В. А. АРАКЕЛОВ, Г. М. ТЕНЕНГОЛЬЦ

НЕКОТОРЫЕ СВОЙСТВА РЕКУРРЕНТНЫХ ПЕРИОДИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Циклические коды, созданные на базе методов современной алгебры, обладая особой математической структурой, наиболее удобны для технической реализации. Процесс кодирования и декодирования таких кодов осуществляется с помощью регистров сдвига с обратной связью, соответствующей некоторому полиному, от свойств которого зависит корректирующая способность и некоторые другие параметры данного кода [1]. Поэтому исследование полиномов, представляющее достаточный самостоятельный интерес, становится важным и в современной теории кодирования. Кроме того, результаты подобных исследований могут быть успешно применены и в ряде других областей.

В статье изучаются свойства рекуррентных периодических последовательностей, получаемых с помощью генератора на регистре сдвига, обратная связь которого соответствует полиному $g(x) = x^n + x^m + 1$. Выводятся конечные формулы для определения периода некоторого класса полиномов над полем $GF(2)$. Устанавливаются взаимосвязи между корнями неприводимых полиномов $f(x)$ и $f(1+x)$, позволяющие строить ортогональные соотношения размера два.

§ 1. Пусть $g(x) = x^n + x^m + 1$ — произвольный полином с коэффициентами из поля $GF(2)$. Рассмотрим множество $\mathfrak{M}$-вычетов*) выражения x^N (целое $N \geqslant 0$) по модулю полинома $g(x)$. Легко видеть, что для всякого целого $N \geqslant 0$ имеет место следующее сравнение:

$$x^N \equiv \varphi_0(N) + \varphi_1(N)\,x + \cdots + \varphi_{n-1}(N)\,x^{n-1} \pmod{g(x)}, \qquad (1)$$

где коэффициенты $\varphi_i(N) \in GF(2)$. Полином обратной связи $g(x)$ определяет рекуррентное соотношение $x^{n+i} = x^{m+i} + x^i$, $(i = 0, 1, 2 \cdots)$, в силу которого, для всякого целого $k \geqslant 0$, имеет место равенство

$$x^{kn} = (1 + x^m)^k = \sum_{i=0}^{k} C_k^i\, x^{im}. \qquad (2)$$

Известно [2], что $C_k^i \equiv 1 \pmod 2$ тогда и только тогда, когда

$$\beta_{r-j} = \beta'_{r-j} + \beta''_{r-j} \quad (j = \overline{0,\ r}), \qquad (3)$$

где β_{r-j}, β'_{r-j}, β''_{r-j} — коэффициенты в двоичном представлении чисел k, i, $k-i$:

*) Здесь и далее имеется в виду наименьший неотрицательный вычет.

$$k = \sum_{j=0}^{r} \beta_{r-j} \cdot 2^{r-j}, \tag{4}$$

$$i = \sum_{j=0}^{r} \beta'_{r-j} \cdot 2^{r-j}, \qquad k - i = \sum_{j=0}^{r} \beta''_{r-j} \cdot 2^{r-j}.$$

Поэтому в разложении (2) будут присутствовать лишь те слагаемые x^{im}, для которых выполняется условие (3). Это позволяет по заданному k находить вычет по модулю полинома $g(x)$ элемента x^{kn}. Пусть среди всех коэффициентов β в (4) только $\beta_{s_1} \cdots \beta_{s_t}$ отличны от нуля. Тогда

$$k = \sum_{i=1}^{t} 2^{s_i} \tag{5}$$

и

$$x^{kn} = 1 + x^{2^{s_1} \cdot m} + x^{2^{s_2} \cdot m} + \cdots + x^{2^{s_t} \cdot m} + x^{(2^{s_1}+2^{s_2})m} +$$

$$+ x^{(2^{s_1}+2^{s_3})m} + \cdots + x^{(2^{s_t-1}+2^{s_t})m} + x^{(2^{s_1}+2^{s_2}+2^{s_3})m} + \cdots$$

$$\cdots + x^{(2^{s_t-2}+2^{s_t-1}+2^{s_t})m} +$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$+ x^{(2^{s_1}+2^{s_2}+\cdots+2^{s_t})m}. \tag{6}$$

