Math-Net.Ru

Общероссийский математический портал

Д. М. Ермилов, Количество полиномиальных преобразований максимального периода над кольцами Галуа нечетной характеристики, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 4, 85–100

DOI: <https://doi.org/10.4213/mvk271>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.172.240.79

26 апреля 2023 г., 14:48:59

**Количество полиномиальных преобразований
максимального периода
над кольцами Галуа нечетной характеристики
Д. М. Ермилов**

ООО «Центр сертификационных исследований», Москва

Получено 18.IV.2018

Аннотация. Пусть $R = GR(q^n, p^n)$ — кольцо Галуа мощности q^n и характеристики p^n , где $q = p^m$, $m, n > 1$. Пусть последовательность $U = \{u_i\}$ определяется соотношением $u_{i+1} = f(u_i)$, $i \in \mathbb{N}_0$, и f — полиномиальное преобразование кольца R . Ранее было показано, что максимально возможный период последовательности U равен $q(q-1)p^{n-2}$. Здесь найдено число полиномиальных преобразований максимального периода над кольцами Галуа при $p \neq 2$.

Ключевые слова: кольца Галуа, нелинейные генераторы, псевдослучайные последовательности, полиномиальный конгруэнтный генератор

The number of maximal period polynomial mappings over the Galois fields of odd characteristics

D. M. Ermilov

Certification Research Center, LLC, Moscow

Abstract. Let $R = GR(q^n, p^n)$ be a Galois ring of cardinality q^n and characteristics p^n , where $q = p^m$, $m, n > 1$. Let the sequence $U = \{u_i\}$ is defined by equations $u_{i+1} = f(u_i)$, $i \in \mathbb{N}_0$, and f be a polynomial mapping of the ring R . It was proved earlier that the maximal possible period of U equals $q(q-1)p^{n-2}$. Here we find the number of polynomial mappings over R having maximal possible periods for $p \neq 2$.

Key words: Galois rings, nonlinear generators, pseudorandom sequences, polynomial congruence generator

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 4, pp. 85–100 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

Введение

Один из возможных способов генерации *псевдослучайных последовательностей* (ПСП) состоит в использовании *полиномиальных генераторов* (ПГ) над некоторым кольцом R . Напомним, что ПГ называют автомат с последовательностью состояний вида

$$u_{i+1} = f(u_i), \quad i = 0, 1, \dots, \quad (1)$$

где $u_0 \in R$ — начальное заполнение ПГ, f — некоторая полиномиальная функция над R . Выходная последовательность ПГ совпадает с его последовательностью состояний. Если f — аффинная функция, то ПГ называют *линейным генератором* (ЛГ).

Наибольший интерес представляют те полиномиальные преобразования, при использовании которых последовательность (1) имеет максимальный возможный период, равный мощности кольца R . Такие полиномиальные преобразования называют *полноцикловыми* или *транзитивными*.

В. С. Анашин описал все конечные коммутативные кольца [1, 2], над которыми существуют транзитивные полиномиальные преобразования. Из его результатов следует, что за исключением случаев, не представляющих практического интереса, транзитивные полиномиальные преобразования существуют над конечными полями и кольцами вычетов. Свойства транзитивных полиномов над кольцами вычетов подробно изучил М. В. Ларин [3]. Он получил критерий транзитивности полинома над кольцом вычетов и нашел количество транзитивных полиномиальных преобразований над кольцами вычетов. ПГ и ЛГ над кольцами вычетов и кольцами Галуа будем называть *полиномиальными конгруэнтными генераторами* (ПКГ) и *линейными конгруэнтными генераторами* (ЛКГ).

Периодические свойства выходных последовательностей (1) ПКГ над кольцами Галуа, отличными от конечных полей и колец вычетов, изучались в [4]. Из результатов указанной работы следует, что наибольший период последовательности (1) над кольцом $GR(q^n, p^n)$ равен $q(q-1)p^{n-2}$, $n \geq 2$. Полиномы с таким свойством названы *полиномами с максимальной длиной цикла*, или *МДЦ-полиномами*. Преобразования, индуцированные указанными полиномами, будем называть *МДЦ-полиномиальными преобразованиями*.

Периодические свойства МДЦ-полиномов изучались в [5]. Алгоритм построения МДЦ-полиномов, а также ряд алгоритмов, полезных при использовании ПКГ над кольцами Галуа в качестве датчика ПСП, предложены в [6, 7].

Верхняя граница периодов выходных последовательностей ПКГ над кольцами Галуа–Эйзенштейна получена О. А. Козлитиним в [8].

Наиболее общий случай рассмотрел В. Е. Викторенков в [9], где изучены общие свойства графов полиномиальных преобразований над конечными коммутативными кольцами с единицей. Периодические свойства многомерных полиномиальных преобразований над кольцами вычетов изучал Д. А. Пронькин, частные результаты получены Н. Г. Парватовым [10].

Насколько известно автору, вопрос о количестве МДЦ-полиномиальных преобразований над кольцами Галуа, отличными от конечных полей и колец вычетов, ранее не рассматривался.

В настоящей работе найдено количество МДЦ-полиномиальных преобразований над кольцами Галуа нечетной характеристики. Случай четной характеристики планируется рассмотреть в одной из следующих работ.

