# ИСПОЛЬЗОВАНИЕ КВАЗИПРОИЗВОДНЫХ ПРИ ПОСТРОЕНИИ ПРОВЕРОЧНОЙ МАТРИЦЫ ПОЛИНОМИАЛЬНОГО КОДА

**В. М. Ширяев**

*Белорусский государственный университет*
*Минск*, *Беларусь*
Shyryae@dsu.by

Предлагается один из способов построения проверочной матрицы полиномиального кода в случае наличия кратных корней у порождающего многочлена.

*Ключевые слова*: полиномиальный код, порождающий многочлен, поле разложения, ряд квазипроизводных, проверочная матрица.

Пусть $p$ – простое число, $l$ – некоторая его степень, $\mathrm{F}_l$ – конечное поле порядка $l$. Зафиксируем натуральные числа $m$, $n \in \mathbb{N}$, такие, что $m < n$, $g(x) = g_0 + g_1 x + \ldots + g_{n-m} x^{n-m} \in \mathrm{F}_l[x]$ – многочлен степени $n - m$, делящий $x^n - 1$. Как известно, [1], [2], [3], линейный $(n, m)$-код $(E, D)$ над полем $\mathrm{F}_l$ является полиномиальным и порождается многочленом $g(x)$, если кодирующая матрица имеет вид

$$A_{g(x)} = \begin{bmatrix} g_0 & g_1 & \ldots & g_{n-m} & 0 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{n-m-1} & g_{n-m} & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & 0 & g_0 & g_1 & \ldots & g_{n-m} \end{bmatrix} \in (\mathrm{F}_l)_{m,\, n}.$$

Для случая, когда многочлен $g(x)$ имеет кратные корни, предлагается один из способов построения проверочной матрицы $B_{g(x)} \in (\mathrm{F}_l)_{n,\, m\, -\, n}$ с использованием квазипроизводных.

Обозначим через $\mathrm{K}_n$ поле разложения (круговое поле) многочлена $x^n - 1$ над полем $\mathrm{F}_l$, множество всех корней этого многочлена обозначаем через $W_n$. Представим число $n$ в виде $n = p^d c$, где $d \in \{0, 1, \ldots\}$, $c$ – натуральное число, не делящееся на $p$, т. е. $p^d$ – элементарный делитель числа $n$). Положим $k_c = \min\{ b \in \mathbb{N} \mid l^b \equiv 1 \pmod{c}\}$. В этих обозначениях имеет место (§ 4 гл. 2 [3]).

**Лемма 1.** Тогда а) если $d = 0$, т. е. $n$ не делится на $p$, то множество $W_n$ является циклической подгруппой порядка $n$ мультипликативной группы поля $K_n$, а само поле $K_n$ имеет $l^{h_n}$ элементов, б) Если $d > 0$, то $K_n = K_c$, $W_n = W_c$ и корнями многочлена $x^n - 1$ являются $c$ элементов множества $W_c$, каждый из которых имеет кратность $p^d$.■

Пусть $f(x) = \sum_{i=0}^{n-1} a_i x^i$ – разложение многочлена $f(x) \in F_l[x]$ по степеням $x$. Определим многочлены $f^{[0]}(x), f^{[1]}(x), \ldots, f^{[n-1]}(x) \in F_l[x]$ по правилу: $f^{[0]}(x) = f(x)$,

$$f^{[j]}(x) = \sum_{i=j}^{n-1} C_i^j a_i x^{i-j} \qquad (1)$$

при $j \in \{1, \ldots, n-1\}$. В частности, $f^{[1]}(x) = \sum_{i=1}^{n-1} C_i^1 a_i x^{i-1}$ – производная многочлена $f(x)$ и $f^{[n-1]}(x) = a_{n-1}$. Полученная последовательность называется последовательностью квазипроизводных для многочлена $f(x)$.

**Лемма 2.** Пусть $h(x) \in F_l[x]$ – допустимый многочлен (т. е. с ненулевым свободным членом) степени больше нуля и меньше $n$ и $\beta$ – его корень в некотором расширении $F$ поля $F_l$. Число $b \in \{1, \ldots, n-1\}$ в том и только в том случае является кратностью корня $\beta$, когда $(h^{[0]}(\beta) = h^{[1]}(\beta) = \ldots = h^{[b-1]}(\beta) = 0) \& (h^{[b]}(\beta) \neq 0)$.

