ПСЕВДОСЛУЧАЙНЫЕ ГЕНЕРАТОРЫ

УДК 519.7

СВОЙСТВА ПОЛИНОМИАЛЬНЫХ ГЕНЕРАТОРОВ С ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТЬЮ НАИБОЛЬШЕГО ПЕРИОДА НАД КОЛЬЦОМ ГАЛУА

Д. М. Ермилов

Лаборатория ТВП, г. Москва, Россия

Пусть $R = \mathrm{GR}(q^n, p^n)$ — кольцо Галуа мощности q^n и характеристики p^n, где $q = p^m$, и $G_{f,R}$ — граф биективного преобразования кольца R, задаваемого полиномом $f(x) \in R[x]$. Если $n > 1$ или $q \neq p$, то граф $G_{f,R}$ не может быть циклом. Максимальная длина цикла в таком графе не превосходит $q(q-1)p^{n-2}$. Полиномы, для которых граф $G_{f,R}$ содержит цикл указанной длины, назовём полиномами с максимальной длиной цикла. Для таких полиномов предложен алгоритм проверки, лежит ли заданный элемент кольца на каком-либо цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$. Алгоритм требует выполнения порядка dq операций умножения и порядка dq операций сложения в кольце R, $d = \deg f(x)$, $d < |R|$. Предложен также алгоритм построения системы представителей различных циклов графа $G_{f,R}$, имеющих длину $q(q-1)p^{n-2}$. Алгоритм построения представителей всех циклов длины $q(q-1)p^{n-2}$ требует выполнения порядка $d(q-1)q^{n-1}$ операций умножения и порядка $d(q-1)q^{n-1}$ операций сложения в кольце R. Алгоритм построения представителей M различных циклов длины $q(q-1)p^{n-2}$ требует выполнения порядка $d(q-1)q^{k-1}$ операций умножения и порядка $d(q-1)q^{k-1}$ операций сложения в кольце R, где $k = \lceil \log_{q/p} M \rceil + 1$.

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

DOI 10.17223/20710410/27/5

FEATURES OF MAXIMAL PERIOD POLYNOMIAL GENERATORS OVER THE GALOIS RING

D. M. Ermilov

Laboratory TVP, Moscow, Russia

E-mail: wwwermilov@gmail.com

For a polynomial mapping over the Galois ring $R = \mathrm{GR}(q^n, p^n)$ with the cardinality q^n and characteristic p^n, the maximal length of a cycle equals $q(q-1)p^{n-2}$. In this paper, we present an algorithm for constructing the system of representatives of all maximal length cycles and an algorithm for constructing an element in a cycle of maximal length for a polynomial substitution $f \in R[x]$. The complexity of the first algorithm equals $d(q-1)q^{n-1}$ multiplication operations and $d(q-1)q^{n-1}$ addition operations in R, the complexity of the second algorithm equals dq multiplication operations and

dq addition operations in R where $d = \deg(f)$.

Keywords: *nonlinear recurrent sequences, Galois ring.*

Введение

При синтезе поточных шифрсистем актуальной задачей является построение генераторов псевдослучайных последовательностей с хорошими криптографическими свойствами. К генераторам псевдослучайных последовательностей предъявляются такие требования, как быстродействие, простота реализации, возможность гарантирования криптографических параметров. Для выработки псевдослучайных последовательностей широко применяются *полиномиальные конгруэнтные генераторы*, которые являются обобщением хорошо известных линейных конгруэнтных генераторов. Полиномиальный конгруэнтный генератор над кольцом R — это автомат с выходной последовательностью $x_0, x_1, \ldots$, которая определяется соотношением

$$x_{i+1} = f(x_i), \tag{1}$$

где $x_0 \in R$; $f(x) \in R[x]$.

Изучение полиномиальных генераторов началось со случая, когда R — кольцо вычетов. Общие свойства функций и полиномиальных преобразований примарных колец вычетов можно найти в работе [1].

Интересен случай, когда последовательность (1) имеет наибольший период. Над кольцом вычетов $\mathbb{Z}_m$ наибольший период последовательности (1) равен m. Из работы [2] следует, что указанный период достижим. Полиномы, задающие последовательность (1) периода m, называют *полноцикловыми* или *транзитивными*. Описание полноцикловых линейных и квадратичных полиномов над кольцами вычетов дано Д. Кнутом в работе [3], а общий случай рассмотрен М. В. Лариным в [4]. В. С. Анашин [5] указал классы полноцикловых полиномиальных преобразований колец вычетов.

