можность более целенаправленно осуществлять расчёты вероятностей правильного декодирования (см. теорему 2.14).

Принятая комбинация:

$$y := (1\ 1\ 1\ 1\ 1) \qquad H := \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

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

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

$$S_{1,i} := \mathrm{mod}(S_{1,i}, 2) \qquad G := \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

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

$S = (0\ 1\ 0)$

$$Sr := G \cdot H^T$$

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

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

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

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

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

Результат декодирования:

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

Рис. 2.12. Программа декодирования

END

СРЕДНЯЯ ВЕРОЯТНОСТЬ ПРАВИЛЬНОГО ДЕКОДИРОВАНИЯ

ТЕОРЕМА 2.14. *Пусть для передачи равновероятных сообщений (кодовых векторов) по ДСК используется групповой (n, k)-код C. Тогда P_c - средняя вероятность правильного декодирования* ***принятых векторов в кодовые вектора*** *совпадает с максимально возможной для данного кода, если в качестве таблицы декодирования используется стандартное расположение, в котором лидер каждого смежного класса имеет минимальный вес в своём классе.*

ДОКАЗАТЕЛЬСТВО. Обозначим вектор, стоящий в i-й строке и в j-м столбце стандартного расположения, через y_{ij}, $i = 1, 2, \ldots, 2^{n-k}$, $j = 1, 2, \ldots, 2^k$. Таким образом, кодовые слова, стоящие в первой, считая сверху вниз, строке, получат обозначения: y_{1j}, $j = 1, 2, \ldots, 2^k$. Обозначим через d_{ij} расстояние Хэмминга между кодовым вектором y_{1j}, в который преобразуется при декодировании принятый вектор y_{ij}.

Тогда, если было передано кодовое слово y_{1j} (j – некоторое произвольное фиксированное число из совокупности чисел $\{1, 2, \ldots, 2^k\}$), вероятность правильного декодирования принятого вектора y_{ij}, очевидно, равна сумме вероятностей перехода под действием шумов в ДСК y_{1j} в один из векторов совокупности $\{y_{ij}\}$ ($i = 1, 2, \ldots, 2^{n-k}$) при j, равном вышеупомянутому фиксированному значению, и согласно (1-53) выражается соотношением:

$$\sum_{i=1}^{2^{n-k}} p_0^{d_{ij}} (1 - p_0)^{n-d_{ij}} \qquad (2\text{-}72б)$$

где p_0 – вероятность ошибки (искажения символа шумом) в ДСК.

Так как групповой (n, k)-код C имеет 2^k кодовых векторов, которые предполагаются *равновероятными*, то при усреднении вероятности правильного декодирования, опреде-

ляемой (2-72б), *по всевозможным кодовым словам совокупности* $\{y_{1j} \mid j = 1, 2, \ldots, 2^k\}$ используется весовой коэффициент – вероятность кодового вектора 2^{-k}:

$$P_c = \sum_{j=1}^{2^k} 2^{-k} \sum_{i=1}^{2^{n-k}} p_0^{d_{ij}} (1 - p_0)^{n-d_{ij}} = 2^{-k} \sum_{i,j} p_0^{d_{ij}} (1 - p_0)^{n-d_{ij}} . \qquad (2\text{-}73)$$

Каждому принятому вектору y_{ij}, в сумме справа в выражении (2-73) соответствует одно слагаемое вида $p_0^{d_{ij}}(1-p_0)^{n-d_{ij}}$, являющееся *монотонно убывающей функцией от* d_{ij}; поэтому каждое такое слагаемое будет принимать максимальное значение, если соответствующее расстояние d_{ij} принимает минимальное значение или, что одно и тоже, если соответствующий принятый вектор y_{ij} декодируется в ближайший в смысле расстояния Хэмминга кодовый вектор. Принятый вектор y_{ij} лежит в i-м смежном классе, лидер которого – вектор ошибки e_i. Из описанного выше способа построения стандартного расположения следует, что y_{ij} расположен под y_{1j} и отстоит от него на расстоянии $d_{ij} = w(e_i)$; поэтому, если e_i обладает минимальным весом в своём смежном классе, то декодирование y_{ij} в кодовый вектор y_{1j}, под которым он расположен, означает, по крайней мере, декодирование в ближайший в смысле расстояния Хэмминга кодовый вектор. Действительно, предположим, что существует некоторый другой кодовый вектор y_{1s}, ближайший к принятому вектору y_{ij} и отличный от y_{1j}. Вес вектора $y_{ij} + y_{1j} = e_i$, лежащего в i-м смежном классе, равен $w(e_i)$. Вектор $y_{ij} + y_{1s} = e_i + (y_{1j} + y_{1s})$ имеет вес $w(y_{ij} + y_{1s})$ и также лежит в i-м смежном классе. Так как предполагалось, что вектор e_i имеет наименьший вес среди всех векторов i-го смежного класса, то $w(y_{ij}+y_{1s}) \geq w(e_i)$.

