Н. Н. Жигулин, Перечисление симметричных циркулянтов над конечным полем фиксированного ранга,
Матем. заметки, 1985, том 38, выпуск 5, 784–794

МАТЕМАТИЧЕСКИЕ ЗАМЕТКИ
т. 38, № 5 (1985)

ПЕРЕЧИСЛЕНИЕ СИММЕТРИЧНЫХ ЦИРКУЛЯНТОВ НАД КОНЕЧНЫМ ПОЛЕМ ФИКСИРОВАННОГО РАНГА

Н. Н. Жигулин

1. Введение. Задачи перечисления и построения матриц над конечным полем с заданными свойствами часто возникают в различных исследованиях и имеют широкие применения (см., например, библиографию в [1, 2]). В данной заметке предлагается развитие метода Берлекэмпа [1] перечисления циркулянтов (циклических матриц) над конечным полем фиксированного ранга при дополнительном условии симметричности (см. [3, с. 100]).

Рассмотрим алгебру $\mathcal{T}$ циркулянтов размера n над полем Галуа $F = GF(q)$:

$$\mathcal{T} = \left\{ A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix}, \quad a_i \in F, \quad (i \in \overline{0, n-1}) \right\}$$

Обозначим через $S_r = S_r(q, n)$ число симметричных (не меняющихся при транспонировании) циркулянтов из $\mathcal{T}$ ранга r, $(r \in \overline{0, n})$. Следующая теорема дает формулу для вычисления нумератора $S(t) = S(t; q, n)$ этих чисел:

$$S(t) = \sum_{r=0}^{n} S_r \cdot t^r,$$

в зависимости от поведения определенных арифметических функций двух аргументов n и q. Для известных теоретико-числовых функций пользуемся общепринятыми [4] обозначениями.

ТЕОРЕМА 1. $S(t) = P_1(t) \cdot P_2(t)$, *где*

$$P_1 = \prod_{\substack{k \mid n' \\ k>2}} (1 + (1 - q^{-\pi_k}) \cdot \sum_{l=1}^{m} (qt^2)^{l \cdot \pi_k})^{\varkappa_k},$$

$$P_2 = \begin{cases} (1 + (1 - q^{-1}) \cdot \sum_{l=1}^{m+1/2} q^l t^{2l-1})^{(n',2)}, & (q, 2) = 1, \\ 1 + (q-1)t + (q-1)\sum_{l=1}^{m/2} q^l t^{2l}, & (q, 2) = 2, \end{cases}$$

причем сумма $\sum_{l=1}^{m/2}$ *считается пустой при* $m = 1$. *Здесь арифметические функции* π_k, $\varkappa_k$, n', m *заданы соответственно следующим образом*:

$$\pi_k = \min \{i \in \mathbf{N} : q^i \equiv 1 \pmod k \text{ либо } q^i \equiv -1 \pmod k\},$$

$$\varkappa_k = \frac{\varphi(k)}{2 \cdot \pi_k}, \quad n' = \max \{k \in \mathbf{N} : k \mid n, (q, k) = 1\}, \quad m = \frac{n}{n'}.$$

Доказательство теоремы дает метод построения симметричных циркулянтов из $\mathcal{T}$ допустимого ранга r.

В качестве непосредственных следствий теоремы 1 получаются соответствующие результаты [5, 6] о невырожденных симметричных циркулянтах. Для примера сформулируем два следствия, напоминающих подобные утверждения [1].

Следствие 1.

$$S_n = q^{[n/2]+1} (1 - q^{-1})^{(n',2)} \prod_{\substack{k \mid n' \\ k>2}} (1 - q^{-\pi_k})^{\varkappa_k},$$

т. е. доля S_n/S *невырожденных симметричных циркулянтов среди всех* $S = q^{[n/2]+1}$ *симметричных циркулянтов над* F *размера* n *зависит только от* n' *и* q, *но не от значения* m.

Следствие 2. $S_n/S \leqslant (1 - q^{-1})^{(n',2)}$, *причем равенство только при* $n' = 1$ *и* $n' = 2$.

