3.13. КОРЕКТИРУЮЩИЕ СВОЙСТВА ЦИКЛИЧЕСКИХ (n, k)-КОДОВ И ВЫБОР ИХ ПОРОЖДАЮЩИХ МНОГОЧЛЕНОВ

Изложение этой темы приведём применительно к БЧХ-кодам, образующим важный и обширный подкласс циклических кодов. Задание БЧХ-кодов основано на использовании корней многочлена $g(X)$ степени r, порождающего идеал в алгебре многочленов по модулю бинома X^n-1; причём корни этого многочлена являются также корнями бинома X^n-1.

БЧХ-коды *позволяют исправлять* ***независимые ошибки кратности*** t. Свойства БЧХ-кодов, процедуры кодирования и декодирования, а также реализация кодеров и декодеров для этих кодов хорошо изучены.

Пусть α – элемент из поля $GF(p^m)$. При любых заданных значениях m_0 и d_0 код, порождённый многочленом $g(X)$, является БЧХ-кодом тогда и только тогда, когда многочлен $g(X)$ является многочленом наименьшей степени над $GF(p)$, для которого $\alpha^{m_0}, \alpha^{m_0+1}, \ldots, \alpha^{m_0+d_0-2}$ – его корни.

Минимальное расстояние между кодовыми векторами не меньше величины d_0, называемой *конструктивным кодовым расстоянием*.

Наибольшее значение имеют так называемые *БЧХ-коды в узком смысле*, получающиеся в том случае, если в качестве α выбрать примитивный элемент поля $GF(p^m)$ и положить $m_0 = 1$, а $d_0 = 2t_0 + 1$ [3.3, с. 304].

В рассматриваемом случае справедлива следующая теорема.

ТЕОРЕМА 3.27. *Для любых целых положительных чисел m и $t_0 < n/2$ существует двоичный БЧХ-код длины $n = 2^m$-1, исправляющий все комбинации из t_0 или меньшего числа ошибок и содержащий не более mt_0 проверочных символов.*

END

ПРИМЕР 3.21. Предположим, что *расширением* основного поля $F_0 = GF(2)$ является поле $F=GF(2^m) = GF(2^3)$ (т.е. $m = 3$). Очевидно, что в этом случае $(2^m - 1) = (2^3-1) = 7$.

При $m = 3$ и $n = 7$ требуется построить БЧХ-код с максимальным значением $R = k/n = (n-r)/n = 1 - r/n$ и определить его конструктивную корректирующую способность d_0, т.е. требуется выбрать минимальное значение r из возможных допустимых его значений.

РЕШЕНИЕ.

Согласно результатам примера 3.10, исключая тривиальные случаи, мы располагаем, вообще говоря, следующими вариантами выбора порождающего многочлена:

$$(X^3+X+1)= g_1(X), \quad (X^3+X^2+1)= g_2(X)$$

и

$$(X^3+X+1)(X^3+X^2+1)= g_1(X)\, g_2(X).$$

Таким образом, учитывая постановку задачи, мы можем выбрать в качестве порождающего многочлена создаваемого БЧХ-кода многочлен (X^3+X+1) или многочлен (X^3+X^2+1).

Зафиксируем примитивный элемент α поля $GF(2^3)$ выбором неприводимого многочлена X^3+X+1 (см. пример 3.10, табл. 3.17):

$$g_1(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^4) = (X-\beta_1)(X-\beta_2)(X-\beta_3) =$$

$$= X^3+X+1,$$

где β_i, $i = 1, 2, 3$, – i-й корень многочлена X^3+X+1:

$$\beta_1 = \alpha \Leftrightarrow (0\ \ 1\ \ 0),$$
$$\beta_2 = \alpha^2 \Leftrightarrow (1\ \ 0\ \ 0),$$
$$\beta_3 = \alpha^2 + \alpha \Leftrightarrow (1\ \ 1\ \ 0).$$

Согласно теореме 3.24, если β – корень $g_1(X)$, то вся последовательность корней может быть представлена в виде $\beta, \beta^p, \ldots, \beta^{p^{r-1}}$, что соответствует последовательности: $\beta=\alpha$, $\beta^2=\alpha^2$, $\beta^4=\alpha^4$.

Все элементы поля, образованного с помощью неприводимого в $F_0[X]$ многочлена $g_1(X) = X^3+X+1$ степени $m = 3$, могут быть выражены в поле $F_0[g_1]$ через степени примитивного элемента α или с помощью линейных комбинаций базисных комбинаций векторного пространства:

$$\beta=a_{m-1}\alpha^{m-1}+\ldots+a_1\alpha+a_0 = a_2\alpha^2 + a_1\alpha + a_0$$

(см. табл. 3.17). Как следует из рассмотрения табл. 3.17 расширенное поле $GF(2^m) = GF(2^3)$ содержит 8 элементов – *многочленов от* α *степени* ***не выше второй***: один нулевой многочлен и семь ненулевых. Подчеркнём, что для создания поля $GF(2^m)$ мы рассматриваем понятие алгебры многочленов по модулю ***неприводимого*** *многочлена* $g_1(X) = X^3+X+1$ степени $m = 3$.

Согласно примеру 3.10 разложение бинома X^7-1 на неприводимые сомножители может быть описано с помощью числовых циклов:

0
1 2 4
3 5 6.

Приведенным числовым циклам соответствует разложение бинома:

$$X^7-1 = (X-1)(X^3+X+1)(X^3+X^2+1).$$

Выберем в качестве *порождающего многочлена* создаваемого циклического кода неприводимый над $GF(2)$ многочлен $g_1(X) = X^3+X+1$ степени $r = m = 3$, тогда мы получим циклический (7, 4)-код, корни порождающего многочлена которого определяются числовым циклом
1 2 4.

