Р. Р. ВАРШАМОВ, Г. А. ГАРАКОВ

К ТЕОРИИ САМОДВОЙСТВЕННЫХ ПОЛИНОМОВ НАД ПОЛЕМ ГАЛУА

Рассмотрим некоторое преобразование полинома $f(x)$*) m-степени над полем Галуа $GF(q)$, состоящее в замене аргумента x через $1/x$ и умножения полученной функции на x^m. В результате такого преобразования полином $f(x)$ переходит в другой полином $f^*(x) = x^m f(1/x)$, коэффициенты которого отличаются от коэффициентов первоначального полинома лишь обратным порядком их следования. Между полиномами $f(x)$ и $f^*(x)$ устанавливается, в некотором роде, принцип двойственности, заключающийся в утверждении, что полиномы $f(x)$ и $f^*(x)$ изоморфно приводимы, т. е. каждому неприводимому множителю $f(x)$ однозначно соответствует неприводимый множитель $f^*(x)$ и наоборот.

Следовательно, полином $f^*(x)$ неприводим тогда и только тогда, когда неприводим полином $f(x)$.

Особый интерес в теории приводимости представляет случай, когда $f(x) = f^*(x)$, т. е. когда полином, полученный в результате указанного преобразования, совпадает с исходным полиномом. Полиномы, удовлетворяющие этому свойству, будем называть самодвойственными. Самодвойственные полиномы, обладая особой алгебраической структурой, занимают важное место в теории кодирования, преимущественно в вопросах синтеза эффективных помехоустойчивых циклических кодов. Так, например, сравнительно недавно Дж. Месси [1] использовал самодвойственные полиномы для синтеза обратимых циклических кодов, которые с успехом могут быть применены в некоторых системах хранения и поиска данных.

В настоящей статье рассматриваются важнейшие свойства неприводимых самодвойственных полиномов, на основании чего выводится конечная формула общего числа неприводимых в поле $GF(q)$ нормированных самодвойственных полиномов степени m. Кроме того, исследуется одно квадратичное преобразование, играющее важную роль в теории синтеза неприводимых самодвойственных полиномов.

---

*) Здесь и в дальнейшем всюду рассматриваются полиномы только с ненулевым свободным членом.

§ 1. Важнейшие свойства самодвойственных полиномов над полем $GF(q)$

Приведем несколько иное и удобное для дальнейшего определение самодвойственного полинома.

Самодвойственным полиномом назовем всякий полином $f(x)$ над полем $GF(q)$, удовлетворяющий следующему условию: если α — произвольный корень $f(x)$ в некотором расширении поля $GF(q)$, то элемент $\beta = 1/\alpha$ также является его корнем, т. е. самодвойственными будем называть полиномы, удовлетворяющие соотношению $f(\alpha) = f(1/\alpha) = 0$. Покажем теперь, что для полиномов, удовлетворяющих условию $f(1) \neq 0$, эти два определения эквивалентны, то есть, что всякий полином $f(x)$ $(f(1) \neq 0)$ степени m, удовлетворяющий равенству $f(\alpha) = f(1/\alpha) = 0$ (где α — любой его корень), связан следующим тождественным соотношением:

$$f(x) = x^m f(1/x), \tag{1}$$

и наоборот.

Как уже отмечалось выше, полиномы $f(x)$ и $f^*(x)$ изоморфно приводимы. А поэтому для краткости изложения можно, не ограничивая общности, исходить из того, что полином $f(x)$ неприводим. Итак, пусть $f(x)$ неприводимый в поле $GF(q)$ полином степени m и α — некоторый его корень. Тогда, как известно, существует единственная минимальная функция для элемента $\beta = 1/\alpha$, т. е. нормированный многочлен $\lambda(x)$ наименьшей степени с коэффициентами из поля $GF(q)$ такой, что $\lambda(\beta) = 0$. Но элемент $\beta = 1/\alpha$ является корнем выражения $f(x)$, а также, согласно (1), и корнем $f^*(x)$. А это значит, что оба эти полинома одновременно делятся на минимальную функцию $\lambda(x)$ и, следовательно, могут отличаться между собой разве лишь на постоянный множитель. Таким образом, имеем

$$f(x) = \zeta x^m f(1/x) \quad (\zeta \in GF(q)). \tag{2}$$

Покажем теперь, что в соотношении (2) $\zeta = 1$. В самом деле, при $x = 1$ из тождества (2) получаем равенство $f(1) = \zeta f(1)$, или $f(1)(\zeta - 1) = 0$. Но поскольку $f(1) \neq 0$, то $\zeta - 1 = 0$ и $\zeta = 1$.