2. Вспомогательные результаты. При доказательстве теоремы 1 будем пользоваться известными понятиями двойственных и самодвойственных многочленов над конечным полем. Согласно [7], всякий многочлен $f(x)$ над F имеет двойственный многочлен

$$f^*(x) = x^{\deg f} \cdot f(x^{-1}), \tag{1}$$

причем $f(x)$ называют самодвойственным при равенстве многочленов $f(x)$ и $f^*(x)$.

Будем называть многочлен $f(x)$ самодвойственным с точностью до константы, если для некоторого $c \in F$

$$f^*(x) = c \cdot f(x).$$

Например, многочлен $x^n - 1$ ($n \in \mathbf{N}$) при $(q, 2) = 1$ является самодвойственным с точностью до константы (-1).

Хорошо известно (см., например, [1, 2, 5, 6]), что

$$x^n - 1 = \prod_{k|n} \Phi_k^m(x),$$

где через $\Phi_k(x)$ обозначен k-й круговой многочлен степени $\varphi(k)$, который в свою очередь над F разлагается в произведение неприводимых множителей одинаковой степени σ_k:

$$\sigma_k = \min \{i \in \mathbf{N}: q^i \equiv 1 \pmod{k}\}.$$

Ясно, что многочлены $\Phi_k(x)$ при $k \geqslant 2$ являются самодвойственными многочленами.

Следующие две леммы очевидны.

ЛЕММА 1. $\sigma_1 = \pi_1 = 1$, $\sigma_2 = \pi_2 = 1$. *При* $k > 2$ *либо* $\sigma_k = \pi_k$, *либо* $\sigma_k = 2\pi_k$, *причем последнее равенство в точности тогда, когда* $q^i \equiv -1 \pmod{k}$ *при некотором* i ($i \in \mathbf{N}$).

ЛЕММА 2. *Пусть* $f(x) = \prod_{i=1}^{\sigma_k} (x - \alpha^{q^i})$ — *неприводимый над* F *делитель кругового многочлена* $\Phi_k(x)$, $k > 2$, *и* α — *корень* $f(x)$ *в некотором поле разложения. Тогда* $f^*(x) = f(0) \cdot \prod_{i=1}^{\sigma_k} (x - \alpha^{-q^i})$ *и многочлен* $f(x)$ *является самодвойственным с точностью до константы, если и только если* $\sigma_k = 2\pi_k$. *При этом константа равна* 1.

Теперь можем уточнить разложение многочленов $\Phi_k(x)$ при $k > 2$.

ЛЕММА 3. *Пусть* $k > 2$. *При* $\sigma_k = 2\pi_k$ *многочлен* $\Phi_k(x)$ *представляет собой произведение* $\varkappa_k$ *неприводимых над* F *самодвойственных многочленов степени* σ_k. *При* $\sigma_k = \pi_k$ *многочлен* $\Phi_k(x)$ *представляет собой произведение* $\varkappa_k$ *самодвойственных многочленов степени* $2\sigma_k$, *каждый из которых есть произведение двух неприводимых над* F (*взаимно*) *двойственных многочленов степени* σ_k.

Доказательство. Так как многочлены $\Phi_k(x)$ при $k > 2$ являются самодвойственными, то $f(x) \mid \Phi_k(x)$ влечет $f^*(x) \mid \Phi_k(x)$. По лемме 2 неприводимые делители $f(x)$ и $f^*(x)$ многочлена $\Phi_k(x)$, $k > 2$, имеют общий корень (и это эквивалентно самодвойственности $f(x)$), если

и только если $\sigma_k = 2\pi_k$. При $\sigma_k = \pi_k$ неприводимые делители $f(x)$ и $f^*(x)$ многочлена $\Phi_k(x)$, $k > 2$, не имеют общих корней и доказательство завершает рассмотрение самодвойственных многочленов $g(x) = f(x) \cdot f^*(x)$ в качестве указанных в формулировке леммы 3.

