УДК 519.725

А. С. Барашко, канд. физ.-мат. наук
(Ин-т прикл. математики и механики АН Украины, Донецк)

ПОЛИНОМЫ, ПОРОЖДАЮЩИЕ КОДЫ ХЭММИНГА

A class of polynomials generating base q Hemming codes (PGHC class) is studied. Criteria for a polynomial to belong to the PGHC class are found in the general case and in the case when the polynomial is prime. Conditions under which reducible polynomials do not belong to the PGHC class are determined.

Досліджено клас поліномів, які породжують q-кові коди Хемінга (клас ППКХ). Знайдені критерії належності полінома до класу ППКХ у загальному випадку та у випадку, коли поліном є простий. Визначені умови, за яких звідні поліноми не наліжать до класу ППКХ.

Настоящая статья посвящена разделу алгебраической теории кодирования, изучающему коды Хэмминга. Известно, что двоичные коды Хэмминга порождаются примитивными полиномами и только ими. Класс полиномов, порождающих примитивные полиномы Хэмминга, в литературе не описан. Рассматриваемая задача связана с исследованием этого класса. Неопределяемые понятия заимствованы из монографий [1, 2].

Между последовательностями элементов поля и полиномами над этим полем существует взаимно однозначное соответствие с точностью до последовательностей нулей в начале последовательностей. Поэтому q-ичный код, порожденный полиномом, можно задать двумя способами: как множество полиномов, которые делятся на порождающий полином, и как нулевое пространство проверочной матрицы, определяемой порождающим полиномом. Зафиксируем $q \geq 2$, являющееся целой степенью некоторого простого числа, и через $\mathfrak{M}$ обозначим множество полиномов переменной x с коэффициентами в поле Галуа $GF(q)$. Пусть $g(x) = x^r + g_{r-1}x^{r-1} + \ldots + g_1 x + g_0$ — полином степени $\deg g(x) = r \geq 2$ и n — целое число, превышающее r. Тогда $(n, n-r)$-код $C_{g(x)}(n)$, порожденный полиномом $g(x)$, можно определить выражением $C_{g(x)}(n) = \{c(x) \in \mathfrak{M} \mid g(x) \mid c(x) \,\&\, \deg c(x) \leq n-1\}$, в котором $g(x) \mid c(x)$ означает деление полинома $c(x)$ на $g(x)$ в поле $GF(q)$ без остатка. Символом β обозначим вектор-столбец размерности r, у которого первая компонента равна 1, а остальные являются нулями. Положим

$$M_{g(x)} = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -g_0 \\ 1 & 0 & 0 & \ldots & 0 & -g_1 \\ 0 & 1 & 0 & \ldots & 0 & -g_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & -g_{r-1} \end{bmatrix}$$

и отметим, что $|M_{g(x)} - xI| \approx g(x)$, где I — единичная матрица порядка r и $\approx$ означает равенство с точностью до мультипликативной константы, не равной нулю. Проверочная матрица кода $C_{g(x)}(n)$ определяется равенством

$$H_{g(x)}(n) = [M_{g(x)}^{n-1}\beta,\ M_{g(x)}^{n-2}\beta, \ldots, M_{g(x)}\beta, \beta].$$

Столбцы матрицы $H_{g(x)}(n)$ можно представить полиномами над $GF(q)$, степень которых не превышает $r-1$. Обозначим через $'$ операцию транспонирования. Тогда если $s = (s_0, s_1, \ldots, s_{r-1})'$ — столбец матрицы $H_{g(x)}(n)$, то ему соответствует полином $s(x) = s_{r-1}x^{r-1} + \ldots + s_1 x + s_0$. Согласно [3] вектору $\hat{s} = M_{g(x)}s$ соответствует полином $xs(x)$, рассматриваемый в кольце полиномов $R_{g(x)}$ по мо-

дулю $g(x)$. Таким образом, в кольце $R_{g(x)}$ матрица $H_{g(x)}(n)$ имеет вид $H_{g(x)}(n) = [x^{n-1}, x^{n-2}, \ldots, x, 1]$.