Для произвольного элемента $x^N \in m$ имеем

$$x^N = x^{\left[\frac{N}{n}\right]n+\left(N-\left[\frac{N}{n}\right]\cdot n\right)} = x^{\left[\frac{N}{n}\right]\cdot n} \cdot x^{N-\left[\frac{N}{n}\right]\cdot n^*)}. \tag{7}$$

Поэтому, приняв $l = N - \left[\frac{N}{n}\right] \cdot n$, получим

$$x^N = x^{kn+l} = (1 + x^{2^{s_1} \cdot m} + \cdots + x^{2^{s_t} \cdot m} + x^{(2^{s_1}+2^{s_2})m} + \cdots$$

$$\cdots + x^{(2^{s_1}+2^{s_t})m} + \cdots + x^{(2^{s_1}+2^{s_2}+\cdots+2^{s_t})m}) x^l. \tag{8}$$

Поскольку $km + l$ может быть больше, чем $2n$, то для получения вычета по модулю $g(x)$ элемента $x^N \in m$ необходимо, вообще говоря, многократное применение формулы (8). При выполнении условия

$$\left[\frac{T}{n}\right] m < n^{**}) \tag{9}$$

это не так. Кроме того, нетрудно видеть, что в этом случае произвольный элемент из множества $\mathfrak{M}$ однозначно представим в виде

---

*) $[x]$ — наибольшее целое число, не превосходящее x.

**) T — период или показатель, которому принадлежит полином $g(x)$, т. е. наименьшее натуральное число, уловлетворяющее сравнению $x^T \equiv 1 \pmod{g(x)}$.

(8), а потому для такого класса полиномов по заданным коэффициентам τ разложения (1) можно определить величину N. Действительно, представление (8) позволяет определить для данного вычета по $\bmod g(x)$ числа l и $k = \left[\frac{N}{n}\right]$ и, следовательно, $N = kn + l$. Величина l определится из последовательного деления на x вычета до тех пор, пока последний не станет представим в виде (6). Следует учесть при этом, что $x^{-1} = x^{n-1} + x^{m-1}$. Число таких делений есть $l < n$, чем, собственно, и определяется число шагов, необходимых для восстановления выражения x^N по его вычету, взятому по $\bmod g(x)$.

Используя приведенный метод и учитывая, что

$$x^{T-1} = x^{n-1} + x^{m-1},$$

для любого полинома из рассматриваемого класса за $l\,(<n)$ шагов можно определить период T. В частности, если $\frac{T-1}{n} = k$, $m = 1$, можно получить формулу периода в конечном виде. Действительно, чтобы $x^{T-1} = 1 + x^{n-1}$ было представимо в виде (8), необходимо, чтобы $n - 1 = 2^p$ (целое $p \geqslant 0$) и тогда $T - 1 = (n-1) \cdot n$. Таким образом, период полинома $g(x) = x^{2^p+1} + x + 1$ равен

$$T = 2^p(2^p + 1) + 1. \qquad (10)$$

Поскольку бесконечный класс полиномов с периодом, удовлетворяющим равенству (10), является некоторым подмножеством множества полиномов вида $g(x) = x^n + x^m + 1$, для которых имеет место неравенство (9), то тем более будет бесконечным указанное множество полиномов. Иными словами, приведенный выше метод распространяется на бесконечный класс полиномов.

Примеры

Пусть $g(x) = x^4 + x + 1$. Определить:

а) вычет для элемента x^{20}:

$$x^{20} = x^{(2^2+2^4)4} = 1 + x^{2^2} + x^{2^4} + x^{(2^2+2^4)} = 1 + x + x^4 + x^5 = x + x^2$$

б) вычет для элемента x^{10}:

$$x^{10} = x^{(2^2+1)\cdot 4} \cdot x^2 = (1 + x^{2^4})\,x^2 = x^2 + x^4 = 1 + x + x^2$$

в) степень для элемента $x^\alpha = 1 + x + x^2 + x^3$:

$$x^\alpha = (1 + x^{2^0} + x^{2^1} + x^{(2^0+2^1)})\,x^0, \qquad \text{т. е.} \quad l = 0, \quad k = 2^0 + 2^1,$$

значит $\alpha = 12$.