Таким образом,

$$x^n - 1 = \prod_f f^m \cdot \prod_g g^m \cdot \Phi_1^m \cdot \Phi_2^{\varepsilon \cdot m} = \prod_h h^m \cdot \Phi_1^m \cdot \Phi_2^{\varepsilon \cdot m}, \quad (2)$$

где $\varepsilon = (n', 2) - 1$, $\prod_h h^m = \prod_f f^m \cdot \prod_g g^m$ и где $\prod_f f^m = \prod_{\substack{k \mid n' \\ \sigma_k = 2 \cdot \pi_k}} \prod_{f \mid \Phi_k} f^m$ обозначает произведение по всем непроводимым делителям $f = f(x)$ многочленов $\Phi_k(x), k > 2$, при $k \mid n'$ и $\sigma_k = 2\pi_k$, $\prod_g g^m = \prod_{\substack{k \mid n' \\ \sigma_k = \pi_k}} \prod_{\substack{g = f \cdot f^* \\ f \mid \Phi_k}} g^m$ обозначает произведение по всем различным самодвойственным многочленам $g = g(x) = f(x) \cdot f^*(x)$ для неприводимых делителей $f = f(x)$ многочленов $\Phi_k(x)$, $k > 2$, при $k \mid n'$ и $\sigma_k = \pi_k$.

3. Доказательство теоремы 1. Хорошо известно (см. [2, с. 484]), что любой циркулянт A из алгебры $\mathcal{T}$ представим в виде $A = \sum_{i=0}^{n-1} a_i T^i$, где $a_i \in F$ и T — матрица подстановки $(0, 1, \ldots, n-1)$, причем соответствие

$$A = \sum_{i=0}^{n-1} a_i T^i \to a(x) = \sum_{i=0}^{n-1} a_i x^i \pmod{(x^n - 1)} \quad (3)$$

задает изоморфизм между алгебрами $\mathcal{T}$ и $F[x]/(x^n - 1)$. В соответствие с этим изоморфизмом симметричность циркулянта A означает выполнение сравнения

$$a(x) \equiv a(x^{n-1}) \pmod{(x^n - 1)}. \quad (4)$$

Согласно [1], дефект циркулянта A совпадает со степенью наибольшего общего делителя $(a(x), x^n - 1)$ многочленов $a(x)$ и $x^n - 1$. Поэтому задача определения числа $S_r(q, n)$ симметричных циркулянтов над F размера n и ранга r эквивалентна задаче определения числа многочленов $a(x)$ над F степени меньшей n, удовлетворяющих условиям (4) и (5):

$$\deg(a(x), x^n - 1) = n - r. \quad (5)$$

С использованием понятия двойственного многочлена ус-

ловие (4) можно переписать в виде

$$a(x) - x^{n-\deg a(x)} a^*(x) \equiv 0 \pmod{(x^n - 1)}. \qquad (6)$$

Из (2) и (6) следует самодвойственность с точностью до константы многочлена $d(x) = (a(x), x^n - 1)$, причем необходимо имеется представление

$$d(x) = \prod_h h^{e_h} \cdot \Phi_1^{e_{\Phi_1}} \cdot \Phi_2^{\varepsilon \cdot e_{\Phi_2}} \quad (e_h, e_{\Phi_1}, e_{\Phi_2} \in \overline{0, m}). \qquad (7)$$

Замечание 1. Дальнейшее изложение будем вести для случая $\varepsilon = 1$, т. е. $(n', 2) = 2$ и Φ_2 присутствует в (2) (и (7)). Для случая $\varepsilon = 0$, т. е. $(n', 2) = 1$ и Φ_2 отсутствует в (2) (и (7)), вычисления, связанные с Φ_2, следует опустить из дальнейших формул без ущерба для доказательства.

Согласно [2, с. 215—224], разложению (2) на взаимно простые сомножители соответствует следующее однозначное покомпонентное представление $a(x)$, составленное с учетом структуры порождающих ортогональных идемпотентов:

$$a(x) \equiv \sum_h a_h \frac{x^n - 1}{h^m} + a_{\Phi_1} \frac{x^n - 1}{\Phi_1^m} + a_{\Phi_2} \frac{x^n - 1}{\Phi_2^m} \pmod{(x^n - 1)}, \qquad (8)$$