В работе [6] изучается орграф полиномиального преобразования над коммутативным локальным кольцом, предложена классификация вершин орграфа, найдено число его циклических точек.

А. А. Нечаевым в [7] описаны биективные полиномиальные преобразования конечных коммутативных колец главных идеалов, а также найдено их количество. Изучение периодических свойств последовательности (1) в случае, когда R — кольцо Галуа, начато в [8].

В настоящей работе на основе результатов [8] исследуются свойства графов полиномиальных преобразований колец Галуа, содержащих циклы максимальной длины.

1. Обозначения

Рассмотрим кольцо Галуа $R = \mathrm{GR}(q^n, p^n)$ мощности q^n и характеристики p^n, где $q = p^m$, $m > 1$, $n > 1$. Пусть $f(x) \in R[x]$ — полином над кольцом R, задающий биективное преобразование этого кольца [7]. Граф указанного преобразования над кольцом R обозначим через $G_{f,R}$. Напомним, что цикловая структура графа — это таблица $[l_1^{k_1}, \ldots, l_t^{k_t}]$, указывающая, что граф состоит из k_1 циклов длины l_1, $\ldots$, k_t циклов длины l_t. В работе [8] показано, что граф полиномиального преобразования кольца R не содержит циклов, длина которых больше $q(q-1)p^{n-2}$.

Биективные полиномы над кольцом R, такие, что граф $G_{f,R}$ содержит цикл длины $q(q-1)p^{n-2}$, назовём *полиномами с максимальной длиной цикла* (*МДЦ-полиномами*). Вычисления на ЭВМ показывают, что указанные полиномы существуют.

Пример 1. Рассмотрим кольцо Галуа $R = \mathrm{GR}(15625, 125)$. Кольцо R изоморфно кольцу $R' = \mathbb{Z}_{125}[y]/(y^2 + y + 1)$. Элементы кольца R' суть классы вида

$$[a_1 y + a_0]_{y^2+y+1},$$

которые будем обозначать векторами $(a_1, a_0) \in \mathbb{Z}_{125}^2$. Например, элемент $[2y+1]_{y^2+y+1} \in$ $\in R'$ будем обозначать вектором $(2, 1)$. Отождествим кольцо R с кольцом R'. Рассмотрим следующий полином $f(x) \in R[x]$:

$$\begin{gathered} f(x) = (1,4)x^{24} + (1,3)x^{23} + (4,2)x^{21} + (4,2)x^{20} + (0,1)x^{19} + (3,1)x^{18} + \\ +(2,2)x^{17} + (3,4)x^{15} + (0,1)x^{14} + (3,3)x^{13} + (3,0)x^{12} + (1,1)x^{11} + (2,2)x^{10} + \\ +(3,3)x^9 + (4,3)x^8 + (2,4)x^7 + (0,24)x^6 + (0,3)x^5 + \\ +(3,0)x^4 + (4,1)x^3 + (3,4)x^2 + (4,3)x + (0,1). \end{gathered}$$

Цикловая структура графа $G_{f,R}$ равна $[3000^5, 600^1, 25^1]$, и $f(x)$ является МДЦ-полином над R.

Критерий того, что полином над кольцом R является МДЦ-полиномом, приведён в работе [8].

Пусть далее $f(x) \in R[x]$ — МДЦ-полином. При использовании $f(x)$ в качестве криптографического примитива представляются актуальными следующие задачи:

1) проверка того, что заданный элемент $a \in R$ лежит на каком-то цикле максимальной длины графа $G_{f,R}$;
2) эффективное построение системы представителей M различных циклов длины $q(q-1)p^{n-2}$ графа $G_{f,R}$.

Параметр M не может превышать значения $(q/p)^{n-2}$, так как в графе $G_{f,R}$ содержится ровно $(q/p)^{n-2}$ циклов длины $(q-1)qp^{n-2}$ [9]. Введём необходимые обозначения.

Обозначим через $f^{[0]}$ тождественное преобразование, а через $f^{[m]}$, $m \in \mathbb{N}$, — преобразование $f \circ f \circ \cdots \circ f$ (m раз), где $\circ$ — операция композиции; $f(x) \in R[x]$.