1. Постановка задачи и обозначения

Пусть $R = GR(q^n, p^n)$ — кольцо Галуа мощности q^n и характеристики p^n , где $q = p^m$, $m > 1$, $n > 1$. Пусть $J = pR$ — радикал кольца R и $R_i = R/J^i$, $i \in \overline{1, n}$ (см., например, [11]).

Введем естественные эпиморфизмы колец

$$\phi_i: R \rightarrow R_i$$

для $i \in \overline{1, n}$, которые естественным образом продолжаются до эпиморфизмов колец многочленов

$$\widehat{\phi}_i: R[x] \rightarrow R_i[x].$$

В случаях когда это не приводит к противоречиям, будем говорить о свойствах полинома $f \in R[x]$ над кольцом R_k , $k \leq n$, подразумевая свойства полинома $\widehat{\phi}_k(f)$.

Образ элемента $a \in R$ (полинома $f \in R[x]$) под действием эпиморфизма ϕ_1 ($\widehat{\phi}_1$) обозначим через $\bar{a}$ (соответственно $\bar{f}$).

Пусть $G_{f,R}$ — граф полиномиального преобразования кольца R , задаваемого полиномом $f \in R[x]$. Множество вершин этого графа состоит из элементов кольца R , и пара $(a, b) \in R^2$ принадлежит множеству дуг графа $G_{f,R}$ в том и только том случае, когда $f(a) = b$. В [4] показано, что длина цикла в графе $G_{f,R}$ не превосходит $q(q-1)p^{n-2}$. Напомним, что полиномы, для которых достигается данная оценка, называются *полиномами с максимальной длиной цикла*, или *МДЦ-полиномами*.

Введем понятие *p-показателя* элемента $a \in R$: $\nu_p(a) = \max\{k: a \in J^k, k \leq n\}$; его естественным обобщением является понятие *p-показателя* $\nu_p(f)$ полинома $f \in R[x]$ как минимума *p-показателей* его коэффициентов. Через $\nu_p^{\max}(f)$ обозначим максимум *p-показателей* ненулевых коэффициентов полинома f .

В дальнейшем нам потребуется доказанный в [5] критерий того, что полином индуцирует МДЦ-полиномиальное преобразование. Критерий, приведенный в теореме 1, является аналогом критерия транзитивности полиномов над кольцами вычетов, предложенного М. В. Лариным в [3].

Теорема 1 ([5]). Пусть $R = GR(q^n, p^n)$, $q \neq p$, $n \geq 3$ при $p \neq 2$, $n \geq 4$ при $p = 2$ и $f \in R[x]$. Полином f индуцирует МДЦ-полиномиальное преобразование R тогда и только тогда, когда

- 1) полином f индуцирует МДЦ-полиномиальное преобразование R_3 и $p \neq 2$,
- 2) полином f индуцирует МДЦ-полиномиальное преобразование R_4 и $p = 2$.

Введем функции

$$\alpha(i) = [i/q] + [i/q^2] + \dots,$$

где $[c]$ — целая часть числа c , и

$$\beta(k) = \min\{i: \alpha(i) \geq k\}.$$

Например, $\alpha(0) = 0$, $\alpha(q) = 1$ и $\alpha(tq) = t$ при $t < q$.

Будем использовать следующую теорему А. А. Нечаева из [12] о представлении полиномиальных преобразований над примарным конечным коммутативным локальным кольцом главных идеалов $\mathfrak{R}$. Обозначим через $J(\mathfrak{R})$ радикал кольца $\mathfrak{R}$, а мощность поля $\mathfrak{R}/J(\mathfrak{R})$ через ϱ . Пусть $\pi \in J(\mathfrak{R}) \setminus J^2(\mathfrak{R})$. Положим $\Upsilon(x) = x^\varrho - x$ и определим последовательность многочленов

$$\Upsilon_0(x) = \Upsilon(x), \quad \Upsilon_t(x) = \Upsilon_{t-1}^\varrho(x) - \pi^{\varrho^t-1} \Upsilon_{t-1}(x), \quad t = 1, 2, \dots$$

Для произвольного $i \in \mathbb{N}$ положим

$$\Phi_i(x) = \Upsilon_0(x)^{i_0} \cdot \Upsilon_1(x)^{i_1} \cdot \dots \cdot \Upsilon_h(x)^{i_h},$$

где числа $i_1, \dots, i_h$ являются разрядами ϱ -ичного представления натурального числа i : $i = i_0 + i_1\varrho + \dots + i_h\varrho^h$, $0 \leq i_t \leq \varrho-1$, $t = 0, 1, \dots, h$.

Теорема 2 ([12]). Пусть $\mathfrak{R}$ — конечное коммутативное локальное кольцо главных идеалов. Произвольное полиномиальное преобразование g кольца $\mathfrak{R}$ может быть представлено полиномом вида

$$g(x) = g_0(x) + g_1(x)\Phi_1(x) + \dots + g_{m-1}(x)\Phi_{m-1}(x), \quad (2)$$

где $\deg g_i < \varrho$ для $i = 0, 1, \dots, m-1$, $m = \beta(n)/\varrho$, n — индекс нильпотентности идеала $J(\mathfrak{R})$. При условии (2) преобразование g тождественно нулевое тогда и только тогда, когда выполняются соотношения

$$\nu_p(g_i) \geq n - \alpha(\varrho^i), \quad i = 0, 1, \dots, m-1. \quad (3)$$

Теорема 2 позволяет построить однозначное соответствие между полиномиальными преобразованиями и соответствующими им *приведенными полиномами*.