где сумма $\sum_h$ соответствует произведению $\prod_h$ и многочлены $a_h = a_h(x)$, $a_{\Phi_1} = a_{\Phi_1}(x)$, $a_{\Phi_2} = a_{\Phi_2}(x)$ удовлетворяют условиям

$$\deg a_h < m \cdot \deg h, \quad \deg a_{\Phi_1} < m, \quad \deg a_{\Phi_2} < m. \qquad (9)$$

Используя (1), (8) и (9), легко получить эквивалентную покомпонентную запись условия (6):

$$\left.\begin{aligned} &a_h + x^{m \cdot \deg h - \deg a_h} a_h^* \equiv 0 \pmod{h^m}, && \deg a_h < m \cdot \deg h, \\ &a_{\Phi_1} + (-1)^m X^{m - \deg a_{\Phi_1}} a_{\Phi_1}^* \equiv 0 \pmod{\Phi_1^m}, && \deg a_{\Phi_1} < m, \\ &a_{\Phi_2} + x^{m - \deg a_{\Phi_2}} a_{\Phi_2}^* \equiv 0 \pmod{\Phi_2^m}, && \deg a_{\Phi_2} < m. \end{aligned}\right\} \qquad (10)$$

Аналогично условию (5) можно дать покомпонентную запись. В соответствии с (5), (7) и (8) имеем

$$r = n - \sum_h e_h \cdot \deg h - e_{\Phi_1} - e_{\Phi_2} = \sum_h (m - e_h) \deg h + m - e_{\Phi_1} + m - e_{\Phi_2} \quad (e_h, e_{\Phi_1}, e_{\Phi_2} \in \overline{0, m}), \qquad (11)$$

$$(a_h, h^m) = h^{e_h}, \quad (a_{\Phi_1}, \Phi_1^m) = \Phi_1^{e_{\Phi_1}}, \quad (a_{\Phi_2}, \Phi_2^m) = \Phi_2^{e_{\Phi_2}}. \qquad (12)$$

Отсюда следует, что нумератор $S(t)$ равен произведению нумераторов:

$$S(t)=\prod_h\left(\sum_{e=0}^{m}R_{m-e}(h)\cdot t^{(m-e)\deg h}\right)\cdot\left(\sum_{e=0}^{m}R_{m-e}(\Phi_1)\,t^{m-e}\right)\left(\sum_{e=0}^{m}R_{m-e}(\Phi_2)\,t^{m-e}\right),\qquad(13)$$

где $\prod_h$ задано, как в (2), и $R_{m-e}(h)$ $(e\in\overline{0,\,m})$ — число многочленов $a_h(x)$ над F степени меньше $m\cdot\deg h$ и удовлетворяющих двум соответствующим $h(x)$ условиям (одно из (10) и другое из (12)), где $R_{m-e}(\Phi_1)$ $(e\in\overline{0,\,m})$ — число многочленов $a_{\Phi_1}(x)$ над F степени меньше m и удовлетворяющих двум соответствующим $\Phi_1(x)$ условиям (из (10) и (12)) и где $R_{m-e}(\Phi_2)$ $(e\in\overline{0,\,m})$ задано аналогично.

Объединяя условия (10), (11), (12) и обозначая

$$b_h=a_h/h^{e_h},\quad b_{\Phi_1}=a_{\Phi_1}/\Phi_1^{e_{\Phi_1}},\quad b_{\Phi_2}=a_{\Phi_2}/\Phi_2^{e_{\Phi_2}},\quad e_h=m-e_h,$$
$$l_{\Phi_1}=m-e_{\Phi_1},\quad e_{\Phi_2}=m-e_{\Phi_2},$$

видим, что задача подсчета вариантов a_h, a_{Φ_1} и a_{Φ_2} с условиями (10), (12) равносильна задаче подсчета вариантов $b_h=b_h(x)$, $b_{\Phi_1}=b_{\Phi_1}(x)$, $b_{\Phi_2}=b_{\Phi_2}(x)$ с условиями

$$\left.\begin{aligned}&b_h+x^{l_h-\deg b_h}\cdot b_h^*\equiv 0\ (\mathrm{mod}\ h^{l_h}),\\&b_{\Phi_1}+(-1)^{l_{\Phi_1}}x^{l_{\Phi_1}-\deg b_{\Phi_1}}b_{\Phi_1}^*\equiv 0\ (\mathrm{mod}\ \Phi_1^{l_{\Phi_1}}),\\&b_{\Phi_2}+x^{l_{\Phi_2}-\deg b_{\Phi_2}}b_{\Phi_2}^*\equiv(\mathrm{mod}\ \Phi_2^{l_{\Phi_2}}),\end{aligned}\right\}\qquad(14)$$