**Доказательство.** Нетрудно проверить, что при последовательном делении с остатком многочлена $h(x)$ на $x - \beta$ и получающихся частных над полем $F_l$ с применением схемы Горнера получим разложение $h(x)$ по степеням $x - \beta$, причем коэффициентами будут как раз значения квазипроизводных при $x = \beta$: $h(x) = h^{[0]}(\beta) + a^{[1]}(\beta)(x - \beta) + h^{[2]}(\beta)(x - \beta)^2 + \ldots + h^{[n-1]}(\beta)(x - \beta)^{n-1}$, откуда будет следовать утверждение.■

**Лемма 3.** Пусть $b \in \mathbb{N}_2 = \{2, 3, \ldots\}$, $g(x) = f(x)^b \in F_l[x]$, где $f(x)$ – допустимый неприводимый многочлен степени $r \in \mathbb{N}_2$ над полем $F_l$. Зафиксируем некоторый корень $\beta$ многочлена $f(x)$ в его поле разложения $F_{l^r}$. Многочлен $h(x) \in F_l[x]$ делится на $g(x)$ в том и только в том случае, когда

$$\forall j \in \{1, \ldots, b\} \; (h^{[j-1]}(\beta) = 0)). \qquad (2)$$

**Доказательство.** Согласно следствию 2.15 гл. 2 [4] для неприводимого многочлена $f(x)$ степени $r$ именно поле $F_{l^r}$ является его полем разложения, а с применением леммы 2.12 *ibid.* получаем, что делимость многочлена $h(x)$ на $f(x)$ равносильна тому, что $h(x)$ аннулирует какой-нибудь корень $\beta$ многочлена $f(x)$ и по следствию из теоремы Безу равносильна делимости $h(x)$ на $x - \beta$. Теперь по свойству взаимно простых многочленов делимость $h(x)$ на $g(x)$ равносильна его делимости на $(x - \beta)^b$, т. е. тому, что кратность корня $\beta$ не должна быть меньше, чем $b$. Остается применить лемму 2. ■

В результате получаем

**Следствие 1.** В обозначениях леммы 1 пусть имеется каноническое разложение многочлена $g(x) \in F_l[x]$ степени $n - m$ над полем $F_l$: $g(x) = \prod_{i=1}^{t} f_i(x)^{b_i}$, где $t, b_1, b_2, \ldots, b_t \in \{1, \ldots, n-1\}$. Далее, предположим, что для каждого индекса $i \in \{1, \ldots, t\}$ выбора но по одному корню $\beta_i \in K_c$ многочлена $f_i(x)$. Тогда многочлен $h(x) \in F_l[x]$ сте-

пени меньше $n$ является кодовым в том и только в том случае, когда для индекса $i \in \{1,...,t\} \downarrow t$, каждого показателя $b_i$ и каждого выбранного корня $\beta_i$ многочлена $f_i(x)$ выполняется соотношение (2). ■

В обозначениях последних двух утверждений построение проверочной матрицы для полиномального $(n, m)$-кода $(E, D)$ с порождающим многочленом $g(x)$ можно осуществить следующим образом. Поле $K_c$ рассматривается как векторное пространство (размерности $k_c$) над полем $F_l$ и фиксируется некоторый его базис. Для каждого $i \in \{1,...,t\}$ вычисляются координаты элементов $\beta_i$ как векторов в этом базисе и степеней этих элементов начиная с нулевой (это 1) и заканчивая $(n - 1)$-й. При этом $j$-я строка строящейся матрицы $B$ будет соответствовать коэффициенту при $(j - 1)$-й степени $x$ многочлена $h(x)$. Вычисленными строчками координат заполняется полоса из $k_c$ столбцов строящейся матрицы $B = B_{g(x)}$. Если $b_i > 1$, то следующая полоса из $k_c$ столбцов заполняется строчками из координат степеней элемента $\beta_i$ и их кратных в соответствии с распределением коэффициентов у многочлена $h^{[1]}(x)$ (которые зависят от коэффициентов исходного многочлена $h(x)$). Если $b_i > 2$, то следующая полоса из $k_c$ столбцов заполняется строчками из координат степеней элемента $\beta_i$ в соответствии с выражением коэффициентов многочлена $h^{[1]}(x)$ через коэффициенты исходного многочлена $h(x)$ как переменных (т. е. подставляя в $h^{[1]}(x)$ $\beta_i$ вместо $x$ и выражая степени $\beta_i$ через базис с помощью коэффициентов из поля $F_l$), и заполняем этими коэффициентами соответствующую полосу из $k_c$ столбцов с учетом биекции между строками и коэффициентами многочлена $h(x)$) и т. д. Построение полосы, соответствующей индексу $i \in \{1,...,t\}$, заканчивается на многочлене $h^{[b-1]}(x)$. Матрица $B$ состоит из построенных полос для каждого индекса $i \in \{1,...,t\}$. Если теперь строку коэффициентов многочлена $h(x)$ умножить на полученную матрицу $B$, то получим нулевую строку, поэтому $h(x)$ будет кодовым многочленом. Обратно, если для строки $a \in (F_l)_{1,n}$ строка $aB$ будет нулевой, то соответствующий многочлен $h(x)$ должен быть кодовым. В результате должна получиться проверочная матрица $B_{g(x)}$ для $(n, m)$-кода $(E, D)$. Такую проверочную матрицу считаем полученной при помощи некоторого множества корней $c$-ой степени из 1.