г) период T

$$x^{T-1} = 1 + x^3, \qquad \text{не представимого в виде (7)}$$

$$x^{T-2} = 1 + x^2 + x^3, \quad \text{не представимого в виде (7)}$$

$$x^{T-3} = 1 + x + x^2 + x^3 = 1 + x^{2^0} + x + x^{(2^0+2^1)}, \text{ т. е.}$$

$$k = 2^0 + 2^1. \text{ Поэтому}$$

$$T - 3 = (2^0 + 2^1) \cdot 4 = 12. \qquad T = 15.$$

§ 2. Задача построения циклических последовательностей заданной длины математически формулируется как задача синтеза полиномов с заранее известным периодом. Поэтому исследование полиномов с этой точки зрения представляет немаловажный интерес.

Пусть функция $T(n_1, n_2, \cdots n_t)$ — показатель, которому принадлежит полином $h(x) = x^{n_1} + x^{n_2} + \cdots + x^{n_t} + 1$ с коэффициентами из поля $GF(2)$ ($n_l > nj$ — натуральные числа, $i > j$, $i, j = \overline{1, t}$). Докажем некоторые соотношения для указанной функции.

I. $T(2^k, 1) = 2^{2k} - 1.$ (11)

Действительно, в случае $h(x) = x^{2^k} + x + 1$ имеем

$$x^{2^k} = x + 1 \tag{12}$$

и, согласно тождеству Галуа,

$$x^{2^{2k}} = x^{2^k} + 1 = x. \tag{13}$$

Следовательно, период полинома T либо равен $2^{2k} - 1$, либо является собственным делителем этого числа.

Используя (12) и тождество Галуа, индукцией по m легко убедиться в справедливости равенства

$$x^{2^{k+l}+m\cdot 2^k+l} = x^l + x^{m+l} + \sum_{l=1}^{m-1} \alpha_l x^{l+l} + x^{2^l+l} + x^{2^l+m+l} +$$

$$+ \sum_{=1}^{m-1} \alpha_l x^{2^l+l+l}, \tag{14}$$

где m, l — натуральные числа $m < 2^l$, $l < 2^k$

$$\alpha_l \equiv S_1^{(l-1)} + S_2^{(l-1)} + \cdots + S_{m-l+1}^{(l-1)} \pmod 2,$$

$S_j^{(i)}$ — сумма i членов в выражении для α_j,

$$S_l^{(0)} = 1 \quad (i = \overline{1, m}).$$

Из (13) и (14) следует (11).

II. $$T\left(\frac{2^{tk}-1}{2^k-1}, \quad \frac{2^{(t-1)k}-1}{2^k-1}, \quad \cdots, 1\right) = 2^k\left(\frac{2^{tk}-1}{2^k-1}\right) + 1. \tag{15}$$

Имеет место следующее соотношение:

$$x^{n_1} = x^{n_2} + x^{n_3} + \cdots + x^{n_t} + 1. \tag{16}$$

Для всякого целого $N \geqslant 0$, следовательно, справедливо равенство

$$\begin{aligned}
x^N &= x^{N-n_1} + x^{N-n_1+n_2} + x^{N-n_1+n_3} + \cdots + x^{N-n_1+n_t} = \\
&= x^{N-2n_1} + x^{N-2n_1+n_2} + x^{N-2n_1+n_3} + \cdots + x^{N-2n_1+n_t} + \\
&+ x^{N-2n_1+n_2} + x^{N-2n_1+2n_2} + x^{N-2n_1+n_2+n_3} + \cdots + x^{N-2n_1+n_2+n_t} + \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&+ x^{N-2n_1+n_t} + x^{N-2n_1+n_2+n_t} + \cdots + x^{N-2n_1+2n_t} = \\
&= x^{N-2n_1} + x^{N-2n_1+2n_2} + \cdots + x^{N-2n_1+2n_t} = \\
&= \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots = \\
&= x^{N-2^k\cdot n_1} + x^{N-2^k\cdot n_1+2^k\cdot n_2} + \cdots + x^{N-2^k\cdot n_1+2^k\cdot n_t}.
\end{aligned} \tag{17}$$