Пусть $T = (q^r - 1)/(q - 1)$. Поскольку $q \geq 2$ и $r \geq 2$, то $T > r$.

Определение. *Полином $g(x)$ порождает код Хэмминга, если в проверочной матрице $H_{g(x)}(T)$ этого кода все столбцы попарно линейно независимы.*

При определении критерия принадлежности полинома классу ППКХ можно ограничиться полиномами, которые не делятся на x. Это утверждение базируется на следующей теореме.

Теорема 1. *Если $g(x)$ — делящийся на x полином над $GF(q)$ и $\deg g(x) \geq 2$, то $g(x)$ не порождает код Хэмминга.*

Доказательство. Пусть $x \mid g(x)$, $\deg g(x) \geq 2$ и $g(x)$ порождает код Хэмминга. Тогда $g_0 = 0$ и, следовательно, $M_{g(x)}$ — особенная матрица. Поэтому существует такой вектор-столбец c размерности r с компонентами в $GF(q)$, что $c \neq \mathbf{0}$, где $\mathbf{0}$ — нулевой вектор, и $M_{g(x)}c = \mathbf{0}$. Поскольку $g(x)$ порождает код Хэмминга и всего существует T ненулевых векторов размерности r, которые линейно независимы, то найдется такое $\alpha \in GF(q)$, что $\alpha \neq 0$ и $c = \alpha M^i_{g(x)}\beta$, где $0 \leq i \leq T-1$. Отсюда следует равенство $M^{i+1}_{g(x)}\beta = \mathbf{0}$, а так как $M^i_{g(x)}\beta \neq \mathbf{0}$ для всех $0 \leq i \leq T-1$, то $M^T_{g(x)}\beta = \mathbf{0}$, что в кольце $R_{g(x)}$ равносильно равенству $x^T = 0$. Из последнего соотношения следует $g(x) = x^r$. В силу неравенства $T > r$ получаем, что в матрице $H_{g(x)}(T)$ имеется нулевой столбец. Это противоречит предположению о том, что $g(x)$ порождает код Хэмминга. Теорема доказана.

В дальнейшем будем рассматривать полиномы, которые не делятся на x. Для любого такого полинома $g(x)$ согласно [3] существует показатель $e_{g(x)}$, которому принадлежит этот полином. По определению $e_{g(x)} = \min\{n \mid g(x) \mid x^n - 1\}$. Из этого определения следует $e_{g(x)} = \min\{n \geq 1 \mid x^n = 1 \text{ в кольце } R_{g(x)}\}$. Полином называется примитивным, если $e_{g(x)} = q^r - 1$. Введем в рассмотрение еще одну характеристику полинома $g(x)$. Положим

$$n_{g(x)} = \min\{n \geq 1 \mid \exists_{\alpha \in GF(q)} (\alpha \neq 0 \;\&\; x^n = \alpha \text{ в кольце } R_{g(x)})\}.$$

Пусть $\{x\} = \{1, x, x^2, \ldots, x^n, \ldots\}$ — циклическая группа в кольце $R_{g(x)}$. Множество различных элементов в этой циклической группе определяется выражением $\{x\} = \{1, x, x^2, \ldots, x^{e_{g(x)}-1}\}$. Определим подгруппу F группы $\{x\}$, являющуюся ее нормальным делителем,

$$F = \{x^i \mid 0 \leq i \leq e_{g(x)} - 1 \;\&\; \exists_{\alpha \in GF(q)}(\alpha \neq 0 \;\&\; x^i = \alpha)\},$$

и порядок этой группы обозначим через $k_{g(x)}$. Для $0 \leq i \leq e_{g(x)} - 1$ x^iF — смежный класс группы $\{x\}$ по нормальному делителю F. Символом z обозначим число различных смежных классов, т. е. z — индекс подгруппы F в группе $\{x\}$. Известно [2], что $e_{g(x)} = zk_{g(x)}$. Пусть $E = \{x\}/F$ — фактор-группа циклической группы $\{x\}$ по нормальному делителю F. Согласно [2] любая факторгруппа циклической группы циклическая. Поэтому $E = \{F, xF, \ldots, x^{z-1}F\}$ и $z = n_{g(x)}$. Таким образом, справедливо равенство

$$e_{g(x)} = n_{g(x)}k_{g(x)}. \tag{1}$$

Отметим, что множество $\{x\} = \{1, x, \ldots, x^{n_{g(x)}-1}\}$ состоит из попарно линейно независимых элементов. Критерий принадлежности полинома классу ППКХ сформулирован в следующей теореме.