где $l_h, l_{\Phi_1}, l_{\Phi_2}\in\overline{0,m}$ и

$$\deg b_h<l_h\cdot\deg h,\quad \deg b_{\Phi_1}<l_{\Phi_1},\quad \deg b_{\Phi_2}<l_{\Phi_2},\qquad(15)$$

$$(b_h,h)=1,\quad (b_{\Phi_1},\Phi_1)=1,\quad (b_{\Phi_2},\Phi_2)=1.\qquad(16)$$

Число вариантов $b(x)$ с условиями (14), (15), (16) равно числу вариантов $b(x)$ с условиями (14), (15) минус число вариантов $b(x)$ с условиями (14), (15) и условием

$$b_h\equiv 0\ (\mathrm{mog}\ h),\quad b_{\Phi_1}\equiv 0\ (\mathrm{mod}\ \Phi_1),\ b_{\Phi_2}\equiv 0\ (\mathrm{mod}\ \Phi_2).\qquad(17)$$

При этом число вариантов $b(x)$ с условиями (14), (15), (17) совпадает с числом вариантов $b(x)$ с условиями (14) и (15), но с заменой l_h, l_{Φ_1} и l_{Φ_2} на $l_h-1, l_{\Phi_1}-1$ и $l_{\Phi_2}-1$.

Обозначим

$$b_h(x)=\sum_{u=0}^{l_h\deg h-1}b_u^h\cdot x^u,\qquad b_u^h\in F,\qquad(18)$$

$$b_{\Phi_1}(x) = \sum_{u=0}^{l_{\Phi_1}-1} b_u^{\Phi_1} \cdot x^u, \qquad b_u^{\Phi_1} \in F, \tag{19}$$

$$b_{\Phi_2}(x) = \sum_{u=0}^{l_{\Phi_2}-1} b_u^{\Phi_2} \cdot x^u, \qquad b_u^{\Phi_2} \in F. \tag{20}$$

Тогда условия (14), (15) переписываются в виде

$$\left.\begin{aligned}
&b_0^h + \sum_{u=1}^{l_h \deg h - 1} (b_u^h + b_{l_h \deg h - u}^h)\, x^u + b_0^h x^{l_h \deg h} \equiv 0 \pmod{h^{l_h}},\\
&b_0^{\Phi_1} + \sum_{u=1}^{l_{\Phi_1}-1} (b_u^{\Phi_1} + (-1)^{l_{\Phi_1}} b_{l_{\Phi_1}-u}^{\Phi_1})\, x^u + (-1)^{l_{\Phi_1}} b_0^{\Phi_1} x^{l_{\Phi_1}} \equiv\\
&\qquad\qquad \equiv 0 \pmod{\Phi_1^{l_{\Phi_1}}},\\
&b_0^{\Phi_2} + \sum_{u=1}^{l_{\Phi_2}-1} (b_u^{\Phi_2} + b_{l_{\Phi_2}-u}^{\Phi_2})\, x^u + b_0^{\Phi_2} x^{l_{\Phi_2}} \equiv 0 \pmod{\Phi_2^{l_{\Phi_2}}}.
\end{aligned}\right\} \tag{21}$$