ЧТД

ПРИМЕР 2.25. Рассмотрим один произвольный из 12 групповых (5, 2)-кодов с $d_{\min}=3$ из примера 2.20 и определим для него P_c. Согласно (2-73)

$$P_c = \sum_{j=1}^{2^k} 2^{-k} \sum_{i=1}^{2^{n-k}} p_0^{d_{ij}} (1 - p_0)^{n-d_{ij}} . \qquad (2\text{-}74)$$

Ниже на рис. 2.13 приведена программа расчёта P_c по этой формуле при n=5, k=2 и $d_{\min}$=3 и построен график зависимости $P_c = P_c(p_0)$, где p_0 – вероятность искажения двоичных символов в ДСК; $p_0 < 0.5$.

Очевидно, что применение синдромного метода декодирования существенно упрощает сложность декодера и, в частности, позволяет избежать экспоненциального роста сложности декодера с ростом $n(ln\ 2)$. Это объясняется тем, что при синдромном декодировании необходимо иметь приблизительный объём памяти:

для вычисления синдрома, т.е. для запоминания принятого вектора y и матрицы $H^T_{(n,k)}$ – $(n+(n-k)n)$ двоичных ячеек;

для запоминания взаимно однозначного соответствия: $S(y_{ij}) \Leftrightarrow e_i$, i=1, 2, …, 2^{n-k}, – $(n-k+n)\cdot 2^{n-k}$ двоичных ячеек.

Предположим, что $n = 50$, $k = 30$.

Таким образом, при синдромном декодировании декодер должен иметь приблизительно общий объём памяти: $(n-k+1)n+(2n-k)2^{n-k} \approx 7.34\cdot 10^7$ двоичных ячеек.

ПРОГРАММА ВЫЧИСЛЕНИЯ P_c

Таким образом, к настоящему моменту мы ознакомились со следующими основными методами декодирования при использовании корректирующих блоковых кодов:

универсальный метод декодирования;

метод декодирования с применением таблицы декодирования, близкий, по сущности, к универсальному методу декодирования;

синдромный метод декодирования.

$n := 5 \quad k := 2 \quad i := 1..8 \quad j := 1..4 \quad q(i) := \begin{cases} 0 & \text{if } i = 1 \\ 1 & \text{if } i = 2 \\ 1 & \text{if } i = 3 \\ 1 & \text{if } i = 4 \\ 1 & \text{if } i = 5 \\ 1 & \text{if } i = 6 \\ 2 & \text{if } i = 7 \\ 2 & \text{if } i = 8 \end{cases}$

$P_c := P(p) \quad p_0 := p \quad d_{i,j} := q(i)$

$p := 0, \left(10^{-4}\right)..0.5$

$$P(p) := \frac{1}{4}\left[\sum_{j=1}^{4}\sum_{i=1}^{8} p^{d_{i,j}}(1-p)^{5-d_{i,j}}\right]$$

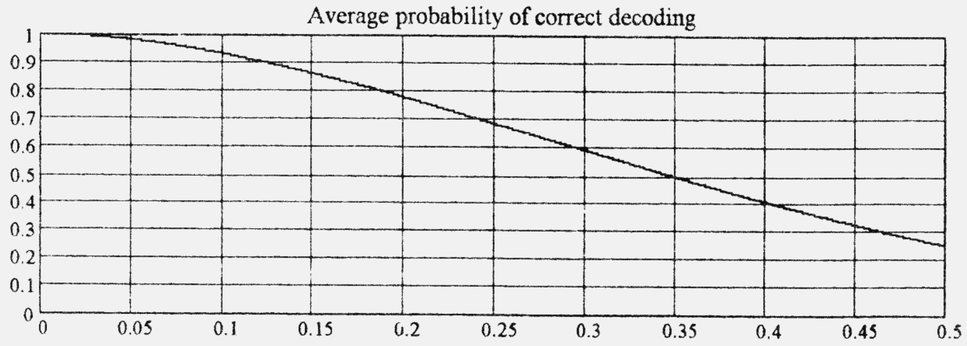

Рис. 2.13. Средняя вероятность правильного декодирования принятых комбинаций $P_c = P(p)$

END

При декодировании же с помощью таблицы декодирования декодер должен иметь приблизительно общий объём памяти $n2^n \approx 5.629 \cdot 10^{16}$ двоичных ячеек.

Из приведенных данных следует, что при прочих равных условиях применение синдромного декодирования по сравнению со случаем декодирования с помощью кодовой таблицы даёт экономию оборудования приблизительно в $7.669 \cdot 10^8$ раз.

2.7. УКОРОЧЕННЫЕ ГРУППОВЫЕ КОДЫ

Предположим, что задан систематический групповой (n, k)-код. Пусть $\boldsymbol{G}_{(n, k)}$ и $\boldsymbol{H}_{(n, k)}$ – порождающая и проверочная матрицы этого кода, имеющие каноническую форму.