Обратное утверждение автоматически следует из тождественного соотношения (1).

Теорема 1. Степень m — любого самодвойственного полинома, удовлетворяющего условию $f(1)f(-1) \neq 0$, является четным числом, т. е. $2/m$.

Доказательство. Действительно, каждый самодвойственный полином $f(x)$ $(f(1) \neq 0)$, как это было показано, удовлетворяет тождественному соотношению (1), из которого при $x = -1$ вытекает равенство $f(-1) = (-1)^m f(-1)$ или $f(-1)(1 - (-1)^m) = 0$. Между тем, согласно условию теоремы, $f(-1) \neq 0$, следовательно,

$1-(-1)^m=0$ и $2/m$ при $2\nmid q$. Аналогичными рассуждениями теорема доказывается и для случая $2/q$.

Как легко видеть, в кольце полиномов над полем $GF(q)$ существуют всего лишь два нормированных самодвойственных неприводимых полинома, не удовлетворяющих условию теоремы 1, а именно $x+1$, $x-1$. Кроме того, в поле характеристики 2, $x+1=x-1$. Следовательно, в кольце полиномов над полем $GF(q)$ существуют всего лишь два (соответственно один, если $2/q$) нормированных самодвойственных неприводимых полинома нечетной степени $m=1$.

В дальнейшем нас будут интересовать только нормированные самодвойственные полиномы, степени которых, если это не будет специально оговорено, $m>1$.

Теорема 2. Каждый неприводимый самодвойственный полином степени m является делителем функции

$$H_m(x)=x^{q^{\frac{m}{2}}+1}-1.$$

Доказательство. Пусть α — корень полинома $f(x)$ степени m в некотором расширении основного поля $GF(q)$. Тогда α, α^q, $\cdots$ $\cdots$, $\alpha^{q^{m-1}}$ суть все его m корней. Но поскольку полином $f(x)$ — самодвойственный, то элемент $\beta=1/\alpha$ также является его корнем, следовательно, $\beta=\alpha^{q^u}$ $(u\leqslant m-1)$ и

$$H_{2u}(\alpha)=0. \tag{3}$$

Соотношение (3) позволяет сделать вывод, что полином $f(x)$, так как он неприводимый, является делителем функции $x^{q^{u+1}}-1$. Между тем, всякий нормированный полином m-ой степени, неприводимый в поле $GF(q)$, делит выражение $x^{q^m-1}-1$, но не является делителем никакой другой функции вида $x^{q^{m'}-1}-1$, если $m'<m$. А поскольку $2/m$, то ясно, что величина u, фигурирующая в соотношении (3), равна $\frac{m}{2}$. Теорема доказана.

Теорема 3. Каждый простой делитель $g(x)$ функции $H_m(x)$ является самодвойственным полиномом и имеет степень n/m, $2+\frac{m}{n}$.

Доказательство. Пусть α — корень $g(x)$. Поскольку $g(x)\,|\,H_m(x)$, то $H_m(\alpha)=0$ и $\alpha^{q^{\frac{m}{2}}}=1/\alpha$. Но если α — корень $g(x)$, то, следовательно, и $\alpha^{q^{\frac{m}{2}}}=1/\alpha$ также является корнем $g(x)$, а это означает, что полином $g(x)$ самодвойственный.

Далее, ввиду $H_m(x)\,|\,x^{q^m-1}-1$ ясно, что $H_m(x)$ может делиться лишь на простые функции, степени которых являются делителями числа m. Следовательно, n/m. Кроме того, как легко понять, согласс-

но теореме 2, выражение $q^{\frac{m}{2}}+1$ должно делиться на $q^{\frac{n}{2}}+1$, а потому $2+\frac{m}{n}$. Этим завершается доказательство теоремы 3.