Так как в левых частях сравнений (21) стоят многочлены от x степеней не выше $l_h \cdot \deg h$, l_{Φ_1}, l_{Φ_2} соответственно, то эти многочлены могут отличаться от h^{l_h}, $\Phi_1^{l_{\Phi_1}} = (x - 1)^{l_{\Phi_1}}$, $\Phi_2^{l_{\Phi_2}} = (x + 1)^{l_{\Phi_2}}$ соответственно лишь множителями c_h, c_{Φ_1}, c_{Φ_2} из F:

$$b_0^h + \sum_{u=1}^{l_h \deg h - 1} (b_u^h + b_{l_h \deg h - u}^h)\, x^u + b_0^h \cdot x^{l_h \deg h} = c_h \cdot h^{l_h}, \tag{22}$$

$$b_0^{\Phi_1} + \sum_{u=1}^{l_{\Phi_1}-1} (b_u^{\Phi_1} + (-1)^{l_{\Phi_1}} b_{l_{\Phi_1}-u}^{\Phi_1})\, x^u + (-1)^{l_{\Phi_1}} b_0^{\Phi_1} x^{l_{\Phi_1}} = c_{\Phi_1} (x - 1)^{l_{\Phi_1}}, \tag{23}$$

$$b_0^{\Phi_2} + \sum_{u=1}^{l_{\Phi_2}-1} (b_u^{\Phi_2} + b_{l_{\Phi_2}-u}^{\Phi_2})\, x^u + b_0^{\Phi_2} x^{l_{\Phi_2}} = c_{\Phi_2} (x + 1)^{l_{\Phi_2}}. \tag{24}$$

Так как многочлены $h(x)$ являются самодвойственными многочленами четной степени, то для каждого из них в силу (22) имеем $\frac{1}{2} l_h \deg h$ линейных связей вида

$$\begin{aligned}
&b_0^h = c_h \cdot h_0,\\
&b_1^h + b_{l_h \deg h - 1}^h = c_h \cdot h_1,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&b_{1/2 l_h \deg h - 1}^h + b_{1/2 l_h \deg h + 1}^h = c_h \cdot h_{1/2 l_h \deg h - 1},\\
&2 \cdot b_{1/2 l_h \deg h}^h = c_h \cdot h_{1/2 l_h \deg h}
\end{aligned}$$

при $h^{l_h} = \sum_{u=0}^{l_h \deg h} h_u \cdot x^u$. Здесь параметрами являются b_u^h и c_h из F, причем для четного q необходимо $h_{1/2^l h^{\deg h}} \neq 0$ и $c_h = 0$. Следовательно, имеется $q^{1/2 l_h \deg h}$ вариантов задания ($l_h \in \overline{0, m}$) многочлена (18). Поэтому

$$R_l(h) = \begin{cases} q^{1/2 l \cdot \deg h} - q^{1/2 (l-1) \deg h}, & l = \overline{1, m}, \\ 1, & l = 0. \end{cases} \tag{25}$$

Согласно лемме 3 и соотношению (2), при $h \mid \Phi_k$ имеем $\frac{1}{2} \deg h = \pi_k$ и (25) можно переписать в виде

$$R_l(h) = \begin{cases} q^{l \cdot \pi_k} - q^{(l-1) \cdot \pi_k}, & l = \overline{1, m}, \\ 1, & l = 0, \end{cases} \tag{26}$$

где $h \mid \Phi_k$, $(k > 2)$. Следовательно, $R_l(h)$, $(l \in \overline{0, m})$ не зависит от h, а лишь от k, удовлетворяющего условию $h \mid \Phi_k$ $(k > 2)$.

Опуская в равенстве (23) для краткости значки Φ_1 и учитывая равенство $(x-1)^l = \sum_{u=0}^{l} (-1)^{l-u} \binom{l}{u} \cdot x^u$, получаем следующие линейные связи для коэффициентов многочлена (19) при четном l $(l \in \overline{1, m})$:

$$\begin{aligned} & b_0 = c, \\ & b_1 + b_{l-1} = -c \binom{l}{1}, \\ & \cdots\cdots\cdots\cdots\cdots\cdots \\ & b_{l/2-1} + b_{l/2+1} = c (-1)^{l/2-1} \binom{l}{l/2-1}, \\ & 2b_{l/2} = c \cdot (-1)^{l/2} \cdot \binom{l}{l/2}, \end{aligned}$$

и при нечетном l $(l \in \overline{1, m})$

$$\begin{aligned} & b_0 = -c, \\ & b_1 - b_{l-1} = c \cdot \binom{l}{1}, \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & b_{l-1/2} - b_{l+1/2} = c \cdot (-1)^{l+1/2} \binom{l}{\frac{l-1}{2}}. \end{aligned}$$

