же циклический код может быть определён из условия, что он является *нулевым пространством* идеала, порождённого многочленом степени k

$$h(X) = \frac{X^n - 1}{g(X)}. \qquad (3\text{-}45)$$

Если степень многочлена $g(X)$ равна $r = n - k$, то, согласно теореме 3.11, размерность циклического кода (циклического подпространства) равна $k = n - r$. При этом элемент $\{f(X)\}$ принадлежит коду в том и только в том случае, если $f(X)$ делится на $g(X)$.

ОПРЕДЕЛЕНИЕ 3.6а. *Многочлен $h(X)$, определяемый соотношением* (3-45), *называется* ***проверочным многочленом*** *для циклического кода C_g, порождаемого многочленом $g(X)$.*

END

Так как многочлен $h(X)$ является делителем бинома X^n-1, то он может быть использован в качестве многочлена, порождающего циклический код C_h, *дуальный* или *двойственный* к коду C_g и являющийся нулевым пространством для C_g.

Если единственное с точностью до порядка следования сомножителей разложение бинома X^n-1 имеет вид

$$X^n - 1 = g_1^{\mu_1}(X) g_2^{\mu_2}(X) \dots g_s^{\mu_s}(X), \qquad (3\text{-}46)$$

где $g_i(X)$ – нормированный неприводимый многочлен, степень которого больше нуля; целые числа $\mu_i \geq 1$, i=1, 2, … s (s – число неразложимых многочленов-множителей бинома X^n-1), то число идеалов алгебры A_n $N_{ид}$ (исключая не имеющие практического значения варианты порождающих многочленов: $g_0(X) = 1$ и бинома X^n-1) выражается соотношением:

$$N_{ид} = (\mu_1+1)(\mu_2+1) \dots (\mu_s+1) - 2 = \prod_{i=1}^{s} (\mu_i + 1) - 2; \qquad (3\text{-}47)$$

в частном случае, при

$$\mu_1 = \mu_2 = \dots = \mu_s = 1 \qquad (3\text{-}48)$$

$$N_{ид} = 2(2^{s-1} - 1). \qquad (3\text{-}48а)$$

В приведенном ниже примере рассматриваются некоторые варианты выбора порождающих многочленов.

ПРИМЕР 3.13. Пусть дан многочлен X^3-1 = $(X - 1)(X^2 + X + 1)$ над полем $GF(2)$ (табл. 3.21).

Согласно сказанному выше, здесь мы не учитываем практически не интересных случаев порождающих многочленов вида: $g_0(X)$=1 и бинома X^3-1.

Таблица 3.21

Порождающий многочлен $g(X)$	Многочленное представление $\boldsymbol{G}$	Векторное представление $\boldsymbol{G}$	(n, k)-код и $h(X)$	$\boldsymbol{H}$
$g_1(X)$= =$(X$-1)	$\lceil Xg_1(X) \rceil$ $\lfloor g_1(X) \rfloor$	$\lceil 110 \rceil$ $\lfloor 011 \rfloor$	(3, 2)-код; X^2+X+1	[111]
$g_2(X)$= =X^2+X+1	$[g_2(X)]$	[111]	(3, 1)-код; (X-1)	$\lceil 011 \rceil$ $\lfloor 110 \rfloor$

Так как в рассматриваемом случае число неприводимых многочленов-сомножителей бинома X^3-1 $s = 2$ и $\mu_1 = \mu_2 = 1$, то согласно (3-48а) $N_{ид} = 2(2^{s-1} - 1) = 2$: (3, 2)-код и (3, 1)-код.

Легко проверить, что для порождающих и проверочных матриц (n, k)-кодов, приведенных в табл. 3.21, выполняются соотношения: $\boldsymbol{G}\boldsymbol{H}^T = \boldsymbol{0} = [0]$.

Отметим, что порождающие многочлены $g_i(X)$ пишутся, *начиная со слагаемых высших степеней* (***в порядке убыва-***

ния степеней слагаемых); при этом многочлену $X^j g_i(X)$ соответствует циклический сдвиг ***влево***.

Следует обратить внимание на способ получения проверочной матрицы ***G***: строки матрицы образованы коэффициентами многочленов вида $\{X^{n-r-j}g(X)\}$, $j = 1, 2, \ldots, k$, (считая с первой верхней строки ***G*** до её последней нижней строки).

END

ПРИМЕР 3.13a. Пусть дан многочлен X^4-1 = $(X - 1)^4$ над полем $GF(2)$ (табл. 3.22).

Таблица 3.22

Порождающий многочлен $g(X)$	Многочленное представление ***G***	Векторное представление ***G***	(n, k)-код и $h(X)$	***H***
$g_1(X)=$ $= X$-1	$\lceil X^2 g_1(X) \rceil$ $\lvert X g_1(X) \rvert$ $\lfloor g_1(X) \rfloor$	$\lceil 1100 \rceil$ $\lvert 0110 \rvert$ $\lfloor 0011 \rfloor$	(4, 3)-код; X^3+X^2+ $+X+1$	[1111]
$g_2(X)=$ $= X^2+1$	$\lceil X g_2(X) \rceil$ $\lfloor g_2(X) \rfloor$	$\lceil 1010 \rceil$ $\lfloor 0101 \rfloor$	(4, 2)-код; X^2+1	$\lceil 0101 \rceil$ $\lfloor 1010 \rfloor$
$g_3(X)=$ $=X^3+X^2+$ $+X+1$	$[g_3(X)]$	[1111]	(4, 1)-код; $X+1$	$\lceil 0011 \rceil$ $\lvert 0110 \rvert$ $\lfloor 1100 \rfloor$

Согласно сказанному выше, здесь мы не учитываем практически не интересных случаев порождающих многочленов вида: $g_0(X)$=1 и бинома X^4-1.

