-м столбце один элемент окажется равным единице: $g_{ij} = 1$, а все остальные элементы нулями: $g_{mj} = 0$, $m \neq i$, то выполнение элементарных операций над строками, отличными от i-й, не меняет этого столбца.

После того как описанные операции будут проделаны над всеми строками, получится матрица, содержащая k столбцов, каждый из которых содержит одну единицу и $(k - 1)$ нулей, причём упомянутые k единиц располагаются по одной в каждой из строк.

Затем перестановкой указанных k столбцов можно сгруппировать их слева так, чтобы они образовали единичную матрицу $\boldsymbol{I}_k$.

В итоге получится некоторая матрица

$$\boldsymbol{G'} = [\boldsymbol{I}_k . \boldsymbol{P}_{k\times(n-k)}], \qquad (2\text{-}13)$$

причём $\boldsymbol{P}_{k\times(n-k)}$ не обязательно равна $\boldsymbol{R}_{k\times(n-k)}$.

Таким образом, п. 1° доказан.

Пункт 2°. Предположим, что $\boldsymbol{P}_{k\times(n-k)} \neq \boldsymbol{R}_{k\times(n-k)}$.

Очевидно, что любой вектор-столбец матрицы $\boldsymbol{P}_{k\times(n-k)}$ может быть сделан равным соответствующему вектору-столбцу матрицы $\boldsymbol{R}_{k\times(n-k)}$:

$$p_{ij} = r_{ij}, \quad i = 1, 2, \ldots, k; j = k + 1, k + 2, \ldots, n, \qquad (2\text{-}14)$$

путём прибавления соответствующих столбцов матрицы $\boldsymbol{I}_k$. В итоге мы получим порождающую матрицу

$$\boldsymbol{G''} = [\boldsymbol{I}_k . \boldsymbol{R}_{k\times(n-k)}]. \qquad (2\text{-}15)$$

Таким образом, п. 2° доказан.

ЧТД

Из приведенных сведений о преобразовании порождающих матриц с помощью элементарных операций вытекает справедливость утверждения: *произвольный* (заданный) общий (n, k)-код *эквивалентен некоторому* систематическому (n, k)-коду, получаемому из заданного кода путём применения элементарных операций к строкам матрицы или элементарной операции – перестановки столбцов матрицы.

ПРИМЕР 2.13. На рис. 2.4 приведено семейство из 16 всевозможных ***различных*** порождающих матриц в канонической форме 16-ти всевозможных ***различных*** *систематических* групповых (4, 2)-*кодов*.

Каждая *конкретная* матрица $[\boldsymbol{I}_k \ \boldsymbol{R}_{k\times(n-k)}]$ из этих 16-ти приведенных матриц путём выполнения нескольких операций транспозиции строк может быть преобразована только в матрицы, имеющие условно каноническую форму $[\boldsymbol{I}_{[k]}\boldsymbol{R}_{[k\times(n-k)]}]$ (см. подраздел 2.8), каждая из которых порождает ***то же самое k-мерное подпространство***, что и ***k-мерное подпространство***, порождаемое рассматриваемой конкретной матрицей $[\boldsymbol{I}_k \ \boldsymbol{R}_{k\times(n-k)}]$.

Отсюда следует, что если некоторый *условно систематический* (n, k)-код (первого типа) задан порождающей матрицей, имеющей *условно каноническую форму* $[\boldsymbol{I}_{[k]}\boldsymbol{R}_{[k\times(n-k)]}]$, то путём выполнения только элементарных операций перестановки строк матрицы её всегда можно преобразовать в порождающую матрицу, имеющую *каноническую форму* $[\boldsymbol{I}_k \ \boldsymbol{R}_{k\times(n-k)}]$ и, следовательно, определяющую систематический групповой (n, k)-код.

{**G**i }, i=0,1, 2, ...,15, - семейство всевозможных порождающих матриц (4, 2)-кодов, имеющих каноническую форму и полученных из матрицы G0 путём прибавления столбцов подматрицы I_2 к столбцам подматрицы $R_{2\times2}$

$$G_0 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad G_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$G_5 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad G_6 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad G_7 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad G_8 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$G_9 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad G_{10} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad G_{11} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad G_{12} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$G_{13} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad G_{14} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad G_{15} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Рис.2.4. Порождающие матрицы в канонической форме 16-ти различных *систематических* кодов

Подчеркнём дополнительно, что в результате применения к матрице $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$, определяющей некоторый ***базис*** и

некоторый систематический (n, k)-код, операции транспозиции строк получается ***новая матрица*** $[\boldsymbol{I}_{[k]}\boldsymbol{R}_{[k\times(n-k)]}]$, определяющая ***тот же самый базис*** и ***то же самое*** *k*-***мерное подпространство***, коим является заданный систематический (n, k)-код.