На основе исходного систематического группового (n, k)-кода можно построить новый, так же групповой $(n - i, k - i)$-код, $i < k$, если из каждой кодовой комбинации этого кода исключить i первых информационных символов.

Порождающая матрица образованного таким образом $(n - i, k - i)$-кода $\boldsymbol{G}_{(n-i, k-i)}$ получается из матрицы $\boldsymbol{G}_{(n, k)}$, имеющей каноническую форму, путём вычёркивания её i первых строк и i первых столбцов.

Проверочная матрица $(n - i, k - i)$-кода $\boldsymbol{H}_{(n-i, k-i)}$ получается путём вычеркивания из матрицы $\boldsymbol{H}_{(n, k)}$, имеющей каноническую форму, её i первых столбцов. Так как при этом число линейно зависимых столбцов проверочной матрицы *уменьшиться не может*, то $d_{\min}$, а следовательно, и корректирующие свойства нового кода оказываются не хуже, чем у кода исходного.

Образованные изложенным способом новые коды называются *укороченными кодами*, а операция получения этих новых кодов иногда называется *операцией укорочения* (см. пример 2.26).

Очевидно, что справедливы следующие соотношения, описывающие процесс образования укороченного $(n - i, k - i)$-кода из исходного (n, k)-кода.

$$0 \le i \le k - 1 < n; \qquad \text{(2-74а)}$$

$$2 \le \text{«}N\text{»} = N(i) = 2^{k-i} = 2^k/2^i \le 2^k, \qquad \text{(2-74б)}$$

$$2^{n-k+1} \le \text{«}N_0\text{»} = N_0(i) = 2^{n-i} = 2^n/2^i \le 2^n. \qquad \text{(2-74в)}$$

Из этих соотношений следует, что при выполнении операций укорочения происходит уменьшение «N»= $N(i)$ и «N_0» = $N_0(i)$ в одно и то же число раз 2^i. Уменьшение «n» = $n - i$ с ростом i ведёт к более простой реализаций нового кода по сравнению со случаем исходного кода, однако уменьшение «N» на практике, вообще говоря, может оказаться меньше мощности ансамбля сообщений, подлежащих передаче, и, следовательно, неприемлемым.

ПРИМЕР 2.26

```
Построение укороченных (4,2)-кода и (3, 1)-кода
  на основе исходного группового (5, 3)-кода
```

$$G_{(5,3)} := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad H_{(5,3)} := \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{(4,2)} := \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad H_{(4,2)} := \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{(3,1)} := \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} \qquad H_{(3,1)} := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Рис. 2.14. Построение порождающих матриц укороченных кодов

END

2.8. РАЗНОВИДНОСТИ ПОРОЖДАЮЩИХ И ПРОВЕРОЧНЫХ МАТРИЦ ГРУППОВЫХ (n, k)-КОДОВ

Предположим, что задана порождающая матрица группового систематического (n, k)-кода в канонической форме

$$\boldsymbol{G}_{(n,k)} = [\boldsymbol{I}_k \boldsymbol{R}_{k\times(n-k)}], \qquad (2\text{-}75)$$

где $\boldsymbol{I}_k$ – единичная матрица порядка $k\times k$, $\boldsymbol{R}_{k\times(n-k)}$ *матрица – обобщённая переменная*, значениями которой являются конкретные матрицы из *совокупности* $2^{k\times(n-k)}$ всевозможных конкретных матриц; конкретная матрица – значение $\boldsymbol{R}_{k\times(n-k)}$.

Тогда порождающая матрица этого группового систематического (n, k)-кода в канонической форме

$$\boldsymbol{H}_{(n,k)} = \left[\boldsymbol{R}^{\mathrm{T}}_{k\times(n-k)} \boldsymbol{I}_{(n-k)}\right], \qquad (2\text{-}76)$$

где $\boldsymbol{I}_{n-k}$ – квадратная единичная матрица порядка $(n - k)\times(n - k)$.

Если в (2-75) $\boldsymbol{R}_{k\times(n-k)}$ пробегает $2^{k(n-k)}$ всевозможных значений, то каждое из этих значений определяет конкретный групповой систематический (n, k)-код.

Пусть $\boldsymbol{I}_{[k]}$ – квадратная двоичная матрица размерности $k\times k$, в каждой строке и в каждом столбце которой имеется по одной единице и при этом $\boldsymbol{I}_k \not\subset \{\boldsymbol{I}_{[k]}\}$. Придадим обозначению $\boldsymbol{I}_{[k]}$ следующий смысл: $\boldsymbol{I}_{[k]}$ есть *матрица обобщённая переменная*, значениями которой являются конкретные матрицы из *совокупности* $k!$ - 1 всевозможных конкретных матриц, имеющих в каждой строке и в каждом столбце по одной единице ($k!$ – число всевозможных перестановок k k-мерных *векторов-строк*, каждая из которых имеет одну единицу и k - 1 нулей и является одной из строк матрицы $\boldsymbol{I}_{[k]}$).