Так как в рассматриваемом случае число неприводимых многочленов-сомножителей бинома X^4-1 = $(X - 1)^4$ $s = 1$ и показатель степени $\mu_1 = 4$, то согласно (3-47) $N_{ид} = [(\mu_1 + 1) - 2] = 3$: (4, 1)-код, (4, 2)-код и (4, 3)-код.

Из рассмотрения табл. 3.22 вытекает, что применение в качестве порождающего многочлена $(X+1)^i$, i =1, 2, 3, приводит к получению циклических (4, 3)-, (4, 2)- и (4, 1)-кодов соответственно. Непосредственная проверка для кодов, определённых в табл. 3.22, показывает, что $\boldsymbol{GH}^T = [0] = \mathbf{0}$.

Следует обратить внимание на способ получения проверочной матрицы ***H***: строки матрицы образованы коэффициентами многочленов вида $\{X^{r-j}h(X)\}$, $j = 1, \ldots, r$, (считая с первой верхней строки ***H*** до её последней нижней строки), которые записаны в *обратном* порядке.

END

ПРИМЕР 3.13b. Пусть алгебра многочленов A_7 определяется биномом $(X^7$-1) = $(X$-1)$(X^3+X+1)(X^3+X^2+1)$ над полем Галуа $GF(2)$. Многочлен $g(X) = (X^3+X^2+1)$ порождает циклический (7, 4)-код. Этот код является нулевым пространства идеала, порождённого многочленом $h(X) = (X$-1$)(X^3+X+1) = (X^4+$ $+X^3+X^2+1)$.

Следующие соотношения определяют построение ***G*** и возможные варианты построения матрицы ***H***:

$\{X^3 g(X)\}, \Leftrightarrow (1101000)$,

$\{X^2 g(X)\}, \Leftrightarrow (0110100)$, $\quad \{X^2 h(X)\} \Leftrightarrow (1110100)$,

$\{Xg(X)\}, \Leftrightarrow (0011010)$ $\quad \{Xh(X)\} \Leftrightarrow (0111010)$,

$\{g(X)\} \Leftrightarrow (0001101)$, $\quad \{h(X)\} \Leftrightarrow (0011101)$.

Приведенные ниже (см. рис. 3.1) два варианта выбора проверочной матрицы ***H*** при уже выбранной порождающей матрице ***G*** иллюстрируют то, что может произойти, если при построении матрицы ***H*** не следовать требованию выписывания её строк «в обратном порядке».

Как мы видим (рис. 3.1), в случае А $\boldsymbol{GH}^T \neq \mathbf{0}$, а в случае Б $\boldsymbol{GH}^T = \mathbf{0}$ и, следовательно, строки матрицы ***H*** следует выписывать в «обратном порядке» (строгое обоснование этого положения приведено ниже).

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

А) Строки матрицы **H** пишутся также, как и строки матрицы **G**.

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

$$\mathbf{S} := \mathbf{G} \cdot \mathbf{H}^{\mathbf{T}} \qquad \mathbf{i} := 1..4 \qquad \mathbf{j} := 1..3 \qquad \mathbf{H}^{\mathbf{T}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\mathbf{S} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \qquad \mathbf{S}_{\mathbf{i},\mathbf{j}} := \mathbf{mod}(\mathbf{S}_{\mathbf{i},\mathbf{j}}, 2)$$

Б) Строки матрицы **H** пишутся "в обратном порядке" по сравнению с предыдущим случаем А.

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

$$\mathbf{S} := \mathbf{G} \cdot \mathbf{H}^{\mathbf{T}} \qquad \mathbf{i} := 1..4 \qquad \mathbf{j} := 1..3 \qquad \mathbf{H}^{\mathbf{T}} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\mathbf{S} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \mathbf{S}_{\mathbf{i},\mathbf{j}} := \mathbf{mod}(\mathbf{S}_{\mathbf{i},\mathbf{j}}, 2)$$

Рис. 3.1. Порядок выписывания строк ***H***

END

На основе рассмотрения данных примеров 3.13, 3.13a, и 3.13b можно сформулировать полезное правило: если некоторый многочлен, степени X слагаемых которого растут или убывают слева направо, умножается на X, то циклический сдвиг осуществляется ***в направлении более высоких степеней*** X его членов.

Так как для важнейших циклических кодов порождающий многочлен имеет, как правило, вид

$$g(X) = g_1(X)\, g_2(X) \ldots g_s(X), \qquad (3\text{-}48б)$$

где $g_i(X)$ – неприводимые многочлены, $i=1, 2, \ldots, s$, то в дальнейшем будем считать, если не оговорено противное, что имеет место именно этот случай.

Остановимся более подробно на необходимости записи строк проверочной матрицы циклического кода ***H*** *в обратном порядке* (при установленном способе записи строк порождающей матрицы ***G***). Эта необходимость проистекает из того, что условия равенства скалярного произведения векторов нулю и равенства нулю произведения соответствующих этим векторам многочленов *не совпадают*.

Пусть

$$a(X) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1}, \quad a(X) \Leftrightarrow \boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1}),$$

$$b(X) = b_0 + b_1X + \ldots + b_{n-1}X^{n-1}, \quad b(X) \Leftrightarrow \boldsymbol{b} = (b_0, b_1, \ldots, b_{n-1}),$$

$$c(X) = c_0 + c_1X + \ldots + c_jX^j + \ldots + c_{n-1}X^{n-1} = a(X)b(X).$$

где

$$c_j = a_0b_j + a_1b_{j-1} + \ldots + a_jb_0 +$$

$$+ a_{j+1}b_{n-1} + a_{j+2}b_{n-2} + \ldots + a_{n-1}b_{j+1}, \qquad (3\text{-}48в)$$

причём слагаемые в (3-48в), содержащие a_{j+1}, …, a_{n-1}, получаются из слагаемых в $a(X)b(X)$, которые содержат X^{n+j}, так как если $X^n - 1 = 0$, то $X^{n+j} = X^j$ [3.2, с. 177].