Теорема 2. *Пусть* $g(x)$ *— не делящийся на* x *полином над* $GF(q)$, $\deg g(x) = r \geq 2$ *и* $T = (q^r - 1)/(q - 1)$. *Полином* $g(x)$ *порождает код Хэмминга тогда и только тогда, когда* $n_{g(x)} = T$.

Доказательство. *Необходимость.* Если $g(x)$ порождает код Хэмминга, то все столбцы матрицы $H_{g(x)}(T)$ попарно линейно независимы и, значит, $n_{g(x)} \geq T$. Поскольку $n_{g(x)} \leq T$ всегда, то $n_{g(x)} = T$.

Достаточность. Если $n_{g(x)} = T$, то все столбцы матрицы $H_{g(x)}(T)$ попарно линейно независимы. Теорема доказана.

Из теоремы 2 и равенства (1) получаем следующий результат.

Следствие 1. *Если* $g(x)$ *— не делящийся на* x *полином над* $GF(q)$, $\deg g(x) = r \geq 2$, $e_{g(x)} = T$ *и* T *просто, то* $g(x)$ *порождает код Хэмминга.*

Заметим, что для полинома $g(x)$ степени $r \geq 2$ всегда выполняются неравенства $e_{g(x)} \leq q^r - 1$, $k_{g(x)} \leq q - 1$, $n_{g(x)} \leq (q^r - 1)/(q - 1)$, причем равенства в них достигаются в случае, когда $g(x)$ примитивный. Поэтому при $q = 2$ имеет место следующий известный результат.

Следствие 2. *Полином над* $GF(2)$ *порождает код Хэмминга тогда и только тогда, когда он примитивный.*

Теперь рассмотрим простые полиномы над $GF(q)$ и найдем условия, при выполнении которых они порождают коды Хэмминга. Напомним, что простым называется неприводимый в $GF(q)$ полином, старший коэффициент которого равен 1.

Пусть $g(x)$ — простой полином над $GF(q)$ степени $r \geq 2$. Поскольку $g(x)$ — простой полином, то элементы поля $GF(q^r)$ можно представить в виде полиномов кольца $R_{g(x)}$. Полином $g(x)$ является минимальным полиномом некоторого ненулевого элемента поля $GF(q^r)$ (таким может быть, например, элемент, который в кольце $R_{g(x)}$ представляется в виде полинома x). Допустим α — примитивный элемент поля $GF(q^r)$ и k — такое целое число, что $1 \leq k \leq q^r - 1$ и $g(x)$ — минимальный полином элемента α^k. Тогда для $n > r$ $(n, n - r)$-код, порожденный полиномом $g(x)$, задается выражением

$$C_{g(x)}(n) = \{ c(x) \in \mathfrak{M} \mid \deg c(x) \leq n - 1 \;\&\; c(\alpha^k) = 0 \},$$

а проверочная матрица этого кода — равенством

$$H_{g(x)}(n) = [\alpha^{(n-1)k},\ \alpha^{(n-2)k},\ \ldots,\ \alpha^k,\ 1].$$

Выясним, при каких условиях матрица $H_{g(x)}(T)$ является проверочной матрицей кода Хэмминга (ПМКХ). Ясно, что

$$H_{g(x)}(T) - \text{ПМКХ} \Leftrightarrow \forall_{1 \leq p \leq T-1}(\alpha^{pk} \notin GF(q)). \tag{2}$$

Для $n \geq 1$ и примитивного $\alpha \in GF(q^r)$ справедлива равносильность

$$\alpha^n \in GF(q) \Leftrightarrow T \mid n. \tag{3}$$

Из (2) и (3) находим

$$H_{g(x)}(T) - \text{ПМКХ} \Leftrightarrow \forall_{1 \leq p \leq T-1}\ (T \nmid pk). \tag{4}$$