Одновременно со сказанным под записью $\{\boldsymbol{I}_{[k]}\}$ условимся понимать множество всех конкретных матриц, которые могут содержаться в обобщённой переменной $\boldsymbol{I}_{[k]}$.

Рассмотрим совокупность всех возможных конкретных матриц $\boldsymbol{I}_k \cup \{\boldsymbol{I}_{[k]}\}$, общее число которых равно $k!$.

ЗАМЕЧАНИЕ 2.3. Очевидно, что *элементарная операция-транспозиция строк или столбцов матрицы* $\boldsymbol{I}_k$ или конкретной матрицы $\boldsymbol{I}_{[k]}$ обладает в $\boldsymbol{I}_k \cup \{\boldsymbol{I}_{[k]}\}$ *свойством замкнутости*: в результате применения этой элементарной операции к

строкам или столбцам матрицы из класса $\boldsymbol{I}_k \cup \{\boldsymbol{I}_{[k]}\}$ получаются только матрицы из этого же класса $\boldsymbol{I}_k \cup \{\boldsymbol{I}_{[k]}\}$.

Следует отметить, что произвольную матрицу $\boldsymbol{I}_{[k]}$ путём применения конечного числа элементарных операций-транспозиций:

1) только к строкам

или

2) только к столбцам

или

3) к строкам и к столбцам

всегда можно преобразовать в любую, наперёд заданную матрицу из $\boldsymbol{I}_k \cup \{\boldsymbol{I}_{[k]}\}$.

END

Очевидно, что множество частных значений переменной $\boldsymbol{I}_k$ состоит из одной конкретной матрицы, в то время как множество частных значений переменной $\boldsymbol{I}_{[k]}$ состоит из $(k!-1)$ различных конкретных матриц.

ОПРЕДЕЛЕНИЕ 2.8. *Назовём конкретный общий групповой (n, k)-код, порождающая матрица которого $[\boldsymbol{I}_{[k]}\ \boldsymbol{R}_{[k\times(n-k)]}]$ получена из порождающей матрицы систематического кода $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$ с помощью элементарной операции транспозиции строк матрицы,* ***условно систематическим кодом первого типа****, а о его порождающей матрице $[\boldsymbol{I}_{[k]}\ \boldsymbol{R}_{[k\times(n-k)]}] \neq [\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$ будем говорить, что она имеет* ***условно каноническую форму****.*

END

ОПРЕДЕЛЕНИЕ 2.9. *Назовём конкретный общий групповой (n, k)-код, порождающая матрица которого $[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}] \subset \subset([\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]\cup\{[\boldsymbol{I}_{[k]}\ \boldsymbol{R}_{[k\times(n-k)]}]\})$ и получена из порождающей матрицы систематического кода с помощью элементарной операции прибавления одной из строк матрицы к другой строке матрицы и, возможно, с помощью элементарной операции перестановки строк матрицы,* ***условно систематическим кодом второго типа****, а о его порождающей матрице $[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}]$ будем говорить, что она имеет* ***условно каноническую форму****.*

END

ОПРЕДЕЛЕНИЕ 2.10. *Назовём общий групповой (n, k)-код* ***асистематическим*** *кодом, если его порождающая матрица $[\Xi_{k\times k}\ \boldsymbol{R}_{k\times(n-k)}] \subset ([\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]\cup\{[\boldsymbol{I}_{[k]}\ \boldsymbol{R}_{[k\times(n-k)]}]\}\cup\{[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}]\})$ и не может быть получена из порождающей матрицы никакого систематического кода путём выполнения элементарных операций* ***только над строками матрицы****; однако $[\Xi_{k\times k}\ \boldsymbol{R}_{k\times(n-k)}]$ может быть приведена к матрице $[\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}]$ путём применения элементарных операций* ***к столбцам и, возможно, к строкам*** *матрицы.*

END

Дополнительно отметим, что имеют место соотношения

$$\boldsymbol{I}_k \subset \{\boldsymbol{I}_{[k]}\} \Rightarrow [\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}] \subset \{[\boldsymbol{I}_{[k]}\ \boldsymbol{R}_{[k\times(n-k)]}]\}, \quad (2\text{-}77)$$

$$[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}] \subset ([\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}] \cup \{[\boldsymbol{I}_{[k]}\ \boldsymbol{R}_{[k\times(n-k)]}]\}), \quad (2\text{-}77\text{а})$$

$$[\Xi_{k\times k}\ \boldsymbol{R}_{k\times(n-k)}] \subset ([\boldsymbol{I}_k\boldsymbol{R}_{k\times(n-k)}] \cup \{[\boldsymbol{I}_{[k]}\ \boldsymbol{R}_{[k\times(n-k)]}]\} \cup \{[\mathfrak{I}_{k\times k}\mathfrak{R}_{k\times(n-k)}]\}). \quad (2\text{-}77\text{б})$$

ПРИМЕР 2.27. На рис. 2.15 приведены порождающие матрицы асистематических кодов.