Тогда, если $\boldsymbol{ab} = 0$, то

$$\boldsymbol{ab} = a_0b_0 + a_1b_1 + \ldots + a_{n-1}b_{n-1} = 0,$$

и если

$$c(X) = a(X)b(X) = 0,$$

то это последнее соотношение с учётом (3-48в) можно переписать в виде:

$$c_j = (a_0, a_1, \ldots, a_{n-1})(b_j, b_{j-1}, \ldots, b_0, b_{n-1}, b_{n-2}, \ldots, b_{j+1}) = 0,$$
$$j = 0, 1, \ldots, n-1. \qquad (3\text{-}48г)$$

В произведении двух векторов в (3-48г) первый вектор – вектор, соответствующий многочлену $a(X)$, а второй вектор содержит коэффициенты многочлена $b(X)$, *расположенные в обратном порядке и сдвинутые циклически на* $j+1$ *элемент* ***вправо***.

Таким образом, если $a(X)b(X) = 0$, то это равносильно тому, что вектор $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ ортогонален вектору $\boldsymbol{b} = (b_{n-1}, b_{n-2}, \ldots, b_0)$, а также всем его циклическим сдвигам.

Именно поэтому, как отмечалось в примерах 3.13а и 3.13b необходима запись строк проверочной матрицы циклического кода $\boldsymbol{H}$ *в обратном порядке* (*при установленном выше способе записи строк порождающей матрицы* $\boldsymbol{G}$).

Справедливо и обратное утверждение: если вектор $(a_0, a_1, \ldots, a_{n-1})$ ортогонален вектору $(b_{n-1}, b_{n-2}, \ldots, b_0)$ и всем циклическим сдвигам этого вектора, то $a(X)b(X) = 0$.

Пусть C – представляет собою двоичный (n, k)-код; $v(X)$ – некоторый кодовый многочлен этого кода; $a(X)$ – некоторый произвольный многочлен из алгебры многочленов A_n. Множество всех *классов вычетов по модулю* $X^n - 1$ обозначим

через R_n. Тогда будет справедлива следующая теорема [3.3, с. 150].

ТЕОРЕМА 3.26. Пусть C – циклический (n, k)-код и $I = \{(v(X)) \in R_n \mid v \in C\}$. Тогда существует такой нормированный многочлен $g(X)$ степени $(n - k)$, делящий $X^n - 1$, что выполнение сравнения

$$a(X) \equiv 0 \pmod{g(X)}$$

является необходимым и достаточным условием того, что $(a(X)) \in I$ (см. также теорему 3.12).

END

3.9. МАТРИЧНОЕ ОПИСАНИЕ ЦИКЛИЧЕСКИХ КОДОВ НА ОСНОВЕ ЗАДАНИЯ ПОРОЖДАЮЩЕГО МНОГОЧЛЕНА $g(X)$ ИЛИ ПРОВЕРОЧНОГО МНОГОЧЛЕНА $h(X)$

В общих чертах мы уже изложили матричное описание циклического кода на основе использования порождающего многочлена $g(X)$ или проверочного многочлена $h(X)$. Теперь приведём более подробное изложение этой темы. В основу изложения и анализа этой темы положим следующие факты.

1) Рассматриваемые циклические коды образуют циклическое подпространство или идеал в линейной алгебре многочленов A_n по модулю многочлена $X^n - 1$.

2) Циклические коды образуют подкласс блоковых групповых (n, k)-кодов, где по-прежнему n – длина кодовой комбинации или кодового вектора, k – число её информационных элементов; $r = n - k$ – число проверочных элементов кодовой комбинации.

3) Степень порождающего многочлена $g(X)$ $r = n - k$;

степень проверочного многочлена $h(X) = \dfrac{X^n - 1}{g(X)}$ равна k.

Если порождающий многочлен циклического кода

$$g(X) = g_r X^r + g_{r-1} X^{r-1} + \ldots + g_0,$$

то все многочлены вида $\{X^{n-r-j} g(X)\}$, $j = 1, 2, \ldots, k$, также являются кодовыми многочленами. Следовательно, все строки приведенной ниже матрицы $\boldsymbol{G}$ размерности $k \times n$ являются кодовыми векторами

$$\boldsymbol{G} = \begin{bmatrix} X^{k-1}g(X) \\ \ldots \\ \ldots \\ \ldots \\ X^2 g(X) \\ Xg(X) \\ g(X) \end{bmatrix} = \begin{bmatrix} g_r & g_{r-1} & \ldots & g_0 & 0 & 0 & \ldots & 0 \\ 0 & g_r & g_{r-1} & \ldots & g_0 & 0 & \ldots & 0 \\ 0 & & & \ldots & & & \ldots & 0 \\ 0 & & & \ldots & & & \ldots & 0 \\ 0 & & & \ldots & & & \ldots & 0 \\ 0 & 0 & & \ldots & 0 & g_r & g_{r-1} \ldots & g_0 \; 0 \\ 0 & 0 & & \ldots & 0 & g_r & \ldots & g_0 \end{bmatrix}. \tag{3-49}$$

Несложно показать, что строки организованной указанным образом порождающей матрицы $\boldsymbol{G}$ являются линейно независимыми кодовыми векторами и ранг матрицы $\boldsymbol{G}$ равен k.