Покажем справедливость равносильности

$$\forall_{1 \leq p \leq T-1}\ (T \nmid pk) \Leftrightarrow k,\ T \text{ — взаимно просты}. \tag{5}$$

В самом деле, если $\forall_{1 \leq p \leq T-1}\ (T \nmid pk)$ и k, T не являются взаимно простыми, то существуют такие i, j и $p \geq 2$, что $k = ip$ и $T = jp$. Так как $jk = ijp$, то $T \mid jk$,

что приводит к противоречию с принятым допущением, если учесть неравенство $j \le T-1$.

Допустим, что k, T — взаимно просты. Тогда $T \mid pk \Leftrightarrow T \mid p$ и поскольку $\forall_{1 \le p \le T-1}\,(T \nmid p)$, то $\forall_{1 \le p \le T-1}\,(T \nmid pk)$. Равносильность (5) доказана.

Из (4) и (5) находим

$$H_{g(x)}(T) - \text{ПМКХ} \Leftrightarrow k, T \text{ — взаимно просты.} \qquad (6)$$

Приведенные рассуждения и соотношение (6) позволяют сформулировать следующую теорему.

Теорема 3. *Пусть $g(x)$ — простой полином над $GF(q)$ степени $r \ge 2$, являющийся минимальным для элемента $\alpha^k \in GF(q^r)$, $1 \le k < q^r - 1$, где α — примитивный элемент поля $GF(q^r)$, и $T = (q^r - 1)/(q-1)$. Полином $g(x)$ порождает код Хэмминга тогда и только тогда, когда k и T — взаимно просты.*

***Пример* 1.** Рассмотрим простой полином $g(x) = x^2 + 2x + 1$ над $GF(4)$. Элементы поля $GF(4^2)$ представим в виде полиномов кольца $R_{g(x)}$. Элемент $\alpha = x + 1$ является примитивным в $GF(4^2)$, так как $\alpha^2 = 2x$, $\alpha^3 = x + 2$, $\alpha^4 = x + 3$, $\alpha^5 = 2$, $\alpha^6 = 2x + 2$, $\alpha^7 = 3x$, $\alpha^8 = 2x + 3$, $\alpha^9 = 2x + 1$, $\alpha^{10} = 3$, $\alpha^{11} = 3x + 3$, $\alpha^{12} = x$, $\alpha^{13} = 3x + 1$, $\alpha^{14} = 3x + 2$, $\alpha^{15} = 1$. В рассматриваемом примере $T = (4^2 - 1)/(4 - 1) = 5$. Поскольку $g(x)$ является минимальным полиномом элемента $x = \alpha^{12}$, 12 и 5 — взаимно просты, то согласно теореме 3 $g(x)$ порождает (5, 3)-код Хэмминга.

Покажем, как находить полиномы степени 2 (примитивные и непримитивные), порождающие (5, 3)-коды Хэмминга. Поиск примитивных полиномов связан с нахождением минимальных полиномов примитивных элементов. Если α — примитивный элемент поля $GF(q^r)$, то согласно теореме 4.23 [4] α^k примитивен тогда и только тогда, когда k, $q^r - 1$ — взаимно просты. В рассматриваемом примере примитивными будут следующие элементы: $\alpha, \alpha^2, \alpha^4, \alpha^7, \alpha^8, \alpha^{11}, \alpha^{13}, \alpha^{14}$. Так как α^{12} — непримитивный элемент, то расмотренный в примере полином $g(x)$ непримитивен. Найдем примитивный полином $f_1(x)$, являющийся минимальным для примитивного элемента α^2:

$$f_1(x) = (x + \alpha^2)(x + \alpha^8) = x^2 + 3x + 3.$$

Так как 6 и 5 — взаимно просты и α^6 — непримитивен, то непримитивный минимальный полином $f_2(x)$ элемента α^6 также будет порождать (5, 3)-код Хэмминга. Этот полином определяется выражением

$$f_2(x) = (x + \alpha^6)(x + \alpha^{24}) = (x + \alpha^6)(x + \alpha^9) = x^2 + 3x + 1.$$

Ниже изучаются приводимые (разложимые на множители) полиномы и установлены условия, при которых эти полиномы не могут порождать коды Хэмминга. Попытки автора найти приводимые полиномы, порождающие коды Хэмминга, не увенчались успехом.

