Math-Net.Ru

Общероссийский математический портал

Д. Н. Былков, Построение новых классов фильтрующих генераторов, не имеющих эквивалентных состояний, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 4, 17–39

DOI: <https://doi.org/10.4213/mvk133>

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: 18.207.199.55

26 апреля 2023 г., 12:59:54

Построение новых классов
фильтрующих генераторов, не имеющих
эквивалентных состояний

Д. Н. Былков

ООО «Центр сертификационных исследований», Москва

Получено 22.IV.2013

Приведены условия, обеспечивающие отсутствие эквивалентных состояний для фильтрующего генератора, состоящего из регистра сдвига с приводимым характеристическим многочленом над кольцом вычетов (кольцом Галуа) и функции усложнения. Построен алгоритм восстановления линейной рекуррентной последовательности максимального периода над кольцом вычетов по линейной комбинации полиномов от знаков её старшей координатной последовательности. Приведен обзор предшествующих результатов.

Ключевые слова: линейные рекуррентные последовательности над кольцами вычетов, координатные последовательности, усложнения линейных рекуррент.

A construction of new classes of filter generators without equivalent states

D. N. Bylkov

LLC «Sertification Research Center», Moscow

Abstract. We find conditions ensuring the nonexistence of equivalent states for the filter generator consisting of a shift register with a reducible characteristic polynomial over residue ring (Galois ring) and a filter function. An algorithm for recovering the maximum period LRS over residue ring by the linear combination of polynomials of the highest coordinate sequence symbols is suggested. The review of previous results is given.

Keywords: linear recurrent sequences over residue rings, coordinate sequences, filtering of linear recurrences.

Введение и постановка задачи

В современной криптографии важной задачей является разработка различных способов получения псевдослучайных последовательностей. С середины прошлого века для построения псевдослучайных последовательностей широко применяются фильтрующие генераторы.

Фильтрующий генератор состоит из линейного регистра сдвига над кольцом R , вырабатывающего линейную рекуррентную последовательность $u : \mathbb{N}_0 \rightarrow R$ порядка $m = \deg F(x)$ с характеристическим многочленом $F(x) \in R[x]$, и функции усложнения $\Psi : R^m \rightarrow R$, преобразующей заполнение $u[i, i + m - 1] = (u(i), \dots, u(i + m - 1))$ регистра на i -м такте работы в знак $v(i) = \Psi(u[i, i + m - 1])$ выходной последовательности. К настоящему времени наиболее изучен случай, когда функция Ψ имеет вид $\Psi : R \rightarrow R$. В этом случае будем называть фильтрующий генератор *локально* фильтрующим генератором.

Для различных приложений теории кодирования и криптографии важна возможность однозначного восстановления начального вектора $u[0, m - 1]$ линейной рекурренты u по выходной последовательности $v = \Psi(u)$. То есть должна выполняться импликация

$$(u[0, m - 1] \neq u'[0, m - 1]) \Rightarrow (\exists l \in \mathbb{N}_0 : \Psi(u)(l) \neq \Psi(u')(l)). \quad (1)$$

К настоящему времени в работах отечественных и зарубежных авторов получено большое число результатов по этой тематике. Данная работа продолжает и развивает эти исследования.

Для большого класса функций $\Psi(x)$ расширен класс приводимых характеристических многочленов $F(x)$ над кольцом Галуа, для которых справедливо свойство (1). В случае, когда $R = \mathbb{Z}_{p^n}$, $p > 2$, линейная рекуррента u раскладывается в сумму своих p -ичных координатных последовательностей $u = \sum_{i=0}^{n-1} p^i u_i$. При некоторых ограничениях на коэффициенты закона рекурсии в работе строится алгоритм, однозначно восстанавливающий u по последовательности v , знаки которой заданы равенством $v(i) = \sum_{s=0}^{m-1} g_s u_{n-1}(i + s)^k \pmod{p}$, $1 < k < p$.

Приведем основные определения и факты, необходимые для понимания настоящей работы. Кольцом Галуа называется конечное коммутативное кольцо R с единицей e , в котором множество всех делителей нуля имеет вид pR для некоторого простого числа p (см., например, [1, 2]). Произвольное кольцо Галуа с точностью до изоморфизма определяется своей характеристикой p^n и числом элементов p^{nr} . Поэтому справедливо

обозначение $R = GR(q^n, p^n)$, $q = p^r$. Хорошо известными примерами колец Галуа являются примарное кольцо вычетов $\mathbb{Z}_{p^n}$ и конечное поле $GF(q)$ из q элементов.