Действительно, так как произвольная линейная комбинация векторов-строк матрицы $\boldsymbol{G}$

$$\Xi(X) = \sum_{i=0}^{k-1} \lambda_i X^i g(X) = g(X) \cdot \sum_{i=0}^{k-1} \lambda_i X^i = g(X)\Lambda(X),$$

то степень произвольного ненулевого многочлена

$$\Lambda(X) = \sum_{i=0}^{k-1} \lambda_i X^i$$

не превышает k-1 < k и, следовательно, степень многочлена $\Xi(X)$ меньше n и $\Xi(X) \neq 0 \pmod{X^n - 1}$.

Следовательно, пространство строк матрицы $\boldsymbol{G}$ представляет собою кодовое пространство.

Аналогично создаётся проверочная матрица $\boldsymbol{H}$. Если проверочный многочлен циклического кода

$$h(X) = h_k X^k + h_{k-1} X^{k-1} + \ldots + h_0,$$

то все многочлены вида $\{X^{r-j} h(X)\}$, $j = 1, \ldots, r$, также являются проверочными многочленами. Следовательно, все строки приведенной ниже матрицы $\boldsymbol{H}$ размерности $(n\text{-}k) \times n$, выписанные в обратном порядке, являются проверочными многочленами

$$\boldsymbol{H} = \begin{bmatrix} X^{r-1}h(X) \\ \ldots \\ \ldots \\ \ldots \\ X^2 h(X) \\ Xh(X) \\ h(X) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & h_0 & \ldots & h_k \\ 0 & 0 & 0 & \ldots & 0 & h_0 & h_1 & \ldots & h_k \; 0 \\ 0 & & & \ldots & & & & \ldots & 0 \\ 0 & & & \ldots & & & & \ldots & 0 \\ 0 & & & \ldots & & & & \ldots & 0 \\ 0 & h_0 & h_1 & \ldots & h_{k-1} & h_k & 0 \ldots & 0 & 0 \\ h_0 & h_1 & & \ldots & h_k & 0 & 0 \ldots & 0 & 0 \end{bmatrix}. \tag{3-50}$$

Несложно показать, что строки организованной указанным образом порождающей матрицы $\boldsymbol{H}$ являются линейно независимыми кодовыми векторами. Ранг матрицы $\boldsymbol{H}$ равен $r = n - k$.

3.10. СПОСОБ ПОСТРОЕНИЯ ПОРОЖДАЮЩЕЙ И ПРОВЕРОЧНОЙ МАТРИЦ, ИМЕЮЩИХ КАНОНИЧЕСКУЮ ФОРМУ, ПО ПОРОЖДАЮЩЕМУ МНОГОЧЛЕНУ

При изложении правил построения порождающей матрицы ($\boldsymbol{G}$ или $\boldsymbol{G}_{(n,\,k)}$) и проверочной матрицы ($\boldsymbol{H}$ или $\boldsymbol{H}_{(n,\,k)}$) потребуем, чтобы эти матрицы имели каноническую форму:

$$\boldsymbol{G} = [\boldsymbol{I}_k \boldsymbol{R}_{k\times(n-k)}], \qquad \boldsymbol{H} = [\boldsymbol{R}^{\mathrm{T}}_{k\times(n-k)} \boldsymbol{I}_{n-k}].$$

В соответствии со сказанным потребуем, чтобы в любом кодовом многочлене циклического кода первые k символов (т.е. коэффициенты при X^{n-1}, X^{n-2}, …, X^{n-k}) выполняли бы роль информационных символов и последние n-k символов (коэффициенты при X^{n-k-1}, X^{n-k-2}, …, 1) выполняли бы роль проверочных символов.

Порождающая матрица любого циклического кода будет иметь каноническую форму при её построении по излагаемому ниже способу.

Пусть деление по алгоритму Евклида X^i на порождающий многочлен $g(X)$ приводит к результату:

$$X^i = g(X)q_i(X) + r_i(X), \qquad (3\text{-}51)$$

где $q_i(X)$ – многочлен-частное, а $r_i(X)$ – многочлен-остаток. Многочлены

$$X^i - r_i(X) = g(X)q_i(X) \qquad (3\text{-}52)$$

являются кодовыми векторами. Если в качестве строк порождающей матрицы $\boldsymbol{G}$ выбрать многочлены вида (3-52) при $i=n-1, n-2, \ldots, n-k$, то

$$\boldsymbol{G} = [\boldsymbol{I}_k \boldsymbol{R}_{k\times(n-k)}], \qquad (3\text{-}53)$$

где $\boldsymbol{I}_k$ – единичная матрица размерности $k\times k$; $\boldsymbol{R}_{k\times(n-k)}$ – матрица размерности $k\times(n-k)$, j-й строкой которой является вектор из коэффициентов многочлена $r_{n-j}(X)$, $j=1, 2, \ldots, n-k$.

В этом случае, согласно теореме 2.8, циклический (n, k)-код является нулевым пространством матрицы:

$$\boldsymbol{H} = [\boldsymbol{R}^{\mathrm{T}}_{k\times(n-k)} \boldsymbol{I}_{n-k}],$$

так как

$$\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}} = [0] = \boldsymbol{0},$$

причём j-я строка матрицы $\boldsymbol{H}^{\mathrm{T}}$, $j = 1, 2, \ldots, n-k, \ldots, n$, является вектором из коэффициентов многочлена $r_{n-j}(X)$ даже при $j > n - k$.

Заметим, что в случае рассматриваемых двоичных кодов $X^i - r_i(X) = X^i + r_i(X)$.