Теорема 4. *Пусть $g(x)$ — такой приводимый полином над $GF(q)$, что $g(x) = f_1(x) \ldots f_w(x)$, где $w \ge 2$ и $f_1(x), \ldots, f_w(x)$ — примитивные попарно различные полиномы над $GF(q)$. Тогда $g(x)$ не порождает код Хэмминга.*

Доказательство. Положим $\deg g(x) = r$, $T = (q^r - 1)/(q-1)$ и для $1 \le i \le w$ $\deg f_i(x) = r_i$, $T_i = (q^{r_i} - 1)/(q-1)$. По предположению $e_{f_i(x)} = q^{r_i} - 1$, $1 \le i \le w$. Согласно [3]

$$e_{g(x)} = \text{н.о.к.}\,(e_{f_1(x)}, \ldots, e_{f_w(x)}) = (q-1)\,\text{н.о.к.}\,(T_1, \ldots, T_w).$$

Поскольку при $q > 1$ $\prod_{i=1}^{w} (q^{r_i} - 1) < q^r - 1$, то

$$e_{g(x)} \le (q-1) \prod_{i=1}^{w} (q^{r_i} - 1) / (q-1)^w < (q^r - 1)/(q-1) = T.$$

На основании теоремы 2, учитывая неравенство $n_{g(x)} \le e_{g(x)} < T$, получаем, что $g(x)$ не порождает код Хэмминга. Теорема доказана.

Теорема 5. *Пусть $g(x)$ — приводимый полином над $GF(q)$ такой, что $g(x) = f_1(x) \ldots f_w(x)$, где $w \ge 2$ и $f_1(x), \ldots, f_w(x)$ — простые непримитивные попарно различные полиномы над $GF(q)$. Если $2^w \ge q - 1$, то $g(x)$ не порождает код Хэмминга.*

Доказательство. При $q = 2$ теорема справедлива на основании следствия 2. Допустим $q > 2$ и положим $\deg g(x) = r$, $T = (q^r - 1)/(q-1)$ и для $1 \le i \le w$ $\deg f_i(x) = r_i$. Так как $f_i(x)$ — простой непримитивный полином, то $e_{f_i(x)} = (q^{r_i} - 1)/a_i$, где $a_i \ge 2$. Поэтому

$$e_{g(x)} = \text{н.о.к.}\left(\frac{q^{r_1}-1}{a_1}, \ldots \frac{q^{r_w}-1}{a_w}\right) \le \prod_{i=1}^{w} \frac{q^{r_1}-1}{a_i} < \frac{q^{r_1}-1}{2^w}.$$

Поскольку $2^w \ge q - 1$, то $e_{g(x)} < (q^r - 1)/(q-1) = T$ и, следовательно, $g(x)$ не порождает код Хэмминга. Теорема доказана.

Пример 2. Полиномы $x + 2$ и $x^2 + 3x + 3$ — примитивные над $GF(4)$. Согласно теореме 4 полином

$$g(x) = (x+2)(x^2+3x+3) = x^3 + x^2 + 2x + 1$$

не порождает код Хэмминга.

Полиномы $x + 1$ и $x^2 + 2x + 1$ — непримитивные над $GF(4)$. Согласно теореме 5 полином

$$g(x) = (x+1)(x^2+2x+1) = x^3 + 3x^2 + 3x + 1$$

не порождает код Хэмминга, так как $2^w = 2^2 \ge 3 = q - 1$.

1. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.
2. *Курош А. Г.* Лекции по общей алгебре. – М.: Наука, 1973. – 399 с.
3. *Гилл А.* Линейные последовательностные машины. – М.: Наука, 1974. – 287 с.
4. *Берлекэмп Э.* Алгебраическая теория кодирования. – М.: Мир, 1971. – 477 с.

Получено 22.10.92