Следствие 2.1. Пусть $\mathfrak{R}$ — конечное коммутативное локальное кольцо главных идеалов. Произвольное полиномиальное преобразование g кольца $\mathfrak{R}$ может быть однозначно представлено полиномом вида

$$g(x) = g_0(x) + g_1(x)\Phi_1(x) + \cdots + g_{m-1}(x)\Phi_{m-1}(x), \quad (4)$$

где $\deg g_i < \varrho$ и p -показатель коэффициентов многочлена g_i меньше $n - \alpha(\varrho i)$ ($\nu_p^{\max}(g_i) < n - \alpha(\varrho i)$) для $i = 0, 1, \dots, m-1$, $m = \beta(n)/q$, n — индекс нильпотентности идеала $J(\mathfrak{R})$.

Полиномы над кольцом $\mathfrak{R}$, удовлетворяющие условиям следствия 2.1, будем называть *приведенными полиномами*. Для удобства изложения будем отождествлять приведенные полиномы и соответствующие им полиномиальные преобразования.

Будем использовать следствие 2.1 в частном случае колец Галуа вида $GR(q^n, p^n)$ при $n = 2, 3$. При $n = 2$ любое полиномиальное преобразование g однозначно задается приведенным полиномом

$$g(x) = g_0(x) + g_1(x)\Phi_1(x),$$

при $n = 3$ — приведенным полиномом

$$g(x) = g_0(x) + g_1(x)\Phi_1(x) + g_2(x)\Phi_1^2(x),$$

где $\nu_p^{\max}(g_i) < n - i$, $\varrho = q$ и $\Phi_1(x) = \Upsilon_0(x) = x^q - x$.

Производные многочленов из кольца $R[x]$ определим стандартным образом (см. [13]).

Следствие 2.2. Пусть $R = GR(q^n, p^n)$, $n = 2, 3$, и $t \in R[x]$ — тождественно нулевое преобразование кольца R . Тогда

$$t'(a) \equiv 0 \pmod{J}, \quad a \in R. \quad (5)$$

Доказательство. По теореме 2 полином $t(x)$ имеет вид

$$t(x) = t_0(x) + t_1(x)\Phi_1(x), \quad \text{причем} \quad \nu_p(t_i) \geq n - i, \quad i = 0, 1. \quad (6)$$

Тогда $t'(x) = t'_0(x) + t'_1(x)\Phi_1(x) + t_1(x)\Phi'_1(x)$. Очевидно, что в силу условия (6) p -показатель каждого слагаемого в последнем равенстве не меньше единицы, поэтому выполняются сравнения (5). $\square$

В силу теоремы 1 при $p \neq 2$ (при $p = 2$) количество МДЦ-полиномиальных преобразований над кольцом R равно произведению количества МДЦ-полиномиальных преобразований над кольцом R_3 (соответственно R_4) на все тождественно нулевые полиномиальные преобразования кольца R_3 (соответственно R_4) над R . Количество тождественно нулевых преобразований указанных колец найдено А. А. Нечаевым в упомянутой работе [12]. Поэтому наша задача сводится к определению количества МДЦ-полиномиальных преобразований над кольцами R_3 в случае $p \neq 2$ и кольцами R_4 в случае $p = 2$. Случай $p = 2$ будет рассмотрен автором в одной из следующих работ.

2. Количество МДЦ-полиномиальных преобразований $GR(q^2, p^2)$

В данном разделе найдено количество МДЦ-полиномиальных преобразований над кольцами Галуа вида $GR(q^2, p^2)$.

Пусть $f \in R[x]$. Введем следующее обозначение:

$$f^{[l]}(x) = f^{[l-1]}(f(x))$$

— l -я композиционная степень полинома $f(x)$ при $l \geq 1$ и $f^{[0]}(x) = x$.

Для обоснования корректности параметров, которые будут введены ниже, понадобится следующее утверждение.

Утверждение 3. Пусть f — МДЦ-полиномиальное преобразование над R и $F = f^{[q]}$. Тогда для произвольных элементов $a_1, a_2 \in R$ выполняется сравнение

$$F'(a_1) \equiv F'(a_2) \pmod{J}. \quad (7)$$

Доказательство. Так как f — МДЦ-полиномиальное преобразование, то $\bar{f}$ является транзитивным полиномом над R_1 и граф $G_{\bar{f}, R_1}$ является циклом. Используя формулу

$$F'(x) = (f^{[q]}(x))' = \prod_{i=0}^{q-1} f'(f^{[i]}(x))$$

и транзитивность полинома $\bar{f}$, легко получить сравнение

$$F'(x) \equiv F'(f(x)) \pmod{J}.$$

Поэтому для произвольных элементов $a_1, a_2 \in R$ выполняется сравнение (7). $\square$

Пусть e — единица кольца R . Определим параметры α_f и δ_f следующим образом:

$$\begin{aligned}\alpha_f &\equiv F'(a) \pmod{J}, & a \in R, \\ \delta_f &= \begin{cases} p, & \text{если } \bar{\alpha}_f \equiv \bar{e} \pmod{J}, \\ \text{ord } \bar{\alpha}_f & \text{в противном случае.} \end{cases}\end{aligned}\tag{8}$$

Параметр α_f определен корректно, поскольку в силу утверждения 3 он не зависит от значения a .