ПРИМЕР 3.14. Задан многочлен $X^7-1=(X-1)(X^3+X+1)(X^3+X^2+1)$ над полем Галуа $GF(2)$, определяющий алгебру многочленов по модулю X^7-1. Требуется найти порождающую матрицу в канонической форме $\boldsymbol{G}$ и проверочную матрицу $\boldsymbol{H}$ в канонической форме для двоичного циклического кода, порождаемого многочленом $g(X)=X^3+X^2+1$ (табл. 3.23).

Таблица 3.23

j	X^{n-j}	$r_{n-j}(X)$	Строки $\boldsymbol{I}_k$	Строки $\boldsymbol{R}_{k\times(n-k)}$	Строки $\boldsymbol{H}^{\mathrm{T}}$
1	X^6	X^2+X	1000	110	110
2	X^5	$X+1$	0100	011	011
3	X^4	X^2+X+1	0010	111	111
4	X^3	X^2+1	0001	101	101
5	X^2	X^2			100
6	X	X			010
7	1	1			001

Из исходных данных следует: $n=7$, $r=n-k=3$; поэтому $k=4$. С помощью пакета Maple V R5 найдём полиномы-остатки $r_{n-j}(X)$ от деления X^{n-j} на $g(X)$ и, следуя приведенной выше методике, найдём порождающую матрицу $\boldsymbol{G}$ и проверочную матрицу $\boldsymbol{H}$ группового (7, 4)-кода.

Табл. 3.23 иллюстрирует процесс нахождения порождающей матрицы $\boldsymbol{G}$ и матрицы $\boldsymbol{H}^{\mathrm{T}}$ группового (7, 4)-кода.

На рис. 3.1 а приведены: порождающая матрица $\boldsymbol{G}$, проверочная матрица $\boldsymbol{H}$ группового (7, 4)-кода, созданного с помощью порождающего многочлена X^3+X^2+1, и синдром $\boldsymbol{S}$.

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

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

$i := 1..4 \qquad j := 1..3$

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

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

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

Рис.3.1 a. Определение $\boldsymbol{G}$ и $\boldsymbol{H}^T$ (7, 4)-кода

END

ПРИМЕР 3.15. Задан многочлен $X^7-1=(X-1)(X^3+X+1)(X^3+X^2+1)$ над полем Галуа $GF(2)$, определяющий алгебру многочленов по модулю X^7-1. Требуется найти порождающую матрицу в канонической форме $\boldsymbol{G}$ и проверочную матрицу $\boldsymbol{H}$ в канонической форме для двоичного циклического кода, порождаемого многочленом $g(X)=X^3+X+1$.

Из исходных данных следует: $n=7$, $r=n-k=3$; поэтому $k=4$. С помощью пакета Maple V R5 найдём полиномы-остатки $r_{n-j}(X)$ от деления X^{n-j} на $g(X)$ и, следуя приведенной выше методике, найдём порождающую матрицу $\boldsymbol{G}$ и проверочную матрицу $\boldsymbol{H}$ группового (7, 4)-кода.

Табл. 3.24 иллюстрирует процесс нахождения порождающей матрицы $\boldsymbol{G}$ и матрицы $\boldsymbol{H}^T$ группового (7, 4)-кода.

Таблица 3.24

j	X^{n-j}	$r_{n-j}(X)$	Строки $\boldsymbol{I}_k$	Строки $\boldsymbol{R}_{k\times(n-k)}$	Строки $\boldsymbol{H}^T$
1	X^6	X^2+1	1000	101	101
2	X^5	X^2+X+1	0100	111	111
3	X^4	X^2+X	0010	110	110
4	X^3	$X+1$	0001	011	011
5	X^2	X^2			100
6	X	X			010
7	1	1			001

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

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

$i := 1..4 \qquad j := 1..3$

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

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

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

Рис.3.1 b. Определение $\boldsymbol{G}$ и $\boldsymbol{H}^T$ (7, 4)-кода

На рис. 3.1 b приведены: порождающая матрица ***G***, проверочная матрица ***H*** группового (7, 4)-кода, созданного с помощью порождающего многочлена X^3+X+1, и синдром ***S***.

END

ПРИМЕР 3.16. При заданном многочлене

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

над полем Галуа $GF(2)$ в двух предыдущих примерах были построены два различных групповых (7, 4)-кода, порождаемых многочленами (X^3+X^2+1) и (X^3+X+1). Требуется определить совокупность всех возможных циклических (n, k)-кодов, исключая тривиальные (k=7 и k=0), которые можно построить в алгебре многочленов по модулю X^7-1.

Для поставленного вопроса имеют место соотношения (см. выражение (3.48а)): s=3, $\mu_1=\mu_2=\mu_3=1$, и, следовательно,

$$N_{ид}=2(2^{s-1}-1)=6.$$

В табл. 3.25 приведены шесть $(7, k)$-кодов, о которых идёт речь.

Таблица 3.25

Порождающий многочлен $g(X)$	Проверочный многочлен $h(X)=(X^7-1)/g(X)$	k	(n, k)
$(X-1)$	$(X^3+X+1)(X^3+X^2+1)$	6	(7, 6)
(X^3+X+1)	$(X-1)(X^3+X^2+1)$	4	(7, 4)
(X^3+X^2+1)	$(X-1)(X^3+X+1)$	4	(7, 4)
$(X-1)(X^3+X+1)$	(X^3+X^2+1)	3	(7, 3)
$(X-1)(X^3+X^2+1)$	(X^3+X+1)	3	(7, 3)
$(X^3+X+1)(X^3+X^2+1)$	$(X-1)$	1	(7, 1)

END

3.11. СПОСОБ ПОСТРОЕНИЯ ПОРОЖДАЮЩЕЙ И ПРОВЕРОЧНОЙ МАТРИЦ ПО КОРНЯМ ПОРОЖДАЮЩЕГО МНОГОЧЛЕНА

Циклический код может быть также задан другим способом, основанном на использовании корней многочлена $g(X)$ степени r, порождающего идеал в алгебре многочленов по модулю многочлена n-й степени X^n-1.