В случае же применения к строкам матрицы $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$ элементарной операции прибавления к одной строке матрицы другой строки этой же матрицы получается новая матрица $[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}]$, определяющая ***другой базис***, отличный от базиса, определяемого матрицей $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$; при этом матрицы $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$, $[\boldsymbol{I}_{[k]}\boldsymbol{R}_{[k\times(n-k)]}]$ и $[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}]$, о которых идёт речь, определяют ***одно и то же*** *k*-***мерное подпространство***.

Однако, если *условно систематический код* (второго типа) задан порождающей матрицей, имеющей *условно каноническую форму* $[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}]$, то путём *только перестановки строк* матриц её нельзя преобразовать в порождающую матрицу заданного *k*-мерного подпространства, имеющую условно каноническую форму $[\boldsymbol{I}_{[k]}\boldsymbol{R}_{[k\times(n-k)]}]$ или каноническую форму $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$; для этого требуется привлечение элементарной операции 2) – операции прибавления к одной строке матрицы другой строки этой же матрицы (см. подраздел 2.8).

END

Если *асистематический код* задан порождающей матрицей $[\Xi_{k\times k}\boldsymbol{R}_{k\times(n-k)}]$, то путём применения элементарных операций *только к строкам матрицы* её нельзя преобразовать в порождающую матрицу *k*-мерного подпространства, коим является заданный *асистематический* код, имеющую каноническую или условно каноническую форму, – таковых порождающих матриц просто *не существует*! См. подраздел 2.8.

Одним из преимуществ систематического (n, k)-кода по сравнению с общим (n, k)-кодом является то обстоятельство, что после выполнения операции кодирования передаваемое сообщение без изменения его структуры оказывается

размещённым в информационных разрядах кодовой комбинации (см. (2-25)).

Поэтому далее мы сконцентрируем наше внимание на рассмотрении *систематических* (n, k)-кодов без потери общности изучения свойств (n, k)-кодов с проверкой на чётность.

ПРИМЕР 2.14. Рассмотрим применение элементарных операций 1) и 2) *к строкам* порождающих матриц $\boldsymbol{G}_{(n,\,k)}$ (n=5, k=3) заданного группового общего (n, k)-кода с проверкой на чётность с целью получения порождающей матрицы $\boldsymbol{G}_{(n,\,k)}$ в канонической форме (рис. 2.5).

a) Приведение порождающей матрицы к канонической форме путём выполнения элементарных операций над строками

(1)

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

(2)

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

(3)

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

b) Последовательность применения элементарных операций к строкам матриц

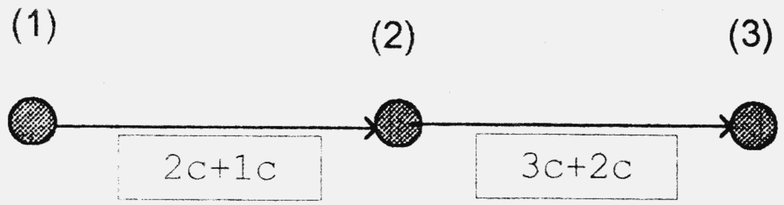

Рис. 2.5. Приведение порождающей матрицы (5, 3)-кода к канонической форме

Полученная порождающая матрица в канонической форме может быть записана следующим образом:

$$\boldsymbol{G}_{(5,\,3)} = [\boldsymbol{I}_3 \boldsymbol{R}_{3\times 2}], \qquad (2\text{-}16)$$

где $\boldsymbol{I}_3$ – *единичная* матрица размерности 3×3, образованная *информационными* элементами; $\boldsymbol{R}_{3\times 2}$ – прямоугольная матрица размерности 3×2, образованная *проверочными* элементами.