Подмножество $K = \{b_0, \dots, b_{q-1}\}$ кольца R называется его *координатным множеством*, если его элементы образуют полную систему вычетов по модулю идеала pR .

В [3] показано, что каждый элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + pa_1 + \dots + p^{n-1}a_{n-1}, \quad a_s = \gamma_s^K(a) \in K, \quad s \in \overline{0, n-1}, \quad (2)$$

называемом *разложением элемента a в координатном множестве K* . Будем говорить, что $\gamma_s^K : R \rightarrow K$, $s \in \overline{0, n-1}$, — координатные функции на кольце R . Зададим на множестве K операции $\oplus$, $\otimes$, полагая для произвольных $a, b \in K$

$$a \oplus b = \gamma_0^K(a + b), \quad a \otimes b = \gamma_0^K(ab). \quad (3)$$

Алгебра $(K, \oplus, \otimes)$ есть поле из p^r элементов. Если не возникает двусмысленности толкования, знак $\otimes$ в формулах может опускаться. Важнейшим примером координатного множества является p -адическое координатное множество $\Gamma(R) = \{a \in R : a^q = a\}$ [1, 3], называемое также *координатным множеством Тейхмюллера*. Соответствующие координатные функции будем обозначать через $\gamma_s(a)$, $s \in \overline{0, n-1}$. В случае $R = \mathbb{Z}_{p^n}$ другим интересным примером является p -ичное координатное множество $\delta(R) = \{0, e, 2e, \dots, (p-1)e\}$, в этом случае соответствующие координатные функции будем обозначать через $\delta_s(a)$, $s \in \overline{0, n-1}$.

Пусть $F(x)$ — унитарный (со старшим коэффициентом e) многочлен степени m , через $L_R(F)$ будем обозначать множество всех линейных рекуррентных последовательностей над R с характеристическим многочленом $F(x)$.

Если u — последовательность над кольцом R , то последовательность $u_s = \gamma_s^K(u)$ над полем K вида

$$u_s(i) = \gamma_s^K(u(i)), \quad i \geq 0, \quad (4)$$

называется ее s -й координатной последовательностью.

Для кольца Галуа R поле $\bar{R} = R/pR$ будем называть его *полем вычетов*. Естественный эпиморфизм $\mu : R \rightarrow \bar{R}$ индуцирует эпиморфизм колец многочленов $R[x] \rightarrow \bar{R}[x]$. Образ многочлена $F(x) = \sum f_i x^i \in R[x]$ будем обозначать $\bar{F}(x) : \bar{F}(x) = \sum \bar{f}_i x^i \in \bar{R}[x]$. Многочлен $F(x) \in R[x]$ будем называть *многочленом Галуа*, если многочлен $\bar{F}(x)$ неприводим над полем $\bar{R}[x]$.

Определим умножение элементов $a \in K$ на элементы $\bar{r} \in \bar{R}$ равенством $\bar{r}a = \gamma_0^K(ra)$. Тогда K есть $\bar{R}$ -алгебра, и мы можем рассматривать любую периодическую последовательность $\xi \in K^\infty$ как ЛРП над полем $\bar{R}$. Обозначим через $M_\xi(x)$ минимальный многочлен ЛРП ξ в кольце $\bar{R}[x]$.

Через $L_R(F)^*$ будем обозначать подмножество линейных рекуррент $u \in L_R(F)$, для которых верно соотношение $u_0 \neq 0$. Будем называть многочлен $F(x)$ многочленом максимального периода (МП многочленом), если его период $T(F)$ равен $p^{n-1}(q^m - 1)$. В этом случае каждую ЛРП $u \in L_R(F)^*$ будем называть линейной рекуррентой максимального периода (МП ЛРП).

В данной работе решается задача о возможности восстановления ЛРП $u \in L_R(F)$ по последовательности $v \in K^\infty$ вида

$$v(i) = \Psi(u[\overline{i, i+m-1}]), \quad u[\overline{i, i+m-1}] = (u(i), \dots, u(i+m-1)), \quad (5)$$

где $\Psi : R^m \rightarrow K$ – некоторая функция. В этом случае будем кратко писать $v = \Psi(u)$. Заметим, что разложение (2) позволяет рассматривать функцию $\Psi(x_1, \dots, x_m)$ как функцию $\psi(x_{1,0}, \dots, x_{m,n-1})$ от переменных $x_{i,s} = \gamma_s^K(x_i) \in K$, $i \in \overline{1, m}$, $s \in \overline{0, n-1}$.