Предположим, что все корни $\alpha_1, \alpha_2, \ldots, \alpha_r$ многочлена $g(X)$, лежащие возможно в расширении поля, *различны*. Тогда циклический код полностью определяется условием: класс вычетов $\{f(X)\}$ принадлежит кодовому пространству в том и только в том случае, если $\alpha_1, \alpha_2, \ldots, \alpha_r$ являются также корнями многочлена $f(X)$ (теоремы 3.10, 3.16). Это означает, что если $m_i(X)$ – минимальная функция для α_i, то многочлен $f(X)$ должен делиться на $m_1(X), m_2(X), \ldots, m_r(X)$ и, следовательно, на наименьшее общее кратное (НОК) этих функций. Поэтому порождающий многочлен циклического кода, являющегося идеалом,

$$g(X)=\text{НОК}[m_1(X), m_2(X), \ldots, m_r(X)]. \qquad (3\text{-}54)$$

Так как бином X^n-1 должен делиться на $g(X)$, то элементы $\alpha_1, \alpha_2, \ldots, \alpha_r$ должны быть также корнями этого бинома и, следовательно, порядок бинома n должен делиться на порядок α_i, $i=1, 2, \ldots, r$. Поэтому n следует выбирать равным наименьшему общему кратному порядков элементов α_i, так как при этом каждый элемент α_i будет корнем X^n-1 [3.2, с.180, 235]. Если порождающим многочленом циклического (n, k)-кода – идеала в алгебре многочленов по модулю X^n-1, где n выбрано надлежащим образом, является *неприводимый* степени r многочлен $g(X)$ над полем $GF(2)$, то $g(X)=m_1(X)=m_2(X)=\ldots=m_r(X)$, и вместо (3-54) для выражения $g(X)$ через минимальные функции $m_i(X)$ следует взять только одну любую из них, так как в противном случае совокупности корней этих мини-

мальных функций будут совпадать. Например, можно сделать такой выбор: $g(X) = m_1(X)$.

ПРИМЕР 3.17. Код, рассмотренный в примере 3.15, может быть однозначно определён как код, корнями кодового многочлена которого является любые корни многочлена X^3+X+1 и, если α – примитивный элемент, определяемый многочленом X^3+X+1 (см. табл. 3.17), то эти корни определяются последовательностью степеней примитивного элемента: α^i, i=1, 2, 4; т.е. $\alpha_1 = \alpha$, $\alpha_2 = \alpha^2$, $\alpha_3 = \alpha^4$.

В этом случае $m_1(X)=m_2(X)=m_3(X)=X^3+X+1$ ($m_i(X)$ – минимальный многочлен для корня α_i) и, следовательно, порождающий многочлен определяемого циклического кода может быть задан, например, в форме: $g_1(X) = m_1(X)= X^3+X+1$.

END

ПРИМЕР 3.18. Код, корнями каждого кодового многочлена которого являются все корни α^i, i=1, 2, 4, многочлена $X^3+X+1= g_1(X)$ и все корни α^i, i=3, 5, 6, многочлена $X^3+X^2+1= g_2(X)$ (α – примитивный элемент поля $GF(2^3)$, определяемый многочленом X^3+X+1), может быть задан порождающим многочленом $g(X) = g_1(X)g_2(X)$ или в эквивалентной форме:

1 2 4 $\quad m_1(X)=m_2(X)=m_4(X) \quad (m = 3)$;

3 5 6 $\quad m_3(X)=m_5(X)=m_6(X) \quad (m = 3)$;

при этом имеется в виду обозначения: $\alpha_i = \alpha^i$, $i = 1, 2, \ldots, 6$.

Таким образом, например, можно положить: $g(X)=m_1(X)m_3(X)$ и степень $g(X)$ при этом равна $2m$ =6. Заметим, что в выражении $g(X)=m_1(X)m_3(X)$ выбраны, как это обычно делается, многочлены с *минимальными* индексами $m_i(X)$ из двух серий минимальных многочленов (см. пример 3.11).

END

Если известно, что элемент α_i должен быть корнем кратности r_i кодового многочлена $f(X)$, то в разложении многочлена $g(X)$ минимальный многочлен $m_i(X)$ должен повторяться r_i раз [3.2, с. 237].

Таким образом, согласно изложенному, многочлен $f(X)$ является кодовым многочленом в том и только в том случае, если элементы расширения α_i , i=1, 2, …, r являются его корнями. Следовательно, если

$$f(X) = f_{n-1}X^{n-1} + f_{n-2}X^{n-2} + \ldots + f_0, \qquad (3\text{-}55)$$

то при i =1, 2, …, r

$$f(\alpha_i)= f_{n-1}\alpha_i^{n-1} + f_{n-2}\alpha_i^{n-2} + \ldots + f_0=0. \qquad (3\text{-}56)$$

Это последнее выражение может быть записано в матричной форме:

$$[f_{n-1} + f_{n-2} + \ldots + f_0][\alpha_i^{n-1} + \alpha_i^{n-2} + \ldots + \alpha_i + \alpha_i^{0}]^{\mathrm{T}}=\mathbf{0}, \quad (3\text{-}57)$$

i =1, 2, …, r. В соответствии с теоремой 3.16 это условие обеспечивает также делимость многочлена $f(X)$ на минимальную функцию $m_i(X)$ для элемента α_i.