Теоремы 2 и 3 приводят к следующим важным фактам.

Следствие 1. Для числа l любого сомножителя выражения $q^{\frac{m}{2}}+1$ $(2/m)$, не являющегося одновременно делителем никакого меньшего числа вида q^s+1, существует в точности $m^{-1}\varphi(l)$*) неприводимых самодвойственных полиномов степени m, показатель**) которых равен l.

Следствие 2. Наибольший из показателей, к которому принадлежат неприводимые самодвойственные полиномы степени m, равен $q^{\frac{m}{2}}+1$. Из этого утверждения, между прочим, следует, что не существует примитивных самодвойственных полиномов четной степени, за исключением полинома x^2+x+1, примитивного в поле $GF(2)$. Однако самодвойственные полиномы, принадлежащие максимально возможному показателю $q^{\frac{m}{2}}+1$, в теории самодвойственных полиномов, как легко понять, играют аналогичную роль примитивных элементов поля. А поэтому естественным было бы называть такие полиномы псевдопримитивными или просто примитивными самодвойственными полиномами.

Следствие 3. Функция $H_m(x)$ делится на любой простой нормированный самодвойственный полином, степень которого n удовлетворяет условие $n2=m(2+\delta)$. Стало быть, если обозначить через $\Phi_n(x)$ произведение всевозможных неприводимых нормированных самодвойственных полиномов степени n, то тогда, очевидно, следствие 3 можно было бы выразить в следующей краткой записи:

$$H_m(x)=(x^{1+\varepsilon_q}-1)\prod_{\substack{n\mid m\\ 2+\frac{m}{n}}}\Phi_n(x), \tag{4}$$

где $\varepsilon_q=\dfrac{1-(-1)^q}{2}$.

§ 2. Число неприводимых в поле $GF(q)$ нормированных самодвойственных полиномов степени m

Обозначим через $S_q(m)$ общее число неприводимых в поле $GF(q)$ нормированных самодвойственных полиномов степени m. Прежде чем приступить к выводу развернутой формулы для функции $S_q(m)$, предварительно докажем следующую лемму.

---

*) $\varphi(n)$ — мультипликативная функция Эйлера.

**) Показателем полинома $f(x)$ называется наименьшее натуральное число h, удовлетворяющее условию $f(x)\mid x^h-1$.

Лемма 1. Для любого натурального числа n

$$\sum_{u|n} \mu(2u) = \begin{cases} 0, & \text{если } n \neq 2^h, \\ -1, & \text{если } n = 2^h, \end{cases}$$

где $\mu(u)$ — функция Мёбиуса.

Доказательство. Имеем $n = 2^h N(2+N)$ и

$$\sum_{u|n} \mu(2u) = \sum_{\substack{u|n \\ 2+n}} \mu(2)\mu(u) = -\sum_{u|N} \mu(u).$$

Но $\sum_{u|N} \mu(u) = 0$ и только при $N=1$, $\sum_{u|N} \mu(u) = 1$, так, что $\sum_{u|N} \mu(2u) = 0$ при $n \neq 2^h$ и $\sum_{u|N} \mu(2u) = -1$ при $n = 2^h$. Лемма доказана.

Приступим теперь к доказательству основной теоремы, которое подобно классическому доказательству формулы обращения для функции $\mu(u)$.

Теорема 4. Для любого натурального m имеет место следующее равенство:

$$S_q(m) = \frac{-1}{m} \sum_{2uv=m} \mu(2u)(q^v - \varepsilon_q). \tag{5}$$

Доказательство. Согласно следствию 3, выражение $H_m(x)$ делится на все неприводимые самодвойственные полиномы степени n, где $n\delta = m(2+\delta)$. Кроме того, полином $H_m(x)$ — сепарабельный, а поэтому степень его $q^{\frac{m}{2}}+1$ равна сумме степеней всех различных неприводимых самодвойственных полиномов, на которые $H_m(x)$ разлагается. Среди этих полиномов находится также и полином нечетной степени $x+1$, а в случае $2+q$ еще и $x-1$. Исключив эти две (соответственно одну) функции из рассмотрения, мы получим

$$q^{\frac{m}{2}} - \varepsilon_q = \sum_{\substack{u\delta=m \\ 2+\delta}} u S_q(u).$$