В рассматриваемом случае кодовые векторы являются элементами векторного пространства и элементами A_7 – алгебры многочленов по модулю бинома (X^7-1) – *многочленами степени* ***не выше шестой***. Число всех элементов алгебры A_7 в этом случае равно $p^{6+1}= 2^7 = 128$, из которых $p^k = 2^4 = 16$ являются кодовыми многочленами – элементами циклического подпространства и идеала, порождаемого в A_7 многочленом $g_1(X) = X^3+X+1$.

Согласно теореме 3.27 $r = 3 = mt_0 = 3t_0$, откуда имеем: $t_0 = 1$; и, следовательно, $d_0 = 2t_0 +1 = 3$.

Другой путь определения корректирующей способности этого кода основан на применении приведенного ниже утверждения 3.3. В последовательности корней многочлена $g(X) = X^3+X+1$ β, β^2, β^4 существует максимальной длины подпоследовательность корней с последовательными степенями (т.е. со степенями, изменяющимися на единицу для каждой пары соседних корней подпоследовательности); вот максимальная длина такой подпоследовательности: β, β^2. Следовательно, в данном случае $m_0= 1$, а $m_0+d_0 - 2 = 2$; откуда находим: $d_0 = 3$.

Параметры этого (7, 4)-кода: $n=7$, $k=4$, $m=r=n-k=3$; $t_0=1$, $mt_0=3$, $d = d_0 = 3$.

Очевидно, что проверочным многочленом рассмотренного (7, 4)-кода является многочлен

$$h(X) = \frac{X^7 - 1}{g(X)} = (X - 1)(X^3+X^2+1).$$

END

Заметим, что в теореме 3.27 в явном виде не оговаривается распределение корней $\{\beta_i\}$, $i = 1, 2, \ldots, r$, порождающего многочлена степени r в поле $GF(2^m)$. В приводимых ниже теоремах 3.28 и 3.29 характер распределения корней порождающего многочлена, напротив, играет *основополагающую роль*.

Пусть m – произвольное целое положительное число и n – один из делителей числа (2^m-1). Согласно теореме 3.20 и лемме 3.2 в поле $GF(p^m)$ всегда существует элемент порядка n; пусть β – один из таких элементов, при этом все элементы β^i, $(0 \le i < n)$, различны. Справедлива следующая теорема [3.3, с. 163].

ТЕОРЕМА 3.28. *Если порождающий многочлен $g(X)$ циклического кода длины n имеет своими корнями $\beta^{l+1}, \beta^{l+2}, \ldots, \beta^{l+r}$ $(1 \le r < n)$, где l $(0 \le l < n)$ – некоторое целое число, то минимальное расстояние этого кода не меньше чем $r+1$.*

END

Данная теорема гарантирует минимальное кодовое расстояние $r+1$, называемое *нижней БЧХ-границей минимального кодового расстояния*.

Циклический (n, k)-код называется БЧХ-кодом, если *корнями его порождающего многочлена* являются элементы β^i, где i пробегает все числа из (p, n)-числовых циклов, содержащих числа $l+1, \ldots, l+r$, *и только они*.

Если требуется, чтобы теорема 3.27 гарантировала исправление ошибок кратности, не превышающей t, то следует положить $r = 2t$.

Согласно теореме 3.28 длина каждого цикла, содержащего число $l+j$ $(1 \le j \le r)$, равна m или некоторому делителю m. Поэтому степень $g(X)$ и, следовательно, число проверочных символов не превосходят $mr = 2mt$.

Если для некоторого БЧХ-кода оба элемента β^l и β^{l+r+1} не являются корнями порождающего многочлена $g(X)$, то $r+1$ называют *конструктивным расстоянием* этого БЧХ-кода.

В частном случае, при $p=2$, $n=2^m-1$, $l=0$, $r=2t$, БЧХ-код называют *примитивным БЧХ-кодом* или *БЧХ-кодом в узком смысле*. При $t=1$, эти коды называются *циклическими кодами Хэмминга* [3.3, с. 164].

Справедливо следующее утверждение [3.3, с. 165].

УТВЕРЖДЕНИЕ 3.2. *Пусть m – минимальное целое число, такое, что $n|(2^m-1)$ и l $(0 \le l < n)$ – некоторое целое число. Тогда число проверочных символов двоичного БЧХ-кода длины n с конструктивным расстоянием $2t+1$ и с $l=0$ не превосходит mt.*

ДОКАЗАТЕЛЬСТВО. Числа i $(0 \le i \le t)$ и $2i$ всегда принадлежат одному и тому же числовому циклу. Так как длина цикла, содержащего i, равна m или некоторому делителю m, то количество целых положительных чисел, не превосходящих n-1 и входящих в циклы, содержащие числа $1, 2, \ldots, 2t$, не превосходит mt.

ЧТД

ТЕОРЕМА 3.29. *Пусть $g(X)$ – порождающий многочлен циклического кода длины n над $GF(q)$ и пусть $\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_{n-k}}$ – корни многочлена $g(X)$, быть может лежащие в расширении поля, где α – элемент порядка n. Минимальное расстояние этого кода больше, чем наибольшее количество* ***последовательных целых чисел*** *по модулю n в множестве $e = \{e_1, e_2, \ldots, e_{n-k}\}$.*

END

Пусть теперь числа $m_0, m_0+1, \ldots, m_0+d_0-2$, где $d_0 \le d$ – минимальное расстояние кода, составляют максимальное подмножество множества e, образованного последовательными по модулю n целыми числами. Таким образом, речь идёт о коде, минимальное кодовое расстояние d которого равно или больше d_0, а d_0 – *конструктивное расстояние* является нижней границей возможных значений d [3.2, с. 301].