Условием того, что все элементы α_i, i=1, 2, …, r, – корни многочлена $f(X)$, является выполнение соотношения:

$$[f_{n-1} + f_{n-2} + \ldots + f_0]\cdot\begin{vmatrix} \alpha_1^{n-1} + \alpha_1^{n-2} + \ldots + \alpha_1 + \alpha_1^{0} \\ \alpha_2^{n-1} + \alpha_2^{n-2} + \ldots + \alpha_2 + \alpha_2^{0} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_r^{n-1} + \alpha_r^{n-2} + \ldots + \alpha_r + \alpha_r^{0} \end{vmatrix}^{\mathrm{T}} = \mathbf{0}. \quad (3\text{-}58)$$

Следовательно, в этом случае многочлен $f(X)$ принадлежит нулевому пространству проверочной матрицы циклического кода

$$\boldsymbol{H} = \begin{vmatrix} \alpha_1^{n-1} + \alpha_1^{n-2} + \ldots + \alpha_1 + \alpha_1^{0} \\ \alpha_2^{n-1} + \alpha_2^{n-2} + \ldots\ldots + \alpha_2 + \alpha_2^{0} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_r^{n-1} + \alpha_r^{n-2} + \ldots\ldots + \alpha_r + \alpha_r^{0} \end{vmatrix} \qquad (3\text{-}59)$$

и поэтому является кодовым многочленом.

3.12. ЧИСЛОВЫЕ ЦИКЛЫ И ИХ СООТВЕТСТВИЕ МИНИМАЛЬНЫМ МНОГОЧЛЕНАМ

Пусть l и p – взаимно простые *целые положительные числа*; пусть также $0 \le i < l$ и целые числа i, ip, …, ip^{r-1} попарно несравнимы по модулю l (т.е. среди остатков от деления этих чисел на l нет одинаковых), но $ip^j \equiv ip^r \pmod{l}$ при некотором $0 \le j \le r\text{-}1$, где r – степень минимального многочлена $m_\beta(X)$ для β [3.3, с. 103].

Так как $<<p, l>> = 1$, то, учитывая свойство сравнений целых чисел № 2 из примера 3.30, получим: $ip^{r-j} \equiv i \pmod{l}$. Следовательно, при сделанных выше предположениях $j = 0$.

Если теперь заменить числа i, ip, …, ip^{r-1} на остатки от деления их на l, то *полученная таким образом совокупность чисел называется* «(p, l)-(***числовым***) ***циклом***, ***содержащим*** i».

Количество чисел, входящих в цикл, называется *длиной цикла*. Длина r цикла, содержащего i, представляет собой минимальное целое положительное число, удовлетворяющее уравнению

$$ip^r \equiv i \pmod{l}. \qquad (3\text{-}60)$$

Пусть теперь основное поле $F_0 = GF(p)$ и $F = GF(p^m)$ – расширение основного поля. Разобьём числа от 0 до p^m-1 на (p, p^m-1)-**циклы**. Пусть i_1, i_2, …, i_r – числа, образующие цикл, содержащий i. Зафиксируем примитивный элемент α поля $GF(p^m)$ и рассмотрим минимальный многочлен $m_\beta(X) \in F_0[X]$ для элемента $\beta = \alpha^i$. Тогда, согласно теореме 3.24, корнями уравнения $m_\beta(X) = 0$ являются элементы $\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_r}$. Степень минимального многочлена равна длине цикла r.

Таким образом, установлено *соответствие между числовыми циклами и минимальными многочленами.*

Приведенный алгоритм построения числовых циклов позволяет определить минимальные многочлены для всех ненулевых элементов поля $GF(p^m)$ и, следовательно, позволяет строить порождающие многочлены циклических кодов, корнями которых являются определённые совокупности элементов $GF(p^m)$.

На практике при выписывании всех числовых циклов, определяющих все сомножители – неразложимые многочлены бинома X^n-1, являющиеся минимальными многочленами для определённых совокупностей элементов $GF(p^m)$, сначала выписывается числовой цикл, содержащий $i = 0$, состоящий из одного числа 0 и соответствующий сомножителю бинома $(X - 1)$.

Далее выписывается числовой цикл, содержащий число $i = 1$, соответствующий сомножителю бинома X^n-1 – неразложимому многочлену, определяющему примитивный элемент α расширения $F = GF(p^m)$.

При выписывании каждого следующего числового цикла (p, p^m - 1) сначала определяется целое положительное число i, принадлежащее этому циклу, как минимальное целое положительное число, не вошедшее в ранее выписанные числовые циклы, а затем по изложенной выше методике опре-

делятся и выписываются все целые числа, принадлежащие этому циклу, содержащему i.

Процесс продолжается до тех пор, пока не будут выписаны все числовые циклы, соответствующие всем сомножителям бинома X^n-1. После завершения этого процесса суммарное число всех чисел, принадлежащих всем выписанным циклам, должно быть равно степени бинома n.

ПРИМЕР 3.19. 1) Используя неприводимый многочлен $g(X) = X^4+X+1$, построить поле $GF(2^4)$ и определить корни $g(X)$ в этом поле.

2) При p=2 и m=4, разбив совокупность целых чисел от 0 до 2^4 - 2 на $(2, 2^4 - 1)$-циклы и выбрав в качестве примитивного элемента α элемент поля $GF(2^4)$, определяемый многочленом X^4+X+1, определить минимальные многочлены, соответствующие всем найденным циклам.