Здесь параметрами являются b_u и c из F. Следовательно, имеется при четном l, $(l > 1)$, в силу $\binom{l}{l/2} \equiv 0 \pmod 2$

$q^{l/2-1+(2,q)}$ вариантов и при нечетном l $q^{(l+1)/2}$ вариантов задания многочлена $b_{\Phi_1}(x)=\sum_{u=0}^{l-1} b_u x^u$ $(l\in\overline{1,m})$, причем при $l=0$ в силу (15) задание b_{Φ_1} необходимо единственное: $b_{\Phi_1}(x)=0$. Поэтому

$$R_0(\Phi_1)=1, \quad R_1(\Phi_1)=q-1, \tag{27}$$

и при $l\in\overline{2,m}$

$$R_l(\Phi_1)=\begin{cases} q^{l/2+1}-q^{l/2}, & l\equiv q\equiv 0 \pmod 2,\\ q^{l+1/2}-q^{l-1/2}, & l\equiv q\equiv 1 \pmod 2,\\ 0, & l\not\equiv q \pmod 2. \end{cases} \tag{28}$$

Опуская в равенстве (24) для кратности значки Φ_2 и учитывая равенство $(x+1)^l=\sum_{u=0}^{l}\binom{l}{u}x^u$, получаем следующие линейные связи для коэффициентов многочлена (20) при четном l $(l\in\overline{1,m})$:

$$\begin{aligned} &b_0=c,\\ &b_1+b_{l-1}=c\cdot\binom{l}{1},\\ &\dots\dots\dots\dots\dots\dots\\ &b_{l/2-1}+b_{l/2+1}=c\cdot\binom{l}{l/2-1},\\ &2\cdot b_{l/2}=c\cdot\binom{l}{l/2}, \end{aligned}$$

и при нечетном l $(l\in\overline{1,m})$:

$$\begin{aligned} &b_0=c,\\ &b_1+b_{l-1}=c\cdot\binom{l}{1},\\ &\dots\dots\dots\dots\dots\dots\\ &b_{l-1/2}+b_{l+1/2}=c\cdot\binom{l}{\frac{l-1}{2}}. \end{aligned}$$

Здесь параметрами являются b_u и c из F. Следовательно, имеется при четном l $q^{l/2}$ вариантов и при нечетном l $q^{\frac{l+1}{2}}$ вариантов задания многочлена $b_{\Phi_2}(x)=\sum_{u=0}^{l-1} b_u\cdot x^u$ $(l\in\overline{1,m})$, причем при $l=0$ в силу (15) задание b_{Φ_2} необходимо единственное: $b_{\Phi_2}(x)=0$. Поэтому

$$R_0(\Phi_2)=1 \tag{29}$$

и при $l \in \overline{1, m}$

$$R_l(\Phi_2) = \begin{cases} q^{(l+1)/2} - q^{(l-1)/2}, & l \equiv 1 \pmod 2, \\ 0, & l \equiv 0 \pmod 2, \end{cases} \tag{30}$$

Учитывая (26), (27), (28), (29), (30), очевидными преобразованиями от соотношения (13) приходим к соотношению, указанному в теореме 1. Теорема 1 доказана.

4. **Дополнение.** Попутно устанавливается следующий результат о самодвойственных многочленах, имеющих фиксированное число корней заданного периода.

ТЕОРЕМА 2. *Пусть* $n \in \mathbf{N}$, n *нечетно. Тогда число самодвойственных многочленов над* $F = GF(q)$ *четной степени не выше* $n - 1$, *имеющих с* $x^n - 1$ *наибольший общий делитель степени* $n - r$, *совпадает с числом* S_r *симметричных циркулянтов над* F *размера* n *и ранга* r ($r \in \overline{0, n}$). *Нумераторы этих чисел доставляются формулами теоремы* 1.