Легко видеть, что в рассматриваемом случае существует $2^{k(n-k)} = 2^6 = 64$ ($k\times(n\text{-}k)$ – число элементов матрицы $\boldsymbol{R}_{k\times(n-k)}$) всевозможных порождающих матриц в канонической форме; все они могут быть согласно теореме 2.6 получены путём прибавления к столбцам, образованным проверочными элементами, соответствующих столбцов матрицы $\boldsymbol{I}_3$.

END

Обсудим теперь вопрос о том, что даёт использование порождающей матрицы для задания систематического группового (n, k)-кода.

Строки порождающей матрицы размерности $k\times n$ содержат k ненулевых линейно независимых (базисных) кодовых комбинаций, через которые может быть выражена любая кодовая комбинация $\boldsymbol{x}_r$, $r = 1, 2, \ldots, 2^k$, (n, k)-кода:

$$\boldsymbol{x}_r = \lambda_{r1}\boldsymbol{x}_1 + \lambda_{r2}\boldsymbol{x}_2 + \ldots + \lambda_{rk}\boldsymbol{x}_k = \sum_{i=1}^{k} \lambda_{ri}\boldsymbol{x}_i, \qquad (2\text{-}17)$$

где $\{\boldsymbol{x}_i\}$, $i = 1, 2, \ldots, k$, – базисные кодовые комбинации; $\{\lambda_{r1}, \lambda_{r2}, \ldots, \lambda_{rk}\}$ – произвольный набор k элементов двоичного поля; так как всего может быть 2^k таких различных двоичных наборов, то любой конкретный базис $\{\boldsymbol{x}_i\}$, $i = 1, 2, \ldots, k$, порождает согласно (2-17) $N = 2^k$ всевозможных различных кодовых комбинаций некоторого конкретного группового (n, k)-кода.

Очевидно, что задание группового (n, k)-кода не путём перечисления всех его 2^k кодовых комбинаций, а путём задания лишь k ненулевых линейно независимых кодовых комбинаций, т.е. задание с помощью порождающей матрицы, по-

зволяет избежать экспоненциальной зависимости сложности кодера от $k(ld\,2)$.

О ЧИСЛЕ РАЗЛИЧНЫХ БАЗИСОВ $N_{(n)}$ В B^n

ПРИМЕР 2.15. Требуется определить $N_{(n)}$ – число различных базисов в B^n. Каждый базис в B_n состоит из n ненулевых линейно независимых векторов. Таким образом, базис рассматривается как неупорядоченное множество элементов, а *различные базисы* – как базисы, отличающиеся хотя бы одним элементом.

Каждый *конкретный* базис, содержащий n *конкретных* ненулевых линейно независимых векторов, может быть представлен с помощью $n!$ различных матриц, обладающих одним и тем же множеством векторов-строк и отличающихся лишь порядком следования этих n *конкретных* ненулевых линейно независимых векторов-строк; при этом любая матрица из числа $n!$ может быть образована из любой другой матрицы из этого же числа $n!$ путём применения элементарной операции транспозиции строк матрицы за один или несколько шагов.

Дополнением к i-мерному подпространству, содержащему 2^i векторов, $i = 1, 2, \ldots, n$, будем называть совокупность всех ненулевых комбинаций множества B_n, не принадлежащих i-мерному подпространству.

Первый *ненулевой* вектор базиса B^n можно выбрать $(2^n - 1)$ способами; при этом выбранный ненулевой вектор сам является базисом, порождающим 1-*мерное подпространство* пространства B^n, состоящее из 2^1 векторов (выбранный ненулевой вектор и нулевой вектор).

Второй ненулевой вектор базиса B^n (при выбранном первом ненулевом векторе) можно выбрать $(2^n - 2)$ способами, а два ненулевых вектора базиса B^n можно выбрать $(2^n - 1)(2^n - 2) = (2^n - 2^{1-1})(2^n - 2^{2-1})$ способами; выбранные

два ненулевых вектора сами образуют базис, порождающий 2-мерное подпространство пространства B^n, состоящее из 2^2 векторов (три ненулевых вектора и нулевой вектор); второй выбираемый ненулевой вектор должен принадлежать дополнению к 1-*мерному подпространству*.

Поступая так и далее,

.....

