$$p(y/\boldsymbol{a}_i)\begin{cases} \geq 1-\varepsilon, & \text{если } y \in M_i, \text{ или } y = \boldsymbol{a}_i, \\ < \varepsilon, & \text{если } y \notin M_i \text{ и } y \neq \boldsymbol{a}_i, \end{cases} \qquad (1\text{-}26)$$

где ε – приемлемо малое положительное число, характеризующее вероятность ошибочного декодирования.

ПРИМЕР 1.11. Важным и универсальным средством, которое математически описывает процесс принятия решения при декодировании получаемых на выходе канала слов, является *таблица декодирования*.

Даны параметры корректирующего кода:

$$L = 2;\ n = 3,\ N = 2,\ N_0 = L^n = 8.$$

Табл. 1.2 иллюстрирует переходы кодовых комбинаций $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$ в выходные комбинации канала вследствие возникновения ошибок различной кратности в канале.

В таблицах декодирования – табл. 1.3 и 1.4 под $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$ приведены два конкретных разбиения $\{M_1, M_2\}$, приводящие к исправлению ошибок кратности $q = 1$ и кратности $q = 2$ соответственно.

Очевидно, что на практике следует выбирать то конкретное разбиение $\{M_1, M_2\}$, которому соответствует кратность q *более вероятных ошибок*.

Основные свойства таблицы декодирования для некоторого конкретного кода и конкретного канала:

первая строка таблицы образована кодовыми словами используемого кода;

если на выходе канала получено некоторое кодовое слово $y = \boldsymbol{x} \in \{\boldsymbol{a}_1, \boldsymbol{a}_2\}$, то при декодировании принимается решение, что было передано именно это кодовое слово $\boldsymbol{x}$;

под каждым кодовым словом $\boldsymbol{x}$, расположенным в первой строке, таблицы помещаются те возможные слова на выходе канала y, которые должны декодироваться в это кодовое слово;

каждое слово y, которое может появиться на выходе канала, входит в таблицу декодирования один и только один раз;

если на выходе канала получено некоторое слово y, то оно *декодируется* с помощью *таблицы декодирования* в кодовое слово $\boldsymbol{x}$, под которым оно стоит: $\boldsymbol{x} = \boldsymbol{x}(y)$.

Таблица 1.2

i	$\boldsymbol{e}_i$	$\boldsymbol{a}_1$= 100	$\boldsymbol{a}_2$= 011	q_i
1	000	100 (=$\boldsymbol{a}_1$)	011 (=$\boldsymbol{a}_2$)	0
2	100	000	111	1
3	010	110	001	1
4	001	101	010	1
5	110	010	101	2
6	101	001	110	2
7	011	111	000	2
8	111	011 (=$\boldsymbol{a}_2$)	100 (=$\boldsymbol{a}_1$)	3

Таблица 1.3

$\boldsymbol{a}_1$= 100	$\boldsymbol{a}_2$= 011
000	111
110	001
101	010

Таблица 1.4

$\boldsymbol{a}_1$= 100	$\boldsymbol{a}_2$= 011
010	101
001	110
111	000

Легко видеть, что табл. 1.3 – таблица декодирования для рассматриваемого кода при гипотетически наиболее вероятных однократных ошибках; и что табл. 1.4 – таблица де-

кодирования для рассматриваемого кода при гипотетически наиболее вероятных двукратных ошибках.

END

ЗАМЕЧАНИЕ 1.3. Легко понять, что выбор конкретного разбиения множества всех запрещённых комбинаций $\{\boldsymbol{b}_j\}$ на подмножества M_i, $i = 1, 2, \ldots, N$, определяет кратность ошибок, подлежащих исправлению при декодировании полученных на выходе канала комбинаций. Зная статистику ошибок в канале, можно целенаправленным образом подбирать подмножества M_i, $i= 1, 2, \ldots, N$, так, чтобы наиболее эффективно исправлять наиболее вероятные ошибки.

END

СЛОЖНОСТЬ КОДЕРА

Будем считать [1.8], что сообщения представлены двоичными последовательностями длины $n_0 = k$ и что выполняется соотношение

$$2^k = N. \qquad (1\text{-}27)$$

Предположим также, что требуемое значение $d_{\min}$ достигается при длине кодовых комбинаций n и, следовательно, число всевозможных двоичных комбинаций длины n

$$N_0 = 2^n, \qquad (1\text{-}28)$$

где $n > k$.

Пусть $\{\boldsymbol{a}_i\}$, $i = 1, 2, \ldots, N$, – множество кодовых комбинаций длины n.

При поступлении на вход кодера канала i-го сообщения – двоичной безызбыточной комбинации длины n_0 кодер должен запомнить эту комбинацию и извлечь из своей памяти соответствующую ей i-ю двоичную кодовую комбинацию $\boldsymbol{a}_i$

длины n. Таким образом, кодер канала должен иметь, по крайней мере,

$$(k + nN) \qquad (1\text{-}29)$$

двоичных ячеек памяти. Найденная величина $(k + nN)$ может служить *приблизительной* оценкой сложности кодера при использовании корректирующего кода. Обычно число сообщений, подлежащих передаче, N является заданным, а следовательно, согласно (1-27) является заданным и $k = n_0$; очевидно, что с ростом мощности шума в канале необходимо увеличивать кодовое расстояние $d_{\min}$ (см. ниже), что влечёт увеличение n и, согласно (1-27) и (1-29), сопровождается увеличением сложности кодера.

В случае группового (n, k)-кода (см. ниже) вместо (1-29) будет справедлива, по крайней мере, приблизительная оценка:

$$(k + nk + n) \qquad (1\text{-}29а)$$

двоичных ячеек памяти.

СЛОЖНОСТЬ ДЕКОДЕРА, РЕАЛИЗУЮЩЕГО УНИВЕРСАЛЬНЫЙ АЛГОРИТМ ДЕКОДИРОВАНИЯ

Важными характеристиками любого корректирующего кода являются простота операции декодирования принятых комбинаций и сложность декодера.

Соотношение (1-25) описывает *универсальный алгоритм декодирования*; на практике процесс декодирования выполняется некоторой логической схемой – декодером, сложность которого определяет его аппаратурную надёжность и стоимость. Быстродействие также является важной характеристикой декодера.

Приведём оценку сложности декодера, реализующего *метод декодирования* (1-25) и применимого для любого корректирующего блокового кода, определяемого параметрами

N, $N_0 = 2^n$ и $N = 2^k$ попарно не пересекающимися подмножествами $\{M_i\}$, $i = 1, 2, \ldots, N$.

Предположим, что декодер имеет число *управляющих входов* n, равное длине принятых комбинаций, и число выходов $N_0 = 2^n$, равное числу принимаемых на выходе канала всевозможных двоичных комбинаций длины n; каждый выход декодера соответствует одной определённой комбинации из числа N_0.