Будем пользоваться следующим критерием из [5].

Теорема 4 ([5]). Пусть $f \in R[x]$. Полином f индуцирует МДЦ-полиномиальное преобразование R_2 в том и только том случае, когда

- 1) полином f индуцирует МДЦ-полиномиальное преобразование R_1 (т. е. является полноцикловым над полем R_1),
- 2) $\delta_f = q - 1$.

Основным результатом раздела является следующее утверждение.

Теорема 5. Количество МДЦ-полиномиальных преобразований кольца Галуа $R = GR(q^2, p^2)$ равно

$$(q-1)! \cdot \varphi(q-1) \cdot (q-1)^{q-1} \cdot q^q,$$

где φ — функция Эйлера.

Доказательство. По теореме 4 полином g индуцирует МДЦ-полиномиальное преобразование R тогда и только тогда, когда α_g — примитивный элемент [14] поля R_1 и $\bar{g}$ — полноцикловый полином над полем R_1 . Обозначим через $P(K)$ множество примитивных элементов поля K , а через $H(R)$ — множество МДЦ-полиномиальных преобразований кольца Галуа R , в частности $H(R_1)$ — множество транзитивных полиномов над полем R_1 . Зададим отображение

$$\chi: H(R_2) \rightarrow H(R_1) \times P(R_1),\tag{9}$$

действующее по правилу

$$\chi(g) = (\bar{g}, \alpha_g).$$

Покажем, что заданное таким образом отображение χ сюръективно и все множества $\chi^{-1}(\bar{g}, c)$ равномощны.

Выберем и зафиксируем такие элементы $c_0, \dots, c_{q-1} \in R$, что

$$c_0 \cdot \dots \cdot c_{q-1} \equiv c \pmod{J}. \quad (10)$$

Зададим множество $\chi_{c_0, \dots, c_{q-1}}^{-1}(\bar{g}, c) \subset R[x]$ следующим образом. Будем полагать, что полином g над кольцом R принадлежит множеству $\chi_{c_0, \dots, c_{q-1}}^{-1}(\bar{g}, c)$ в том и только том случае, когда выполняются равенства

$$\chi(g) = (\bar{g}, c), \quad g'(g^{[i]}(0)) \equiv c_i \pmod{J}, \quad i \in \overline{0, q-1}. \quad (11)$$

Выберем произвольный транзитивный полином $\bar{g} \in H(R_1)$ и рассмотрим прообраз $\chi_{c_0, \dots, c_{q-1}}^{-1}(\bar{g}, c)$. Тогда

$$\chi^{-1}(\bar{g}, c) = \bigsqcup_{\substack{c_i \in R_1, i \in \overline{0, q-1}, \\ c_0 \cdots c_{q-1} \equiv c \pmod{J}}} \chi_{c_0, \dots, c_{q-1}}^{-1}(\bar{g}, c). \quad (12)$$

Далее посчитаем мощность $\chi_{c_0, \dots, c_{q-1}}^{-1}(\bar{g}, c)$ для фиксированных $\bar{g}, c$ и набора $c_0, \dots, c_{q-1}$. Положим $v_i = g^{[i]}(0)$, $i = 0, \dots, q-1$. Из условий (11) следует, что полином g над R принадлежит множеству $\chi_{c_0, \dots, c_{q-1}}^{-1}(\bar{g}, c)$ в том и только том случае, когда

$$\begin{aligned} g(v_i) &\equiv v_{(i+1) \pmod{q}} \pmod{J}, \\ g'(v_i) &\equiv c_i \pmod{J}, \quad i \in \overline{0, q-1}. \end{aligned} \quad (13)$$

По следствию 2.1 каждый полином g над R однозначно представляется в виде

$$g(x) = g_0(x) + g_1(x)\Phi_1(x), \quad (14)$$

причем $\nu_p^{\max}(g_0) < 2$ и $\nu_p^{\max}(g_1) < 1$. Очевидно, что $\bar{g} = \overline{g_0}$, и первое условие системы (13) эквивалентно системе

$$\overline{g_0}(v_i) \equiv v_{(i+1) \pmod{q}} \pmod{J}.$$

Из последней системы следует, что полином $\overline{g_0}(x)$ определен однозначно.

Так как

$$\nu_p^{\max}(g_0) < 2 \quad \text{и} \quad \deg g_0 < q,$$

то существует q^q способов достроить полином $\overline{g_0}$ до g_0 .

Теперь покажем, что при каждом выборе полинома g_0 ему соответствует единственный полином g_1 , при котором $g(x)$ удовлетворяет системе (13).

Заметим, что так как $\Phi_1(x) = x^q - x$, то

$$g'(x) \equiv g'_0(x) - g_1(x) \pmod{J}.$$

Тогда если $g(x) = g_0(x) + g_1(x)\Phi_1(x)$ удовлетворяет системе (13), то

$$g_1(v_i) \equiv g'_0(v_i) - c_i \pmod{J}, \quad i \in \overline{0, q-1}.$$

Поскольку $\nu_p^{\max}(g_1) < 1$, из последней системы сравнений следует, что полином g_1 определен однозначно.