Пусть теперь d какой-нибудь делитель числа $\frac{m}{2}$, тогда

$$q^{\frac{m}{2d}} - \varepsilon = \sum_{\substack{u\delta=\frac{m}{d} \\ 2+\delta}} u S_q(u). \tag{6}$$

Умножив обе части (6) на $\mu(2d)$ и, просуммировав относительно всех делителей d числа $\frac{m}{2}$, получим

$$\sum_{d \left| \frac{m}{2} \right.} \mu(2d)(q^{\frac{m}{2d}} - \varepsilon_q) = \sum_{d \left| \frac{m}{2} \right.} \sum_{\substack{u\delta=\frac{d}{m} \\ 2+\delta}} \mu(2d) u S_q(u). \tag{7}$$

Суммируя в правой части (7) сначала по d, а затем по u, учитывая, что $\frac{m}{ud} = \delta$ нечетное число, так что d считая делителем $\frac{m}{u}$, получим

$$\sum_{d \mid \frac{m}{2}} \mu(2d)\,(q^{\frac{m}{2d}} - \varepsilon_q) = \sum_{\substack{u=1 \\ 2 \nmid u}}^{\frac{m}{2}} u\, S_q(u) \sum_{d \mid \frac{m}{u}} \mu(2d). \tag{8}$$

Но, согласно лемме 1, $\sum_{d \mid \frac{m}{u}} \mu(2d) = 0$, за исключением случая, когда $\frac{m}{u} = 1$, т. е. при $u = m$, $\sum_{d \mid \frac{m}{u}} \mu(2d) = -1$.

Следовательно, в правой части (8) только одно слагаемое внешней суммы не равно нулю, а поэтому

$$\sum_{d \mid \frac{m}{2}} \mu(2d)\,(q^{\frac{m}{2d}} - \varepsilon_q) = -mS_q(m),$$

куда получаем соотношения

$$S_q(m) = \frac{-1}{m} \sum_{d \mid \frac{m}{2}} \mu(2d)\,(q^{\frac{m}{2d}} - \varepsilon_q),$$

или

$$S_q(m) = \frac{-1}{m} \sum_{2uv=m} \mu(2u)\,(q^v - \varepsilon_q),$$

являющееся содержанием теоремы 4.

§ 3. Квадратичные преобразования и синтез неприводимых самодвойственных полиномов

Пусть дан произвольно полином $f(x) = \sum_{u=0}^{m} a_u x^u$ $(a_0 \neq 0)$ степени m с коэффициентами из поля $GF(q)$. Введем в рассмотрение следующее квадратичное преобразование над $f(x)$, состоящее в замене аргумента x через $\frac{x}{1+x^2}$ и умножения полученной функции на $(1+x^2)^m$. В результате такого преобразования первоначальный полином $f(x)$ степени m перейдет в другой полином $\bar{f}(x)$ степени $2m$, который в удобной записи примет следующий вид:

$$\bar{f}(x) = \sum_{u=0}^{m} a_u x^u (1+x^2)^{m-u}. \tag{9}$$

При этом, как легко заметить, выполняется следующее важное условие: если $f(x) = f_1(x)\ f_2(x)$, то $\widetilde{f}(x) = \widetilde{f}_1(x)\widetilde{f}_2(x)$. Кроме того, полином $\widetilde{f}(x)$ степени $2m > 1$, при любой функции $f(x)$, является самодвойственным полиномом, а поэтому, согласно (1), $\widetilde{f}(x) = \widetilde{f}^*(x)$.

В самом деле,

$$\widetilde{f}^*(x) = x^{2m}\,\widetilde{f}(1/x) = x^{2m}\left(1+\frac{1}{x^2}\right)^m f\left(\frac{\frac{1}{x}}{1+\frac{1}{x^2}}\right) = (1+x^2)^m f\left(\frac{x}{1+x^2}\right)$$

и

$$\widetilde{f}^*(x) = \widetilde{f}(x).$$

Эти два обстоятельства, как в дальнейшем выяснится, играют важную роль в теории синтеза неприводимых самодвойственных полиномов. Они позволяют строить непосредственно (практически) любой неприводимый самодвойственный полином заданной степени в явном виде. Настоящий параграф посвящен решению этой проблемы. Однако, прежде чем приступить к изложению материала, сделаем следующее замечание. Ради простоты изложения и большей наглядности в этом параграфе мы ограничимся рассмотрением поля характеристики 2, т. е. случаем, который является наиболее интересным и важным в приложении. Целесообразность такого выбора обуславливается еще и тем обстоятельством, что почти все полученные здесь результаты без особого труда могут быть распространены и на случай поля с более высокой характеристикой.