На рис. 1.1, *a* приведено обозначение переключательного элемента на 2 направления; *переключательный элемент* имеет один ***не показанный*** на рисунке *управляющий вход*, один отмеченный крестиком *переключаемый вход* и *два выхода*, с одним из которых соединяется переключаемый вход в зависимости от значения двоичного сигнала на его управляющем входе.

На рис. 1.1, *b* приведена схема рассматриваемого декодера; здесь: большой кружок – переключательный элемент, маленький кружок – выходная клемма, с которой снимается элементарный сигнал ноль или единица. Применяя формулу суммы первых n членов геометрической прогрессии, первый член которой равен 1, а знаменатель равен 2, можно показать, что число переключательных элементов декодера в общем случае равно

$$(2^n - 1), \qquad (1\text{-}29б)$$

т.е. имеет место *экспоненциальная зависимость* числа переключательных элементов декодера от $n\ln 2$; а в рассматриваемом примере оно равно $(2^3 - 1) = 7$.

На практике могут использоваться корректирующие коды с $n \approx 1000 = 10^3$; оценим с помощью соотношения (1-29б) число переключательных элементов рассматриваемого декодера для этого случая

$$(2^n - 1) = (2^{1000} - 1) \approx 2^{1000} \approx (2^{10})^{100} \approx$$

$$\approx (1024)^{100} \approx (10^3)^{100} \approx 10^{300}, \qquad (1\text{-}29в)$$

и так как это число является очень большим, то такой декодер не реализуем. Поэтому, приступая к выбору кода, *необходимо учитывать сложность декодера*, реализующего вместе с кодером выбираемый код.

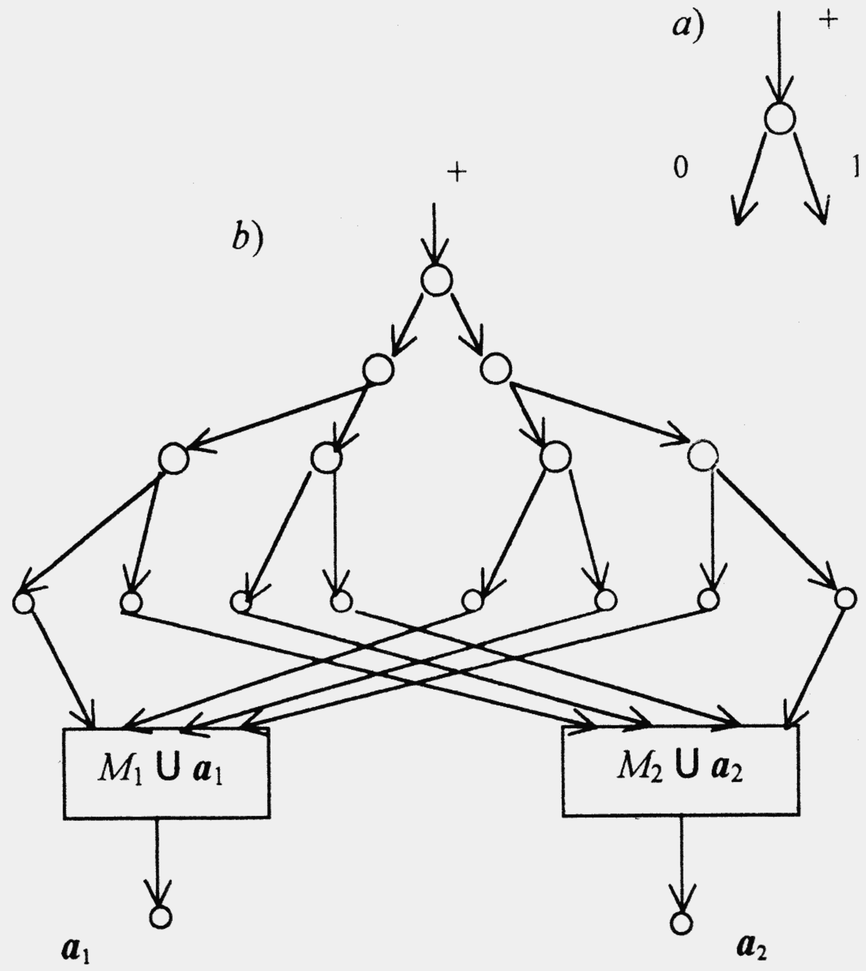

Рис.1.1. Переключающий элемент на 2 направления (*a*); схема рассматриваемого декодера (*b*)

1.6. БЛОКОВЫЕ КОРРЕКТИРУЮЩИЕ КОДЫ С ДЕКОДИРОВАНИЕМ ПО МЕТОДУ МАКСИМАЛЬНОГО ПРАВДОПОДОБИЯ. КОРРЕКТИРУЮЩАЯ СПОСОБНОСТЬ КОДА И КОДОВОЕ РАССТОЯНИЕ

ОПРЕДЕЛЕНИЕ 1.3. *Весом Хэмминга L-ичной* ($L \geq 2$) *комбинации длины n* $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ *называется целое число* $w(\boldsymbol{v}) \geq 0$, *равное* ***числу всех её ненулевых разрядов*** *или* ***нулю***, ***если все её разряды являются нулевыми***:

$$w(\boldsymbol{v}) = \sum_{i=1}^{n} \Phi(v_i - 1) \ , \qquad (1\text{-}30)$$

где $\Phi = \Phi(x)$ – единичная ступенька (функция Хевисайда).

В двоичном случае ($L = 2$) вес $w(\boldsymbol{v}) \geq 0$ равен числу единичных разрядов $\boldsymbol{v}$ $n_{[1]} \geq 0$.

END

ПРИМЕР 1.12

$$w(00000) = 0,$$

$$w(01010) = 2,$$

$$w(11111) = 5.$$

END

В качестве меры удалённости одной кодовой комбинации от другой часто используется понятие «расстояние Хэмминга» или «хэммингово расстояние».

ОПРЕДЕЛЕНИЕ 1.4. *Расстоянием Хэмминга между двумя L-ичными* ($L \geq 2$) *комбинациями одной и той же длины n* $\boldsymbol{v}_i = (v_{i1}, v_{i2}, \ldots, v_{in})$ и $\boldsymbol{v}_j = (v_{j1}, v_{j2}, \ldots, v_{jn})$, $i, j = 1, 2, \ldots, n$, *называется целое число* d, $0 \leq d = d(\boldsymbol{v}_i, \boldsymbol{v}_j) \leq n$, *равное суммарному числу разрядов, в которых эти комбинации* ***различаются***.

END

В случае двоичных кодов

$$d(\boldsymbol{v}_i, \boldsymbol{v}_j) = \sum_{s=1}^{n} | v_{is} - v_{js} |, \quad i, j = 1, 2, \ldots, N_0 \ . \qquad (1\text{-}31)$$

Введённое понятие «расстояние Хемминга» $d(\boldsymbol{v}_i, \boldsymbol{v}_j)$ является метрикой (см. приложение 1.11).