на i-м шаге построения базиса пространства B^n придём к ситуации: i-й ненулевой вектор базиса B^n (при выбранных уже $(i - 1)$-м ненулевых векторах, образующих $(i - 1)$-*мерное подпространство* пространства B^n) можно выбрать $(2^n - 2^{i-1})$ способами, а i ненулевых векторов базиса B^n можно выбрать

$$(2^n - 2^{1-1})(2^n - 2^{2-1}) \ldots (2^n - 2^{i-1}) \qquad (2\text{-}18)$$

способами; эти i выбранные ненулевые линейно независимые векторы сами образуют базис, порождающий i-мерное подпространство пространства B^n, состоящее из 2^i векторов ($2^i - 1$ ненулевых векторов и нулевой вектор); i-й выбираемый ненулевой вектор должен принадлежать дополнению к $(i - 1)$-*мерному подпространству*.

Поступая так и далее,

.....

на n-м шаге построения базиса пространства B^n придём к ситуации: n-й ненулевой вектор базиса B^n (при выбранных уже $(n - 1)$-м ненулевых векторах, образующих $(n - 1)$-*мерное подпространство* пространства B^n) можно выбрать $(2^n - 2^{n-1})$ способами, а n ненулевых векторов базиса B^n можно выбрать

$$(2^n - 2^{1-1})(2^n - 2^{2-1}) \ldots (2^n - 2^{n-1}) \qquad (2\text{-}19)$$

способами; при этом выбранные n ненулевых векторов образуют базис пространства B^n, состоящего из 2^n векторов ($2^n - 1$ ненулевых векторов и нулевой вектор); n-й выбираемый не-

нулевой вектор должен принадлежать дополнению к $(n-1)$-*мерному подпространству*.

Очевидно, что полученное в (2-19) число n-наборов ненулевых линейно независимых кодовых комбинаций учитывает каждый базис B^n $n!$ раз (одинаковые по составу n-наборы, отличающиеся лишь *порядком выбора* образующих их кодовых комбинаций); поэтому искомое число всех *различных* базисов в B^n

$$N_{(n)} = \frac{(2^n - 1)(2^n - 2)(2^n - 2^2)\cdot\ldots\cdot(2^n - 2^{n-1})}{n!}. \qquad (2\text{-}20)$$

END

ПРИМЕР 2.16. Табл. 2.5 содержит конкретные примеры для n=1, 2 и 3.

На рис. 2.6 приведены все 28 различных базисов линейного пространства B^3. Заметим, что по техническим причинам каждый базис – совокупность ненулевых линейно независимых комбинаций мы приводим здесь не с помощью пары скобок {}, а с помощью матриц, подобно тому, как мы представляем совокупность кодовых комбинаций некоторого кода C с помощью его кодовой матрицы C или $\boldsymbol{C}$.

Таблица 2.5

n	$N_{(n)}$	B^n	Базисы B^n
1	1	{0, 1}	{1}
2	3	{00, 01, 10, 11}	{01, 10}, {01, 11}, {10, 11}
3	28	{000, 001, 010, 011, 100, 101, 110, 111}	См. ниже

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

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

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

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

Рис. 2.6. Всевозможные базисы B^3

END

КОДИРОВАНИЕ СООБЩЕНИЙ

Порождающая матрица (n, k)-кода с проверкой на чётность является эффективным средством кодирования сообщений.

Рассмотрим кодирование сообщений с помощью порождающей матрицы $\boldsymbol{G}_{(n,\,k)}$ в случае использования группового (n, k)-кода.

Если

$$\boldsymbol{v}_i = (v_{i1}, v_{i2}, \ldots, v_{ik}), \quad i=1, 2, \ldots, 2^k, - \qquad (2\text{-}21)$$

сообщения, подлежащие передаче по каналу связи, а

$$\boldsymbol{x}_j = (x_{j1}, x_{j2}, \ldots, x_{jk}, x_{j(k+1)}, \ldots, x_n), \quad j=1, 2, \ldots, 2^k, - \qquad (2\text{-}22)$$

кодовые комбинации группового (n, k)-кода.