Положим $J = pR$ и $R_i = R/J^i$, $i \in \{1, \ldots, n\}$. *Координатным множеством* $\Gamma(R)$ кольца R называют множество элементов $\{x \in R : x^q = x\}$. Согласно [10], всякий элемент $a \in R$ однозначно представляется в виде

$$a = \gamma_0(a) + p\gamma_1(a) + p^2\gamma_2(a) + \cdots + p^{n-1}\gamma_{n-1}(a),$$

где $\gamma_i(a) \in \Gamma(R)$, $i = 0, 1, \ldots, n-1$. Это представление называют *разложением Тейхмюллера* элемента $a \in R$. Кольцо R_i состоит из непересекающихся классов $a + J^i$, $a \in R$. Элемент a называют представителем класса $a + J^i$ в кольце R. Там, где это не будет приводить к недоразумению, элементы кольца R_i будем отождествлять с их представителями в кольце R и вместо координатного множества $\Gamma(R_i)$ писать $\Gamma(R)$, $i \in \{1, \ldots, n\}$. Рассмотрим естественные эпиморфизмы колец

$$\varphi_i : R \to R_i$$

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

$$\widehat{\varphi}_i : R[x] \to R_i[x].$$

Положим $f_i(x) = \widehat{\varphi}_i(f(x))$, $i = 1, \ldots, n$. Производную многочлена $f(x)$ кольца $R[x]$ будем обозначать $f'(x)$ [11].

В дальнейшем понадобится следующее утверждение.

Утверждение 1 [8]. Пусть $f(x) \in R[x]$. Для любых $s \in \mathbb{N}$ и $x, y \in R$ верно соотношение

$$f(x + p^s y) \equiv f(x) + p^s y f'(x) \,(\mathrm{mod}\ J^{s+1}).$$

2. Определение принадлежности элемента циклу максимальной длины

Для решения первой задачи докажем

Утверждение 2. Пусть $f(x) \in R[x]$ — МДЦ-полином, $F(x) = f^{[q]}(x)$. Элемент $a \in R$ лежит на цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$ в том и только в том случае, если $\gamma_1(a)$ не является решением сравнения

$$F(\gamma_0(a)) - \gamma_0(a) \equiv p(e - F'(\gamma_0(a)))x \pmod{J^2}. \tag{2}$$

Доказательство. Так как $f(x)$ — МДЦ-полином, из результатов работы [8] следует, что цикловая структура графа G_{f_2,R_2} имеет вид $[q(q-1)^1, q^1]$. При этом для того чтобы элемент $a \in R$ лежал на каком-либо цикле длины $q(q-1)p^{n-2}$, необходимо и достаточно, чтобы элемент $\varphi_2(a)$ лежал на цикле длины $q(q-1)$ графа G_{f_2,R_2}. Найдём необходимое и достаточное условие, при котором элемент $\varphi_2(a)$ лежит на цикле длины q графа G_{f_2,R_2}.

Из условия, что $\varphi_2(a)$ лежит на цикле длины q графа G_{f_2,R_2} и утверждения 1, имеем

$$F(\gamma_0(a) + p\gamma_1(a)) \equiv F(\gamma_0(a)) + p\gamma_1(a)F'(\gamma_0(a)) \equiv \gamma_0(a) + p\gamma_1(a) \pmod{J^2}.$$

Последнему сравнению равносильно сравнение

$$F(\gamma_0(a)) - \gamma_0(a) \equiv p(e - F'(\gamma_0(a)))\gamma_1(a) \pmod{J^2},$$

из которого следует доказываемое утверждение. ■

Замечание 1. Выполнению сравнения (2) равносильно выполнение некоторого сравнения по модулю J. Действительно, так как $F(\gamma_0(a)) \equiv \gamma_0(a) \pmod{J}$, найдётся элемент $a' \in \Gamma(R)$, такой, что $F(\gamma_0(a)) \equiv \gamma_0(a) + pa' \pmod{J^2}$. В таком случае сравнение (2) запишется в виде $pa' \equiv p(e - F'(\gamma_0(a)))x \pmod{J^2}$. Последнему сравнению равносильно сравнение по модулю J:

$$a' \equiv (e - F'(\gamma_0(a)))x \pmod{J}. \tag{3}$$

Сформулируем алгоритм, определяющий, лежит ли заданный элемент на каком-либо цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$.

Замечание 2. Пусть $f(x) = a_0 + a_1x + a_2x^2 + \ldots = a_0 + x(a_1 + x(a_2 + \ldots)\ldots)$; отсюда видно, что для нахождения значения многочлена в точке требуется d умножений и d сложений элементов кольца, где $d = \deg f(x)$.

Оценим сложность алгоритма 1. Пусть $d = \deg f(x)$. На шаге 1 алгоритма необходимо последовательно вычислить значения $f(\gamma_0(a))$, $f^{[2]}(\gamma_0(a))$, $\ldots$, $f^{[q]}(\gamma_0(a))$. При этом параллельно с шагом 1 можно выполнять шаг 2, вычисляя произведение элементов указанной цепочки, и по формуле (4) найти $F'(\gamma_0(a)) \pmod{J^2}$. Таким образом, для выполнения шагов 1 и 2 потребуется $dq + q = (d+1)q$ операций умножения и столько же операций сложения в кольце R.