ЛЕММА 1.1. *Расстояние Хэмминга между двумя двоичными комбинациями* $\boldsymbol{v}_i$ *и* $\boldsymbol{v}_j$ *равно* ***весу комбинации***, *являющейся результатом поразрядного сложения* (по mod 2) *этих двух комбинаций*:

$$d(\boldsymbol{v}_i, \boldsymbol{v}_j) = w(\boldsymbol{v}_i \oplus \boldsymbol{v}_j). \qquad (1\text{-}32)$$

ДОКАЗАТЕЛЬСТВО. В комбинации $\boldsymbol{v}_i \oplus \boldsymbol{v}_j$ единицы стоят в тех разрядах, в которых различаются комбинации $\boldsymbol{v}_i$ и $\boldsymbol{v}_j$. Согласно определению веса кодовой комбинации $w(\boldsymbol{v}_i \oplus \boldsymbol{v}_j)$ равно целому числу – числу разрядов, в которых различаются комбинации $\boldsymbol{v}_i$ и $\boldsymbol{v}_j$.

Учитывая сказанное и определение расстояния Хэмминга, получим, что (1-32) выполняется.

ЧТД

Важное значение для оценки обнаруживающей и исправляющей способностей корректирующего кода имеет понятие «минимальное хэммингово расстояние корректирующего кода».

ОПРЕДЕЛЕНИЕ 1.5. *Минимальным хэмминговым расстоянием корректирующего кода* (кратко: *кодовым расстоянием*) *называется целое число*

$$d_{\min} = \min_{i, j / i \neq j} d(\boldsymbol{v}_i, \boldsymbol{v}_j). \qquad (1\text{-}33)$$

END

ОПРЕДЕЛЕНИЕ 1.6. *Максимальным хэмминговым расстоянием корректирующего кода называется целое число*

$$d_{\max} = \max_{i,j} d(\boldsymbol{v}_i, \boldsymbol{v}_j). \qquad (1\text{-}34)$$

END

ОПРЕДЕЛЕНИЕ 1.7. *Средним (по множеству всевозможных неупорядоченных пар $\{\boldsymbol{v}_i, \boldsymbol{v}_j\}$) хэмминговым расстоянием корректирующего кода называется число*

$$d_{av} = \frac{1}{2C_N^2} \sum_i \sum_j d(v_i, v_j). \qquad (1\text{-}35)$$

END

ОПРЕДЕЛЕНИЕ 1.8. *Код, для которого выполняются соотношения*

$$d_{\min} = d_{\max} \qquad (1\text{-}36)$$

и, следовательно, выполняются соотношения

$$d_{\min} = d_{av} = d_{\max}, \qquad (1\text{-}36а)$$

называется ***эквидистантным*** [1.5, с. 160].

END

Пусть s – максимальная кратность гарантированно (т.е. с вероятностью 1) *обнаруживаемых* кодом ошибок, а t – максимальная кратность гарантированно *исправляемых* кодом ошибок; очевидно, что при этом имеет место соотношение

$$t \le s. \qquad (1\text{-}37)$$

Комбинация (b_1, b_2, ..., b_n), компоненты которой принимают значения из множества {0, 1}, называется *двоичной комбинацией* или *двоичным вектором*. *Длина вектора* – целое число $n \ge 1$.

Пусть теперь (до следующего явным образом объявленного переобозначения) $\boldsymbol{b}_i$, $i = 1, 2, \ldots, 2^n$ – произвольный двоичный вектор или двоичная комбинация длины n.

Множество *всевозможных* двоичных векторов или комбинаций длины n

$$B^n = \{\boldsymbol{b}_i\},\ i = 1, 2, \ldots, 2^n, \qquad (1\text{-}38)$$

называется «единичным n-мерным кубом» (рис. 1.2). Сами двоичные комбинации называются вершинами этого куба. Две вершины $\boldsymbol{b}_i$ и $\boldsymbol{b}_j$ n-мерного куба называются *соседними*, если хэммингово расстояние $d(\boldsymbol{b}_i, \boldsymbol{b}_j) = 1$, и называются *противоположными*, если $d(\boldsymbol{b}_i, \boldsymbol{b}_j) = n$. Неупорядоченная пара соседних вершин $\{\boldsymbol{b}_i, \boldsymbol{b}_j\}$ называется ребром куба.

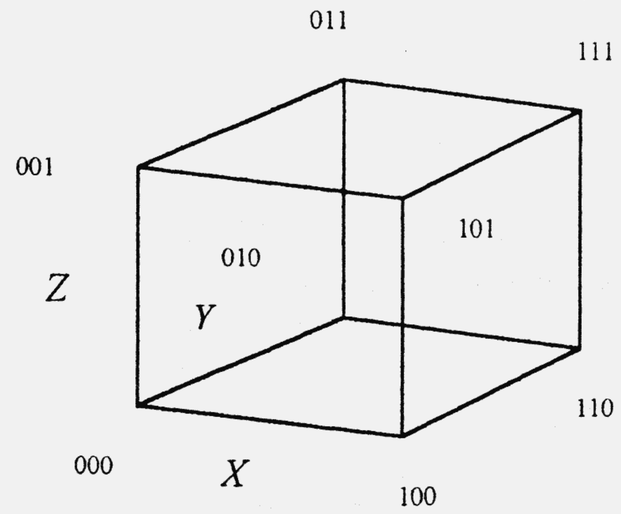

Рис. 1.2. Единичный куб при n=3

Множество всех вершин куба B^n, имеющих один и тот же вес k, будем обозначать как B_k^n и называть «k-м слоем куба B^n».

Каждому двоичному вектору длины n $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)$ можно сопоставить число

$$\gamma(\boldsymbol{b}) = \sum_{i=1}^{n} b_i 2^{n-i}, \qquad (1\text{-}39)$$

называемое номером этого вектора.

Множество

$$B_k^n(\boldsymbol{b}_i) = \{\boldsymbol{b}_s | d(\boldsymbol{b}_i, \boldsymbol{b}_s) = k\} \qquad (1\text{-}40)$$

называется *сферой*, а множество

$$S_k^n(\boldsymbol{b}_i) = \{\boldsymbol{b}_s | d(\boldsymbol{b}_i, \boldsymbol{b}_s) \le k\} - \qquad (1\text{-}41)$$

шаром радиуса $k \le n$ с центром в точке $\boldsymbol{b}_i$.

ЛЕММА 1.2. *Чтобы корректирующий код был способен обнаруживать все ошибки кратности $q \le s$, необходимо и достаточно, чтобы минимальное хэммингово расстояние этого кода удовлетворяло соотношению*

$$d_{\min} \ge s+1. \qquad (1\text{-}42)$$

ДОКАЗАТЕЛЬСТВО.