Требуется указать классы характеристических многочленов $F(x)$ и функций Ψ , обеспечивающих возможность однозначного восстановления исходной ЛРП u по последовательности v .

Обзор предшествующих результатов

В работах [1, 4, 5, 6] рассматривался случай, когда $F(x)$ – многочлен максимального периода (МП многочлен), а $\Psi(x_1, \dots, x_m) = \Psi(x)$, т. е. функция усложнения зависит только от одного знака исходной последовательности. В этом случае получены достаточные условия возможности восстановления u по v и предъявлены алгоритмы вычисления начального вектора $u[\overline{0, m-1}]$ по последовательности v . Часть этих результатов представлена ниже.

Теорема 1 ([4]). Пусть $R = \mathbb{Z}_{p^n}$, $K = \delta(R)$, $F(x) \in \mathbb{Z}_{p^n}[x]$ – МП многочлен, $u \in L_R(F)^*$ – МП ЛРП. Тогда начальный вектор ЛРП u однозначно восстанавливается со сложностью $O(mr^n)$ операций поля K по $O(mr^n)$ знакам последовательности $u_{n-1} = \delta_{n-1}(u)$, расположенным на её отрезке длины $(p^m - 1)p^{n-2} + m$.

Этот результат имеет обобщение на случай, когда R – произвольное кольцо Галуа, при некоторых ограничениях на координатное множество K .

Предложение 1 ([6]). Для любого координатного множества K кольца Галуа R существует единственный многочлен $\psi_K(x) \in R[x]$ со свойствами

$$\psi_K(\Gamma(R)) = K, \quad \deg \psi_K(x) \leq q - 1, \quad \psi_K(x) \equiv x \pmod{pR}.$$

Назовем многочлен $\psi_K(x)$ интерполяционным многочленом координатного множества K . Отметим, что в частном случае, когда $K = \Gamma(R)$, справедливо равенство $\psi_K(x) = x$. Рассмотрим p -ичное разложение числа $t \in \mathbb{N}$:

$$t = t_0 + pt_1 + \dots + p^k t_k, \quad t_0, \dots, t_k \in \overline{0, p-1},$$

и назовем индексом нелинейности ненулевого одночлена lx^t число $\text{ind } lx^t = t_0 + \dots + t_k$. Положим $\text{ind } 0 = -\infty$ и определим индекс нелинейности $\text{ind } \psi(x)$ произвольного многочлена $\psi(x)$ как максимум индексов нелинейности его одночленов. Заметим, что так как интерполяционный многочлен любого координатного множества K удовлетворяет соотношениям $\deg \psi_K(x) \leq q - 1, q = pr$, то $1 \leq \text{ind } \psi_K(x) \leq (p - 1)r$.

Теорема 2 ([6]). Если интерполяционный многочлен координатного множества K удовлетворяет условию $\text{ind } \psi_K(x) \leq (p - 1)$, то последовательность и однозначно восстанавливается по последовательности $\gamma_{n-1}^K(u)$. В частности, эта последовательность однозначно восстанавливается по старшей координатной последовательности $\gamma_{n-1}(u)$ из разложения Тейхмюллера.

Автором в работе [7] впервые рассмотрен случай, когда функция Ψ существенно зависит более чем от одного знака исходной последовательности, а многочлен $F(x)$ не является МП многочленом.

Скажем, что отображение $\Psi(x_1, \dots, x_l) : R^l \rightarrow K$ биективно по старшему разряду переменной x_1 , если при произвольной фиксации $nl - 1$ переменных

$$(x_{1,0}, \dots, x_{1,n-2}, x_{2,0}, \dots, x_{l,n-1}) = (c_{1,0}, \dots, c_{1,n-2}, c_{2,0}, \dots, c_{l,n-1}) \in K^{nl-1}$$

функция $\hat{\psi}(x) = \psi(c_{1,0}, \dots, c_{1,n-2}, x, c_{2,0}, \dots, c_{l,n-1})$ — биекция.