Шаг 3 алгоритма осуществляется за одну операцию умножения и одну операцию сложения в кольце R. Общая сложность алгоритма равна $(d+1)q + 1$ операций умножения и $(d+1)q + 1$ операций сложения в кольце R.

В итоге верна

Алгоритм 1. Определение принадлежности элемента кольца R циклу максимальной длины графа $G_{f,R}$

Вход: $f(x) \in R[x]$ — МДЦ-полином, элемент $a \in R$

Выход: ДА, если элемент a лежит на цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$; НЕТ — иначе

1: Найти значение $F(\gamma_0(a)) \pmod{J^2}$.

2: Найти значение $F'(\gamma_0(a)) \pmod{J^2}$, используя формулу

$$F'(\gamma_0(a)) \equiv (f^{[q]}(x))'_{x=\gamma_0(a)} \equiv \prod_{i=0}^{q-1} f(f^{[i]}(\gamma_0(a))) \pmod{J^2}. \tag{4}$$

3: Проверить, является ли $\gamma_1(a)$ решением сравнения

$$a' \equiv (e - F'(\gamma_0(a)))x \pmod{J},$$

где a' находится из сравнения $F(\gamma_0(a)) \equiv \gamma_0(a) + pa' \pmod{J^2}$.

4: **Если** является, **то**

5: выдать ответ НЕТ,

6: **иначе**

7: выдать ответ ДА.

Теорема 1. Пусть $f(x) \in R[x]$ — МДЦ-полином. Существует алгоритм, проверяющий, лежит ли заданный элемент $a \in R$ на каком-либо цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$, требующий порядка dq операций умножения и порядка dq операций сложения в кольце R.

3. Построение системы представителей циклов максимальной длины

Сначала решим задачу для $M = (q/p)^{n-2}$. Обозначим систему представителей всех различных циклов графа $G_{f,R}$ длины $q(q-1)p^{n-2}$ через $W_{f,R}$. Строить набор $W_{f,R}$ будем итеративно, последовательно строя цепочку множеств

$$W_{f_1,R_1}, W_{f_2,R_2}, \ldots, W_{f_n,R_n}, \tag{5}$$

где $f_i(x) = \widehat{\varphi}_i(f(x))$, $i = 1, \ldots, n$. Тогда $W_{f,R} = W_{f_n,R_n}$.

Из результатов работы [8] следует, что цикловые структуры графов G_{f_1,R_1} и G_{f_2,R_2} равны $[q^1]$ и $[q(q-1)^1, q^1]$ соответственно, а для $k \geqslant 3$ в графе G_{f_k,R_k} содержится $(q/p)^{k-2}$ циклов длины $q(q-1)p^{k-2}$.

Множество W_{f_1,R_1} состоит из одного элемента, так как граф G_{f_1,R_1} является циклом. Поэтому в качестве W_{f_1,R_1} можно выбрать любое одноэлементное множество $\{a\}$, $a \in R_1$. Цикловая структура графа G_{f_2,R_2} имеет вид $[q(q-1)^1, q^1]$. Тогда $W_{f_2,R_2} = \{a'\}$, где $\gamma_0(a') = a$, а координату $\gamma_1(a')$ необходимо взять отличной от решения сравнения (3).

Далее покажем, как по известному множеству W_{f_k,R_k} построить $W_{f_{k+1},R_{k+1}}$, $k \geqslant 2$. Рассмотрим естественные эпиморфизмы $\varphi_i : R_{i+1} \to R_i$ для $i = 1, \ldots, n-1$. Для каждого $a \in W_{f_k,R_k}$ обозначим через C_a цикл графа G_{f_k,R_k}, на котором лежит элемент a.

Элементы прообраза $\varphi_k^{-1}(C_a)$ лежат на q/p циклах длины $q(q-1)p^{k-1}$ графа $G_{f_{k+1},R_{k+1}}$ [8, теорема 30]. Пусть $A_a = \{a_1, a_2, \ldots, a_{q/p}\}$ — множество представителей этих циклов. Для разных элементов $a_1, a_2 \in W_{f_k,R_k}$ прообразы $\varphi_k^{-1}(C_{a_1})$ и $\varphi_k^{-1}(C_{a_2})$ не пересекаются, значит, множества A_{a_1} и A_{a_2} также не пересекаются. Из равен-

ства $\frac{q}{p}|W_{f_k,R_k}| = |W_{f_{k+1},R_{k+1}}|$ следует, что $\bigcup\limits_{a\in W_{f_k,R_k}} A_a = W_{f_{k+1},R_{k+1}}$. Это означает, что для построения системы представителей $W_{f_{k+1},R_{k+1}}$ достаточно для каждого элемента $a \in W_{f_k,R_k}$ построить множество A_a.