Введем в рассмотрение функцию $\sigma_m(x, \delta) = \delta + \sum_{u=0}^{m-1} x^{2^u}$, полагая $\sigma_0(x, \delta) = \delta$, и укажем на ряд ее важных свойств и особенностей.

Свойство 1. Для любой пары натуральных чисел m и $n \leqslant m$ имеет место следующее тождественное равенство:

$$\sigma_m(x, \delta) = \sum_{u=0}^{k-1} \sigma_n(x, \delta')\, 2^{un} + \sigma_r(x, \delta - k\delta')^{2^{kn}}, \qquad (10)$$

где k и r связаны соотношением $m = nk + r\ (k > 0)$, а δ и δ' произвольные элементы основного поля.

Справедливость этого утверждения вытекает непосредственно из самого определения функции $\sigma_m(x, \delta)$. Действительно, полагая $m \geqslant n$, мы получим

$$\sigma_m(x, \delta) = \sigma_n(x, \delta') + x^{2^n} + \cdots + x^{2^{m-1}} + \delta - \delta'.$$

Откуда, в силу тождества Галуа, будем иметь

$$\sigma_m(x, \delta) = \sigma_n(x, \delta') + \sigma_{m-n}(x, \delta - \delta')^{2^n}\ (k = 1).$$

Если $k>1$ и, следовательно, $m-n>n$, то, аналогично рассуждая, взяв в качестве исходных функций $\sigma_{m-n}(x, \delta-\delta')$ и $\sigma_n(x, \delta')$, получим

$$\sigma_m(x, \delta)=\sigma_n(x, \delta')+\sigma_n(x, \delta')2^n+\sigma_{m-2n}(x, \delta-2\delta')2^{2n} \quad (k=2).$$

Если же $k>2$, то, повторяя этот процесс соответствующее число раз, в конце концов получим интересующее нас равенство (10). Основываясь на (10), можно сделать следующий вывод.

Свойство 2. Для того чтобы функция $\sigma_m(x, \delta)$ делилась на выражение $\sigma_n(x, \delta')$, необходимо и достаточно, чтобы выполнялись следующие два условия: $n|m$ и $\frac{m}{n}\delta' \equiv \delta \pmod 2$. Из сказанного, ввиду $F_m(x, \delta)|\sigma_m(x, \delta)$, автоматически вытекают тождественные соотношения

$$\sigma_m(x, 1)=\lambda_1(x)\prod_{\substack{n|m \\ 2\nmid \frac{m}{n}}} F_n(x, 1), \tag{11}$$

$$\sigma_m(x, 0)=\lambda_2(x)\prod_{n|m} F_n(x, 0)\left(\prod_{n\left|\frac{m}{2}\right.} F_n(x, 1)\right), \tag{12}$$

где $F_n(x, \delta)$ означает произведение всевозможных неприводимых полиномов степени n, коэффициент при x^{n-1} у которых равен δ, а $\lambda_1(x)$ и $\lambda_2(x)$ — некоторые целые рациональные функции над полем $GF(2)$. В дальнейшем будет показано, что $\lambda_1(x)=\lambda_2(x)\equiv 1$, а поэтому два последних равенства могут быть записаны в виде

$$\sigma_m(x, 1)=\prod_{\substack{n|m \\ 2\nmid \frac{m}{n}}} F_n(x, 1) \tag{13}$$

и

$$\sigma_m(x, 0)=\prod_{n|m} F_n(x, 0)\left(\prod_{n\left|\frac{m}{2}\right.} F_n(x, 1)\right). \tag{14}$$

Действительно, из (11) следует, что степень $\lambda_1(x)$ равна

$$2^{m-1}-\sum_{\substack{n|m \\ 2\nmid \frac{m}{n}}} stF_n,$$

где stF_n — степень полинома $F_n(x, 1)$.