Теорема 3 ([7]). Пусть $l \in \overline{1, m-1}$, функция Ψ биективна по старшему разряду переменной x_1 , $F(x)$ — многочлен Галуа степени m над кольцом R и верно неравенство

$$T(F) \geq p^{2(n-1)}(q^{nl} - 1) \cdot q^{\frac{m}{2}}. \quad (6)$$

Тогда ЛРП и однозначно определяется по последовательности $\{\Psi(u(i), \dots, u(i + l))\}_{i=0}^\infty$.

Также в статье [7] автором была показана возможность однозначного восстановления ЛРП u в случае, когда $l = 1$ и многочлен $F(x)$ представляется в виде произведения двух многочленов Галуа. В настоящей работе этот результат обобщается на случай большего числа сомножителей.

В серии зарубежных публикаций [8, 9, 10, 11] рассматривается случай $R = \mathbb{Z}_{p^n}$, $K = \delta(R)$, $\Psi(x_1, \dots, x_m) = \Psi(x)$, в этих работах доказывается лишь принципиальная возможность восстановления исходной ЛРП, без предъявления алгоритмов восстановления.

Зададим многочлен $\Phi(x) \in R[x]$ равенством

$$x^{p^m-1} \stackrel{F}{\equiv} e + p\Phi(x), \quad \deg \Phi(x) < m.$$

Теорема 4 ([8], [10]). Пусть $F(x)$ – МП многочлен над кольцом $\mathbb{Z}_{p^n}$, пусть также $\eta(x_0, \dots, x_{n-2})$ – многочлен над полем $\mathbb{Z}_p$. Последовательность $u \in L_{\mathbb{Z}_p}(F)^*$ однозначно восстанавливается по усложнённой последовательности $\Psi(u) = \psi(\delta_0(u), \dots, \delta_{n-1}(u))$ в следующих ситуациях:

- 1) $p \geq 5$, $\psi(x_0, \dots, x_{n-1}) = x_{n-1}^k \oplus \eta(x_0, \dots, x_{n-2})$, $k \in \overline{2, p-1}$,
- 2) $p \geq 3$, $\deg \bar{\Phi}(x) \geq 1$,
 $\psi(x_0, \dots, x_{n-1}) = g(x_{n-1}) \oplus \eta(x_0, \dots, x_{n-2})$, $1 \leq \deg g(x_{n-1}) \leq p-1$

Теорема 5 ([12]). Пусть $p > 2$, $F(x) \in \mathbb{Z}_{p^n}[x]$ – МП многочлен и

$$\begin{aligned} \psi(x_0, \dots, x_{n-1}) &= x_{n-1}[\mu(x_{n-2}) \oplus \eta_{n-3}(x_0, \dots, x_{n-3})] \oplus \\ &\oplus \eta_{n-2}(x_0, \dots, x_{n-2}), \end{aligned} \quad (7)$$

причем $\text{НОД}(1 + \deg(\mu(x)), p-1) = 1$. Тогда ЛРП $u \in L_{\mathbb{Z}_p}(F)^*$ однозначно восстанавливается по последовательности $\psi(\delta_0(u), \dots, \delta_{n-1}(u))$.

Значительную часть этих результатов обобщает теорема 6.

Теорема 6 ([5]). Пусть $p > 2$, $R = \mathbb{Z}_{p^n}$, $K = \delta(R)$, $F(x) \in \mathbb{Z}_{p^n}[x]$ – МП многочлен, $u \in L_R(F)^*$ – МП ЛРП. Пусть также функция $\psi(x_0, \dots, x_{n-1}) = x_{n-1}^k \oplus c_{k-1}x_{n-1}^{k-1} \oplus \psi'(x_0, \dots, x_{n-1})$ удовлетворяет следующим условиям.

- 1) Если $k = 1$, то $\psi'(x_0, \dots, x_{n-1})$ не зависит от переменной x_{n-1} и $\deg \psi'_{x_{n-2}} \leq p-2$.
- 2) Если $k > 1$, то $\deg \psi'_{x_{n-1}} \leq k-2$ и выполняется хотя бы одно из условий
 - а) k нечетно, $n \geq 4$,

$$б) 2c_{k-1} \not\equiv k \pmod{p}.$$

$$в) (k, p-1) = 1.$$

Тогда начальный вектор ЛРП и однозначно восстанавливается со сложностью $O(p^{\frac{m}{2}} + mkr^n)$ операций поля K по $O(mkr^n)$ знакам последовательности $\psi(u_0, \dots, u_{n-1})$, расположенным на её отрезке длины $(p^m - 1)p^{n-2} + m$.