Пусть a принадлежит множеству W_{f_k,R_k}. Установим связь между элементами α кольца R_{k+1}, которые лежат на одном цикле максимальной длины и обладают свойством $\varphi_k(\alpha) = a$.

Утверждение 3. Пусть элемент $a \in W_{f_k,R_k}$ является представителем цикла C максимальной длины графа G_{f_k,R_k}. Тогда на любом цикле $C^{'}$ максимальной длины графа $G_{f_{k+1},R_{k+1}}$, таком, что $\varphi_k(C^{'}) = C$, лежат ровно p элементов, образ которых под действием эпиморфизма φ_k совпадает с a.

Доказательство. Пусть $F(x) = f^{[q(q-1)p^{k-2}]}(x)$ есть $q(q-1)p^{k-2}$-я композиционная степень полинома $f(x)$ и $a^{'}-$ элемент на цикле $C^{'}$ максимальной длины графа $G_{f_{k+1},R_{k+1}}$ со свойством $\varphi_i(a^{'}) = a$. Тогда для каждого $k \in \{1,\dots,p\}$ выполняется равенство $\varphi_i(F^{[k]}(a^{'})) = a$. ■

Лемма 1. Пусть $f(x)$ — МДЦ-полином над кольцом R. Тогда существует элемент $c \in R$, такой, что для любого элемента $a \in R$, лежащего на цикле длины t графа $G_{f,R}$, верно равенство

$$\left(f^{[t]}(x)\right)^{'}_{x=a} = c.$$

Доказательство. Обозначим через $F(x) = f^{[t]}(x)$. Достаточно доказать, что $F'(x) = F^{'}(f(x))$ для всех $x \in R$, лежащих на цикле длины t графа $G_{f,R}$.

По формуле производной сложной функции для указанных $x \in R$ имеем

$$F^{'}(x) = \left(f^{[t]}(x)\right)^{'} = f^{'}\left(f^{[t-1]}(x)\right)\left(f^{[t-1]}(x)\right)^{'} = \prod_{i=0}^{t-1} f^{'}\left(f^{[i]}(x)\right).$$

С другой стороны,

$$F^{'}(f(x)) = \prod_{i=0}^{t-1} f^{'}\left(f^{[i]}(f(x))\right) = \prod_{i=1}^{t} f^{'}\left(f^{[i]}(x)\right) = f^{'}(x)\prod_{i=1}^{t-1} f^{'}\left(f^{[i]}(f(x))\right) = \prod_{i=0}^{t-1} f^{'}\left(f^{[i]}(x)\right).$$

Лемма доказана. ■

Теорема 2. Пусть $a_1 = a + p^k a_1^{'}$, $\dots$, $a_p = a + p^k a_p^{'}$ — элементы на некотором цикле максимальной длины $q(q-1)p^{k-1}$ графа $G_{f_{k+1},R_{k+1}}$, образ которых под действием эпиморфизма φ_k совпадает с $a \in W_{f_k,R_k}$. Тогда для некоторого $r \in \Gamma(R)$ выполняется соотношение $a_{i+1}^{'} = a_i^{'} + r$, $i = 1, 2, \dots, p-1$.

Доказательство. Пусть $G(x) = f^{[q(q-1)p^{k-2}]}(x)$ есть $q(q-1)p^{k-2}$-я композиционная степень полинома $f(x)$. Тогда выполняются сравнения $G(a_i) \equiv a_{i+1} \pmod{J^{k+1}}$ для $i = 1,\dots,p-1$. Кроме того, так как $G(a) \equiv a \pmod{J^k}$ и $G(a) \not\equiv a \pmod{J^{k+1}}$, то $G(a) \equiv a + p^k r \pmod{J^{k+1}}$ для некоторого $r \in R$. Воспользуемся результатом утверждения 1 и запишем последовательность сравнений

$$a_{i+1} \equiv G(a_i) \equiv G(a + p^k a_i^{'}) \equiv G(a) + p^k a_i^{'} G^{'}(a) \equiv a + p^k(a_i^{'} G^{'}(a) + r) \pmod{J^{k+1}}.$$