Доказательство. Свяжем самодвойственный многочлен $\mathcal{A}(x)$ четной степени 2ν ($2\nu \leqslant n - 1$) с некоторым многочленом $a(x) = \sum_{i=0}^{n-1} a_i x^i$ степени не выше $n - 1$ посредством соотношения

$$\mathcal{A}(x) \equiv x^{\nu} \cdot a(x) \pmod{(x^n - 1)}. \tag{31}$$

Это сравнение определяет $a(x)$ однозначно. Так как для самодвойственного многочлена $\mathcal{A}(x)$ имеет место равенство

$$\mathcal{A}(x) = x^{2\nu} \cdot \mathcal{A}(x^{-1}),$$

то, используя соотношение (31) для $\mathcal{A}(x)$ и $\mathcal{A}(x^{-1})$, получаем соотношение (4), означающее симметричность соответствующего (см. (3)) циркулянта $A = \sum_{i=0}^{n-1} a_i T^i$. В силу (31) также имеем

$$(a(x), x^n - 1) = (\mathcal{A}(x), x^n - 1). \tag{32}$$

Очевидно, соотношение (31) вместе с (3) устанавливает биекцию множества самодвойственных многочленов $\mathcal{A}(x)$ степени 2ν ($2\nu \leqslant n - 1$) на множество симметричных циркулянтов A с условием $\nu = \max\left\{i \in \overline{1, \frac{n-1}{2}} : a_i \neq 0\right\}$, причем в силу (32) и (5)

$$\operatorname{rang} A = n - \deg(\mathcal{A}(x), x^n - 1).$$

Отсюда следует справедливость теоремы 2.

Замечание 2. Допустимые (т. е. $S_r(q, n) \neq 0$) значения ранга r симметричных циркулянтов размера n над конечным полем из q элементов, согласно теореме 1, задаются при $(n', 2) = 2$ формулой

$$r = l_1 + l_2 + 2\sum_{\substack{k|n' \\ k>2}} \pi_k \sum_{j=1}^{\varkappa_k} l_k(j),$$

где $l_k(j) \in \overline{0, m}$ и $l_1, l_2 \in \{0\} \cup \{1, 3, \ldots, (m-1)/2\}$, и при $(n', 2) = 1$ формулой

$$r = l + 2\sum_{\substack{k|n' \\ k>2}} \pi_k \sum_{j=1}^{\varkappa_k} l_k(j),$$

где $l_k(j) \in \overline{0, m}$ и либо $l \in \{0\} \cup \{1, 3, \ldots, (m-1)/2\}$ при $(2, q) = 1$, либо $l \in \{1\} \cup \{0, 2, \ldots, m/2\}$ при $(2, q) = 2$. Отсюда следует, что значения ранга $0, 1, n-1, n$ гарантированы всегда, а значения ранга $2, 3, \ldots, n-2$ являются допустимыми лишь в зависимости от арифметической структуры чисел n и q. Например, если n — нечетное простое число и $q = 2$, то

$$r = l + 2\pi_n \sum_{j=1}^{\varkappa_n} l_n(j),$$

где l и $l_n(j)$ равны 0 или 1, т. е. r принимает $2(\varkappa_n + 1)$ значений, в частности, в случае $2\pi_n = n - 1$ r принимает ровно 4 значения: $0, 1, n-1, n$.

Поступило
05.03.84

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] Berlekamp E. R. Distribution of cyclic matrices in a finite field.— Duce Math. J., 1966, v. 33, № 1, p. 45—48.
[2] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки.— М.: Связь, 1979.
[3] Копылова А. Н. Пятый Всесоюзный семинар по комбинаторному анализу.— В кн.: Комбинаторный анализ, вып. 6. М.: МГУ, 1983, с. 87—104.
[4] Виноградов И. М. Основы теории чисел.— М.: Наука, 1972.
[5] Mac Williams F. J. Orthogonal circulant matrices over a finite field and how to find them.— J. Comb. Theory, 1971, A10, № 1, p. 1—17.
[6] Byrd K. A. Vaughan T. P. Counting and constructing orthogonal circulants.— J. Comb. Theory, 1978, A24, № 1, p. 34—49.
[7] Варшамов Р. Р., Гараков Г. А. К теории самодвойственных полиномов над полем Галуа.— В кн.: Математические вопросы кибернетики и вычислительной техники. Теория информации и кодирования, Ереван, 1970, т. 6, с. 5—17.