Автором совместно с А.А. Нечаевым построен алгоритм восстановления МП ЛРП по линейному усложнению отрезков старшей координатной последовательности.

Теорема 7 ([13]). Пусть $F(x) \in R[x]$ — МП-многочлен степени m и $g(x) \in \bar{R}[x]$ — многочлен со свойством $(g(x), \bar{F}(x)) = \bar{e}$.

Тогда для любой МП ЛРП $u \in L_R(F)^*$ существует алгоритм, восстанавливающий рекурренту и по последовательности $v = g(x)u_{n-1}$

(а) однозначно при $p > 2$ или $p = n = 2$;

(б) не более чем в двух вариантах при $p = 2$, $n > 2$.

В работах Qun-Xiong Zheng, Wen-Feng Qi и Tian Tian рассматривается другой способ усложнения рекуррент над кольцами вычетов — приведение каждого знака по другому модулю.

Теорема 8 ([14]). Пусть $F(x) \in \mathbb{Z}_{p^n}[x]$ — МП многочлен и натуральное число $M > 1$ делится на простое число, взаимно простое с p . Тогда для любых двух рекуррент $u, v \in L_{\mathbb{Z}_{p^n}}(F)^*$ справедливы импликации

$$(u = v) \Leftrightarrow (u \equiv v \pmod{M}).$$

Такой способ усложнения применим и в других ситуациях.

ЛРП над непримарными кольцами вычетов

Пусть натуральное число M имеет каноническое разложение $M = p_1^{l_1} \cdot \dots \cdot p_r^{l_r}$. Будем называть унитарный многочлен $F(x) \in \mathbb{Z}_M[x]$ примитивным многочленом, если $F(x) \pmod{p_i^{l_i}}$ — МП многочлен для всех $i \in \overline{1, r}$. Рекурренту $u \in L_{\mathbb{Z}_M}(F)$ будем называть рекуррентой максимального периода, если $u \pmod{p_i^{l_i}}$ — МП ЛРП для всех $i \in \overline{1, r}$. Через $L_{\mathbb{Z}_M}(F)^*$ будем обозначать подмножество линейных рекуррент максимального периода над непримарным кольцом $\mathbb{Z}_M$.

Теорема 9 ([15]). Пусть $M = 2^{32} - 1$ и для любой МП рекуррентны ранга n на её цикле встретятся все элементы из множества $\overline{0, 2^{32} - 2}$. Пусть натуральное число H делится на простое число, взаимно простое с M . Пусть также $F(x) \in \mathbb{Z}_M[x]$ — примитивный многочлен степени n . Тогда для любых двух рекуррент $u, v \in L_{\mathbb{Z}_M}(F)^*$ справедливы импликации

$$(u = v) \Leftrightarrow (u \equiv v \pmod{H}).$$

Пусть $M = p_1^{l_1} \cdot \dots \cdot p_r^{l_r}$ и n — натуральные числа. Назовем пару (M, n) *различимой* если для всех $i \neq j$ верно соотношение

$$\left(\frac{p_i^n - 1}{p_i - 1}, p_j^n - 1 \right) = 1.$$

Теорема 10 ([16]). Пусть каноническое разложение натурального числа M свободно от квадратов и на цикле каждой МП ЛРП ранга 1 появится хотя бы один четный элемент. Пусть n имеет вид $n = 2k + 1$ и пара чисел (M, n) различима. Пусть также $F(x) \in \mathbb{Z}_M[x]$ — примитивный многочлен степени n и для произвольной ЛРП $u \in L_{\mathbb{Z}_M}(F)^*$ найдутся такие $t_1, t_2 \in \mathbb{N}_0$, что

$$u(t_1) = 0, \quad u(t_2) \in \{M - 1, 1\}.$$

Тогда для любых двух рекуррент $u, v \in L_{\mathbb{Z}_M}(F)^*$ справедливы импликации

$$(u = v) \Leftrightarrow (u \equiv v \pmod{2}).$$

Пусть натуральное число M свободно от квадратов и $M = p_1 \cdots p_r$ — его каноническое разложение. Пусть $f(x) \in \mathbb{Z}_M[x]$ — примитивный многочлен степени n . Выберем число $t = \text{НОД} \left(\frac{p_1^n - 1}{p_1 - 1}, \dots, \frac{p_r^n - 1}{p_r - 1} \right)$. В силу выбора t справедливо соотношение $\deg x^t \pmod{f(x)} = 0$, поэтому можно считать, что $x^t \stackrel{f(x)}{\equiv} \xi_f \in \mathbb{Z}_M$. Будем называть элемент ξ_f ассоциированным с многочленом $f(x)$.