Следовательно, система (13) имеет q^q решений относительно $g(x)$ над кольцом R .

Так как для фиксированной пары $(g, c) \in H(R_1) \times P(R_1)$ ввиду условий (10) имеется $(q-1)^{q-1}$ различных систем вида (13) (ровно столькими способами можно задать коэффициенты $c_0, \dots, c_{q-1}$) и количество примитивных элементов поля R_1 равно $\varphi(q-1)$, то число МДЦ-полиномиальных преобразований кольца R_2 равно

$$(q-1)! \cdot \varphi(q-1) \cdot (q-1)^{q-1} \cdot q^q. \quad \square$$

3. Количество МДЦ-полиномиальных преобразований $GR(q^3, p^3)$

В этом разделе найдем количество МДЦ-полиномиальных преобразований кольца Галуа вида $GR(q^3, p^3)$.

Положим $\Gamma(R) = \{x \in R \mid x^q = x\}$. Согласно [11] всякий элемент $a \in R$ однозначно представляется в виде

$$a = a(0) + pa(1) + p^2a(2) + \dots + p^{n-1}a(n-1), \quad (15)$$

где $a(i) \in \Gamma(R)$ называют i -м разрядом элемента a , $i = 0, 1, \dots, n-1$. Такое представление называется p -адическим разложением, или представлением Тейхмюллера элемента a (см. [11]).

Утверждение 6. Пусть $R = GR(q^n, p^n)$, $f \in R[x]$ и t — полином, задающий тождественно нулевое преобразование кольца R_m , $m < n$. Положим $g = f + t$. Тогда для произвольных $a \in R$ и $k \in \mathbb{N}$ выполняется сравнение

$$g^{[k]}(a) \equiv f^{[k]}(a) + \sum_{i=0}^{k-1} t(f^{[i]}(a)) \cdot \prod_{j=i+1}^{k-1} f'(f^{[j]}(a)) \pmod{J^{m+1}}. \quad (16)$$

Доказательство проведем индукцией по параметру k . База индукции при $k = 1$, очевидно, выполняется. Для $a \in R$ рассмотрим цепочку сравнений

$$\begin{aligned} g^{[k+1]}(a) &\equiv g(g^{[k]}(a)) \equiv g\left(f^{[k]}(a) + \sum_{i=0}^{k-1} t(f^{[i]}(a)) \cdot \prod_{j=i+1}^{k-1} f'(f^{[j]}(a))\right) \equiv \\ &\equiv g(f^{[k]}(a)) + g'(f^{[k]}(a)) \sum_{i=0}^{k-1} t(f^{[i]}(a)) \cdot \prod_{j=i+1}^{k-1} f'(f^{[j]}(a)) \equiv \\ &\equiv f^{[k+1]}(a) + t(f^{[k]}(a)) + \\ &\quad + (f'(f^{[k]}(a)) + t'(f^{[k]}(a))) \sum_{i=0}^{k-1} t(f^{[i]}(a)) \cdot \prod_{j=i+1}^{k-1} f'(f^{[j]}(a)) \pmod{J^{m+1}}. \end{aligned}$$

Согласно следствию 2.2 последнее выражение сравнимо по модулю J^{m+1} с

$$f^{[k+1]}(a) + \sum_{i=0}^k t(f^{[i]}(a)) \cdot \prod_{j=i+1}^k f'(f^{[j]}(a)).$$

Утверждение доказано. $\square$

По определению f индуцирует МДЦ-полиномиальное преобразование кольца R в том и только том случае, когда граф $G_{f,R}$ преобразования f содержит цикл длины $q(q-1)p^{n-2}$. Согласно результатам работы [5] в графе $G_{f,R}$ содержится $(q/p)^{n-2}$ циклов длины $q(q-1)p^{n-2}$. Обозначим множество элементов кольца R , лежащих на циклах длины $q(q-1)p^{n-2}$, через $M_{f,R}$.

Утверждение 7. *Равносильны следующие утверждения:*

- 1) f — МДЦ-полиномиальное преобразование кольца R_3 ,
- 2) $f^{[q(q-1)]}(a) \not\equiv a \pmod{J^3}$ для любого элемента $a \in M_{f,R_3}$,
- 3) существует хотя бы один элемент $a \in R_3$ со свойством

$$f^{[q(q-1)]}(a) \not\equiv a \pmod{J^3}.$$

Доказательство. Равносильность первого утверждения второму, а второго третьему очевидна. Также очевидно, что из первого утверждения следует третье.

Докажем, что из п. 3 следует п. 1. Пусть для какого-то элемента $a \in R_3$ выполняется условие

$$f^{[q(q-1)]}(a) \not\equiv a \pmod{J^3}.$$

Тогда согласно [4, следствие 4] элемент a лежит на цикле длины $q(q-1)p$ графа G_{g,R_3} . Это означает, что g индуцирует МДЦ-полиномиальное преобразование R_3 . $\square$

Лемма 1. Пусть $f \in R[x]$ и f индуцирует МДЦ-полиномиальное преобразование R_2 . Тогда существует такой элемент $a \in R_2$ на цикле длины $q(q-1)$ графа G_{f,R_2} , что $a \notin \Gamma(R_2)$.