Для завершения доказательства осталось показать, что $G^{'}(a) \equiv e \pmod{J}$. Положив $F(x) = f^{[q]}(x)$, получим

$$G^{'}(x) = (F^{[(q-1)p^{k-2}]}(x))^{'} = \prod_{i=0}^{(q-1)p^{k-2}-1} F^{'}(F^{[(q-1)p^{k-2}]}(x)).$$

По лемме 1 существует элемент $c \in R$, такой, что для всех элементов $a \in R$ выполняется равенство $F^{'}(a) \equiv c \pmod J$. Тогда для любого элемента $y \in R$ верны сравнения

$$G^{'}(y) \equiv \prod_{i=0}^{(q-1)p^{k-2}-1} F^{'}(F^{[(q-1)p^{k-2}]}(y)) \equiv c^{(q-1)p^{k-2}} \equiv e^{p^{k-2}} \equiv e \pmod J.$$

Теорема доказана. ■

Определим на $\Gamma(R)$ операции $\oplus$ и $\otimes$: если $\alpha, \beta \in \Gamma(R)$, то

$$\alpha \oplus \beta = \gamma_0(\alpha + \beta), \quad \alpha \otimes \beta = \gamma_0(\alpha\beta) = \alpha\beta.$$

Алгебра $(\Gamma(R), \oplus, \otimes)$ изоморфна полю $\mathrm{GF}(q)$. Далее вместо поля $(\Gamma(R), \oplus, \otimes)$ будем писать просто $\Gamma(R)$.

Следствие 1. Пусть $a \in W_{f_k,R_k}$. Два элемента $a + p^k a^{'}$ и $a + p^k a^{''}$ кольца R_{k+1} лежат на одном и том же цикле максимальной длины графа $G_{f_{k+1},R_{k+1}}$ в том и только в том случае, если элементы $a^{'}, a^{''} \in \Gamma(R)$ лежат на одном цикле графа $G_{x+r,\Gamma(R)}$ полиномиального преобразования $x + r$, где элемент $r \in \Gamma(R)$ находится из сравнения

$$G(a) \equiv a + p^k r \pmod{J^{k+1}},$$

а $G(x) = f^{[q(q-1)p^{k-2}]}(x)$ есть $q(q-1)p^{k-2}$-я композиционная степень полинома $f(x)$.

Граф $G_{x+r,\Gamma(R)}$ состоит из q/p циклов длины p. Элементы каждого цикла графа $G_{x+r,\Gamma(R)}$ образуют смежный класс аддитивной группы поля $\Gamma(R)$ по подгруппе $\langle r \rangle$. Это означает, что для нахождения q/p элементов поля $\Gamma(R)$, которые лежат на разных циклах графа $G_{x+r,\Gamma(R)}$, достаточно найти представителей смежных классов группы $(\Gamma(R), \oplus)$ по подгруппе $\langle r \rangle$.

Обозначим через $\Gamma_0(R)$ простое подполе [11] поля $\Gamma(R)$. Если на группе $(\Gamma(R), \oplus)$ ввести внешнюю операцию умножения на элементы $\Gamma_0(R)$, то получим векторное пространство размерности m. Дополнив до базиса пространства элемент r, получим базис $r, r_2, \ldots, r_m$. Рассмотрим представление пространства в виде прямой суммы подпространств

$$\Gamma(R) = \langle r \rangle \oplus \langle r_2 \rangle \oplus \cdots \oplus \langle r_m \rangle.$$

Тогда множество

$$\{\langle r_2 \rangle \oplus \cdots \oplus \langle r_m \rangle\}$$

совпадает с множеством представителей смежных классов группы $(\Gamma(R), \oplus)$ по подгруппе $(\langle r \rangle, \oplus)$.

Изложим алгоритм построения системы $W_{f,R}$ представителей циклов максимальной длины графа $G_{f,R}$.

Как отмечалось выше, в качестве W_{f_1,R_1} можно взять любое одноэлементное множество $\{a\}$, $a \in R_1$, а в качестве W_{f_2,R_2} — одноэлементное множество $\{a^{'}\}$, где $a^{'}$ — элемент на цикле длины $q(q-1)$ графа G_{f_2,R_2}.

Покажем, как по имеющемуся элементу $a \in W_{f_k,R_k}$ построить множество из q/p элементов $A_a \subset W_{f_{k+1},R_{k+1}}$, $k \geqslant 3$.

Оценим сложность алгоритма 2.