При переходе от матрицы к матрице по горизонтали слева направо применяется элементарная операция преобразования порождающих матриц – операция прибавления одной из строк матрицы к другой строке матрицы.

При переходе от матрицы к матрице по вертикали сверху вниз применяется элементарная операция транспозиции строк порождающих матриц.

Асистематические групповые (4,2)-коды
и их порождающие матрицы

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

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

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

Рис. 2.15. Асистематические коды и их порождающие матрицы

END

ПРИМЕР 2.28. Рассмотрим преобразование только порождающей матрицы группового (5, 2)-кода с d_{min}=3, который мы уже изучали выше в примере 2.23.

На рис. 2.16 приведена программа, показывающая, что при транспозиции двух строк порождающей матрицы $[\boldsymbol{I}_2\boldsymbol{R}_{2\times3}]$, имеющей каноническую форму, получается матрица $[\boldsymbol{I}_{[2]}\boldsymbol{R}_{[2\times3]}]$, имеющая условно каноническую форму; при этом конкретное соответствие (2-71б), естественно, остаётся тем же, что и в примере 2.23.

Принятая комбинация:

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

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

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

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

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

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

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

$S = (1\ 1\ 1)$

$e(S) :=$
- $(0\ 0\ 0\ 0\ 0)$ if $S = (0\ 0\ 0)$
- $(0\ 0\ 0\ 0\ 1)$ if $S = (0\ 0\ 1)$
- $(0\ 0\ 0\ 1\ 0)$ if $S = (0\ 1\ 0)$
- $(0\ 0\ 1\ 0\ 0)$ if $S = (1\ 0\ 0)$
- $(0\ 1\ 0\ 0\ 0)$ if $S = (0\ 1\ 1)$
- $(1\ 0\ 0\ 0\ 0)$ if $S = (1\ 1\ 0)$
- $(1\ 1\ 0\ 0\ 0)$ if $S = (1\ 0\ 1)$
- $(0\ 1\ 1\ 0\ 0)$ if $S = (1\ 1\ 1)$

$Sr := G \cdot H^T$

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

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

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

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

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

Результат декодирования:

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

Рис. 2.16. Программа декодирования принятой комбинации

END

ПРИМЕР 2.29. Рассмотрим преобразование порождающей и проверочной матриц группового (5, 2)-кода с d_{min}=3, который мы уже изучали выше в примере 2.23.

На рис. 2.17 приведена программа, показывающая, что: при транспозиции двух строк порождающей матрицы $[\boldsymbol{I}_2\boldsymbol{R}_{2\times3}]$, имеющей каноническую форму, получается матрица $[\boldsymbol{I}_{[2]}\boldsymbol{R}_{[2\times3]}]$, имеющая условно каноническую форму; и

Принятая комбинация:

$y := (0\ 1\ 1\ 0\ 0)$ $\quad H := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$ $\quad H_{old} := \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

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

$S := S(y)$ $\quad i := 1..3$ $\quad G := \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$ $\quad G_{old} := \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

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

$S = (1\ 1\ 1)$

$e(S) :=$
- $(0\ 0\ 0\ 0\ 0)$ if $S = (0\ 0\ 0)$
- $(0\ 0\ 0\ 0\ 1)$ if $S = (0\ 0\ 1)$
- $(0\ 0\ 0\ 1\ 0)$ if $S = (1\ 0\ 0)$
- $(0\ 0\ 1\ 0\ 0)$ if $S = (0\ 1\ 0)$
- $(0\ 1\ 0\ 0\ 0)$ if $S = (1\ 0\ 1)$
- $(1\ 0\ 0\ 0\ 0)$ if $S = (1\ 1\ 0)$
- $(1\ 1\ 0\ 0\ 0)$ if $S = (0\ 1\ 1)$
- $(0\ 1\ 1\ 0\ 0)$ if $S = (1\ 1\ 1)$

$Sr := G \cdot H^T$

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

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

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

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

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

Результат декодирования:

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

Рис. 2.17. Программа декодирования принятой кодовой комбинации

при транспозиции первой и второй, считая сверху вниз, строк проверочной матрицы $[\boldsymbol{R}^{\mathrm{T}}_{k\times(n-k)}\boldsymbol{I}_{(n-k)}]$, имеющей каноническую форму, получается матрица $[\boldsymbol{R}^{\mathrm{T}}_{[k\times(n-k)]}\boldsymbol{I}_{[n-k]}]$, имеющая условно каноническую форму;

в этом случае конкретное соответствие (2-71б) становится уже отличным от конкретного соответствия, имеющего место в примере 23.