Доказательство. Утверждение эквивалентно тому, что на цикле длины $q(q-1)$ существует такой элемент a , что в его разложении Тейхмюллера (см. (15)) второй разряд не нулевой. Обозначим цикл длины $q(q-1)$ через C .

Пусть вторые разряды всех элементов на цикле C нулевые. Возьмем произвольный элемент $a \in C$. Для него выполняются сравнения

$$f^{[q]}(a) \equiv a + pr \pmod{J^2}, \quad r \neq 0,$$

иначе f — не МДЦ-полином. Элемент $a + pr$ является искомым. $\square$

Напомним, что в данном разделе рассматриваются кольца Галуа $R = GR(q^3, p^3)$. Основным результатом раздела является следующее утверждение.

Теорема 8. Пусть $f \in R[x]$ — МДЦ-полиномиальное преобразование кольца Галуа R_2 и t — полином, задающий тождественно нулевое преобразование кольца R_2 , но не тождественно нулевое преобразование R . Тогда количество МДЦ-полиномиальных преобразований, индуцированных приведенными полиномами вида $g = f + t$, равно $q^{2q-1}(q-1)$.

Доказательство. Полином g индуцирует МДЦ-полиномиальное преобразование над R в том и только том случае, когда

$$g^{[q(q-1)]}(a) = a + s(a) \quad \text{для любого } a \in R, \quad (17)$$

где $s(x)$ — приведенный полином, индуцирующий тождественно нулевое преобразование кольца R_2 . Представление (17) существует и единственно. По следствию 2.1 полиномиальное преобразование $g^{[q(q-1)]}$ представимо единственным образом некоторым приведенным полиномом s_1 . Положив $s(x) = s_1(x) - x$, получим представление (17). От противного легко показать, что s индуцирует тождественно нулевое преобразование кольца R_2 . Как было сказано ранее (после следствия 2.1), мы отождествляем полиномиальные преобразования и соответствующие им приведенные полиномы. Поэтому рассуждения, аналогичные вышеприведенным, будем в дальнейшем опускать и писать $g^{[q(q-1)]}(x) = x + s(x)$.

Искомое число равно количеству таких приведенных полиномов t , что в равенстве (17) полином s является не тождественным преобразованием кольца R .

Так как f индуцирует МДЦ-полиномиальное преобразование R_2 , то согласно приведенным выше рассуждениям

$$f^{[q(q-1)]}(x) = x + z(x) \quad (18)$$

для некоторого тождественно нулевого над кольцом R_2 полинома $z(x)$. По утверждению 6 имеем

$$g^{[q(q-1)]}(x) \equiv f^{[q(q-1)]}(x) + \sum_{i=0}^{q(q-1)-1} t(f^{[i]}(x)) \cdot \prod_{j=i+1}^{q(q-1)-1} f'(f^{[j]}(x)) \pmod{J^3}. \quad (19)$$

Подставив (17) и (18) в (19), получим

$$s(x) \equiv z(x) + \sum_{i=0}^{q(q-1)-1} t(f^{[i]}(x)) \cdot \prod_{j=1+1}^{q(q-1)-1} f'(f^{[j]}(x)) \pmod{J^3}. \quad (20)$$

Сравнение (20) и утверждение 7 обосновывают следующую цепочку равносильных утверждений:

$$\begin{aligned} & (g \text{ индуцирует МДЦ-полиномиальное преобразование } R) \Leftrightarrow \\ & \Leftrightarrow (\forall a \in M_{f,R} : g^{[q(q-1)]}(a) \not\equiv a \pmod{J^3}) \Leftrightarrow \\ & \Leftrightarrow (\forall a \in M_{f,R} : s(a) \not\equiv 0 \pmod{J^3}) \Leftrightarrow \\ & \Leftrightarrow (\forall a \in M_{f,R} : z(a) + \sum_{i=0}^{q(q-1)-1} t(f^{[i]}(a)) \cdot \prod_{j=1+1}^{q(q-1)-1} f'(f^{[j]}(a)) \not\equiv 0 \pmod{J^3}) \Leftrightarrow \\ & \Leftrightarrow (\exists a \in M_{f,R_3} : z(a) + \sum_{i=0}^{q(q-1)-1} t(f^{[i]}(a)) \cdot \prod_{j=i+1}^{q(q-1)-1} f'(f^{[j]}(a)) \not\equiv 0 \pmod{J^3}). \end{aligned} \quad (21)$$

Из последнего следует, что искомое число равно количеству таких тождественных над R_2 полиномов t , что для некоторого $a \in R$

$$z(a) + \sum_{i=0}^{q(q-1)-1} t(f^{[i]}(a)) \cdot \prod_{j=1+1}^{q(q-1)-1} f'(f^{[j]}(a)) \not\equiv 0 \pmod{J^3}$$

при фиксированных полиномах z и f .