ДОСТАТОЧНОСТЬ. Дано: соотношение (1-42) - выполняется. В этом случае никакая ошибка кратности $q \le s$ не сможет перевести никакую переданную кодовую комбинацию ни в какую другую кодовую комбинацию.

НЕОБХОДИМОСТЬ. Если (1-42) не выполняется, т.е. если

$$d_{\min} \le s, \qquad (1\text{-}43)$$

то возможен вариант q-кратной ошибки, $q \le s$, которая переведёт переданную кодовую комбинацию в другую кодовую комбинацию.

ЧТД

Ошибка может быть не только обнаружена, но также может быть и исправлена, если содержащая ошибку принятая

комбинация расположена в смысле хэммингова расстояния ближе к переданной кодовой комбинации, чем к любой другой кодовой комбинации.

ЛЕММА 1.3. *Чтобы корректирующий код был способен исправлять все ошибки кратности $q \le t$, необходимо и достаточно, чтобы минимальное хэммингово расстояние этого кода удовлетворяло соотношению*

$$d_{\min} \ge 2t + 1. \qquad (1\text{-}44)$$

ДОКАЗАТЕЛЬСТВО.

ДОСТАТОЧНОСТЬ. Дано: неравенство (1-44) выполняется; следовательно,

$$t \le (d_{\min} - 1)/2 < d_{\min}/2 \qquad (1\text{-}45)$$

и принятая комбинация, содержащая любую ошибку кратности $q \le t$, оказывается расположенной ближе к переданной кодовой комбинации, чем к любой другой кодовой комбинации.

НЕОБХОДИМОСТЬ. Чтобы принятая комбинация, содержащая ошибку кратности $q \le t$, оказалась бы расположенной ближе к переданной кодовой комбинации, чем к любой другой кодовой комбинации, необходимо, чтобы выполнялись соотношения

$$q \le t < d_{\min}/2; \qquad (1\text{-}46)$$

и, следовательно,

$$2t < d_{\min}; \qquad (1\text{-}47)$$

так как t и d_{min} – целые числа, то необходимо, чтобы выполнялось соотношение

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

ЧТД

ЛЕММА 1.4. *Для одновременного обнаружения всех ошибок кратности $q \le s$ и исправления всех ошибок кратности $q \le t$ (при $t \le s$) достаточно, чтобы минимальное хэммингово расстояние удовлетворяло условию*

$$d_{\min} \ge t + s + 1. \qquad (1\text{-}49)$$

ДОКАЗАТЕЛЬСТВО.
ДОСТАТОЧНОСТЬ. Дано: соотношение (1-49) выполняется, но тогда выполняются следующие неравенства

$$d_{\min} \ge t + s + 1 \ge s + 1, \quad \text{так как } t \ge 0; \qquad (1\text{-}50)$$

$$d_{\min} \ge t + s + 1 \ge 2t + 1, \quad \text{так как } s \ge \text{t}. \qquad (1\text{-}51)$$

Из (1-50) и (1-51) вытекает справедливость доказываемой леммы.

ЧТД

Пусть переданная по ДСК кодовая комбинация $\boldsymbol{a}_s$ под действием ошибки $\boldsymbol{e}_i$ преобразуется в полученную на его выходе комбинацию $\boldsymbol{y}$ (см. (1-7)). Очевидно, что в этом случае

$$d(\boldsymbol{y}, \boldsymbol{a}_s) = w(\boldsymbol{y} \oplus \boldsymbol{a}_s) = w(\boldsymbol{e}_i), \qquad (1\text{-}52)$$

а вероятность перехода

$$p(\boldsymbol{y}/\boldsymbol{a}_s) = p_0^{d(\boldsymbol{y}, \boldsymbol{a}_s)} \cdot (1 - p_0)^{(n - d(\boldsymbol{y}, \boldsymbol{a}_s))} =$$

$$= p_0^{w(\boldsymbol{e}_i)} \cdot (1 - p_0)^{(n - w(\boldsymbol{e}_i))}. \qquad (1\text{-}53)$$

Из (1-53) следует, что при сделанных предположениях вероятность перехода переданной кодовой комбинации $\boldsymbol{a}_s$ в выходную комбинацию $\boldsymbol{y}$ резко падает с увеличением $d(\boldsymbol{y}, \boldsymbol{a}_s)$ при $p_0 \ll 1$. Поэтому принятая комбинация при использовании корректирующего блокового кода *с декодированием по методу максимального правдоподобия* декодируется в ближайшую (в смысле хэммингова расстояния) кодовую комбинацию.

1.7. БЛОКОВЫЕ КОРРЕКТИРУЮЩИЕ КОДЫ СО СТИРАНИЕМ СИМВОЛОВ

ПРИМЕР 1.13. Предположим, что дан двоичный стационарный без памяти канал (СБПК) со стиранием (erasure channel), который характеризуется переходными вероятностями p и q [1.8, задача 6.15].

Приёмник (декодер или решающее устройство) этого канала, получая искажённый символ, при определённой степени его искажения выдаёт «символ стирания θ», характеризующий принятый сигнал как «сомнительный»; в этом случае говорят, что принятый сомнительный сигнал был стёрт.

Пусть (в этом примере) q^* – кратность стирания, т.е. число стёртых символов в пределах одной переданной двоичной кодовой комбинации; очевидно, что в общем случае

$$0 \le q^* \le n. \qquad (1\text{-}54)$$

При этом в полученной комбинации с q^*-кратным стиранием будет иметься q^* символов стирания θ.

Допустим, что стирание отдельных символов в пределах одной переданной кодовой комбинации являются статистически независимыми событиями, а все нестёртые символы являются неискажёнными (правильными). В этом случае низкократные стирания являются более вероятными, чем высокократные (см. пример 1.2).

Предположим, что t^* – максимальная кратность *гарантированно восстанавливаемых* кодом символов стирания θ в пределах одной комбинации; очевидно, что при этом выполняются соотношения

$$0 \le q^* \le t^* < n. \qquad (1\text{-}55)$$

При этом будем считать, что суммарная вероятность высокократных стираний с $q^* \geq t^* + 1$ является пренебрежимо малой (обоснованием этому является сделанное выше допущение о статистической независимости стираний отдельных символов в пределах одной и той же кодовой комбинации).

Оказывается, что принятая на выходе канала комбинация с $q^* \leq t^*$ символами стирания θ может быть при определённых условиях декодирована в переданную кодовую комбинацию; в этом случае говорят о «восстановлении $q^* \leq t^*$ стёртых символов».