END

ЗАМЕЧАНИЕ 2.4. Отметим ещё одно обстоятельство: каким бы не был групповой код (систематический, условно систематический первого или второго типа или асистематический) с заданными порождающей и проверочной матрицами $\boldsymbol{G}_{\mathrm{old}}$ и $\boldsymbol{H}_{\mathrm{old}}$ ($\boldsymbol{G}_{old} \cdot \boldsymbol{H}^{\mathrm{T}}_{old} = \boldsymbol{0}$) совершенно независимое или зависимое применение элементарных операций только к строкам $\boldsymbol{G}_{\mathrm{old}}$ и/или $\boldsymbol{H}_{\mathrm{old}}$ приводит нас к новым матрицам $\boldsymbol{G}_{\mathrm{new}}$ и/или $\boldsymbol{H}_{\mathrm{new}}$, для которых по-прежнему выполняется соотношение: $\boldsymbol{G}_{new} \cdot \boldsymbol{H}^{\mathrm{T}}_{new} = \boldsymbol{0}$.

END

Весь приведенный выше материал, посвящённый рассмотрению разновидностей порождающих и проверочных матриц групповых (n, k)-кодов, важен для правильного понимания возможностей задания систематических и не являющихся систематическими групповых (n, k)-кодов. Однако при практическом использовании (n, k)-кодов канонические формы порождающей и проверочных матриц обладают очевидными преимуществами.

2.9. ПРИЛОЖЕНИЕ. ЛИНЕЙНЫЕ ВЕКТОРНЫЕ ПРОСТРАНСТВА И ЛИНЕЙНЫЕ АЛГЕБРЫ

ЛИНЕЙНЫЕ ВЕКТОРНЫЕ ПРОСТРАНСТВА

Пусть R – кольцо с (мультипликативной) единицей 1; элементы α, β, χ, … кольца R называются *скалярами*. Класс V объектов (элементов) $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, … называется (*линейным*) *векторным пространством над кольцом* R, а элементы класса V называются *векторами*, если определены ***две*** бинарные опе-

рации: векторное ***сложение*** и ***умножение*** вектора на скаляр такие, что:

1) V есть коммутативная группа по векторному сложению: для каждой пары элементов $\boldsymbol{a}, \boldsymbol{b} \in V$ пространство V содержит их векторную сумму $\boldsymbol{a}+\boldsymbol{b}$ и

$$\boldsymbol{a}+\boldsymbol{b} = \boldsymbol{b}+\boldsymbol{a}, \qquad \boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c}) = (\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c},$$

$$\boldsymbol{a}+\mathbf{0} = \boldsymbol{a}, \qquad \boldsymbol{a}+(-\boldsymbol{a}) = \boldsymbol{a}-\boldsymbol{a} = \mathbf{0},$$

где $\mathbf{0}$ – аддитивный нулевой элемент (нулевой вектор) пространства V, а $-\boldsymbol{a}$ – элемент, аддитивный обратный элементу $\boldsymbol{a}$;

2) если $\boldsymbol{a}$ – любой вектор из V, а α – любой скаляр из R, то V содержит вектор $\alpha\boldsymbol{a}$ – произведение скаляра α на вектор $\boldsymbol{a}$ (*замкнутость* по отношению к умножению на скаляр);

3) $(\alpha\beta)\boldsymbol{a} = \alpha(\beta\boldsymbol{a})$ (*ассоциативный закон* для умножения на скаляр);

4) $\alpha(\boldsymbol{a}+\boldsymbol{b}) = \alpha\boldsymbol{a} + \alpha\boldsymbol{b}$, $\quad (\alpha + \beta)\boldsymbol{a} = \alpha\boldsymbol{a} + \beta\boldsymbol{a}$ (дистрибутивные законы);

5) $1\boldsymbol{a} = \boldsymbol{a}$.

Имеют место также соотношения:

$$0\boldsymbol{a} = \mathbf{0}, \qquad (-1)\boldsymbol{a} = -\boldsymbol{a}, \qquad (-\alpha)\boldsymbol{a} = -(\alpha\boldsymbol{a}).$$

ЛИНЕЙНЫЕ АЛГЕБРЫ

Пусть R – кольцо скаляров α, β, χ, ... с (мультипликативной) единицей 1. Класс V объектов (элементов-векторов) $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \ldots$ называется *линейной алгеброй* (*линейной ассоциативной алгеброй*) над кольцом R, если определены ***три*** бинарные операции: ***сложение*** и ***умножение*** в V и *умножение* элементов из V на скаляры, такие что:

1) V есть кольцо,

2) V есть линейное векторное пространство над кольцом скаляров R.

Рангом линейной алгебры называется её размерность как *векторного пространства*. Если линейная алгебра есть поле, то она называется *алгеброй с делением* [2.8].

Очевидно, что «Линейное векторное пространство» является более общим понятием, нежели понятие «Линейная алгебра» в том смысле, что «Линейная алгебра» всегда является «Линейным векторным пространством», в котором дополнительно введена бинарная операция – «***умножение*** в V» (по определению V есть кольцо), а «Линейное векторное пространство» «Линейной алгеброй» может не являться.

