# Системы цифрового телевидения для тех, кто хочет понять: кодирование, исправляющее ошибки

*Константин Гласман*

Часть 4. Начало в №№ 6-8

## Код Хэмминга: кодирование

Целью разработки систем, исправляющих ошибки в каналах связи, является создание кодов с особыми структурными закономерностями. Наличие таких закономерностей обеспечивает возможность практической реализации операций кодирования и декодирования без составления огромных таблиц кодирования и декодирования для длинных кодов, когда трудно даже перечислить все кодовые слова.

Многие хорошие коды основаны на идеях проверки на четность. В разделе о коде с одной проверкой на четность (MediaVision № 7/2020, стр. 26) используется одна проверка на четность. Слово на выходе кодера ***x*** формируется путем добавления к информационным символам одного проверочного символа *p* так, чтобы число единиц в каждом кодовом слове было четным. Добавляемый символ *p* называют битом проверки на четность. Полученный код обладает минимальным расстоянием $d^*=2$. Он способен только обнаруживать одну ошибку в кодовом слове. Для увеличения минимального расстояния можно добавлять проверочные биты, которые должны вычисляться путем выполнения некоторых арифметических процедур над символами информационного слова.

Рассмотрим кодирование четырехразрядного двоичного информационного слова $\boldsymbol{u}=(u_1, u_2, u_3, u_4)$ с помощью кода Хэмминга [10] путем добавления трех проверочных символов: $p_1$, $p_2$, $p_3$. Будем считать код систематическим. Тогда первые четыре символа кодового слова $\boldsymbol{x}=(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ будут равны информационным символам: $x_1=u_1$, $x_2=u_2$, $x_3=u_3$, $x_4=u_4$. Последние три символа кодового слова представляют собой проверочные символы: $x_5=p_1$, $x_6=p_2$, $x_7=p_3$. Длина кодового слова равна $n=7$, мощность равна $M=2^k=2^4=16$. Это блоковый код с параметрами $(n, k)=(7,4)$.

Каждый проверочный символ проверяет некоторое множество предварительно заданных информационных символов. Определим проверочные символы равенствами:

$$p_1=u_1+u_2+u_3,$$
$$p_2=u_2+u_3+u_4, \qquad (7)$$
$$p_3=u_1+u_2+u_4.$$

Результаты вычисления шестнадцати кодовых слов приведены в табл. 9. Определение важнейшего параметра кода – минимального расстояния – требует попарного сравнения кодовых слов. Даже для 16 слов это превращается в трудоемкую процедуру. Но, как было отмечено, заложенные в основу кода математические структуры могут помочь в решении многих задач.

Код Хэмминга относится к классу линейных кодов. Напомним, что код называется линейным,

***Таблица 9. Кодирование для (7, 4)-кода Хэмминга***

| Информационные слова | | | | Кодовые слова | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| u1 | u2 | u3 | u4 | x1 | x2 | x3 | x4 | x5 | x6 | x7 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

если сумма любых кодовых слов дает кодовое слово. В том, что код Хэмминга является линейным, нетрудно убедиться, складывая поразрядно слова табл. 9 по правилам сложения поля из двух элементов (табл. 5 и табл. 6, часть 3, № 8/2020). Например, складывая поразрядно слова из второй и третьей строк (0+0)=0, (0+0)=0, (0+1)=1, (1+0)=1, (0+1)=1, (1+1)=0, (0+1)=1 получаем кодовое слово, которое находится в четвертой строке табл. 9. Из свойства линейности вытекает, что нулевое слово (слово, состоящее из одних нулей) входит в число кодовых слов, так как складывая слово с самим собой, мы получаем нулевое слово.

Для нахождения минимального расстояния линейного кода не надо сравнивать все пары кодовых слов. Достаточно найти слова, ближайшие к нулевому слову. Для линейного кода минимальное расстояние равно минимальному весу ненулевого слова. Это означает, что надо подсчитать число ненулевых символов в кодовых словах, ближайших к нулевому. Нетрудно убедиться, что минимальный вес *(7, 4)*-кода Хэмминга равен *3*, следовательно, минимальное расстояние $d^*=3$. С помощью *(7, 4)*-кода Хэмминга можно исправить одну ошибку в каждом кодовом слове.