Тогда справедливо также следующее утверждение [3.2, с. 303].

УТВЕРЖДЕНИЕ 3.3. *Циклический код, среди корней порождающего многочлена которого имеются элементы*

$$\beta^{m_0}, \beta^{m_0+1}, \ldots, \beta^{m_0+d_0-2}, \qquad (3\text{-}62)$$

где β *– элемент порядка* n*, имеет минимальное кодовое расстояние, не меньшее* d_0.

END

Конструктивное расстояние является нижней границей для минимального кодового расстояния и в некоторых случаях может не совпадать с ним. Можно показать, что примитивный БЧХ-код с конструктивным расстоянием d_0 имеет минимальное кодовое расстояние d, удовлетворяющее неравенствам: $d_0 \le d \le 2d_0$ [3.2, с. 303, 305].

ПРИМЕР 3.22. Предположим, что *расширением* основного поля $F_0 = GF(2)$ является поле $F=GF(2^m) = GF(2^3)$ (т.е. $m = 3$). Очевидно, что в этом случае $n = (2^3\text{-}1) = 7$.

Требуется построить при $m = 3$ и $n = 7$ БЧХ-код с максимально возможным кодовым расстоянием d и определить его конструктивную корректирующую способность t_0.

РЕШЕНИЕ. Очевидно, что решение поставленной задачи следует искать на пути объединения нескольких циклов, чтобы максимально возможным образом *удлинить* последовательность корней порождающего многочлена *с* ***последовательными*** (т.е. отличающимися на единицу) *степенями*.

Зафиксируем предварительно α - примитивный элемент поля $GF(2^3)$ с помощью многочлена $g_1(X) = (X^3+X+1)$.

Выберем в качестве порождающего многочлена кода многочлен $g(X) = g_1(X)g_2(X) = (X^3+X+1)(X^3+X^2+1)$. Очевидно, что в этом случае (см. пример 3.10) распределение корней $g(X)$ в $GF(2^m)$ определяется двумя числовыми циклами:

1 2 4
3 5 6,

и, следовательно, последовательность корней многочлена $g(X)$ имеет вид:

$$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$$

или

$$\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6,$$

при условии, что $\beta=\alpha$.

Как видно из полученного результата, нам удалось сконструировать код с требуемым распределением корней в поле $GF(2^3)$. Подчеркнём, что этот результат мы получили за счёт *объединения двух подмножеств корней*, соответствующих двум числовым циклам 1 2 4 и 3 5 6, или, что то же самое, двум неприводимым многочленам (X^3+X+1) и (X^3+X^2+1) в одно множество. Проверочным полиномом в рассматриваемом случае является

$$h(X) = \frac{X^7 - 1}{(X^3 + X + 1)(X^3 + X^2 + 1)} = X\text{-}1.$$

Параметры найденного (n, k)-кода: $n= 7$, $k= 1$, $r= 6$. Порождающая матрица

$$\boldsymbol{G} = [1111111] = [\boldsymbol{I}_1\ \boldsymbol{R}_{1\times 6}],$$

проверочная матрица

$$\boldsymbol{H} = \begin{bmatrix} 1&1&0&0&0&0&0 \\ 1&0&1&0&0&0&0 \\ 1&0&0&1&0&0&0 \\ 1&0&0&0&1&0&0 \\ 1&0&0&0&0&1&0 \\ 1&0&0&0&0&0&1 \end{bmatrix} = [\boldsymbol{R}^{\mathrm{T}}_{1\times 6}\ \boldsymbol{I}_6].$$

Очевидно, что $\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}} = \boldsymbol{0}$.

Таким образом, поставленная задача решена -- созданный (7, 1)-код удовлетворяет условиям теорем 3.28 и 3.29 и утверждений 3.2 и 3.3.

Согласно теореме 3.28 минимальное кодовое расстояние $d \geq r+1 = 7$, а так как $l = 0$, то это примитивный БЧХ-код или БЧХ-код в узком смысле.

Согласно утверждению 3.3, имеем: $m_0=1$, $m_0+d_0 - 2= 6$; и, следовательно, $d = d_0 = 7$, а $t_0 =](d_0 - 1)/2[= 3$.

Основное назначение данного примера – наглядная иллюстрация возможностей компоновки нескольких числовых циклов с целью создания кодов с увеличенным значением d.

END

В Приложении 5.5 приведена таблица циклических (n, k)-кодов и пояснения по пользованию ею [3.10].

ПРИМЕР 3.23. Рассмотрим (n, k)-коды из Приложения 5.5, основанные на разложении бинома $X^{15}+1$.

Таблица 3.29

n	k	$d_{мин}$	$f_i(X)$
…	…	…	…
15	11	3	23
	7	5	37
	5	7	7

Таблица 3.30

n	k	$d_{мин}$	$f_i(X)$
…	…	…	…
15	11	3	X^4+X+1
	7	5	$X^4 + X^3 + X^2 + X + 1$
	5	7	$X^2 + X + 1$

Таблица 3.31

$X^{15}+1$	$(X^2 + X + 1)(X + 1)(X^4 + X^3 + X^2 + X + 1)(X^4 + X^3 + 1)(X^4 + X + 1)$

Таблица 3.32

Степень бинома	Последовательности степеней корней неприводимых многочленов	Неприводимые сомножители	m
1	2	3	4
…	…	…	…
15	01 02 04 08	023	4
	03 06 12 09	037	4
	05 10	007	2
	07 14 13 11	031	4

Табл. 3.29 является фрагментом таблицы из Приложения 5.5. Табл. 3.30 получена из табл. 3.29 путём декодирования кодов, приведенных в её четвёртом столбце (переход от восьмеричной системы к двоичной).