Приняв на выходе канала комбинацию $\boldsymbol{b}$ с $q^* \leq t^*$ символами стирания θ, создадим $(n - q^*)$-значный «укороченный код» путём вычёркивания во всех кодовых комбинациях исходного кода позиций со стёртыми символами (см. 2.7. Укороченные коды). Заметим, что существует взаимно однозначное соответствие между множествами кодовых комбинаций исходного кода и полученного укороченного кода. Чтобы образованные таким путём кодовые комбинации укороченного кода отличались друг от друга, необходимо, чтобы хэммингово расстояние для их всевозможных пар было бы не менее единицы. Для выполнения этого условия достаточно, чтобы полученная на выходе канала комбинация, содержащая $q^* \leq t^*$ символов стирания θ и не содержащая ни одного другого искажённого символа, гарантированно отличалась бы от любой другой (т.е. не переданной) кодовой комбинации хотя бы одним нестёртым символом; иначе говоря, потребуем, чтобы для исходного не укороченного кода выполнялось соотношение

$$d_{\min} \geq t^* + 1. \qquad (1\text{-}56)$$

Таким образом, если выполняется соотношение (1-56), то принятая на выходе канала комбинация $\boldsymbol{b}$ с $q^* \leq t^*$ символами стирания θ может быть следующим образом декодирована в

переданную кодовую комбинацию. Перейдём к $(n - q^*)$-значному укороченному коду, имеющему N различных укороченных кодовых комбинаций; одновременно укоротим комбинацию $\boldsymbol{b}$ путём вычёркивания в ней q^* символов стирания θ; таким образом, при преобразовании исходного кода в укороченный принятая комбинация $\boldsymbol{b}$ преобразуется в укороченную комбинацию $\boldsymbol{c}$, которой однозначно соответствует некоторая кодовая комбинация исходного не укороченного кода $\boldsymbol{a}$ ($\boldsymbol{c}$ есть результат укорочения на q^* символов как $\boldsymbol{a}$, так и $\boldsymbol{b}$); отсюда следует, что комбинация $\boldsymbol{b}$ образовалась из переданной комбинации $\boldsymbol{a}$; это и означает восстановление $q^* \leq t^*$ символов стирания θ в принятой на выходе канала комбинации $\boldsymbol{b}$.

Из (1-48) и (1-56) следует

$$t \leq (d_{\min} - 1)/2, \qquad (1\text{-}57)$$

$$t^* \leq (d_{\min} - 1). \qquad (1\text{-}58)$$

Имея в виду соотношения (1-57) и (1-58) иногда говорят, «о том, что восстанавливать стёртые символы легче, чем исправлять ошибки» [1.9].

В [1.2, с. 238 – 240] и в [1.3, с. 337 – 339] рассматривается вопрос одновременного декодирования стираний и ошибок.

END

1.8. БЛОКОВЫЕ КОРРЕКТИРУЮЩИЕ КОДЫ С ПРОВЕРКОЙ НА ЧЁТНОСТЬ

Эффективным обобщением одной проверки на чётность, при которой для проверки используется *один* проверочный разряд или символ, является использование *множества* проверочных разрядов или символов, когда каждый

символ этого множества используется для проверки некоторого предварительно определённого множества информационных разрядов или символов.

Пусть $\boldsymbol{v} = (v_1, v_2, \ldots, v_k)$ – информационная последовательность $k = n_0$ двоичных информационных символов; при этом число сообщений, подлежащих передаче, равно $N = 2^k$. Кодовое слово $\boldsymbol{x} = (x_1, x_2, \ldots, x_k, x_{k+1}, \ldots x_n)$ произвольной длины $n > k$ образуется по правилу (алгоритму кодирования)

$$x_j = \begin{cases} v_j; & 1 \le j \le k, \\ \sum_{i=1}^{k} v_i g_{i,j}\ ; & k+1 \le j \le n, \end{cases} \qquad (1\text{-}59)$$

здесь $\sum$ – сумма по mod 2.

Коэффициенты $g_{i,j}$ при $1 \le i \le k$ и $k + 1 \le j \le n$ в соотношении (1-59) являются *фиксированными* двоичными символами, не зависящими от v; поэтому соотношение (1-59) определяет взаимно однозначное отображение множества 2^k возможных информационных последовательностей в множество 2^k кодовых слов. Первые k символов каждого кодового слова называются *информационными символами*, а последние $(n - k)$ символов – *проверочными*.

ОПРЕДЕЛЕНИЕ 1.9. *Двоичный блоковый код с произвольной длиной кодовых комбинаций n, для которого множество сообщений представляет собою множество 2^k двоичных последовательностей некоторой фиксированной длины k, $1 \le k < n$, и в котором каждому сообщению $\boldsymbol{v} = (v_1, v_2, \ldots, v_k)$ сопоставлено кодовое слово $\boldsymbol{x} = (x_1, x_2, \ldots, x_k, x_{k+1}, \ldots x_n)$, определяемое соотношением* (1-59), *где множество двоичных чисел $\{g_{i,j}\}$ при $1 \le i \le k$ и $k + 1 \le j \le n$ является произвольным, но фиксированным и независимым от* **v**, *называется* ***систематическим кодом с проверкой на чётность***.

END

Очевидно, что *различным наборам двоичных символов* $\{g_{i,j}\}$ соответствуют *различные систематические коды с проверкой на чётность*.

ОПРЕДЕЛЕНИЕ 1.10. *Двоичный блоковый код с произвольной длиной кодовых комбинаций n, для которого множество сообщений представляет собою множество 2^k двоичных последовательностей некоторой фиксированной длины $k < n$ и в котором каждому сообщению $\boldsymbol{v} = (v_1, v_2, \ldots, v_k)$ сопоставлено кодовое слово $\boldsymbol{x} = (x_1, x_2, \ldots, x_k, x_{k+1}, \ldots x_n)$, определяемое соотношением*

$$x_j = \sum_{i=1}^{k} v_i g_{i,j}\ ; \quad 1 \le j \le n, \qquad (1\text{-}60)$$

где $\sum$ - сумма по mod 2, *а множество двоичных чисел $\{g_{i,j}\}$ при $1 \le i \le k$ и $1 \le j \le n$ является произвольным, но фиксированным и независимым от* **v**, *называется* ***общим кодом с проверкой на чётность***.

END

ЗАМЕЧАНИЕ 1.4. Из определений (1-9) и (1-10) следует, что систематический код с проверкой на чётность является *выделенным* частным случаем общего кода с проверкой на чётность, в котором при $1 \le j \le k$

$$g_{i,j} = \begin{cases} 1, & i = j, \\ 0, & i \ne j. \end{cases} \qquad (1\text{-}61)$$

END

В случаях, когда требуется обратить внимание на длину блока n и на длину информационной последовательности k, используется обобщающее название «(n, k)-код с проверкой на чётность», при этом может иметься в виду как систематический так и общий (n, k)-код с проверкой на чётность.