В таблице кодирования *(7, 4)*-кода находится 16 кодовых слов. В таблице декодирования этого кода должно быть 128 кодовых слов, что затрудняет построение декодера даже для такого сравнительно простого кода. Но линейность кода позволяет найти сравнительно простую процедуру, если ввести матричное описание кода как подпространства в векторном пространстве.

Обобщением трехмерного пространства на случай слов с длиной *n* является *n*-мерное векторное пространство. Информационное слово $\boldsymbol{u}=(u_1, u_2, u_3, u_4)$ можно рассматривать как вектор в четырехмерном пространстве. Кодовое слово $\boldsymbol{x}=(x_1, x_2, \ldots, x_7)$, полученное с помощью канального кодера Хэмминга путем добавления трех проверочных символов, представляет собой вектор в семимерном пространстве. Множество кодовых слов *(7,4)*-кода Хэмминга представляет собой кодовое подпространство в пространстве всех векторов семимерного пространства.

## Матричное описание линейных блоковых кодов

### *Порождающая матрица*

Вернемся к обсуждению кодирования четырехразрядного двоичного информационного слова $\boldsymbol{u}=(u_1, u_2, u_3, u_4)$ с помощью кода Хэмминга $(n, k)=(7, 4)$ путем добавления трех проверочных символов. Информационное слово $\boldsymbol{u}=(u_1, u_2, u_3, u_4)$ является вектором в четырехмерном пространстве. Кодовое слово $\boldsymbol{x}=(x_1, x_2, \ldots, x_7)$, полученное с помощью канального кодера, можно рассматривать как вектор в семимерном пространстве.

Найдем обобщенное описание процедуры кодирования. Последние $(n-k)=3$ символа кодового слова представляют собой проверочные символы $p_1$, $p_2$, $p_3$, рассчитываемые с использованием соотношений (7), которые можно переписать с использованием чисел $p_{ij}$ (табл.10):

$$p_1=u_1+u_2+u_3=u_1 p_{11}+u_2 p_{21}+u_3 p_{31}+u_4 p_{41},$$
$$p_2=u_2+u_3+u_4=u_1 p_{12}+u_2 p_{22}+u_3 p_{32}+u_4 p_{42}, \qquad (8)$$
$$p_3=u_1+u_2+u_4=u_1 p_{13}+u_2 p_{23}+u_3 p_{33}+u_4 p_{43},$$

***Таблица.10. Элементы матрицы четности P для (7, 4)-кода Хэмминга***

| $P_{ij}$ | | j | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| i | 1 | 1 | 0 | 1 |
| | 2 | 1 | 1 | 1 |
| | 3 | 1 | 1 | 0 |
| | 4 | 0 | 1 | 1 |

Для того, чтобы, например, первая строка (8) совпадала с первой строкой (7), необходимо, чтобы $p_{11}=1$, $p_{21}=1$, $p_{31}=1$, $p_{41}=0$, что и записано в табл. 10. Более длинная запись соотношений (8) позволила добиться единообразия форм записи всех проверочных символов. Как видно из соотношений (8), вычисления теперь ведутся по подобным формулам, строки отличаются только числами $p_{ij}$,

поэтому (8) можно переписать с использованием одного выражения:

$$p_j = \sum_{i=1}^{k} u_i\, p_{ij}; \quad 1 \le j \le n-k, \qquad (9)$$

Здесь надо сделать отступление и напомнить некоторые сведения о матрицах.

Матрица ***A*** размерности *m*×*n* – это упорядоченное множество из mn элементов (в нашем случае элементами матицы являются числа из поля Галуа), расположенных в виде прямоугольной таблицы, которая содержит *m* строк и *n* столбцов:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = [a_{ij}]$$

$$= \boldsymbol{A},\ 1 \le i \le m, 1 \le j \le n.$$

Матрицы можно поэлементно складывать. Их можно умножать на скаляр, умножая на него каждый элемент. Напомним правила перемножения матриц как таблиц чисел. Можно перемножать и квадратные и прямоугольные матрицы. Надо иметь в виду, что произведение матриц не является коммутативным, то есть, ***A*B ≠ B*A***. Произведение матриц имеет смысл только в том случае, если число столбцов первой матрицы равно числу строк второй матрицы. Найдем произведение ***C=A*B***:

$$[c_{ij}] = [a_{ij}][b_{ij}].$$

Если матрица ***A*** имеет *m* строк и *n* столбцов, а матрица ***B*** имеет *n* строк и *k* столбцов, то матрица ***C*** будет иметь *m* строк и *k* столбцов. Элемент матрицы ***C***, который находится на пересечении строки *i* и столбца *j*, представляет собой скалярное произведение строки *i* матрицы ***A*** и столбца *j* матрицы ***B***:

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} =$$

$$= \sum_{l=1}^{n} a_{il}\ b_{lj}; \le i \le m, 1 \le j \le k.$$

Строки и столбцы матрицы, представляющие собой наборы элементов, можно рассматривать как векторы. Вектор можно рассматривать как матрицу, состоящую из одной строки. Если умножается вектор-строка ***A*** из *n* элементов $[a_{1j}]$ на матрицу ***B***, то ***C*** представляет собой вектор-строку $[c_{1j}]$ из *k* элементов:

$$c_{1j} = a_{11}b_{1j} + a_{12}b_{2j} + \cdots + a_{1n}b_{nj} =$$

$$= \sum_{l=1}^{n} a_{1l}\ b_{lj}; \quad 1 \le j \le k.$$

Вернемся к обобщенному описанию процедуры кодирования кода Хэмминга. Если рассматривать ***u***=($u_1$, $u_2$, $u_3$, $u_4$) и ***p***=($p_1$, $p_2$, $p_3$) как векторы, то формулы (8) и (9) представляют собой произведение вектора ***u*** на матрицу четности ***P***:

$$\boldsymbol{p} = \boldsymbol{u}\,\boldsymbol{P} = [u_j][p_{i,j}], \qquad (10)$$

где $\boldsymbol{P} = [p_{ij}] = \begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \\ p_{41} & p_{42} & p_{43} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$, (11)

Матрица – это матрица из трех строк и четырех столбцов, элементы которой взяты из табл. 10. Она описывает линейное преобразование вектора ***u*** в вектор ***p*** проверочных символов. Произведение ***u*** на ***P*** выполняется по правилам перемножения матриц. Но при этом ***u*** и ***p*** рассматриваются как вектор-строки, или матрицы из одной строки. Эти правила фактически описываются соотношениями (8) и (9). Для получения ***j***-го символа вектора ***p***, обозначаемого как $p_j$, надо сложить поэлементные произведения компонент вектора-строки ***u*** и *j*-го столбца матрицы ***P***, как это предписывают формулы (8) и (9).

Формула (10) задает формирование трех старших разрядов кодового слова, в которых находятся проверочные символы. Подобное выражение надо получить для формирования при кодировании всего кодового слова. Как уже было отмечено, код систематический, поэтому первые *k* символов (*k*=4) кодового слова $x_1$, $x_2$, $x_3$, $x_4$ равны информационным символам: $x_j=u_j$ при *j*=1, 2, 3, 4. Объединяя это равенство с правилом (9) вычисления проверочных символов, которые смещаются вправо на *k* разрядов и располагаются в *(n-k)* старших разрядах кодового слова, получаем:

$$x_j = u_j; \quad 1 \le j \le k, \qquad (12)$$

$$x_j = \sum_{i=1}^{k} u_i\, p_{i,j-k}; \quad k+1 \le j \le n, \qquad (13)$$

Правило расчета символов кодового слова может быть записано с помощью одного общего выражения вместо двух выражений (12) и (13):

$$x_j = \sum_{i=1}^{k} u_i\, g_{i,j}; \quad 1 \le j \le n, \qquad (14)$$

где

$g_{ij} = 1$; $i = j,\ 1 \le j \le k$,

$g_{ij} = 0$; $i \ne j,\ 1 \le j \le k$,

$g_{ij} = p_{i,j-k}$; $k+1 \le j \le n$,

Числа приведены в табл. 11 для значений индексов и . Индекс *i* показывает номер информационного символа, который входит в выражение для расчета кодового символа; индекс ***j*** показывает номер кодового символа.