2.10. ЗАДАЧИ

2.1. Показать, что число двоичных векторов из B^n, представимых линейными комбинациями вида

$$\lambda_1 \boldsymbol{x}_1 + \lambda_2 \boldsymbol{x}_2 + \ldots + \lambda_s \boldsymbol{x}_s, \qquad (2\text{-}77)$$

в которых $\sum_{i=1}^{s} \lambda_i \le t$, а $\{\boldsymbol{x}_i\}$ – совокупность линейно независимых комбинаций, не превосходит $\sum_{i=0}^{t} C_s^i$.

Рекомендуется решить эту же задачу, отказавшись от условия линейной независимости комбинаций $\{\boldsymbol{x}_i\}$, $i = 1, 2, \ldots, s$.

2.2. Показать, что кодовые слова чётного веса двоичного группового (n, k)-кода C образуют подгруппу.

2.3. Показать, что в каждом двоичном линейном коде либо каждый кодовый вектор имеет чётный вес, либо половина кодовых векторов имеет чётные веса и половина – нечётные.

2.4. Убедиться, что множество всех кодовых слов чётного веса $C_ч$ группового (n, k)-кода C есть подпространство и найти смежные классы кода C по этому подпространству.

2.5. Проверить утверждение: множество всех кодовых слов группового (n, k)-кода, содержащих 0 в некоторой фиксированной позиции, есть подпространство. Найти разложение (n, k)-кода на смежные классы по этому подпространству. Проверку провести на примере (5, 3)-кода.

2.6. Может ли порождающая матрица группового (n, k)-кода иметь:

a) нулевую вектор-строку,
b) нулевой вектор-столбец?

2.7. Может ли проверочная матрица группового (n, k)-кода иметь:

a) нулевую вектор-строку,
b) нулевой вектор-столбец?

2.8. Определить $N^{сис}_{(n,k)}$ – число всех различных систематических (n, k)-кодов.

2.9. Определить $N^{асис}_{(n,k)}$ – число всех различных групповых асистематических (n, k)-кодов.

2.10. Доказать, что двоичный линейный код исправляет любые однократные ошибки тогда и только тогда, когда все

столбцы его проверочной матрицы H – ненулевые и различные. Привести для рассматриваемого случая оценку $d_{мин}$ сверху и снизу.

2.11. Показать, что если систематический (n, k)-код с проверкой на чётность имеет нечётный минимальный кодовый вес $d_{мин}$, то добавление ко всем его словам одного проверочного символа и модификация порождающей G и проверочной H матриц с сохранением их канонических форм создаёт новый систематический $(n + 1, k)$-код с проверкой на чётность с кодовым весом $d^*_{мин} = d_{мин} + 1$.

2.12. Доказать, что код с повторением и код с общей проверкой на чётность – дуальные друг к другу коды.

2.13. Найти число векторов из B^n ортогональных к данному вектору $\boldsymbol{v}$ из B^n_k.

2.14. Показать, что множество всех векторов из B^n, ортогональных к каждой из строк порождающей матрицы $G_{(n, k)}$, образует линейное пространство. Всегда ли это пространство имеет размерность $(n - k)$?

2.15. Может ли ненулевой вектор принадлежать одновременно групповому (n, k)-коду и дуальному к нему групповому $(n, n - k)$-коду?

2.16. Пусть C – кодовая матрица двоичного (n, k)-кода, не содержащая нулевых столбцов. Показать, что:

1) каждый столбец матрицы C имеет 2^{k-1} единиц и столько же нулей;
2) сумма весов строк матрицы C равна $n2^{k-1}$.

2.17. Показать, что кодовое расстояние (n, k)-кода не превосходит $[n2^{k-1}/(2^k - 1)]$.

2.18. Показать, что при $n = 2d_{\min} - 1$ мощность линейного $<n, d_{\min}>$-кода не превосходит $2d_{\min}$.

2.19. Чему равно минимальное число элементов следующих алгебраических структур: 1) группы; 2) кольца, 3) поля, 4) идеала?

2.20. Пусть задан систематический (n, k)-код с кодовым расстоянием $d_{\min}$. Верно ли, что в этом случае существует систематический (n, k)-код с кодовым расстоянием $(d_{\min} - 1)$?

2.21. Показать, что не существует кода длины $n = 20$, содержащего 1000 кодовых слов и исправляющего все трёхкратные и менее кратные ошибки.

2.22. Двоичный (8, 4)-код задан порождающей матрицей

$$G_{(8,4)} := \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}. \qquad (2\text{-}78)$$

Найти его проверочную матрицу и кодовое расстояние. К какому виду (асистематический или условно систематический первого или второго типа) относится (8, 4)-код, порождаемый приведенной в (2-78) матрицей, и к какому виду (из приведенных в табл. 2.11) относится эта матрица?

2.23. Показать, что существует группа из двух элементов.

2.24. Как изменится кодовое расстояние двоичного линейного кода при добавлении ко всем его словам одного *проверочного символа*, задающего общую проверку?