Но $\sum\limits_{\substack{n|m \\ 2\nmid \frac{m}{n}}} stF_n=2^{m-1}$, так как, согласно [2],

$$st\,F_n = {}^1/_2 \sum_{\substack{u|n \\ 2+u}} \mu(u)\, 2^{\frac{n}{u}} \quad \text{и} \quad {}^1/_2 \sum_{\substack{n|m \\ 2+\frac{m}{n}}} \sum_{\substack{u|n \\ 2+u}} \mu(u)\, 2^{\frac{n}{u}} = 2^{m-1}.$$

Следовательно, степень $\lambda_1(x)$ равна нулю и $\lambda_1(x) \equiv 1$. Аналогичными рассуждениями, учитывая, что степень полинома $F_n(x, 0)$ определяется выражением $\sum_{u|n} \mu(u)\, 2^{\frac{n}{u}} - {}^1/_2 \sum_{\substack{u|n \\ 2+u}} \mu(u)\, 2^{\frac{n}{u}}$, можно показать, что и $\lambda_2(x) \equiv 1$.

Свойство 3. Для любого натурального числа n имеет место следующее соотношение:

$$\tilde{\sigma}_m(x, \delta) = \begin{cases} \dfrac{x}{1+x}\,(x^{2^m-1} - 1), & \text{если } \delta = 0. \\ \dfrac{1}{1+x}\, H_{2m}(x), & \text{если } \delta = 1. \end{cases} \tag{15}$$

В самом деле, согласно определению,

$$\tilde{\sigma}_m(x, \delta) = \sum_{u=0}^{m-1} x^{2^u} (1 + x^{2^u})^{2^{m-1} - 2^u} + \delta\,(1 + x^{2^u})^{2^{m-1}}.$$

Перепишем полученное выражение в несколько ином виде:

$$\tilde{\sigma}_m(x, \delta) = \sum_{u=0}^{m-1} x^{2^u} \prod_{i=1}^{m-u-1} (1 + x^{2^{m-i}}) + \delta + \delta x^{2^m},$$

Далее, как легко понять, $\prod_{i=1}^{m-u-1} (1 + x^{2^{m-i}}) = \sum_{v=0}^{2^{m-u-1}-1} x^{2^u+1}\, v$,

а поэтому

$$\tilde{\sigma}_m(x, \delta) = \sum_{u=0}^{m-1} \sum_{v=0}^{2^{m-u-1}-1} x^{v 2^{u+1} + 2^u} + \delta + \delta x^{2^m}$$

откуда

$$\tilde{\sigma}_m(x, \delta) = \sum_{u=1}^{2^m-1} x^u + \delta + \delta x^{2^m},$$

но это и есть по существу соотношение (15).

Приступим теперь к изложению основного результата настоящего параграфа, который заключается в следующем альтернативном утверждении.

Теорема 5. Пусть дана произвольно простая функция $f(x)$ степени m. Тогда самодвойственный полином $\tilde{f}(x)$ степени $2m$ либо не-

приводим, либо разлагается на произведение двух двойственных неприводимых полинома степени m каждый. Причем для того, чтобы полином $\bar{f}(x)$ был неприводим, необходимо и достаточно, чтобы выполнялось следующее условие: $f^*(0)' \neq 0$.

Доказательство. Приступая к доказательству теоремы 5, покажем сначала, что для любого натурального числа m имеет место следующее тождественное соотношение:

$$\bar{F}_m(x, 1) = \Phi_{2m}(x). \tag{16}$$

Предварительно рассмотрим случай, когда m является простым числом. Тогда наши рассуждения разобьются на два случая в зависимости от того, будет ли простое число m четным или нечетным. В случае нечетного m, согласно (13), будем иметь

$$\sigma_m(x, 1) = F_m(x, 1)(x + 1)$$

и в силу (15)

$$\bar{\sigma}_m(x, 1) = \frac{1}{1+x} H_{2m}(x) = \bar{F}_m(x, 1)(x^2 + x + 1).$$