Если $N = T$, то из (17) следует

$$x^T = x^{T-2^k\cdot n_1} + x^{T-2^k\cdot n_1+2^k\cdot n_t}. \tag{18}$$

С другой стороны, на основании (16) имеем, что

$$x^T = x^{n_1} + x^{n_2} + \cdots + x^{n_t}. \tag{19}$$

Так как $n_i > n_{i+1}\ (i = \overline{1, t})$ и

$$T - 2^k \cdot n_1 + 2^k \cdot n_t > T - 2^k \cdot n_1 + 2^k \cdot n_{t+1}$$

($i = \overline{2, t}$, $n_{t+1} = 0$), то, сравнивая (18) и (19), получим следующую систему равенств:

$$\begin{aligned}
x^{n_t} &= x^{T-2^k\cdot n_1} \\
x^{n_{t-1}} &= x^{T-2^k\cdot n_1+2^k\cdot n_t} \\
x^{n_{t-2}} &= x^{T-2^k\cdot n_2+2^k\cdot n_{t-1}} \\
&\cdots\cdots\cdots\cdots \\
x^{n_1} &= x^{T-2^k\cdot n_1+2^k\cdot n_2},
\end{aligned}$$

откуда следует, что

$$\begin{aligned}
T &= n_t + 2^k\cdot n_1 \\
T &= n_{t-1} + 2^k\cdot n_1 - 2^k\cdot n_t \\
T &= n_{t-2} + 2^k\cdot n_1 - 2^k n_{t-1} \\
&\cdots\cdots\cdots\cdots
\end{aligned} \tag{20}$$

$$T = n_1 + 2^k n_1 - 2^k \cdot n_2.$$

Из (20) имеем:

$$n_{t-1} = n_t\,(2^k + 1)$$

$$n_{t-2} = n_t + 2^k \cdot n_{t-1} = n_t(2^{2k} + 2^k + 1) = n_t \cdot \frac{2^{3k} - 1}{2^k - 1}$$

. . . . . .

$$n_{t-i} = n_t + 2^k \cdot n_{t-i+1} = n_t(2^{ik} + 2^{(i-1)k} + \cdots + 1) =$$

$$= n_t \cdot \frac{2^{(i+1)k} - 1}{2^k - 1}, \quad (i = \overline{1, t-1}) \tag{21}$$

. . . . . .

$$n_1 = n_t + 2^k \cdot n_2 = n_t \cdot \frac{2^{tk} - 1}{2^k - 1}.$$

Период

$$T\left(n_t \cdot \frac{2^{tk} - 1}{2^k - 1},\ n_t \cdot \frac{2^{(t-1)k} - 1}{2^k - 1},\ \cdots 1\right) = n_t\left(2^k \cdot \frac{2^{tk} - 1}{2^k - 1} + 1\right), \tag{22}$$

откуда и следует (15).

Подобные формулы могут быть полезны при исследовании полиномов. В частности (11) позволяет утверждать, что полиномы вида $g(x) = x^{2^k} + x + 1$ при $k > 2$ не могут быть примитивными. Аналогичное заключение, при некоторых ограничениях, можно сделать и для полиномов с периодом, удовлетворяющим равенству (15).

§ 3. В настоящем параграфе предлагается метод построения ортогональных соотношений размера два для класса кодов, проверочный полином которых $h(x)$ неприводим в поле $GF(2)$.

Рассмотрим сначала случай, когда полином $h(x)$ — примитивный. Пусть k — степень $h(x)$, α — его корень и пусть $f(x)$ — минимальная функция для $\beta = \alpha^l \in GF(2^k)$*). Множество всех корней $f(x)$ обозначим через

$$B = \{\beta, \beta^2, \cdots, \beta^{2^{k-1}}\}.$$

Полином $f(1 + x) = f^*(x)$ является минимальной функцией для некоторого элемента $\gamma = \alpha^l$ поля $GF\ (2^k)$**). Множество всех корней $f^*(x)$ обозначим через

$$\Gamma = \{\gamma, \gamma^2, \cdots, \gamma^{2^{k-1}}\}. \tag{23}$$

Имеет место следующая

---

*) При определении минимальной функции $f(x)$ степени $k \leqslant 16$ по соответствующему элементу $\alpha^l \in GF(2^k)$ можно использовать таблицу Питерсона [1].

**) Если $f(x)$ — неприводим, то $f(1 + x)$ также неприводим.

Теорема. Множества всех корней полиномов $f(x)$ и $f^*(x)$ ортогональны, т. е. для всякого $\beta^i \in B$ существует единственный элемент $\gamma^j \in \Gamma (i, j = \overline{2^s, s = 0, k-1})$ такой, что

$$\beta^i + \gamma^j = 1. \tag{24}$$

Доказательство. Известно [3], что для любого $\alpha^i \in GF(2^k)$ существует единственный элемент $\alpha^j \in GF(2^k)$, что $\alpha^i + \alpha^j = 1$. Имеем $f(\alpha^i) = f(\alpha^j + 1)$, где $f(x)$ — произвольный полином с коэффициентами из поля $GF(2)$. Если $f(x)$ — минимальная функция для α^i, т. е. $f(\alpha^i) = 0$, то $f(\alpha^j + 1) = 0$ и, следовательно, α^j является корнем функции $f^*(x) = f(1 + x)$. Откуда, принимая во внимание тождество Галуа, и следует утверждение теоремы.