ПРИМЕР 1.14. Предположим, что дано множество информационных последовательностей {00, 01, 10, 11}. Применительно к этому множеству информационных последовательностей

рассмотрим код с одной проверкой на чётность и систематический (5, 2)-код с проверкой на чётность.

Применение кода с одной проверкой на чётность породит множество кодовых комбинаций {000, 011, 101, 110}, которому соответствует кодовое расстояние $d_{\min} = 2$, обеспечивающее обнаружение всех ошибок нечётной кратности q, но не позволяющее исправлять ошибки чётной кратности.

В табл. 1.5 приведен систематический код с проверкой на чётность (с тремя проверками), имеющий параметры:

$k = 2$, $N = 2^2 = 4$; $n = 5$, $N_0 = 2^5 = 32$; $r = n - k = 3$;

$R = k/n = 2/5$ [бит/симв]; $d_{\min} = 3$.

Очевидно, что этот код позволяет гарантированно обнаруживать все ошибки кратности $q \le 2$ (лемма 1.2) и исправлять все однократные ошибки (лемма 1.3).

Таблица 1.5

Алгоритм кодирования	Информационные последовательности v_i, i=1, 2, 3, 4	Кодовые слова x_i i=1, 2, 3, 4
$x_1 = v_1$; $x_2 = v_2$; $x_3 = g_{1,3}v_1 \oplus g_{2,3}v_2 = v_1$; $x_4 = g_{1,4}v_1 \oplus g_{2,4}v_2 = v_2$; $x_5 = g_{1,5}v_1 \oplus g_{2,5}v_2 = v_1 \oplus v_2$.	00	00000
	01	01011
	10	10101
	11	11110

Соотношения (1-59) и (1-60) могут быть представлены в более компактной форме с помощью понятия *порождающей матрицы* $\boldsymbol{G}_{(n, k)}$.

Попробуйте, основываясь на данных, приведенных в табл. 1.5, записать порождающую матрицу $\boldsymbol{G}_{(5, 2)}$ для рассматриваемого здесь (5, 2)-кода.

END

В случае общего (n, k)-кода с проверкой на чётность

$$\boldsymbol{G}_{(n, k)} = \begin{bmatrix} g_{1,1} & g_{1,2} & \dots & g_{1,k} & g_{1,k+1} & \dots & g_{1,n} \\ g_{2,1} & g_{2,2} & \dots & g_{2,k} & g_{2,k+1} & \dots & g_{2,n} \\ \cdot & \cdot & & \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & \cdot & & \cdot \\ g_{k,1} & g_{k,2} & \dots & g_{k,k} & g_{k,k+1} & \dots & g_{k,n} \end{bmatrix}. \qquad (1\text{-}62)$$

В случае группового (n, k)-кода с проверкой на чётность порождающая матрица может иметь, а может и не иметь вид:

$$\boldsymbol{G}_{(n, k)} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & g_{1,k+1} & \dots & g_{1,n} \\ 0 & 1 & 0 & \dots & 0 & g_{2,k+1} & \dots & g_{2,n} \\ \cdot & \cdot & & & \cdot & \cdot & & \cdot \\ \cdot & \cdot & & & \cdot & \cdot & & \cdot \\ 0 & 0 & \dots & & 1 & g_{k,k+1} & \dots & g_{k,n} \end{bmatrix}, \qquad (1\text{-}63)$$

однако во втором случае она всегда может быть приведена к этому виду (см. раздел 2.2 настоящей книги).

Рассматривая $\boldsymbol{v}$ и $\boldsymbol{x}$ как матрицы-строки, будем иметь

$$\boldsymbol{x} = \boldsymbol{v}\boldsymbol{G}_{(n, k)}, \qquad (1\text{-}64)$$

где $\boldsymbol{G}_{(n, k)}$ определяется соотношением (1-62) или (1-63).

Большую роль в теории (n, k)-кодов с проверкой на чётность играет понятие *проверочной матрицы* (или *матрицы проверок*) $\boldsymbol{H}_{(n, k)}$ и понятие *синдрома* $\boldsymbol{S}$.

Как будет показано ниже, характерным свойством проверочной матрицы является выполнение соотношения:

$$\boldsymbol{G}_{(n,k)}\boldsymbol{H}^{T}_{(n,k)} = \boldsymbol{S}, \qquad (1\text{-}65)$$

где $\boldsymbol{S} = [s_{ij}] = [0] = \boldsymbol{0}$, $i = 1, 2, \dots, k$; $j = 1, 2, \dots, (n - k)$, – (1-65а)

обычно называемая *синдромом* (см. ниже) *в рассматриваемом случае* ***нулевая*** *матрица* размерности $k \times (n - k)$; равенство

всех элементов матрицы $\boldsymbol{S}$ нулю в данном случае означает взаимную ортогональность каждого вектора-строки *порождающей матрицы* $\boldsymbol{G}_{(n,k)}$ с каждым вектором-строкой *проверочной матрицы* $\boldsymbol{H}_{(n,k)}$; или выполнение соотношения:

$$\boldsymbol{x}_i \boldsymbol{H}^T_{(n,k)} = \boldsymbol{S} = [s_{i1}\ \ s_{i2} \ldots\ s_{i(n-k)}] = \boldsymbol{0}\ ,\ \ i = 1, 2, \ldots, 2^k, \qquad \text{(1-65б)}$$

где $[s_{i1}\ s_{i2} \ldots s_{i(n-k)}]$ – ***нулевая*** *матрица-строка* размерности $1\times(n - k)$; равенство всех элементов матрицы $\boldsymbol{S}$ нулю в данном случае означает взаимную ортогональность ***любого*** *кодового вектора* $\boldsymbol{x}_i$ (записанного в форме матрицы-строки размерности $1\times n$) с каждым вектором-строкой проверочной матрицы $\boldsymbol{H}_{(n,k)}$.

Если же некоторая комбинация $\boldsymbol{x}$ длины n *не является кодовой комбинацией*, то её синдром

$$\boldsymbol{x}\ \boldsymbol{H}^T_{(n,k)} = \boldsymbol{S} = \boldsymbol{S}(\boldsymbol{x}) = [s_1\ \ s_2 \ldots\ s_j \ldots\ s_{(n-k)}] \neq \boldsymbol{0}\,; \qquad \text{(1-65в)}$$

причём, если элемент синдрома $\boldsymbol{S}$ $s_j \neq 0$, $1 \le j \le n-k$, то $\boldsymbol{x}$ и j-я строка проверочной матрицы $\boldsymbol{H}_{(n,k)}$ не являются взаимно ортогональными векторами.

1.9. ПОНЯТИЕ СВЁРТОЧНОГО (НЕПРЕРЫВНОГО) КОРРЕКТИРУЮЩЕГО КОДА

В отличие от блоковых кодов, применение которых сопровождается разбиением информационной последовательности на блоки одной и той же длины длины k и последующей *независимой* обработкой этих блоков – введения $(n - k)$ избыточных символов, в случае *свёрточных* кодов каждой информационной последовательности ставится в соот-

ветствие кодовая последовательность. Простейшим способом определения этого соответствия является использование кодового дерева.