***Таблица 11. Элементы порождающей матрицы G для (7, 4)-кода Хэмминга***

| $g_{i,j}$ | | j | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| i | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| | 2 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| | 3 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| | 4 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |

Соотношение (14) можно выразить в более компактной форме, если рассматривать числа таблицы 11 как компоненты матрицы с размерами 4 строки и 7 столбцов, а информационное и кодовое слова как вектор-строки:

$$\boldsymbol{x} = \boldsymbol{u}\,\boldsymbol{G} = [u_j]\,[g_{i,j}], \qquad (15)$$

где $\boldsymbol{G} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{17} \\ g_{21} & g_{22} & \cdots & g_{27} \\ \vdots & \vdots & \vdots & \vdots \\ g_{41} & g_{42} & \cdots & g_{47} \end{bmatrix} = [g_{ij}]$, (16)

$\boldsymbol{u} = (u_1, u_2, u_3, u_4) =$ , (17)

$\boldsymbol{x} = (x_1, x_2, \ldots, x_7) =$ . (18)

Матрица ***G*** называется порождающей матрицей кода. Она задает линейное отображение множества $2^k$ информационных слов в множество $2^k$ кодовых слов с длиной блока *n*. Порождающая матрица – это компактное описание кода, она заменяет таблицу кодирования.

Выше было отмечено, что код Хэмминга является линейным кодом. Подтвердим это с использованием выражения (15). Пусть сумма двух информационных слов $\boldsymbol{u}_A$ и $\boldsymbol{u}_B$ дает информационное слово $\boldsymbol{u}_C$. Если соответствующие кодовые слова равны $\boldsymbol{x}_A=\boldsymbol{u}_A\boldsymbol{G}$ и $\boldsymbol{x}_B=\boldsymbol{u}_B\boldsymbol{G}$, то

$$\boldsymbol{x}_A+\boldsymbol{x}_B=\boldsymbol{u}_A\boldsymbol{G}+\boldsymbol{u}_B\boldsymbol{G}=(\boldsymbol{u}_A+\boldsymbol{u}_B)\boldsymbol{G}=\boldsymbol{u}_C\boldsymbol{G}=\boldsymbol{x}_C. \qquad (19)$$

Из равенства (19) следует, что сумма двух кодовых слов равна другому кодовому слову.

Из соотношений (14) и (15) следует, что если в информационном слове есть только один символ, равный 1, например, в позиции ***j***, то рассчитанное слово равно ***j***-той строке порождающей матрицы ***G***, (строка *j* обозначена как $\boldsymbol{g}_j$). С учетом соотношения (19) получаем, что произвольное кодовое слово можно представить как линейную комбинацию строк порождающей матрицы ***G***:

$$\boldsymbol{x} = \sum_j u_j\, g_j \qquad (20)$$

Соотношение (20) означает, что множество кодовых слов является пространством строк порождающей матрицы кода ***G***.

Можно также отметить, что строки порождающей матрицы линейно независимы. В общем случае размерность всего пространства слов равна *n*. Число строк матрицы *k* равно размерности подпространства кодовых слов. Всего существует $q^k$ кодовых слов над полем Галуа ***GF(q)***. Таким образом, $q^k$ различных информационных наборов длины *k* могут быть отображены на множество кодовых слов длины *n*.

Матрицы можно разбивать на блоки. Матрица четности ***P*** с размерами *k*=4 строки на *(n-k)*=3 столбца была введена ранее в соотношении (11). Ее можно выделить в качестве одного блока порождающей матрицы ***G***. Тогда вторым блоком будет так называемая единичная матрица с размерами 4 строки и 4 столбца. Элементы главной диагонали единичной матрице равны 1. Остальные элементы равны 0:

$$\boldsymbol{I}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad (21)$$

Тогда порождающая матрица ***G*** может быть представлена в виде комбинации единичной матрицы $\boldsymbol{I}_4$ и матрицы четности ***P***:

$$\boldsymbol{G} = [\boldsymbol{I}_4 \vdots \boldsymbol{P}] = [\boldsymbol{I}_k \vdots \boldsymbol{P}] \qquad (22)$$

Надо напомнить, что порождающая матрица рассматриваемого примера была найдена для систематического кода. Справедливо и обратное утверждение. Если порождающая матрица состоит из двух блоков вида (22), то она отображает информационные символы в кодовые слова систематического кода.