Табл. 3.31 является фрагментом табл. из Приложения 5.2.

Табл. 3.32 является фрагментом табл. из Приложения 5.4.

Таблица 3.33

n	k	$d_{мин}$	Последовательность степеней корней $g(X)$	$g(X)$
…	…	…	…	…
15	11	3	01 02 04 08	X^4+X+1
15	7	5	01 02 04 08 03 06 12 09	$(X^4+X+1)(X^4 + X^3 + X^2 + X+ 1)$
15	5	7	01 02 04 08 03 06 12 09 05 10	$(X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1)$

Табл. 3.33 построена на основе данных, содержащихся в табл. 3.32, и в соответствии с пояснениями, приведенными в конце Приложения 5.5.

В качестве упражнения самостоятельно определим $d=d_{мин}$ для циклических (n, k)-кодов, приведенных в табл.

3.33, предварительно зафиксировав примитивный элемент α в поле $GF(2^m) = GF(2^4)$ с помощью многочлена X^4+X+1.

(15, 11)-код

Последовательность корней $g(X)$: α, α^2, α^4, α^8. Максимальная подпоследовательность корней порождающего многочлена с последовательными степенями: α, α^2; следовательно, согласно утверждению 3.3 m_0=1 и m_0+d - 2=2.Откуда имеем $d=d_{мин}$ = 3.

(15, 7)-код

Последовательность корней $g(X)$: α, α^2, α^3, α^4, α^6, α^8, α^9, α^{12}. Максимальная подпоследовательность корней порождающего многочлена с последовательными степенями: α, α^2, α^3, α^4; следовательно, согласно утверждению 3.3 m_0=1 и m_0+d - 2=4.Откуда имеем $d=d_{мин}$ = 5.

(15, 5)-код

Последовательность корней $g(X)$: α, α^2, α^3, α^4, α^5, α^6, α^8, α^9, α^{10}, α^{12}. Максимальная подпоследовательность корней порождающего многочлена с последовательными степенями: α, α^2, α^3, α^4, α^5, α^6; следовательно, согласно утверждению 3.3 m_0=1 и m_0+d - 2= 6. Откуда имеем $d=d_{мин}$ = 7.

END

3.14. НЕКОТОРЫЕ ВИДЫ БЧХ-КОДОВ

В настоящем разделе мы только перечислим важнейшие виды *двоичных* циклических БЧХ-кодов и в краткой форме укажем некоторые их характеристики.

Приведём, также некоторые дополнительные определения и сведения об этих кодах.

БЧХ-КОДЫ

Циклический (n, k)-код называется БЧХ-кодом, если корнями его порождающего многочлена являются элементы β^i , где i пробегает все числа из (p, n)-циклов, содержащих числа l+1, …, $l+r$, и только они.

Читатель, по-видимому уже заметил, что в ряде случаев l+1 и m_0 в различных выражениях означают одно и то же, и поэтому можно было бы просто положить в этих выражениях $l+1= m_0$; однако, мы этого не делаем, в первую очередь, из-за того, чтобы не затруднять работу читателя с различными цитируемыми основными литературными источниками.

ПРИМИТИВНЫЕ БЧХ-КОДЫ ИЛИ БЧХ-КОДЫ В УЗКОМ СМЫСЛЕ

В частном случае, при p=2, $n=2^m$-1, l=0, r=2t, БЧХ коды называют *примитивными БЧХ-кодами* или *БЧХ-кодами в узком смысле* [3.3, с. 164].

В [3.2, с. 306–307] приведена таблица двоичных БЧХ-кодов в узком смысле, порождаемых примитивными элементами порядков, меньших 2^{10}. Все коды из этой таблицы, длина которых не превосходит 15, и все коды, исправляющие двойные ошибки, являются *оптимальными* кодами.

КОДЫ ХЭММИНГА

В частном случае, при: p=2, $n=2^m$ - 1, l=0, r=2t, t=1 и $d \geq d_0 \geq r+1=2t+1=3$; эти *примитивные* БЧХ коды называют *циклическими кодами Хэмминга* (Hamming R.W., 1950). Код Хэмминга является *совершенным* кодом.

Проверочная матрица $\boldsymbol{H}$ кода Хэмминга состоит из r различных ненулевых строк и 2^r - 1 различных ненулевых столбцов – двоичных ненулевых наборов длины r. Никакая

совокупность из двух (и менее) столбцов этой проверочной матрицы $\boldsymbol{H}$ не является линейно зависимой, но существуют линейно зависимые совокупности из трёх столбцов. Следовательно, минимальное хэммингово расстояние нулевого пространства этой матрицы $d_{\min} = 3 = 2t+1$; $t = 1$. Это нулевое пространство является кодом, исправляющим все одиночные ошибки. Очевидно, что: $n = 2^r - 1$; $k = 2^r - 1 - r$.

В примерах 3.15 и 3.17 мы рассматривали циклический (7, 4)-код Хэмминга, имеющий минимальное кодовое расстояние $d=d_{\text{мин}}=3$ [3.2, с. 247–249].