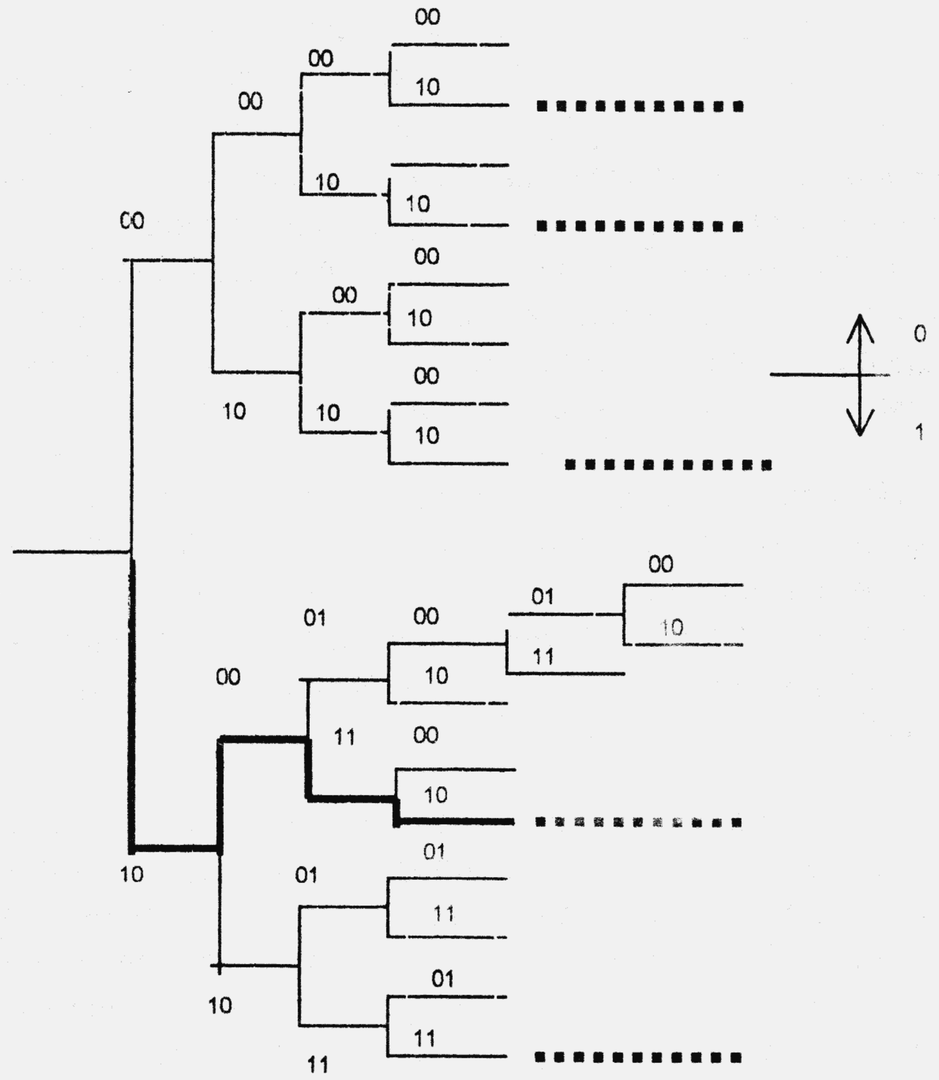

Рис.1.3. Кодовое дерево, соответствующее рассматриваемому свёрточному коду Хегельбергера с R=1/2

В качестве примера рассмотрим кодовое дерево, изображённое на рис. 1.3. Каждую горизонтальную линию мы

будем отождествлять здесь с вершиною, а каждую вертикальную линию будем считать образованной двумя рёбрами, исходящими из вершины – горизонтальной линии, подходящей к ней слева. Таким образом, первая, считая слева направо, горизонтальная линия является корнем графа дерева – т.е. вершиною нулевого ранга [1.8]. Из каждой вершины графа-дерева исходит $2^{k_0} = 2$ рёбер и, следовательно, $k_0 = 1$. Каждой вершине графа-дерева ранга r соответствует двоичная последовательность длины $n_0 = 2$ (и, следовательно, $n_0 - k_0 = 1$), у которой первый символ является r-м символом информационной последовательности, а второй символ – r-м символом последовательности проверочных символов, вырабатываемых кодером (см. рис. 1.3) и, следовательно, скорость кода

$$R = k_0/n_0 = 1/2. \qquad \text{(1-65в)}$$

На рис. 1.3 представлен ключ, содержащий правило появления символов 0 или 1 информационной последовательности при перемещении из корня графа-дерева по некоторому пути (последовательности чередующихся вершин и рёбер): ходу из некоторой вершины вверх соответствует появление 0, а вниз – появление 1.

Будем называть блоки информационных символов длины k_0 кадрами информационных символов, а сопоставляемые им кодером кодовые слова длины n_0 – кадрами кодового слова. Кодирование каждого кадра информационных символов длины k_0 в отдельный кадр кодового слова длины n_0 производится с учётом m предыдущих кадров информационных символов.

Таким образом, в отличие от случая блоковых кодов, когда кодер, порождающий кодовые слова никоим образом не связывает их между собою, в случае древовидных кодов кодер связывает между собою кадры кодовых слов длины n_0. Наиболее важными древовидными кодами являются так называемые свёрточные коды. Свёрточные коды – это древовидные коды, обладающие дополнительными свойствами *линейности* и *постоянства во времени* [1.7, с. 399 – 403].

Пусть информационная последовательность, поступающая с выхода кодера источника на вход кодера канала (начиная с u_1),

$$\boldsymbol{u} = u_1\ u_2\ u_3\ \ldots\ u_n\ \ldots\ . \qquad \text{(1-66)}$$

Очередной символ информационной последовательности u_n, поступающий в каждую единицу времени в кодер канала (рис. 1.4), а каждый ранее поступивший символ кодера источника, находящийся в регистре сдвига, сдвигается на один разряд вправо; этот очередной информационный символ источника поступает непосредственно в канал и, следовательно, $x_n^{(1)} = u_n$, $n = 1, 2, 3, \ldots$ За каждым таким информационным символом следует проверочный символ, правило образования которого, вообще говоря, задаётся заранее, а в рассматриваемом примере определяётся структурой кодера (рис. 1.4):

$$x_n^{(2)} = u_n \oplus u_{n-2} \oplus u_{n-4} = x_n^{(1)} \oplus x_{n-2}^{(1)} \oplus x_{n-4}^{(1)}. \qquad \text{(1-67)}$$