2.25. Согласно примеру 2.17 каждому конкретному групповому (n, k)-коду, являющемуся k-мерным подпространством, соответствует $N_{(k)}$ ***различных*** базисов, которые можно выписать с помощью некоторой ***конкретной*** совокупности $N_{(k)}$ порождающих матриц, *множества векторов-строк которых являются попарно* ***различными***, т.к. только в этом случае они будут представлять $N_{(k)}$ различных базисов.

Доказать, что для *любого конкретного* k-мерного подпространства, определяемого некоторым конкретным *систематическим* групповым (n, k)-кодом, найдётся, по крайней мере, одна совокупность из $N_{(k)}$ различных порождающих матриц, среди которых имеется одна матрица типа $[\boldsymbol{I}_k \boldsymbol{R}_{k\times(n-k)}]$, а остальные $N_{(k)} - 1$ матрицы являются матрицами типа $[\mathcal{T}_{k\times k} \mathcal{R}_{k\times(n-k)}]$.

Доказать также, что с помощью применения элементарной операции транспозиции только к строкам порождающих матриц из некоторой конкретной одной упомянутой выше совокупности (содержащей матрицу $[\boldsymbol{I}_k \boldsymbol{R}_{k\times(n-k)}]$) $N_{(k)}$ порождающих матриц, рассматриваемое конкретное k-мерное подпространство может быть в общем случае представлено:

-с помощью $k!$ различных порождающих матриц, среди которых имеется одна матрица типа $[\boldsymbol{I}_k \boldsymbol{R}_{k\times(n-k)}]$ и $(k! - 1)$ различных матриц типа $[\boldsymbol{I}_{[k]} \boldsymbol{R}_{[k\times(n-k)]}]$;

или

-с помощью $k!(N_{(k)} - 1)$ различных матриц типа $[\mathcal{T}_{k\times k} \mathcal{R}_{k\times(n-k)}]$.

2.26. Доказать, что в любом конкретном семействе из $N_{(k)}$ *различных* порождающих матриц любого конкретного асистематического группового (n, k)-кода (см. задачу 25), множества

векторов-строк которых *попарно различны*, ***все*** порождающие матрицы являются матрицами типа $[\Xi_{k\times k}\, \boldsymbol{R}_{k\times(n-k)}]$.

Доказать также, что с помощью применения элементарной операции транспозиции только к строкам порождающих матриц из упомянутого выше семейства, рассматриваемый конкретный асистематический групповой (n, k)-код может быть в общем случае представлен помощью $k!N_{(k)}$ различных порождающих матриц типа $[\Xi_{k\times k}\, \boldsymbol{R}_{k\times(n-k)}]$.

2.11. ВЫВОДЫ

В настоящем разделе рассматриваются вопросы описания блоковых двоичных групповых (n, k)-кодов, вопросы кодирования передаваемых сообщений и декодирования принятых комбинаций на выходе ДСК.

Приведены необходимые сведения из алгебры о таких алгебраических структурах, как группа, кольцо, поле.

Изложены вопросы описания групповых (n, k)-кодов с помощью порождающих и проверочных матриц и кодирования и декодирования.

Приведены сведения по оценке корректирующих свойств групповых (n, k)-кодов.

Изложены принципы подсчёта различных однородных объектов и некоторые результаты выполненных подсчётов.

Приведена классификация порождающих матриц, позволившая дать определение условно систематических и асистематических кодов.

Рассмотрены укороченные групповые коды.

Наряду с классическими результатами, здесь приведены также оригинальные результаты:

классификация блоковых (n, k)-кодов с проверкой на чётность (систематические, условно систематические первого и второго типов и асистематические коды);

классификация форм порождающих их матриц (каноническая и условно каноническая);

описание обобщённого ДСК.

Табл. 2.11 содержит некоторые обозначения понятий, введённых и рассмотренных в текущем разделе книги.

Таблица 2.11

Порождающие матрицы групповых (n, k)-кодов с проверкой на чётность	
Порождающие матрицы систематических и условно систематических (n, k)-кодов	Порождающие матрицы асистематических (n, k)-кодов
$[\boldsymbol{I}_k\, \boldsymbol{R}_{k\times(n-k)}]$, $[\boldsymbol{I}_{[k]}\, \boldsymbol{R}_{[k\times(n-k)]}]$, $[\mathfrak{I}_{k\times k}\, \mathfrak{R}_{k\times(n-k)}]$	$[\Xi_{k\times k}\, \boldsymbol{R}_{k\times(n-k)}]$

2.12. ЛИТЕРАТУРА

Основная

2.1. Галлагер Р. Теория информации и надёжная связь. М.: Советское радио, 1974.

2.2. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, 1976.

2.3. Касами Т., Токура Н., Ивадари Ё и др. Теория кодирования. М.: Мир, 1978.

2.4. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.

2.5. Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977.

2.6. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.