КОДЫ РИДА-СОЛОМОНА

Важным подклассом БЧХ-кодов является коды Рида-Соломона (Reed I.S., Solomon G., 1960), имеющие параметры: $m_0 = 1$ и, следовательно, $l=0$; $n= q - 1$ ($q = 2^m$). Точнее говоря, коды Рида-Соломона – это *примитивные* БЧХ-коды с порождающим многочленом

$$g(X) = \prod_{i=1}^{r} (X - \beta^i), \qquad (3\text{-}63)$$

где β – один из примитивных элементов поля $GF(q)$. Минимальное кодовое расстояние для кодов Рида-Соломона

$$d = r+1. \qquad (3\text{-}64)$$

На основе кодов Рида-Соломона строятся наиболее мощные из известных кодов, исправляющих пакеты ошибок, и коды, одновременно исправляющие пакеты ошибок и случайные ошибки [3.2, с. 309; 3.3, с. 166].

Выше в примере 3.22 был рассмотрен циклический (7, 1)-код, являющийся кодом Рида-Соломона.

ЦИКЛИЧЕСКИЙ (23, 12)-КОД ГОЛЕЯ

Двоичный циклический (23, 12)-код Голея (Golay M.J.E., 1949) – это *совершенный* код, порождающим многочленом которого является многочлен одиннадцатой степени:

$$g(X) = (X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1),$$

являющийся делителем бинома $X^{23}+1$ (см. табл. 3.34). Табл. 3.34 является фрагментом табл. 5.1 из Приложения 5.2.

Таблица 3.34

$X^{23}+1$	$(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1)(X + 1)(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)$

Кодовое расстояние $d=d_{\text{мин}} = 7$ (см. Приложение 5.5).

См. также [3.2, с. 267–270; 3.3, с. 31, 165].

Завершая этот небольшой раздел, отметим, что, несмотря на всю важность БЧХ-кодов, они всё же являются лишь подклассом весьма обширного класса циклических кодов.

Вот цитата, поясняющая эту мысль [3.2, с. 305]: «Найдено около 8000 циклических кодов длины 63, лучших, чем БЧХ…» (см. Приложение 5.4).

3.15. КОДИРОВАНИЕ И ДЕКОДИРОВАНИЕ ЦИКЛИЧЕСКИХ (n, k)-КОДОВ

Сейчас мы приведём частный пример, иллюстрирующий одно из *важнейших достоинств* циклических кодов – *простоту схемотехнической реализации их кодеров*.

На рис. 3.1 с приведена схема умножения произвольного входного многочлена $b(X)$ над полем $GF(2)$ на фиксированный многочлен $g(X) = X^3 + X + 1$.

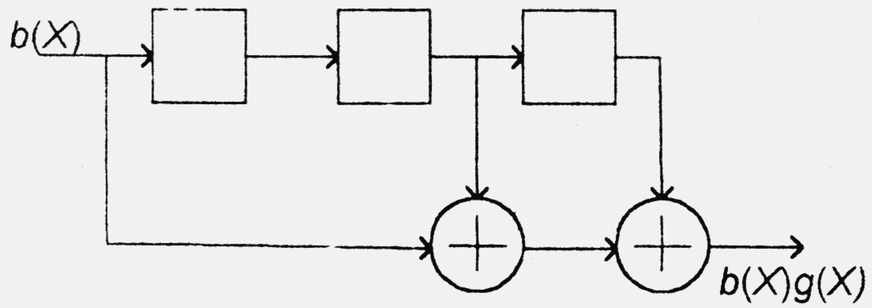

Рис. 3.1 с. Умножитель произвольного входного многочлена $b(X)$ на фиксированный многочлен $g(X)=X^3+X+1$

Умножитель полиномов, приведенный на рис. 3.1 с, собран из бистабильных (триггерных) ячеек памяти, изображённых в виде квадратиков, и сумматоров по модулю два, изображённых в виде кружка со знаком «+» внутри.

Занумеруем, считая слева направо, ячейки памяти номерами 1, 2 и 3, а двоичные сумматоры – номерами 1 и 2.

Согласно выше изложенному, все кодовые многочлены должны делиться на порождающий многочлен $g(X)=X^3+X+1$ рассмотренного выше (7, 4)-кода. Поэтому, если мы имеем безызбыточный вектор-сообщение $b = (b_{k-1}, b_{k-2}, \ldots, b_0) = (b_3, b_2, b_1, b_0)$, поступающий с выхода источника информации на вход кодера канала, то, отождествляя кодовые комбинации с многочленами, мы можем изложить операцию кодирования в терминах выполнения операций над многочленами. Заметим, что в рассматриваемом случае речь идёт об обычном умножении многочленов, так как сумма степеней многочленов $b(X)$ и $g(X)$ не превосходит числа $n = 7$.

На вход кодера-умножителя многочленов поступает безызбыточный многочлен-сообщение $b(X) = b_3X^3 + b_2X^2 + b_1X + b_0$, а на выходе кодера появляется кодовый многочлен

$$b(X)g(X) = (b_3X^3 + b_2X^2 + b_1X + b_0)(X^3+X+1).$$

Первоначально все ячейки памяти содержат нули, а коэффициенты многочлена $b(X)$ *поступают на вход кодера, начиная с коэффициентов при* ***старших*** *степенях* X.

В приложении 3.16 в общем виде и с техническими деталями строго доказывается, что общая схема, частным случаем которой является обсуждаемая схема, действительно выполняет функцию умножения многочленов.

Таким образом, при поступлении на вход кодера многочлена $b(X)$ в виде последовательности его коэффициентов на выходе кодера появляется последовательность коэффициентов кодового многочлена $b(X)g(X)$.