Пары элементов, удовлетворяющие (24), определяются следующим образом. Элемент $\beta^{-i} = \beta^{2^k - i - 1}$ есть корень некоторой минимальной функции $g(x)$. Множество всех корней $g(1 + x) = g^*(x)$, ортогональное множеству всех корней $g(x)$, обозначим через

$$C = \{c, c^2, \cdots, c^{2^{k-1}}\}.$$

Умножим все элементы C на $\beta^i \in B$, т. е. $C^1 = \{\beta^i \cdot c, \cdots, \beta^i c^{2^{k-1}}\}$. Если в множестве $\Gamma \cap C^1$ окажется единственный элемент, то это и будет тот самый γ^j, который удовлетворяет (24). В противном случае для произвольной пары элементов $\beta^i \in B$ и $\gamma^j \in \Gamma$ достаточно определить вычеты по модулю полинома $h(x)$ (для i, j больших можно использовать метод, приведенный в работе [2]). Если окажется, что $\beta^i + \gamma^j \neq 1$, то последовательным возведением в квадрат вычета элемента γ^j найдем такой $\gamma^{j \cdot 2^s} (s = \overline{1, k-1})$, что

$$\beta^i + \gamma^{j \cdot 2^s} = 1. \tag{25}$$

В силу тождеств Галуа, остальные $k - 1$ ортогональные пары элементов множеств B и Γ получим из (25):

$$\beta^{i \cdot 2^p} + \gamma^{j \cdot 2^{s+p}} = 1 \qquad (p = \overline{1, k-1}). \tag{26}$$

Кроме того, из (24) следует, что

$$\gamma^{-j} + \beta_n^i \gamma^{-j} = 1,$$

$$\beta^{-i} + \gamma^j \cdot \beta^{-i} = 1.$$

Поэтому любая ортогональная проверка размера два задает $t \leqslant 3k$ различных ортогональных пар, удовлетворяющих равенству (24). Используя приведенные рассуждения и результат теоремы, можно построить все ортогональные проверки. В случае, когда полином $h(x)$ — — неприводимый, корень которого $\beta = \alpha_x^i$ (α — примитивный элемент поля), из всех ортогональных пар множеств для соответствующего примитивного полинома выбираются лишь те, элементы которых имеют вид α^{it} ($t = \overline{0, n-1}$, n — показатель, которому принадлежит непри-

водимый полином $h(x)$). Полученные проверки затем тривиальным образом выражаются через β. Интересно отметить, что ортогональные пары множеств для всех неприводимых полиномов заданной степени достаточно строить один раз.

Предлагаемый метод требует по заданному $f(x)$ построения $f(1+x)$. Пусть $f(x) = x^{n_1} + x^{n_2} + \cdots + x^{n_t} + 1$ — произвольный полином над полем $CF(2)$. Тогда $f(1+x) = \sum_{i=0}^{t} (1+x)^{n_i} + 1$. Формула (6) позволяет по двоичному представлению числа n_i найти полином $f_i(x) = (1+x)^{n_i}$ $(i = \overline{0, t})$. Сложив по модулю 2 всевозможные $f_i(x)$, получим полином

$$f(1+x) = \sum_{i=0}^{t} f_i(x) + 1.$$

Примеры

1. Пусть требуется построить всевозможные ортогональные проверки размера два для кода с проверочным полиномом $h(x) = x^6 + x + 1$, корнем которого является примитивный элемент α поля $GF(2^6)$. Все корни $h(x)$:

$$\alpha,\ \alpha^2,\ \alpha^4\ \alpha^8,\ \alpha^{16},\ \alpha^{32}.$$

Все корни $h(1+x) = x^6 + x^4 + x^2 + x + 1$:

$$\alpha^3,\ \alpha^6,\ \alpha^{12},\ \alpha^{24},\ \alpha^{48},\ \alpha^{33}.$$

На основании теоремы, множества корней $h(x)$ и $h(1+x)$ ортогональны. Составим для элементов этих множеств всевозможные $k = 6$ проверок, для чего, как было указано, достаточно найти одну. В данном случае указанная проверка находится из полинома

$$h(\alpha) = \alpha^6 + \alpha + 1 = 0,$$

откуда

$$\alpha^6 + \alpha = 1. \qquad \text{(I)}$$

Остальные проверки получаются последовательным возведением в квадрат соотношения (I):

$$\begin{array}{cccccc} \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^{32} \\ + & + & + & + & + & + \\ \alpha^6 & \alpha^{12} & \alpha^{24} & \alpha^{48} & \alpha^{33} & \alpha^3 \\ \hline & & & = 1 & & \end{array}$$

Из (I) следует, что

$$\alpha^3 + \alpha^{62} = 1, \quad \alpha^{57} + \alpha^{58} = 1,$$

следовательно, мы получим еще 12 проверок:

$$\begin{array}{cccccc} \alpha^{5} & \alpha^{10} & \alpha^{20} & \alpha^{40} & \alpha^{17} & \alpha^{34} \\ + & + & + & + & + & + \\ \alpha^{62} & \alpha^{61} & \alpha^{59} & \alpha^{55} & \alpha^{47} & \alpha^{31} \\ \hline & & & =1 & & \end{array} \qquad \begin{array}{cccccc} \alpha^{37} & \alpha^{11} & \alpha^{22} & \alpha^{44} & \alpha^{25} & \alpha^{50} \\ + & + & + & + & + & + \\ \alpha^{39} & \alpha^{13} & \alpha^{26} & \alpha^{52} & \alpha^{41} & \alpha^{19} \\ \hline & & & =1 & & \end{array}$$

Далее, элемент α^7 не вошел в указанные проверки, а элементы (В) α^7, α^{14}, α^{28}, α^{56}, α^{49} α^{35} — есть корни минимальной функции $g(x) = x^6 + x^5 + x^3 + 1$. Всеми корнями полинома $g(1+x) = x^6 + x^4 + x^3 + x + 1$ будут элементы

(Г) α^{13}, α^{26}, α^{52}, α^{41}, α^{19}, α^{38}.

На основании теоремы:

$$\alpha^7 + \alpha^r = 1, \quad \alpha^r \in \Gamma,$$

откуда следует, что $\alpha^{-7} + \alpha^{r-7} = 1$.

Множество C, ортогональное множеству $\{\alpha^{-7} = \alpha^{56}\}$, совпадает с Г. Тогда $C^1 = \alpha^7\{\alpha^{13}, \alpha^{26}, \alpha^{52}, \alpha^{41}, \alpha^{19}, \alpha^{38}\}$. Так как $\Gamma \cap C^1 = \alpha^{26}$ состоит из одного элемента, то $\alpha^r = \alpha^{26}$ и, следовательно, $\alpha^7 + \alpha^{26} = 1$, а все проверки для элементов ортогональных множеств В и Г будут иметь вид:

$$\begin{array}{cccccc} \alpha^{7} & \alpha^{14} & \alpha^{28} & \alpha^{56} & \alpha^{49} & \alpha^{35} \\ + & + & + & + & + & + \\ \alpha^{26} & \alpha^{52} & \alpha^{41} & \alpha^{19} & \alpha^{38} & \alpha^{13} \\ \hline & & & =1 & & \end{array}$$

Элемент α^9 является корнем неприводимого полинома $g(x) = x^3 + x^2 + 1$. Полином $g(1+x) = x^3 + x + 1$ [в данном случае $g(1+x) = x^3 \cdot g\left(\frac{1}{x}\right)$] имеет своими корнями

α^{54}, α^{45}, α^{27}.