Согласно следствию 2.1 полиномиальное преобразование t представляется приведенным полиномом

$$\begin{aligned} t(x) &= p^2 t_1(x) + p(x^q - x) t_2(x) + (x^q - x)^2 t_3(x), \\ \nu_p(t_i) &< 1, \quad \deg(t_i) < q, \quad i = 1, 2, 3. \end{aligned} \quad (22)$$

Рассмотрим сумму из сравнения (20):

$$\begin{aligned} & \sum_{i=0}^{q(q-1)-1} t(f^{[i]}(a)) \cdot \prod_{j=i+1}^{q(q-1)-1} f'(f^{[j]}(a)) \equiv \\ & \equiv \sum_{i=0}^{q(q-1)-1} \left(p^2 t_1(f^{[i]}(a)) + p(f^{[i]}(a)^q - f^{[i]}(a)) t_2(f^{[i]}(a)) + \right. \\ & \quad \left. + (f^{[i]}(a)^q - f^{[i]}(a))^2 t_3(f^{[i]}(a)) \right) \cdot \\ & \quad \cdot \prod_{j=i+1}^{q(q-1)-1} f'(f^{[j]}(a)) \pmod{J^3}. \end{aligned}$$

Покажем, что последняя сумма не зависит от полинома t_1 . Раскроем скобки в последнем сравнении и рассмотрим первую сумму

$$\sum_{i=0}^{q(q-1)-1} p^2 t_1(f^{[i]}(a)) \cdot \prod_{j=i+1}^{q(q-1)-1} f'(f^{[j]}(a)) \pmod{J^3}. \quad (23)$$

Чтобы упростить формулы, положим

$$f^{[j]}(a) = a_j, \quad f'(f^{[j]}(a)) = \alpha_j, \quad j \geq 0,$$

тогда (23) можно переписать в виде

$$\sum_{i=0}^{q(q-1)-1} t_1(a_i) \cdot \prod_{j=i+1}^{q(q-1)-1} \alpha_j \pmod{J}. \quad (24)$$

Так как f индуцирует МДЦ-полиномиальное преобразование, то выполняются сравнения

$$a_j \equiv a_{j+q} \pmod{J}, \quad \alpha_j \equiv \alpha_{j+q} \pmod{J}, \quad j \geq 0, \quad (25)$$

и, кроме того, $\alpha_0 \cdot \alpha_1 \cdot \dots \cdot \alpha_{q-1} \equiv \alpha \pmod{J}$, где α — элемент поля R_1 порядка $q-1$.

Тогда (23) можно представить в виде

$$\sum_{i=0}^{q(q-1)-1} t_1(a_j) \frac{\prod_{j=0}^{q(q-1)-1} \alpha_j}{\prod_{k=0}^i \alpha_k} \pmod{J} \equiv \sum_{i=0}^{q(q-1)-1} t_1(a_j) \frac{\alpha^{q-1}}{\prod_{k=0}^i \alpha_k} \pmod{J}. \quad (26)$$

С учетом равенств (25) перегруппируем слагаемые в сумме (26):

$$\begin{aligned} & \sum_{i=0}^{q-1} t_1(a_i) \frac{\alpha^{q-1}}{\prod_{k=0}^i \alpha_k} + \sum_{i=0}^{q-1} t_1(a_i) \frac{\alpha^{q-2}}{\prod_{k=0}^i \alpha_k} + \cdots + \sum_{i=0}^{q-1} t_1(a_i) \frac{\alpha}{\prod_{k=0}^i \alpha_k} \equiv \\ & \equiv t_1(a_0) \sum_{k=1}^{q-1} \frac{\alpha^k}{\alpha_0} + t_1(a_1) \sum_{k=1}^{q-1} \frac{\alpha^k}{\alpha_0 \alpha_1} + \cdots + t_1(a_{q-1}) \sum_{k=1}^{q-1} \frac{\alpha^k}{\prod_{k=0}^{q-1} \alpha_k} \equiv \\ & \equiv \frac{\alpha^{q-1} - e}{\alpha - e} \delta \sum_{i=0}^{q-1} \frac{t_1(a_i)}{\prod_{k=0}^i \alpha_k} \equiv 0 \pmod{J}. \end{aligned}$$

Таким образом, мы установили, что полином t_1 в представлении (22) полинома t можно выбирать произвольно. Это можно сделать q^q способами. Теперь найдем количество полиномов t_2 и t_3 , при которых полином t удовлетворяет условию (21). Условие (21) ввиду последних рассуждений равносильно соотношению

$$z(a_0) + \sum_{i=0}^{q(q-1)-1} (p(a_i^q - a_i)t_2(a_i) + (a_i^q - a_i)^2 t_3(a_i)) \cdot \prod_{j=i+1}^{q(q-1)-1} \alpha_j \not\equiv 0 \pmod{J^2}. \quad (27)$$

Найдем такие t_2 и t_3 , которые дают равенство в (27).