Легко видеть, что проверочным многочленом для циклического (7, 4)-кода является многочлен $h(X) = (X^7-1)/(X^3+X+1)=(X-1)(X^3+X^2+1)$ и, следовательно,

$$b(X)g(X)h(X) \equiv 0 \pmod{(X^7-1)}.$$

ПРИМЕР 3.24. Рассмотрим работу схемы умножителя, приведенной на рис.3.1, при поступлении на её вход кодового многочлена $b(X) = X^3 + X^2 + 1$. При построении табл. 3.35 считалось, что символ «-» соответствует нулю.

Таблица 3.35

j	Входной символ после j-го сдвига	Содержимое регистра сдвига после j-го сдвига	Выходной символ после j-го сдвига (сумма входного символа и выходных символов 2-й и 3-й ячеек)
0	-	000	0
1	1	000	1
2	1	100	1
3	0	110	1
4	1	011	1
5	-	101	1
6	-	010	1
7	-	001	1
8	-	000	0

Таким образом, на выходе рассматриваемой схемы появится кодовый полином $X^6+X^5+X^4+X^3+X^2+X+1$. Непосредственной проверкой убеждаемся (Maple V R5), что $(X^3 + X^2 + +1)(X^3+X+1) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \Leftrightarrow (1111111)$.

END

Рассмотренная схема кодера в смысле её технической реализации действительно является *предельно простой.*

Оказывается, что и схемы – делители многочленов могут быть использованы в качестве кодеров и эти схемы столь же просты, как и схемы – умножители многочленов [3.2].

Задача декодирования циклических кодов, вообще говоря, не допускает столь простой схемотехнической реализации, как задача кодирования.

Помимо синдромного декодирования существуют также другие методы декодирования, связанные с вычислением синдрома, полученного на выходе канала слова. На рис. 3.2 приведена схема декодера, реализующего подобные методы декодирования.

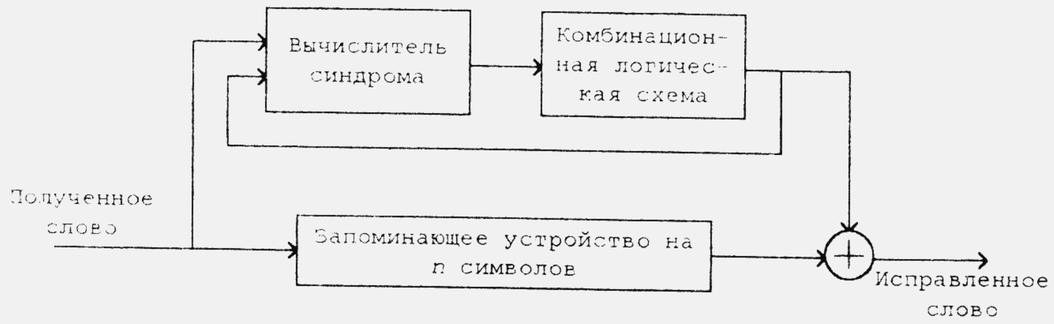

Рис. 3.2. Декодер циклического кода

Вычислитель синдрома реализуется по тем же принципам, что и кодеры для циклических кодов.

Сложность реализации комбинационной логической схемы определяется *выбранным алгоритмом декодирования.*

3.16. ПРИЛОЖЕНИЕ. ЭЛЕМЕНТЫ ЛИНЕЙНЫХ ПЕРЕКЛЮЧАТЕЛЬНЫХ СХЕМ И НЕКОТОРЫЕ СТАНДАРТНЫЕ СХЕМЫ

Линейными переключательными схемами с конечным числом состояний являются любые схемы, состоящие из конечного числа элементов - ячеек сдвиговых регистров, сумматоров и умножителей на константу, соединённых любым допустимым способом. В линейных переключательных схемах ***допустимо*** *соединение любого числа входов с любым выходом*, однако *соединение никаких двух выходов* ***является недопустимым***.

ЯЧЕЙКА СДВИГОВОГО РЕГИСТРА

Для осуществления функций запоминания и временной задержки сигнала на постоянную величину $\tau_з$, равную доле периода τ_0 последовательности тактирующих прямоугольных импульсов длительности τ (длительности переднего и заднего фронтов много меньше τ), может быть использован так называемый Master-Slave (двухступенчатый) D-триггер со срабатыванием по заднему (или переднему) фронту, имеющий один информационный D-вход (Delay – задержка), один тактирующий C-вход, на который поступает периодическая последовательность прямоугольных импульсов (см. рис. 3.3, на котором представлены временные диаграммы, поясняющие работу ячейки памяти), один информационный Q-выход (и один информационный $\bar{Q}$-выход; [3.15, с. 118; 3.16, с. 125]). Этот D-триггер, являющийся ячейкой сдвигового регистра, состоит из двух бистабильных ячеек – ведущем (Master) и ведомом (Slave) триггерах.

При увеличении напряжения тактирующего импульса (передний фронт) и достижения или превышения им определённого значения на входе C ведомый триггер отключается от

ведущего и при дальнейшем увеличении напряжения тактирующего импульса и достижении значения, равного или большего некоторой определённой величины, близкой к напряжению логической единицы, в ведущий триггер записывается «входная информация»; при этом ведомый триггер отключен от ведущего, а выход D-триггера соответствует содержимому ведомого триггера. При уменьшении напряжения тактирующего импульса (задний фронт) на входе С сначала ведущий триггер снова отключится от входов D-триггера, и при дальнейшем его уменьшении до значения, равного или меньшего некоторой определённой величины, выходы ведущего триггера подключатся ко входам ведомого триггера, и содержимое ведущего триггера перезаписывается в ведомый триггер. Далее процесс записи «входной информации» с D-входа в ведущий триггер и её перезаписи из ведущего триггера в ведомый триггер периодически повторяется.