Опираясь далее на формулу (4) и учитывая, что m является нечетным простым числом, получим

$$\frac{1}{1+x} H_{2m}(x) = (x^2 + x + 1)\, \Phi_{2m}(x)$$

и, стало быть,

$$\bar{F}_m(x, 1) = \Phi_{2m}(x).$$

В случае $m = 2$; 1 будем иметь

$$F_2(x, 1) = x^2 + x + 1, \quad \bar{F}_2(x, 1) = \Phi_4(x)$$

и

$$F_1(x, 1) = x + 1, \quad \bar{F}_1(x, 1) = \Phi_2(x).$$

Таким образом, показано, что соотношение (16) имеет место для произвольного простого числа m, а также и при $m = 1$.

Рассмотрим теперь случай, когда m является произведением $(t > 0)$ равных или неравных простых сомножителей. При $t = 1$ справедливость (16) доказана. Примем, что оно имеет место для всех чисел, меньше $t\,(t > 1)$, т. е. справедливо для всякого числа m, представимого в виде произведения самое большее $t - 1$ равных или неравных простых сомножителей.

Перепишем формулу (13) в следующем виде:

$$\sigma_m(x, 1) = F_m(x, 1) \prod_{\substack{n|m \\ 2+\frac{m}{n}}}' F_n(x, 1), \tag{17}$$

где произведение Π' распространяется по всем $\left(2+\frac{m}{n}\right)$ собственным делителям числа m.

Проведя в (17) соответствующее преобразование, с учетом (15) и (4), получим

$$\prod_{\substack{n|m \\ 2+\frac{m}{n}}}' \Phi_{2n}(x) = \overline{\widetilde{F}}_m(x, 1) \prod_{\substack{n|m \\ 2+\frac{m}{n}}} \overline{\widetilde{F}}_n(x, 1).$$

Далее, поскольку всякий собственный делитель числа m представим в виде произведения, меньшего чем t, равных или неравных простых делителей, то, согласно допущению, в произведении $\prod_{\substack{n|m \\ 2+\frac{m}{n}}} \overline{\widetilde{F}}_n(x, 1)$ выражение $\overline{\widetilde{F}}_n(x, 1)$ можно будет заменить через $\Phi_{2n}(x)$ и таким образом получить соотношение

$$\prod_{\substack{n|m \\ 2+\frac{m}{n}}} \Phi_{2n}(x) = \overline{\widetilde{F}}_m(x, 1) \prod_{\substack{n|m \\ 2+\frac{m}{n}}}' \Phi_{2n}(x),$$

из которого автоматически будет вытекать соотношение (16). Таким образом, можно считать, что (16) имеет место при любом натуральном m. А это означает, что данное квадратичное преобразование переводит всякий неприводимый полином $f(x)$ степени m, коэффициент при x^{m-1} у которого равен 1, в неприводимый самодвойственный полином $\overline{\widetilde{f}}(x)$ степени $2m$. При том, как это из (16) также следует, любой неприводимый самодвойственный полином четной степени может быть получен с помощью указанного преобразования. Иными словами, можно утверждать, что для всякого неприводимого самодвойственного полинома $g(x)$ степени $2m$ найдется, и притом единственный, неприводимый полином $f(x)$ степени m, удовлетворяющий условию $\overline{\widetilde{f}}(x) = g(x)$. Отсюда, в частности, следует, что для того чтобы самодвойственный полином $\widetilde{f}(x)$ степени $2m$ был неприводим, необходимо и достаточно, чтобы

$$f^*(0)' \neq 0. \tag{18}$$

Для завершения доказательства теоремы 5 остается показать, что для всех полиномов $f(x)$ степени m, не удовлетворяющих условие (18), выражение $\overline{\widetilde{f}}(x)$ распадается на произведение двух двойственных не-

приводимых полиномов, с одинаковыми степенями, равными m. Для этого, очевидно, достаточно будет показать, что при любом натуральном m выполняется соотношение

$$\tilde{F}_m(x, 0) = F_m(x)\,\Phi_m(x)^{-1}, \tag{19}$$

где $F_m(x)$ означает произведение всевозможных неприводимых полиномов степени m. Аналогично предыдущему рассмотрим вначале случай, когда m является простым нечетным числом. Тогда, согласно (14), будем иметь

$$\sigma_m(x, 0) = x\,F_m(x, 0)$$

и в силу (15) и (4) окончательно получим

$$\frac{x}{1+x}(x^{2^m-1} - 1) = x\,\tilde{F}_m(x, 0),$$

т. е.