**Пример 1.** Рассмотрим пример построения такой матрицы при $l = 2$, $n = 12$, $g(x) = 1 + x + x^2 + x^6 + x^7 + x^7$. Здесь $x^{12} - 1 = (1 + x)^4(1 + x + x^2)^4$, поэтому $K_{12} = F_4$. Пусть $\alpha$ – первообразный элемент этого поля и $\alpha^3 = 1$, $\alpha^2 = 1 +$ . Элементы 1, $\alpha$ можно взять в качестве базиса поля $F_4$. Далее $g(x) = (1 + x)^2(1 + x + x^2)^3$, поэтому $\Theta_{g(x)}(2, 4) = \{ 1, \alpha, \alpha^2 \}$ – множество корней многочлена $g(x)$. Значит, в качестве корня $\beta$ в изложенном алгоритме построения матрицы $B$ можно последовательно использовать корни 1 и $\alpha$. Пусть сначала $\beta = 1$. Так как его кратность равна 2, то для построения первых двух столбцов привлекаем многочлены $h^{[0]}(x) = \sum_{i=0}^{11} a_i x^i$, $h^{[1]}(x) = \sum_{i=0}^{5} a_{2i+1} x^{2i}$. Каждому коэффициенту $a_i$ в матрице $B$ соответствует $(i + 1)$-я строка. Поэтому, следуя соотношениям (1), надо подставить 1 вместо $x$ и заполнить первый и второй столбец коэффициентами при соответствующих $a_i$ уже как переменных. В результате первый столбец будет состоять из 1, а второй будет состоять из нулей на нечетных и единиц на четных местах. Теперь пусть $\beta = \alpha$. Так как

кратность корня α равна 3, то, кроме выписанных, еще надо привлечь многочлен $a^{[2]}(x) = a_2 + a_3x + a_6x^4 + a_7x^5 + a_{10}x^8 + a_{11}x^9$. Теперь надо в эти три квазипроизводные вместо $x$ подставить α и степени α выразить через базис и записать как вектор в арифметическом двумерном пространстве. В результате из $h^{[0]}(\alpha)$ выводится в этом пространстве выражение $\sum_{i=0}^{3} a_{3i}(1,0) + a_{3i+1}(0,1) + a_{3i+2}(1,1)$ и ему соответствует заполнение третьего и четвертого столбцов, из $h^{[1]}(\alpha)$ и $h^{[2]}(\alpha)$ выводятся в этом пространстве выражения $\sum_{i=0}^{1} a_{6i+1}(1,0) + a_{6i+3}(0,1) + a_{6i+5}(1,1)$ и $a_2(0, 1) + a_3(1, 0) + a_6(1, 0)+ +a_7(1, 1) + a_{10}(1, 1) + a_{11}(0, 1)$. В соответствии с этим заполняются последние четыре столбца. В результате получим матрицу

$$B = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

## ЛИТЕРАТУРА


1. *Биркгоф*, *Г.* Современная прикладная алгебра / Г. Биркгоф, Т. Барти. М.: Мир, 1976. 400 с.

2. *Блейхут*, *Р.* Теория и практика кодов, контролирующих ошибки / Р. Блейхут.М.: Мир, 1986. 576 с.

3. *Lidl*, *R.* Applied Abstract Algebra / R. Lidl, G. Pilz. Berlin, Heidelberg, New-York: Springer-Verlag, 1989. 545 p.

4. *Лидл, Л.* Конечные поля / Л. Лидл, Г. Нидеррайтер. М.: Мир, 1988. Т. 1. 428 с.