*Проверочная матрица*

Выше было отмечено, что порождающая матрица – это компактное описание кода, заменяющее таблицу кодирования кода. Еще более желательным является компактное описание кода, заменяющее таблицу декодирования. Для достижения этой цели вводится проверочная матрица кода ***H***. Она объясняется на примере рассматриваемого кода Хэмминга.

Для получения проверочной матрицы надо сначала найти матрицу, транспонированную к матрице четности ***P***. Транспонирование матрицы производится путем замены строк матрицы ее столбцами. Заменяя строки матрицы ***P*** в выражении (11) ее столбцами, получаем:

$$P^T = \begin{bmatrix} p_{11} & p_{21} & p_{31} & p_{41} \\ p_{12} & p_{22} & p_{32} & p_{42} \\ p_{13} & p_{23} & p_{33} & p_{43} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \quad (23)$$

Матрица ***P*** насчитывала 4 строки и 3 столбца, а в транспонированной матрице $P^T$ насчитывается 3 строки и 4 столбца. В соответствии с выражением (22) порождающая матрица ***G*** в первых k столбцах содержит единичную матрицу $I_4$, а в последних ***(n-k)*** столбцах – матрицу ***P***. Проверочная матрица ***H*** в первых ***(n-k)*** столбцах содержит транспонированную матрицу $P^T$, взятую со знаком минус, а в последних ***k*** столбцах - единичную матрицу $I_3$:

$$H = [-P^T : I_3] = \left[\begin{array}{cccc|ccc} p_{11} & p_{21} & p_{31} & p_{41} & 1 & 0 & 0 \\ p_{12} & p_{22} & p_{32} & p_{42} & 0 & 1 & 0 \\ p_{13} & p_{23} & p_{33} & p_{43} & 0 & 0 & 1 \end{array}\right] =$$

$$= \left[\begin{array}{ccccc|cc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]. \quad (24)$$

Для двоичного поля Галуа вычитание выполняется по правилам сложения, поэтому знак минус в выражении (23) можно не учитывать. Транспонированная матрица $H^T$ может быть найдена, если в выражении (24) поменять местами строки и столбцы:

$$H^T = \begin{bmatrix} -P \\ \cdots \\ I_3 \end{bmatrix} = \begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \\ p_{41} & p_{42} & p_{43} \\ \cdots & \cdots & \cdots \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ \cdots & \cdots & \cdots \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (25)$$

***Таблица 13. Элементы транспонированной проверочной матрицы HT для (7, 4)-кода Хэмминга***

| $h^T_{ij}$ | j | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| i 1 | 1 | 0 | 1 |
| 2 | 1 | 1 | 1 |
| 3 | 1 | 1 | 0 |
| 4 | 0 | 1 | 1 |
| 5 | 1 | 0 | 0 |
| 6 | 0 | 1 | 0 |
| 7 | 0 | 0 | 1 |

***Таблица 12. Элементы проверочной матрицы H для (7, 4)-кода Хэмминга***

| $h_{ij}$ | J | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| i 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 2 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 3 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |

Элементы проверочной матрицы ***H*** и транспонированной проверочной матрицы $H^T$ для (7, 4)-кода Хэмминга приведены в табл. 12 и 13.

Важный результат позволяет получить перемножение порождающей матрицы ***G*** и транспонированной проверочной матрицы $H^T$, заданных для систематического кода формулами (22) и (25):

$$GH^T = [I_4 : P] \begin{bmatrix} -P \\ \cdots \\ I_3 \end{bmatrix} = -P + P = 0. \quad (26)$$

Вычисления в соотношении (26) выполнялись по правилам перемножения матриц с учетом того, что умножение некоторой матрицы на единичную матрицу дает исходную матрицу ($I_4*(-P)=-P$, $P*I_3=P$).

Как следует из (26), замечательное свойство проверочной матрицы заключается в том, что слово ***x*** является кодовым в том и только в том случае, когда

$$x H^T = 0. \quad (27)$$

Произведение кодового вектора на проверочную матрицу всегда равно нулю. Это свойство может использоваться при декодировании, чтобы проверять, является ли принятое слово кодовым.