$$\tilde{F}_m(x, 0) = F_m(x)\,\Phi_m(x)^{-1}.$$

Непосредственной проверкой легко убедиться, что соотношение (19) справедливо для $m = 2$, $m = 1$ и, следовательно, оно имеет место для любого простого числа m, а также и при $m = 1$.

Рассмотрим теперь случай, когда m является произведением $t\,(t > 0)$ равных или неравных простых сомножителей. При $t = 1$ справедливость (19) доказана. Примем, что оно имеет место для всех чисел n, представимых в виде произведения самое большее $t - 1$ простых сомножителей. Тогда, переписав формулу (14) в виде

$$\sigma_m(x, 0) = \bar{F}_m(x, 0) \prod_{n|m}{}' F_n(x, 0) \left(\prod_{n \left| \frac{m}{2} \right.} F_n(x, 1) \right)$$

и проводя соответствующее преобразование с учетом (15), (4), (16) и теоремы 1, получим

$$\frac{x}{1+x}(x^{2^m-1} - 1) = \bar{F}_m(x, 0) \prod_{n|m}{}' \bar{F}_n(x, 0) \left(\prod_{n \left| \frac{m}{2} \right.} \bar{F}_n(x, 1) \right) =$$

$$= \bar{F}_m(x, 0) \prod_{n|m}{}' F_n(x)\,\Phi_n(x)^{-1} \left(\prod_{n \left| \frac{m}{2} \right.} \Phi_{2n}(x) \right),$$

откуда

$$F_m(x) = \bar{F}_m(x, 0)\,\Phi_m(x)$$

или окончательно

$$\tilde{F}_m(x, 0) = F_m(x)\,\Phi_m(x)^{-1}.$$

Полученный результат позволяет заключить, что формула (19) имеет место для любого натурального m. Тем самым теорема 5 полностью доказана.

Из теоремы 5, в частности, вытекает, что общее число всех различных неприводимых самодвойственных полиномов степени $2m$ совпадает с общим числом различных неприводимых полиномов степени m, удовлетворяющих условию $f^*(0)' \neq 0$. В работе [2], как уже отмечалось, приводится конечная формула общего числа таких полиномов. Следовательно, имеется возможность косвенным путем получить рассмотренную во втором параграфе формулу количества неприводимых самодвойственных полиномов и тем самым частично проверить (5). Кроме того, сопоставляя между собой (16) и (19), будем иметь следующее рекуррентное соотношение: разность между удвоенным числом всех неприводимых самодвойственных полиномов степени $2m$ и количеством всех неприводимых полиномов степени m совпадает с общим числом неприводимых самодвойственных полиномов степени m.

Р. Р. ВАРШАМОВ, Г. А. ГАРАКОВ

ГАЛУИАЗЫ ДАННЫХ ВРА ИНКВАЗИКАКИХ БАЗМАНДАМНЕРЫ ТЕСНОТНЫЙ ВЕРХНЕБЕРЗАЛ

Аннотация

Հոդվածում տրվում է ինքնաերկակի բազմանդամների կարևորագույն սպեցիֆիկ հատկությունների նկարագրությունը։ Ստացված արդյունքների հիման վրա դուրս է բերվում $GF(q)$ դաշտում բոլոր չբերվող m աստիճանի նորմավորված ինքնաերկակի բազմանդամների վերջավոր բանաձևը։

Բացի դրանից, հետազոտվում է մի քառակուսային ձևափոխություն, որը կատարում է կարևոր դեր չբերվող ինքնաերկակի բազմանդամների սինթեզի տեսության մեջ։

ЛИТЕРАТУРА

1. *J. Massey.* Reversible Codes Information and Control, vol. 7, № 3, September, 1964.
2. *Р. Р. Варшамов.* К математической теории кодов, Докторская диссертация. ИАТ АН СССР, 1966.