Теорема 11 ([17]). Пусть при сделанных выше обозначениях справедливы условия:

(1) на цикле произвольной рекуррент $u \in L_{\mathbb{Z}_M}(F)^*$ появляются все элементы кольца $\mathbb{Z}_M$;

(2) для каждого делителя $R > 1$ числа M существует натуральное такое число $k_R > 0$, что число $\xi_f^{k_R} \pmod{R}$ четное.

Тогда для любых двух рекуррент $u, v \in L_{\mathbb{Z}_M}(F)^*$ справедливы импликации

$$(u = v) \Leftrightarrow (u \equiv v \pmod{2}).$$

Отсутствие эквивалентных состояний у фильтрующего генератора с приводимым многочленом обратной связи

Как уже отмечалось выше, в большинстве работ изучается случай, когда $F(x)$ является многочленом максимального периода. Однако однозначное восстановление последовательности $u \in L_R(F)$ по последовательности $\Psi(u)$ возможно и в случае, когда многочлен $F(x)$ приводим.

Теорема 12. Пусть $F(x) = F_1(x) \cdot \dots \cdot F_k(x)$, где $F_1(x), \dots, F_k(x)$ — взаимно простые, унитарные, реверсивные многочлены Галуа над R . Положим $m_i = \deg F_i(x)$, $t_i = T(F_i)$, $i \in \overline{1, k}$, $\hat{t}_s = \prod_{i \in \overline{1, k} \setminus \{s\}} t_i$. Пусть для

всех $i = 1, \dots, k$ выполнены условия:

$$1) \quad \frac{t_i}{(t_i, \hat{t}_i)} \geq p^{2(n-1)}(q^n - 1) \cdot q^{\frac{m_i}{2}}; \quad (8)$$

$$2) \quad \left(T(\bar{F}_i), \prod_{j \in \overline{1, k} \setminus \{i\}} T(\bar{F}_j) \right) = 1. \quad (9)$$

Тогда для произвольной функции $\Psi(x) : R \rightarrow K$, биективной по старшему разряду переменной x , последовательность u однозначно определяется по последовательности $\Psi(u)$.

Нам потребуются несколько вспомогательных утверждений. Определим норму элемента $a \in R$ и норму последовательности $y \in R^\infty$ следующим образом:

$$\begin{aligned} \|a\| &= \max\{t \in \overline{0, n} \mid a \in p^t R\}, \\ \|y\| &= \max\{t \in \overline{0, n} \mid y \in p^t R^\infty\}. \end{aligned}$$

Лемма 1. Пусть $c, d \in R$. Справедлива импликация

$$(\|c - d\| = n - 1) \Rightarrow (c_j = d_j \text{ для всех } j \in \overline{0, n-2}; c_{n-1} \neq d_{n-1}).$$

Доказательство легко следует из (2). $\square$

Будем говорить, что семейство $L_R(F)^*$ сюръективно по норме, если для произвольной ЛРП $w \in L_R(F)^*$ для каждого $s \in \overline{0, n}$ найдется такое i_s , что $\|w(i_s)\| = s$.

Лемма 2 ([7]). Пусть $F(x)$ — такой унитарный многочлен над R , что семейство $L_R(F)^*$ сюръективно по норме. Тогда для любой последовательности w из $L_R(F)$ существует натуральное число j , для которого $w(j) = 0$.

Лемма 3 ([7]). Пусть семейство $L_R(G)^*$ сюръективно по норме и функция $\Psi(x): R \rightarrow K$ биективна по старшему разряду переменной x . Тогда последовательность $u \in L_R(G)$ однозначно определяется по последовательности $\Psi(u)$.

Отсюда следует, что для доказательства теоремы 12 достаточно доказать сюръективность по норме семейства последовательностей $L_R(F)^*$.