Пусть $d = \deg f(x)$. Тогда значение многочлена $f(x)$ в точке $a \in R$ можно найти за d операций умножения и d операций сложения в кольце R. Для выполнения шага 1 алгоритма необходимо $q(q-1)p^{k-2}$ раз вычислить значение многочлена $f(x)$ степени d. На шаге 2 не требуется выполнения элементарных операций.

Алгоритм 2. Построение множества A_a

Вход: $f(x) \in R[x]$, $a \in W_{f_k,R_k}$
Выход: множество $A_a \subset W_{f_{k+1},R_{k+1}}$
1: Находим элемент $r \in \Gamma(R)$, такой, что

$$f^{[q(q-1)p^{k-2}]}(a) \equiv a + p^k r \pmod{J^{k+1}}.$$

2: Дополняем до базиса пространства $\Gamma(R)$ элемент r, получим базис $r, r_2, \ldots, r_m$. Тогда множество A_a совпадает с множеством

$$\{c_2 r_2 + \cdots + c_m r_m : c_i \in \Gamma(R), i = 2, \ldots, m\}.$$

Для построения множества $W_{f_{k+1},R_{k+1}}$ необходимо применить алгоритм 2 для каждого элемента $a \in W_{f_k,R_k}$. Следовательно, для построения множества $W_{f_{k+1},R_{k+1}}$ по имеющемуся множеству W_{f_k,R_k} требуется

$$|W_{f_k,R_k}| dq(q-1)p^{k-2} = \left(\frac{q}{p}\right)^{k-2} dq(q-1)p^{k-2} = d(q-1)q^{k-1}$$

операций умножения и столько же операций сложения в кольце R.

Для построения системы представителей циклов максимальной длины $W_{f,R}$ графа $G_{f,R}$ необходимо построить цепочку множеств (5), которая требует

$$\sum_{i=3}^{n} d(q-1)q^{k-1} = d(q-1)\sum_{i=1}^{n-2}\left(\frac{q}{p}\right)^{k-2} = d(q-1)q^{n-1}$$

операций умножения и столько же операций сложения в кольце R.

В итоге верна

Теорема 3. Пусть $f(x) \in R[x]$ — МДЦ-полином. Существует алгоритм построения системы $W_{f,R}$ представителей всех различных циклов длины $(q-1)qp^{n-2}$ графа $G_{f,R}$, требующий порядка $d(q-1)q^{n-1}$ операций умножения и порядка $d(q-1)q^{n-1}$ операций сложения в кольце R, где $d = \deg f$.

В работе [9] показано, что в графе $G_{f,R}$ ровно q^{n-1} точек не лежат на циклах максимальной длины. Отсюда следует, что алгоритм тотального опробования построения системы представителей циклов максимальной длины графа $G_{f,R}$ требует не менее $d(q-1)q^{n-1}$ и не более dq^n операций умножения и столько же операций сложения в кольце R и требует объём памяти, необходимый для хранения элементов кольца R. Предложенный алгоритм требует порядка $d(q-1)q^{n-1}$ операций умножения и порядка $d(q-1)q^{n-1}$ операций сложения в кольце R и не требует хранить в памяти все элементы кольца R.

Пусть далее $1 \leqslant M < (q/p)^{n-2}$. Необходимо построить множество W_M представителей M различных циклов длины $q(q-1)p^{n-2}$. Для этого построим множество W_{f_k,R_k} указанным выше способом, где k — минимальное натуральное число, удовлетворяющее условию $|M| < (q/p)^k$. Старшие $n-k-1$ разрядов элементов множества W_{f_k,R_k} зададим произвольно, например нулями. Обозначим полученное множество через W'_{f_k,R_k}. Имеет место включение $W_M \subseteq W'_{f_k,R_k}$. Таким образом, для построения множества W_M

требуется порядка $d(q-1)q^{k-1}$ операций умножения и порядка $d(q-1)q^{k-1}$ операций сложения, где $k = \lceil \log_{q/p} M \rceil + 1$. Хранить в памяти все элементы кольца R не требуется.

Теорема 4. Пусть $f(x) \in R[x]$ — МДЦ-полином. Существует алгоритм построения системы W_M представителей M различных циклов длины $(q-1)qp^{n-2}$ графа $G_{f,R}$, требующий порядка $d(q-1)q^{k-1}$ операций умножения и порядка $d(q-1)q^{k-1}$ операций сложения в кольце R, где $k = \lceil \log_{q/p} M \rceil + 1$.

Алгоритм тотального опробования построения множества W_M требует не менее $dMq(q-1)p^{n-2}$ и не более $dq^{n-1} + dMq(q-1)p^{n-2}$ операций умножения и столько же операций сложения в кольце R и требует хранить в памяти все элементы кольца R.