На рис. 3.3 использованы обозначения:

t – текущее время;

τ_0 – период последовательности прямоугольных импульсов;

τ – длительность тактирующих прямоугольных импульсов;

a_i – i-й двоичный символ рассматриваемой последовательности символов, i=1, 2, …, 5;

a^* – символ логического нуля; при этом предполагается, что длительности переднего и заднего фронтов тактового импульса пренебрежимо малы по сравнению с его длительностью;

τ_y – время упреждения;

$\tau_з$ – время задержки выходного символа относительно соответствующего ему входного символа.

При этом обычно выполняются соотношения

$$0 < \tau \le \tau_0/2, \quad (3\text{-}65) \qquad 0 < \tau < \tau_з \le \tau_0, \quad (3\text{-}66)$$

$$0 < \tau_y \le (\tau_0 - \tau). \quad (3\text{-}67)$$

В данной книге рассматривается лишь случай:

$$\tau_з = \tau_0, \quad (3\text{-}68) \qquad \tau_y = (\tau_0 - \tau), \quad (3\text{-}69)$$

который реализуется, например, когда на вход рассматриваемой ячейки символы поступают с выхода аналогичной ячейки, являющейся элементом некоторой схемы, тактируемой теми же самыми тактирующими импульсами, представленными на рис. 3.3.

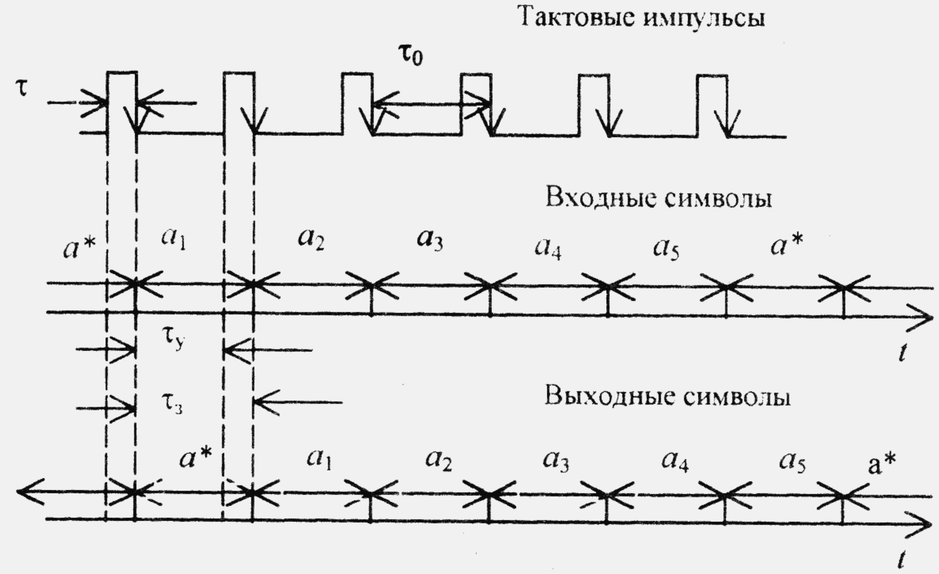

Рис.3.3. Временные последовательности входных и выходных символов ячейки сдвигового регистра

Таким образом, изменение входного символа D-триггера определяется изменением выходного символа предыдущей схемы, подающей символы на вход рассматриваемого триггера, а изменение выходного символа D-триггера происходит на *заднем фронте* тактирующего импульса. Если

же чередующиеся символы на входе рассматриваемого D-триггера поступают с выхода аналогичного D-триггера, тактируемого теми же самыми тактирующими импульсами, то *изменения входных и выходных символов рассматриваемого* D-триггера (сдвиг) *происходят одновременно на заднем фронте тактирующих импульсов.*

Далее для определённости будем рассматривать устройства, реализованные на D-триггерах *со срабатыванием по заднему фронту.*

Из рис. 3.3 следует, что входные и выходные символы ячейки сдвигового регистра – D-триггера имеют одну и ту же длительность τ_0; выходной символ задержан во времени относительно соответствующего ему входного на $\tau_з = \tau_0$ и всегда соответствует содержимому ведомого триггера; время упреждения $\tau_y = (\tau_0 - \tau)$.

Мы будем использовать упрощенное изображение D-триггера в виде квадратика с одним информационным (D-) входом и одним информационным (Q-) выходом (рис. 3.4, *a*; C-вход и $\bar{Q}$-выход здесь не показаны; *a* –двоичный символ).

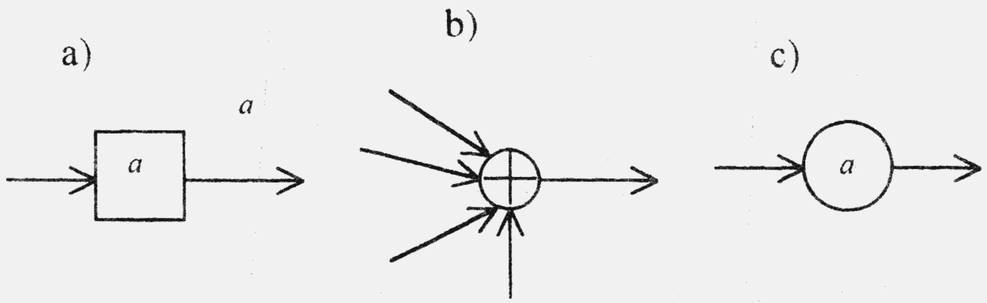

Рис. 3.4. Элементы линейных переключательных схем

СУММАТОР ПО МОДУЛЮ ДВА

На рис. 3.4, *b* изображён сумматор по модулю два, имеющий n входов ($n \geq 2$) и один выход.