Лемма 4. Пусть $F(x) = F_1(x) \cdots F_k(x)$, где $F_1(x), \dots, F_k(x)$ — взаимно простые унитарные многочлены над R . Пусть семейства $L_R(F_i)^*$, $i \in \overline{1, k}$, сюръективны по норме. Пусть также для произвольной последовательности $v \in L_R(F_b)$, $b \in \overline{1, k}$, существует такое натуральное число i_0 , что

$$u(i_0 \cdot \hat{t}_b) = 0. \quad (10)$$

Тогда семейство $L_R(F)^*$ сюръективно по норме.

Доказательство. Так как многочлены $F_1(x), \dots, F_k(x)$ взаимно просты, то верно равенство $L_R(F) = L_R(F_1) \dot{+} \dots \dot{+} L_R(F_k)$, поэтому последовательность u однозначно представляется в виде $u = u^{[1]} + \dots + u^{[k]}$, где $u^{[i]} \in L_R(F_i)$, $i \in \overline{1, k}$. Из свойств операции $+$ в кольце R следует импликация

$$(\|u\| = 0) \Rightarrow (\min(\|u^{[1]}\|, \dots, \|u^{[k]}\|) = 0).$$

Пусть, для определенности, $\|u^{[1]}\| = 0$. В силу сюръективности по норме семейства $L_R(F_1)^*$ для произвольного $s \in \overline{0, n}$ существует такое $j_s \in \mathbb{N}_0$, что $\|v(j_s)\| = s$.

Так как последовательность $x^{j_s}u^{[2]}$ принадлежит $L_R(F_2)$, то по условию леммы $(x^{j_s}u^{[2]})(t_1i_1) = u^{[2]}(j_s + t_1i_1) = 0$ для некоторого i_1 .

Аналогичными рассуждениями можно показать, что существуют натуральные числа $i_2, \dots, i_{k-1}$, удовлетворяющие условиям

$$\begin{aligned} u^{[3]}(j_s + t_1i_1 + t_1t_2i_2) &= 0, \\ u^{[4]}(j_s + t_1i_1 + t_1t_2i_2 + t_1t_2t_3i_3) &= 0, \\ &\dots \\ u^{[k]}(j_s + t_1i_1 + t_1t_2i_2 + \dots + t_1t_2 \cdots t_{k-1}i_{k-1}) &= 0. \end{aligned}$$

В силу равенств

$$u(j_s + t_1 i_1 + \dots + t_1 \cdots t_{k-1} i_{k-1}) = \sum_{i=1}^k u^{[i]}(j_s + t_1 i_1 + \dots + t_1 \cdots t_{k-1} i_{k-1}) = u^{[1]}(j_s)$$

имеем: $\|u(j_s + t_1 i_1 + \dots + t_1 t_2 \cdots t_{k-1} i_{k-1})\| = s$. Лемма доказана. $\square$

Теорема 13 ([18]). Пусть $F(x)$ — многочлен Галуа степени m над кольцом R и верно неравенство (6). Тогда в цикле произвольной ЛРП $u \in L_R(F)^*$ содержатся все элементы кольца R .

Отсюда и из условия (8) следует сюръективность по норме семейств $L_R(F_i)^*$, $i \in \overline{1, k}$. Покажем, что для произвольной последовательности $w \in L_R(F_b)$ найдётся такое j_0 , что $w(j_0 \hat{t}_b) = 0$.

Рассмотрим последовательность $\hat{w}$, знаки которой заданы равенством

$$\hat{w}(i) = w(\hat{t}_b \cdot i), \quad i \in \mathbb{N}_0.$$

Пусть θ — корень многочлена $F_b(x)$ в расширении $S = GR(q^{m_b n}, p^n)$ кольца R . По теореме 18 существует единственная константа $\xi \in S$, для которой верны равенства

$$w(i) = \text{Tr}_R^S(\xi \theta^i), \quad i \in \mathbb{N}_0.$$

Из способа задания последовательности $\hat{w}$ следует, что

$$\hat{w}(i) = w(\hat{t}_b \cdot i) = \text{Tr}_R^S \left(\xi \left(\theta^{\hat{t}_b} \right)^i \right), \quad i \in \mathbb{N}_0. \quad (11)$$

Обозначим через $G(x)$ некоторый минимальный многочлен элемента $\beta = \theta^{\hat{t}_1}$. Докажем что $G(x)$ является многочленом Галуа.