Представим порождающую матрицу, заданную в *произвольной форме*, в виде

$$\boldsymbol{G}_{(n,\,k)} = \begin{bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \ldots\ldots\ldots \\ \boldsymbol{x}_{(k-1)} \\ \boldsymbol{x}_k \end{bmatrix}, \qquad (2\text{-}23)$$

где $\boldsymbol{x}_i$, $i = 1, 2, \ldots, k$, – базисные кодовые комбинации; а кодовая комбинация $\boldsymbol{x}_j$, соответствующая передаваемому сообщению $\boldsymbol{v}_j$, $j = 1, 2, \ldots, 2^k$, выражается как

$$\boldsymbol{x}_j = \boldsymbol{v}_j \boldsymbol{G}_{(n,\,k)} = v_{j1}\,\boldsymbol{x}_1 + v_{j2}\,\boldsymbol{x}_2 + \ldots + v_{j(k-1)}\,\boldsymbol{x}_{(k-1)} + v_{jk}\,\boldsymbol{x}_k, \qquad (2\text{-}24)$$

откуда следует, что $\boldsymbol{x}_j$ действительно является кодовой комбинацией как *линейная комбинация* базисных кодовых комбинаций $\boldsymbol{x}_i$, $i = 1, 2, \ldots, k$.

В том случае, когда матрица $\boldsymbol{G}_{(n,\,k)}$ задана в канонической форме

$$\boldsymbol{x}_j = \boldsymbol{v}_j\,[\boldsymbol{I}_k\,\boldsymbol{R}_{k\times(n-k)}] =$$

$$= [v_{j1}\ v_{j2}\ \ldots\ v_{j(k-1)}\ v_{jk}] \begin{bmatrix} 1\ \ldots\ 0\ \ldots\ 0\ g_{11}\ \ldots\ldots\ g_{1r} \\ 0\ \ldots\ 1\ \ldots\ 0\ g_{21}\ \ldots\ldots\ g_{2r} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0\ \ldots\ 0\ \ldots\ 1\ 0\ g_{(k-1)1}\ \ldots\ g_{(k-1)r} \\ 0\ \ldots\ 0\ \ldots\ 1\ g_{k1}\ \ldots\ldots\ g_{kr} \end{bmatrix} =$$

$$= [x_{j1}\,x_{j2}\ \ldots\ x_{jn}] = [v_{j1}\ \ v_{j2}\ \ldots\ v_{j(k-1)}\ v_{jk}\,x_{j(k+1)}\ \ldots\ x_{jn}], \quad (2\text{-}25)$$

где $r = n - k$. В рассматриваемом случае местоположение информационных символов $\{v_{j1},\ v_{j2},\ \ldots,\ v_{j(k-1)},\ v_{jk}\}$ и проверочных символов $\{x_{j(k+1)},\ \ldots,\ x_{jn}\}$ в кодовой комбинации $\boldsymbol{x}_j$ является строго определённым.

2.3. О ЧИСЛЕ РАЗЛИЧНЫХ (n, k)-КОДОВ В B^n. ГРУППОВОЙ (n, k)-КОД И ЕГО КОРРЕКТИРУЮЩИЕ СВОЙСТВА. ОПИСАНИЕ ГРУППОВЫХ (n, k)-КОДОВ С ПОМОЩЬЮ ПРОВЕРОЧНЫХ МАТРИЦ

О ЧИСЛЕ РАЗЛИЧНЫХ (n, k)-КОДОВ В B^n

Зададимся теперь вопросом: сколько при заданных двух целых числах n и k $(n \geq k \geq 1)$ существует различных (n, k)-кодов в B^n ? Ответ на этот вопрос даётся в следующем примере.

ПРИМЕР 2.17. Определить $N_{(n,k)}$ – число различных (n, k)-кодов в B^n.

Для упрощения рассуждений допустим, что информационные символы кодовых комбинаций рассматриваемых далее кодов занимают первые k разрядов, считая слева направо.

Согласно примеру 2.15 число *всевозможных различных* k-наборов ненулевых линейно независимых кодовых комбинаций в B^n:

$$N_{[1]} = \frac{(2^n - 1)(2^n - 2)(2^n - 2^2)\ \ldots\ (2^n - 2^{k-1})}{k!}. \qquad (2\text{-}26)$$

Согласно примеру 2.15 *число различных базисов* в каждом пространстве B^k, образованном k информационными разрядами векторов пространства B^n ($|B^n| = 2^n = 2^k 2^{n-k} = 2^k 2^r = |B^k| 2^{n-k}$) и *соответствующем некоторому одному и тому же конкретному групповому* (n, k)-коду, имеющему $2^k = |B^k|$ кодовых комбинаций:

$$N_{(k)} = \frac{(2^k - 1)(2^k - 2)(2^k - 2^2)\ \ldots\ (2^k - 2^{k-1})}{k!}. \qquad (2\text{-}27)$$