Пусть $w(x_1, x_2, \ldots, x_n) = w(\boldsymbol{x})$ – вес комбинации $\boldsymbol{x} = x_1, x_2, \ldots, x_n$; x_i – двоичная переменная, принимающая значения 0 или 1, i=1, 2, …, n. Выходная последовательность двоичных символов y этого устройства связана с входными двоичными символами $x_1, x_2, \ldots, x_n$ соотношением

$$y = x_1 \oplus x_2 \oplus \ldots, \oplus x_n = \begin{cases} 0, & w(\boldsymbol{x}) \text{ – чётное число,} \\ 1, & w(\boldsymbol{x}) \text{ – нечётное число.} \end{cases} \quad (3\text{-}70)$$

При n = 2 сумматор по модулю 2 с n входами может быть реализован на логических элементах:

два элемента НЕ, два элемента И и один элемент типа ИЛИ

или другой вариант:

один элемент ИЛИ, один элемент И-НЕ и один элемент И;

а при n > 2 сумматор по модулю 2 с n входами может быть реализован на (n - 1) двоичных сумматорах с двумя входами [3.4, 3.15, 3.16].

УМНОЖИТЕЛЬ НА КОНСТАНТУ

На рис. 3.4, *c* изображён элемент – умножитель на константу *a*: выходной символ умножителя равен его входному символу, умноженному на константу *a*, которой может быть любой элемент поля. Этот элемент имеет один вход и один выход.

Если *a* – двоичная константа, то необходимость изображения этого элемента на схеме отпадает: наличие в схеме умножителя при a = 1 равносильно введению дополнительного соединения, а при a = 0 равносильно отсутствию такого соединения.

В данной книге считается, что сумматор по модулю два и умножитель на константу являются безынерционными элементами.

НЕКОТОРЫЕ СТАНДАРТНЫЕ СХЕМЫ

В приводимых ниже схемах входной и выходной сигналы образованы последовательностями двоичных символов одной и той же длительности τ_0. Эти двоичные символы могут интерпретироваться как коэффициенты многочленов (полиномов), над которыми производятся определённые операции.

Входные и выходные многочлены передаются, *начиная с коэффициентов, соответствующих высшим степеням*, так как, например, при делении (когда деление возможно) в первую очередь должны быть обработаны коэффициенты входного многочлена-делимого, соответствующие высшим степеням X. Например, многочлен

$$b(X) = b_nX^n + b_{n-1}X^{n-1} + \ldots + b_i + \ldots + b_1X + b_0, \qquad (3\text{-}71)$$

$b_n \neq 0$ и $b_0 \neq 0$, будет поступать на вход или появляться на выходе схемы в виде: b_n, b_{n-1}, …, b_1, b_0 – последовательности $(n+1)$ элементов поля – двоичных символов, являющихся коэффициентами этого многочлена; натуральное число $i \in \{n, (n-1), \ldots, 1, 0\}$.

Символ X в полиноме $b(X)$ называется *неопределённым символом* или *формальной переменной* [3.1 – 3.3].

Сдвиговый регистр

Если соединить последовательно несколько идентичных вышерассмотренных бистабильных ячеек, то получится так называемый сдвиговый регистр с последовательным вводом данных. В качестве примера на рис. 3.5 приведен четырёхразрядный сдвиговый регистр. Пусть ячейки регистра – MS-триггеры занумерованы слева направо цифрами 1, 2, 3, 4, а на вход регистра сдвига поступает двоичная последовательность символов $a_1\ a_2\ \ldots\ a_6\ a_7$.

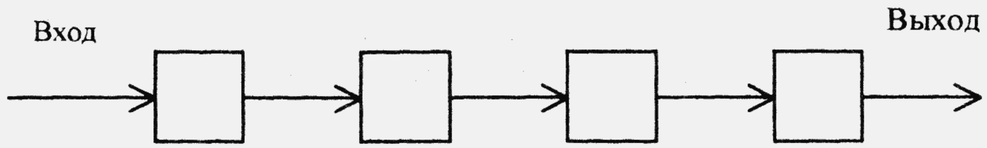

Рис.3.5. Сдвиговый регистр с последовательным вводом данных

Таблица 3.36

Номер тактового импульса	Символ на входе регистра	Q_1	Q_2	Q_3	Q_4
0	a_1	a^*	a^*	a^*	a^*
1	a_2	a_1	a^*	a^*	a^*
2	a_3	a_2	a_1	a^*	a^*
3	a_4	a_3	a_2	a_1	a^*
4	a_5	a_4	a_3	a_2	a_1
5	a_6	a_5	a_4	a_3	a_2
6	a_7	a_6	a_5	a_4	a_3
7	a^*	a_7	a_6	a_5	a_4
8	a^*	a^*	a_7	a_6	a_5
9	a^*	a^*	a^*	a_7	a_6
10	a^*	a^*	a^*	a^*	a_7
11	a^*	a^*	a^*	a^*	a^*

Табл. 3.36 иллюстрирует состояние выходов ячеек памяти Q_i, i=1, …, 4, рассматриваемого сдвигового регистра. При построении табл. 3.36 считалось, что символ входной по-