Можно отметить несколько общих свойств проверочных матриц. С использованием проверочной матрицы ***H*** можно построить линейный код, дуальный по отношению к коду, построенному на базе порождающей матрицы ***G***. Для этого надо использовать матрицу ***H*** как порождающую, то есть умножать информационные векторы на матрицу ***H***. Это будет давать кодовые слова дуального кода. Кодовые слова такого дуального кода будут представлять собой линейные комбинации строк матрицы ***H***. Интересно, что матрица ***G*** будет проверочной матрицей для дуального кода.

Один из способов проектирования нового кода заключается в создании новой порождающей матрицы ***G***. Но можно использовать и другой способ – создавать новую проверочную матрицу ***H***. Речь идет о создании не дуального, а нового кода, в котором стартовой точкой является построение проверочной матрицы этого нового кода. Это означает, что первым этапом является разработка процедуры декодирования с использованием матрицы ***H*** как компактного описания декодирования. Чтобы создать линейный *(n, k)*-код, исправляющий *t* ошибок, достаточно найти *(n-k)*×*n* матрицу ***H***, в которой *2t* столбцов линейно независимы [10]. Для разработки кодера на втором этапе создается порождающая матрица ***G*** как компактное описание процесса кодирования. Коды с малой плотностью проверок на четность были изобретены на базе второго подхода, когда создание кода начинается с построения проверочной матрицы.

## *Синдром*

Декодирование можно выполнять с помощью таблицы декодирования. Систематизированную форму декодирования дает стандартное расположение, описанное в разделе «Стандартное расположение» (MediaVision № 8/2020, стр. 53). Использование проверочной матрицы позволяет формализовать построение стандартного расположения. В декодере выполняется перемножение принятого слова ***y*** на транспонированную проверочную матрицу $H^T$. Результат перемножения $yH^T$ равен нулю в том и только в том случае, если принятое слово равно кодовому, как устанавливает выражение (27). Результат перемножения $yH^T$, не равеный нулю, можно использовать для нахождения и исправления ошибки. Произведение принятого слово на транспонированную проверочную матрицу называется синдромом:

$$s = y H^T. \quad (28)$$

Элементы транспонированной проверочной матрицы $h^T_{ij}$ приведены в табл. 13. Перемножая вектор-строку ***y***, которая имеет ***n*** компонентов (в рассматриваемом примере *n*=7), и матрицу $H^T$, в которой *n* строк и (*n-k*) столбцов (в рассматриваемом примере это дает ***n=7*** строк и (*n-k*)=3 столбцов), мы получаем вектор-строку, имеющую (*n-k*) компонент (для (7, 4)-кода это 3 компоненты):
$\mathbf{s} = (s_1, s_2, \ldots, s_{(n-k)})$.

Компоненты синдрома вычисляются в соответствии с правилами перемножения матриц (в данном случае это произведение вектора, или матрицы с одной строкой, на матрицу с размерами 7 строк и 3 столбца):

$$s_j = \sum_{i=1}^{n} y_i h^T_{ij}; \quad 1 \le j \le n-k. \quad (29)$$

Передаваемый по каналу связи блок символов ***x*** может претерпеть искажения. Разницу между принятым блоком ***y*** и посланным блоком ***x*** можно трактовать как шумовой блок:

$$e = y - x \quad (30)$$

Подставляя в выражение для синдрома (28) представление принятого блока как сумму кодового блока, отправленного в канал связи, и шумового блока, с учетом соотношения (27) получаем:

$$s = yH^T = (x + e) H^T = xH^T + eH^T = eH^T. \quad (31)$$

Таким образом, синдром не зависит от отправленного кодового блока и определяется только шумовым блоком. Синдром в общем случае – это совокупность симптомов, характеризующих некоторое заболевание. Вектор-строка синдрома зависит только от конфигурации ошибок, то есть является синдромом, или описанием ошибок.

***Таблица 14. Синдромы разных конфигураций шумовых блоков для (7, 4)-кода Хэмминга***

| Шумовой блок e | | | | | | | Синдром s | | |
|---|---|---|---|---|---|---|---|---|---|
| e1 | e2 | e3 | e4 | e5 | e6 | e7 | s1 | s2 | s3 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |

Результаты вычисления синдромного вектора для (7, 4)-кода Хэмминга по формуле (31) для разных конфигураций шумовых блоков приведены в табл. 14.

*Продолжение следует*