Заключение

В работе исследуется граф преобразования, задаваемого МДЦ-полиномом. Предложены алгоритмы построения системы представителей циклов максимальной длины графа преобразования, задаваемого МДЦ-полиномом. Построен алгоритм проверки, лежит ли заданный элемент кольца на каком-либо цикле максимальной длины графа преобразования.

Изучение полиномиальных конгруэнтных генераторов над кольцами Галуа далеко от завершения. По мнению автора, перспективными задачами являются вычисление ранга и изучение статистических свойств выходной последовательности полиномиального конгруэнтного генератора над кольцом Галуа.

ЛИТЕРАТУРА

1. *Carlitz L.* Functions and polynomials (mod p^n) // Acta Arithm. 1964. No. 9. P. 66–78.
2. *Анашин В. С.* О группах и кольцах, обладающих транзитивными полиномами // XVI Всес. алгебраическая конф. Тезисы. Ч. II. Л., 1981. С. 4–5.
3. *Кнут Д.* Искусство программирования. Т. 2. М.: Вильямс, 2000.
4. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика. 2002. Т. 14. Вып. 2. С. 20–32.
5. *Анашин В. С.* Равномерно распределенные последовательности целых p-адических чисел // Дискретная математика. 2002. Т. 14. Вып. 4. С. 1–63.
6. *Викторенков В. Е.* Орграф полиномиального преобразования над коммутативным локальным кольцом // Обозрение прикл. и промышл. матем. 2000. Т. 7. Вып. 2. С. 327.
7. *Нечаев А. А.* Полиномиальные преобразования конечных коммутативных колец главных идеалов // Матем. заметки. 1980. Т. 27. Вып. 6. С. 885–899.
8. *Ермилов Д. М., Козлитин О. А.* Цикловая структура полиномиального генератора над кольцом Галуа // Матем. вопросы криптографии. 2013. Т. 4. Вып. 1. С. 27–57.
9. *Ермилов Д. М.* О цикловой структуре биективных полиномиальных преобразований колец Галуа максимального периода // Обозрение прикл. и промышл. матем. 2013. Т. 20. Вып. 3.
10. *Елизаров В. П.* Конечные кольца. М.: Гелиос АРВ, 2006. 304 с.
11. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. М.: Гелиос АРВ, 2003. 749 с.

REFERENCES

1. *Carlitz L.* Functions and polynomials (mod p^n). Acta Arithm., 1964, no. 9, pp. 66–78.
2. *Anashin V. S.* O gruppah i kol'cah, obladajushhih tranzitivnymi polinomami. XVI Vsesojuznaja algebraicheskaja konferencija. Tezisy. P. II. Leningrad, 1981, pp. 4–5. (in Russian)

3. *Knuth D.* The Art of Computer Programming. V. 2. Reading, Massachusetts, Addison-Wesley, 1997.
4. *Larin M. V.* Tranzitivnye polinomial'nye preobrazovanija kolec vychetov. Diskretnaya matematika, 2002, vol. 14, no. 2, pp. 20–32. (in Russian)
5. *Anashin V. S.* Ravnomerno raspredelennye posledovatel'nosti celyh p-adicheskih chisel. Diskretnaya matematika, 2002, vol. 14, no. 4, pp. 1–63. (in Russian)
6. *Viktorenkov V. E.* Orgraf polinomial'nogo preobrazovanija nad kommutativnym lokal'nym kol'com. Obozrenie prikl. i promyshl. matem., 2000, vol. 7, no. 2, pp. 327. (in Russian)
7. *Nechaev A. A.* Polinomial'nye preobrazovanija konechnyh kommutativnyh kolec glavnyh idealov. Matem. Zametki, 1980, vol. 27, no. 6, pp. 885–899. (in Russian)
8. *Ermilov D. M., Kozlitin O. A.* Ciklovaja struktura polinomial'nogo generatora nad kol'com Galua. Matem. Voprosy Kriptografii, 2013, vol. 4, no. 1, pp. 27–57. (in Russian)
9. *Ermilov D. M.* O ciklovoj strukture biektivnyh polinomial'nyh preobrazovanij kolec Galua maksimal'nogo perioda. Obozrenie prikl. i promyshl. matem., 2013, vol. 20, no. 3. (in Russian)
10. *Elizarov V. P.* Konechnye kol'ca. Moscow, Gelios ARV Publ., 2006. 304 p. (in Russian)
11. *Gluhov M. M., Elizarov V. P., Nechaev A. A.* Algebra. Moscow, Gelios ARV Publ., 2003. 749 p. (in Russian)