Для этого рассмотрим свойства полинома $x^q - x$ над R . Пусть $a \in R$,

$$a = a(0) + pa(1) + \cdots + p^{n-1}a(n-1) = a(0) + pa(1, n-1)$$

— разложение Тейхмюллера элемента a и

$$a^q - a = a(1, n-1) = pa(1) + \cdots + p^{n-1}a(n-1).$$

Верны сравнения

$$\begin{aligned} & (a(0) + pa(1, n-1))^q - (a(0) + pa(1, n-1)) \equiv \\ & \equiv a(0)^q + \binom{q}{1} pa(1, n-1) + \cdots + \binom{q}{q} (pa(1, n-1))^q - a(0) - pa(1, n-1) \equiv \\ & \equiv -pa(1, n-1) \pmod{J^2}. \end{aligned} \quad (28)$$

Из (28) следует, что

$$(a^q - a)^2 \equiv -p^2 a^2(1, n-1) \pmod{J^3}.$$

С учетом последних сравнений соотношение (27) можно переписать в следующем виде:

$$\begin{aligned} z(a_0) + \sum_{i=0}^{q(q-1)-1} (p^2 a_i(1, n-1)t_2(a_i) + p^2 a_i^2(1, n-1)t_3(a_i)) \cdot \prod_{j=i+1}^{q(q-1)-1} \alpha_j &\not\equiv 0 \pmod{J^3} \Leftrightarrow \\ \Leftrightarrow z(a_0) + \sum_{i=0}^{q(q-1)-1} (a_i(1, n-1)t_2(a_i) + a_i^2(1, n-1)t_3(a_i)) \cdot \prod_{j=i+1}^{q(q-1)-1} \alpha_j &\not\equiv 0 \pmod{J}. \end{aligned} \quad (29)$$

Из леммы 1 следует, что среди элементов $a_i(1, n-1)$, $i \in \overline{0, q-1}$, существует хотя бы один ненулевой по модулю J , пусть $d \in \overline{0, q-1}$ — номер такого элемента. Все значения полинома t_3 можно выбирать произвольно. Всего возможно q^q способов. Также можно выбрать все значения полинома t_2 в точках a_i , $i \neq d$, произвольно. При выполнении равенства (29) значение $t_2(a_d)$ будет определено однозначно. Таким образом, количество полиномов t_2 , которые дают равенство в (29), равно q^{q-1} .

В итоге получаем, что количество приведенных полиномов t , индуцирующих МДЦ-полиномиальное преобразование вида $g = f + t$, равно произведению количеств полиномов t_1 и t_3 и количества подходящих полиномов t_2 и равно $q^{2q}(q^q - q^{q-1}) = q^{3q-1}(q-1)$. $\square$

Сформулируем основной результат работы.

Теорема 9. *Количество МДЦ-полиномиальных преобразований кольца Галуа $GR(q^3, p^3)$, $q = p^m$, $m > 1$, равно*

$$(q-1)! \cdot \varphi(q-1) \cdot (q-1)^q \cdot q^{4q-1},$$

где φ — функция Эйлера.

Заключение

Для окончательного определения количества МДЦ-полиномиальных преобразований над кольцами Галуа осталось рассмотреть случай колец Галуа четной характеристики, что сводится к поиску количества МДЦ-полиномиальных преобразований над кольцами Галуа вида $GR(q^4, 2^4)$, $q = 2^m$, $m > 1$. Эта задача будет рассмотрена автором в одной из следующих работ.

Список литературы

- [1] Анашин В. С., “О группах и кольцах, обладающих транзитивными полиномами”, В сб.: XVI Всесоюзная алгебр. конф. Тезисы (Ленинград), **2**, 1981, 4–5.
- [2] Анашин В. С., “Равномерно распределенные последовательности целых p -адических чисел”, *Дискретная математика*, **14**:4 (2002), 1–63.
- [3] Ларин М. В., “Транзитивные полиномиальные преобразования колец вычетов”, *Дискретная математика*, **14**:2 (2000), 20–32.
- [4] Ермилов Д. М., Козлитин О. А., “Цикловая структура полиномиального генератора над кольцом Галуа”, *Математические вопросы криптографии*, **4**:1 (2013), 27–57.
- [5] Ермилов Д. М., Козлитин О. А., “О строении графа полиномиального преобразования кольца Галуа”, *Математические вопросы криптографии*, **6**:3 (2015), 47–73.
- [6] Ермилов Д. М., “Алгоритм построения систем представителей циклов максимальной длины полиномиальных подстановок над кольцом Галуа”, *Прикл. дискр. матем. Приложение*, № 7 (2014), 64–67.
- [7] Ермилов Д. М., “Свойства полиномиальных генераторов с выходной последовательностью наибольшего периода над кольцом Галуа”, *Прикл. дискр. матем.*, **27**:1 (2015), 52–61.
- [8] Козлитин О. А., “Оценка длины максимального цикла в графе полиномиального преобразования кольца Галуа–Эйзенштейна”, *Дискретная математика*, **29**:4 (2017), 41–58.
- [9] Викторенков В. Е., “О строении орграфов полиномиальных преобразований над конечными коммутативными кольцами с единицей”, *Дискретная математика*, **29**:3 (2017), 3–23.
- [10] Parvatov N. G., “On the period length of vector sequences generated by polynomials modulo prime powers”, *Прикл. дискр. матем.*, **31**:1 (2016), 57–61.
- [11] Елизаров В. П., *Конечные кольца*, М. : Гелиос-АРВ, 2006, 304 с.
- [12] Нечаев А. А., “Полиномиальные преобразования конечных коммутативных колец главных идеалов”, *Матем. заметки*, **27**:7 (1980), 885–899.
- [13] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, 2-е изд., испр. и доп., СПб.: Лань, 2015, 608 с.
- [14] Лидл Р., Нидеррайтер Г., *Конечные поля*, М. : Мир, 1988, 822 с.