Из $g(\alpha^9) = 0$ следует, что $\alpha^{18} + \alpha^{27} = 1$, т. е.

$$\begin{array}{ccc} \alpha^{18} & \alpha^{36} & \alpha^{9} \\ + & + & + \\ \alpha^{27} & \alpha^{54} & \alpha^{45} \\ \hline & =1 & \end{array}$$

Наконец, элемент α^{11} имеет минимальную функцию $g(x) = x^6 + x^5 + x^3 + x^2 + 1$. Полином $g(1+x) = g(x)$. Поэтому ортогональная пара множеств будет составлена из элементов одного и того же множества корней полинома $g(x)$:

(В) α^{11} α^{22} α^{44} (Г) α^{25} α^{50} α^{37}

$\alpha^{11} + \alpha^r = 1$ $\alpha^r \in \Gamma$

$\alpha^{-11} + \alpha^{r-11} = 1$

Множество С, ортогональное множеству корней $\{\alpha^{-11} = \alpha^{52}\}$, состоит из следующих элементов:

$$C = \{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}\}.$$

Пересечение $\alpha^{11} \times C \cap \Gamma$ содержит единственный элемент $\alpha^{25} = \alpha^x$, удовлетворяющий равенству $\alpha^{11} + \alpha^{25} = 1$. Следовательно,

$$\begin{array}{r} \alpha^{11} \quad \alpha^{22} \quad \alpha^{44} \\ + \quad + \quad + \\ \alpha^{25} \quad \alpha^{50} \quad \alpha^{37} \\ \hline = 1 \end{array}$$

Элемент α^{21} имеет минимальную функцию $g(x) = x^2 + x + 1$, и так как $g(1 + x) = g(x)$, то $\alpha^{21} + \alpha^{42} = 1$.

Таким образом, мы построили все нетривиальные проверки, которые фактически можно задать следующими ортогональными парами:

$$\alpha + \alpha^6 = 1, \quad \alpha^7 + \alpha^{26} = 1,$$

$$\alpha^9 + \alpha^{45} = 1, \quad \alpha^{11} + \alpha^{25} = 1,$$

$$\alpha^{21} + \alpha^{42} = 1.$$

2. Пусть дан проверочный полином кода $h_1(x) = x^6 + x^4 + x^2 + x + 1$, который неприводим и имеет корнем $\beta = \alpha^3$, где α—примитивный элемент поля $GF(2^6)$. Из всех ортогональных пар множеств, для примитивного полинома $h(x)$, мы должны выбрать лишь те, элементы которых представимы в виде α^{3i}:

$$\begin{array}{r} \alpha^{9} \quad \alpha^{18} \quad \alpha^{36} \\ + \quad + \quad + \\ \alpha^{45} \quad \alpha^{27} \quad \alpha^{57} \\ \hline = 1 \end{array} \qquad \alpha^{21} + \alpha^{42} = 1.$$

Так как $\alpha^3 = \beta$, то искомыми проверками будут:

$$\beta^3 + \beta^{15} = 1, \quad \beta^6 + \beta^9 = 1,$$

$$\beta^{12} + \beta^{19} = 1, \quad \beta^7 + \beta^{14} = 1.$$

Վ. Ա. ԱՌԱՔԵԼՈՎ, Գ. Մ. ՏԵՆՆԵՀՈԼՑ

ՌԵԿՈՒՐԵՆՏ ՊԱՐԲԵՐԱԿԱՆ ՀԱՋՈՐԴԱԿԱՆՈՒԹՅՈՒՆՆԵՐԻ ՄԻ ՔԱՆԻ ՀԱՏԿՈՒԹՅՈՒՆՆԵՐ

Ա մ փ ո փ ո ւ մ

Հոդվածում ուսումնասիրվում են ռեկուրենտ պարբերական հաջորդականությունների հատկությունները՝ ստացված տեղաշարժի ռեգիստորի վրա գեներատորի օգնությամբ, որի հակադարձ կապը համապատասխանում է $h(x) = x^n + x^m + 1$ բազմանդամին, $GF(r)$ դաշտից վերցրած գործակիցներով։

Դուրս են բերվում վերջավոր բանաձևեր՝ բազմանդամների որոշ դասի պարբերությունը սահմանման համար։ Սահմանվում են փոխադարձ կապեր $f(x)$ և $f(1 + x)$ չբերվող բազմանդամների արմատների միջև, որոնք թույլատրում են կառուցել երկու չափի օրթոգոնալ առնչություններ։

ЛИТЕРАТУРА

1. *У. Питерсон.* Коды, исправляющие ошибки. М., Изд-во „Мир", 1964.
2. *В. А. Аркелов.* Об одном методе исследования периодических рекуррентных последовательностей. Труды Третьей конференции по теории передачи и кодирования информации. Ташкент, Изд-во „ФАН" УзССР, 1967.
3. *Дж. Месси.* Пороговое декодирование. М., Изд-во „Мир", 1965.