РЕШЕНИЕ. 1) Следуя методике, приведенной в примере 3.10, строим табл. 3.26, содержащую ненулевые элементы поля $GF(2^4)$. Элементы второго столбца таблицы при $i \geq 4$ следует находить методом Евклида – деления многочленов с остатком. При $i \geq 4$ многочлен вида α^i делится на многочлен $\alpha^4 + \alpha + 1$ и остаток заносится в соответствующую ячейку второго столбца таблицы. Для вычисления элементов четвёртого столбца таблицы вычисляется значение многочлена X^4+X+1 при $X=\alpha^i$, $i = 0, 1, 2, \ldots, 15$; при этом в случае необходимости применяется алгоритм деления многочленов Евклида.

Согласно данным, приведенным в четвёртом столбце табл. 3.26, корнями многочлена $g(X) = X^4+X+1$ в расширении $GF(2^4)$ являются: $\alpha, \alpha^2, \alpha^4, \alpha^8$ (цикл: 1 2 4 8).

2) Следуя приведенному выше способу построения числовых циклов, находим всевозможные числовые циклы и соответствующие им минимальные многочлены (табл. 27).

Элементы третьего столбца табл. 3.27 находятся на основании соотношений:

$$X-\alpha^0 = X - 1,$$

$$(X-\alpha^1)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8)=X^4+X+1,$$

$$(X-\alpha^3)(X-\alpha^6)(X-\alpha^{12})(X-\alpha^9)=X^4+X^3+X^2+X+1,$$

$$(X-\alpha^5)(X-\alpha^{10})=X^2+X+1,$$

$$(X-\alpha^7)(X-\alpha^{14})(X-\alpha^{13})(X-\alpha^{11})=X^4+X^3+1.$$

Таблица 3.26

Степенное представление	Многочленное представление	Векторное представление	$g(\alpha^i)$
α^0	1	(0001)	1
α	α	(0010)	0
α^2	α^2	(0100)	0
α^3	α^3	(1000)	$\alpha^2 + \alpha$
α^4	$\alpha + 1$	(0010)	0
α^5	$\alpha^2 + \alpha$	(0110)	1
α^6	$\alpha^3 + \alpha^2$	(1100)	$\alpha^2 + \alpha + 1$
α^7	$\alpha^3 + \alpha + 1$	(1011)	$\alpha^2 + \alpha + 1$
α^8	$\alpha^2 + 1$	(0101)	0
α^9	$\alpha^3 + \alpha$	(1010)	$\alpha^2 + \alpha + 1$
α^{10}	$\alpha^2 + \alpha + 1$	(0111)	1
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	(1110)	$\alpha^2 + \alpha$
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	(1111)	$\alpha^2 + \alpha$
α^{13}	$\alpha^3 + \alpha^2 + 1$	(1101)	$\alpha^2 + \alpha + 1$
α^{14}	$\alpha^3 + 1$	(1001)	$\alpha^2 + \alpha$
α^{15}	1	(0001)	1

Следовательно, мы доказали, что

$$\prod_{i=0}^{14}(X-\alpha^i) = (X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+X^2+$$

$$+X+1)(X^4+X^3+1) = X^{15}+1. \qquad (3\text{-}61)$$

(см. Приложение 5.2). Соотношения (3-39а) и (3-61) являются примерами того, что полю $GF(2^m)$ соответствует число $n=(2^m-1)$ – число ненулевых элементов и бином X^n-1, определяющий алгебру многочленов по модулю X^n-1 (см. Приложения 5.2, 5.4, 5.5).

Таблица 3.27

Числовые циклы	$\beta=\alpha^i$	$m_\beta(X)$
0	α^0	$X+1$
1 2 4 8	α^1	X^4+X+1
3 6 12 9	α^3	$X^4+X^3+X^2+X+1$
5 10	α^5	X^2+X+1
7 14 13 11	α^7	X^4+X^3+1

END

ПРИМЕР 3.20. С помощью Приложения 5.4 определим разложение бинома X^n+1 при $n=31$.

Используя коды многочленов – неприводимых сомножителей (третий столбец табл. 3.28), выпишем неприводимые сомножители – минимальные многочлены степени $m=5$ (четвёртый столбец табл. 3.28) для ненулевых элементов поля $GF(2^5)$ $\beta=\alpha^i$, $i=1, 3, 5, 7, 11, 15$ (второй столбец табл. 3.28):

Таблица 3.28

Степень бинома	Последовательности степеней корней неприводимых многочленов	Неприводимые сомножители	m
1	2	3	4
…	…	…	…
31	01 02 04 08 16	045	5
	03 06 12 24 17	075	5
	05 10 20 09 18	067	5
	07 14 28 25 19	057	5
	11 22 13 26 21	073	5
	15 30 29 27 23	051	5

$045 \Leftrightarrow 000100101 \Leftrightarrow X^5+X^2+1,$
$075 \Leftrightarrow 000111101 \Leftrightarrow X^5+X^4+X^3+X^2+1,$
$067 \Leftrightarrow 000110111 \Leftrightarrow X^5+X^4+X^2+X+1,$
$057 \Leftrightarrow 000101111 \Leftrightarrow X^5+X^3+X^2+X+1,$
$073 \Leftrightarrow 000111011 \Leftrightarrow X^5+X^4+X^3+X+1,$
$051 \Leftrightarrow 000101001 \Leftrightarrow X^5+X^3+1.$

Учитывая, что в бином $X^{31}+1$ по умолчанию входит неприводимый многочлен сомножитель $X+1$, найдём:

$$X^{31}+1=(X^5+X^2+1)(X^5+X^4+X^3+X^2+1)(X^5+X^4+X^2+X+1)(X^5+X^3+$$
$$+X^2+X+1)(X^5+X^4+X^3+X+1)(X^5+X^3+1)(X+1).$$

Отметим также, что $31=(2^5-1)$.

END