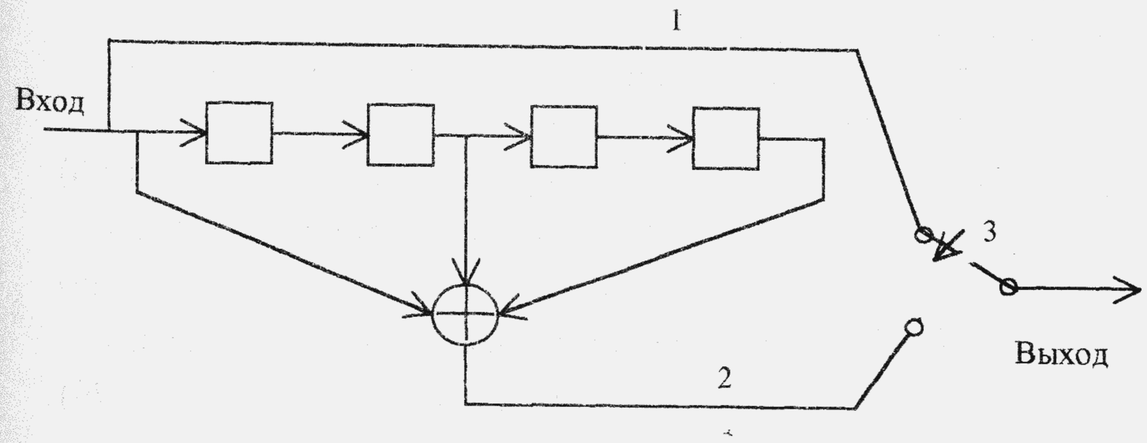

Рис.1.4. Пример кодера для свёрточного кода

Легко непосредственно убедиться в том, что жирная линия на кодовом дереве, представленном на рис. 1.3, соответствует началу информационной последовательности символов, поступающей на вход кодера, представленного на рис. 1.4.

Таблица 1.6

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15 …
$x^{(1)}_j$	1	0	1	1	0	0	1	0	1	0	1	0	0	1	1 …
$x^{(1)}_{j-1}$	0	1	0	1	1	0	0	1	0	1	0	1	0	0	1 …
$x^{(1)}_{j-2}$	0	0	1	0	1	1	0	0	1	0	1	0	1	0	0 …
$x^{(1)}_{j-3}$	0	0	0	1	0	1	1	0	0	1	0	1	0	1	0 …
$x^{(1)}_{j-4}$	0	0	0	0	1	0	1	1	0	0	1	0	1	0	1 …
$x^{(2)}_j$	1	0	0	1	0	1	0	1	0	0	1	0	0	1	0 …

Первая строка табл. 1.6 содержит значения эквивалента времени j. Вторая строка табл. 1.6 содержит информационную последовательность, а седьмая строка таблицы содержит последовательность проверочных символов, образованную с помощью соотношения (1-67). Третья, четвёртая, пятая и шестая строки табл. 1.6 содержат последовательности информационных символов, появляющиеся на выходах четырёх ячеек памяти (квадраты на рис. 1.4), задержанные соответственно на 1, 2, 3 и 4 временных единицы (см. подраздел 3.16).

Очевидно, что по линии 1 (рис. 1.4) идёт информационная последовательность символов

$$x_1^{(1)} x_2^{(1)} x_3^{(1)} \ldots x_n^{(1)} \ldots ; \qquad (1\text{-}68)$$

по линии 2 идёт последовательность проверочных символов

$$x_1^{(2)} x_2^{(2)} x_3^{(2)} \ldots x_n^{(2)} \ldots . \qquad (1\text{-}69)$$

При этом передаваемая кодовая последовательность

$$\boldsymbol{x} = x_1^{(1)} x_1^{(2)} x_2^{(1)} x_2^{(2)} x_3^{(1)} x_3^{(2)} \ldots x_n^{(1)} x_n^{(2)} \ldots ; \qquad (1\text{-}70)$$

предположим, что принятая последовательность

$$y = y_1^{(1)} y_1^{(2)} y_2^{(1)} y_2^{(2)} y_3^{(1)} y_3^{(2)} \ldots y_n^{(1)} y_n^{(2)} \ldots , \qquad (1\text{-}71)$$

тогда шумовая последовательность

$$z = z_1^{(1)} z_1^{(2)} z_2^{(1)} z_2^{(2)} z_3^{(1)} z_3^{(2)} \ldots z_n^{(1)} z_n^{(2)} \ldots , \qquad (1\text{-}72)$$

где

$$\boldsymbol{z} = \boldsymbol{x} \oplus \boldsymbol{y} . \qquad (1\text{-}73)$$

Как и в случае блоковых кодов с проверкой на чётность определим *синдром* с помощью выражения:

$$\boldsymbol{S} = S_1 S_2 S_3 \ldots S_n \ldots , \qquad (1\text{-}74)$$

где

$$S_n = y_n^{(2)} \oplus y_n^{(1)} \oplus y_{n-2}^{(1)} \oplus y_{n-4}^{(1)} . \qquad (1\text{-}75)$$

Блок-схема кодера, выполняющего операцию кодирования (1-67), представлена на рис. 1.5 (k_0=1, n_0=2, R=k_0/n_0= =1/2).

Из (1-73) и (1-75) следует, что

$$S_n = z_n^{(2)} \oplus z_n^{(1)} \oplus z_{n-2}^{(1)} \oplus z_{n-4}^{(1)} . \qquad (1\text{-}76)$$

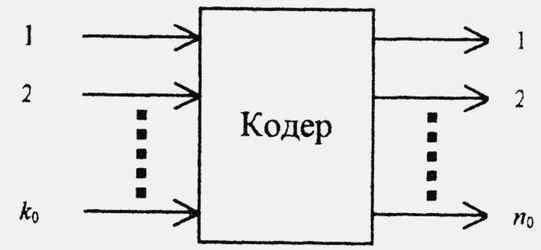

Рис. 1.5. Кодер для древовидного кода с R=k_0/n_0

Согласно (1-76) при $1 \le n \le 5$:

$$S_1 = z_1^{(2)} \oplus z_1^{(1)} ; \quad S_2 = z_2^{(2)} \oplus z_2^{(1)} ; \quad S_3 = z_3^{(2)} \oplus z_3^{(1)} \oplus z_1^{(1)} ; \qquad (1\text{-}77)$$

$$S_4 = z_4^{(2)} \oplus z_4^{(1)} \oplus z_2^{(1)} ; \quad S_5 = z_5^{(2)} \oplus z_5^{(1)} \oplus z_3^{(1)} \oplus z_1^{(1)} . \qquad (1\text{-}78)$$

Рассмотрим теперь декодирование первого информационного символа u_1 , чтобы проиллюстрировать стратегию декодирования рассматриваемого свёрточного кода. Декоди-