Теорема 14 ([19]). Пусть T — расширение Галуа степени k кольца Галуа R . Тогда для любого элемента $\alpha \in T$ равносильны утверждения

- 1) $T = R[\alpha]$;
- 2) $\bar{T} = \bar{R}[\bar{\alpha}]$;
- 3) α — корень многочлена Галуа степени k над кольцом R .

Из условия (9) следует, что степень расширения $\bar{R}[\bar{\beta}]$ поля $\bar{R}$ равна m_b . Отсюда и из теоремы 14 следует, что элемент β — корень многочлена Галуа степени m_b над кольцом R .

Период многочлена $G(x)$ равен порядку его корня β :

$$T(G) = \text{ord } \beta = \text{ord } \theta^{t_b} = \frac{\text{ord } \theta}{(\text{ord } \theta, \hat{t}_b)}. \quad (12)$$

Отсюда и из условия (8) следует, что верно неравенство

$$T(G) \geq p^{2(n-1)}(q^n - 1) \cdot q^{\frac{m_b}{2}}. \quad (13)$$

Из (11) получаем, что последовательность $\hat{w}$ есть ЛРП с характеристическим многочленом $G(x)$. Так как для многочлена $G(x)$ выполнены условия теоремы 13, то по лемме 2 существует такое натуральное число j_0 , что $\hat{w}(j_0) = 0$. Остается заметить, что $w(\hat{t}_b j_0) = \hat{w}(j_0) = 0$. $\square$

Восстановление ЛРП МП над кольцом $\mathbb{Z}_{p^n}$ по линейному усложнению степеней знаков её старшей координатной последовательности

Как уже отмечалось выше, в работе [13] построен алгоритм восстановления рекурренты максимального периода над кольцом $\mathbb{Z}_{p^n}$ по линейному усложнению её старшей координатной последовательности. В настоящей работе рассматривается случай, когда выходная последовательность получается линейным усложнением степеней знаков старшей координатной последовательности. При некоторых ограничениях на характеристический многочлен предъясняется алгоритм восстановления исходной ЛРП по её усложнению.

Всюду далее $p > 2$, $u_0, \dots, u_{n-1}$ — координатные последовательности ЛРП $u \in L_R(F)$, полученные разложением знаков последовательности u в p -ичном координатном множестве.

Наша цель состоит в восстановлении ЛРП u по последовательности v , полученной по правилу

$$v(i) = \sum_{t=0}^{m-1} b_t(u_{n-1}(i+t)), \quad (14)$$

где $b_t : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ — некоторые функции, причем хотя бы одна из них не является константой.

Обозначим через k число $\max_t \deg b_t(x)$. Пусть $b_t(x) = \sum_{i=0}^k b_t^{(i)} x^i$; положим $g(x) = \sum_{t=0}^{m-1} b_t^{(k)} x^t$.

Теорема 15. Пусть $F(x) \in R[x]$ — МП многочлен вида $\bar{F}(x) = x^m \ominus bx \ominus c$. Тогда МП ЛРП $u \in L_R(F)^*$ однозначно восстанавливается по последовательности v в следующих случаях:

- 1) если известна ЛРП u_0 ;
- 2) если выполнены условия $\text{НОД}(k, p^m - 1) = 1$ и $g(\bar{w}^k) \neq \bar{0}$, где $\bar{w}$ — корень многочлена $\bar{F}(x)$.

Доказательство теоремы 15 приводится в конце статьи.

Сначала рассмотрим более простой случай, когда знаки последовательности v получаются из линейной комбинации степеней знаков координатной последовательности u_{n-1} .

Зафиксируем многочлен $g(x) = g_0 + \dots + g_{l-1}x^{l-1} \in \bar{R}[x]$; для удобства будем считать, что $g_0 \cdot g_{l-1} \neq 0$. Рассмотрим последовательность $v = g(x)(u_{n-1})^k$, $1 < k < p$, знаки которой определяются равенствами

$$v(i) = \sum_{s=0}^{l-1} g_s u_{n-1}(i+s)^k. \quad (15)$$

Теорема 16. Пусть $F(x) \in R[x]$ — такой МП многочлен степени m , что $\bar{F}(x) = x^m \ominus bx \ominus c$. Пусть $\deg g(x) \leq m-1$ и при $k > 2$ выполнены условия

$$g(\bar{w}^k) \neq \bar{0}, \quad g(\bar{w}^{k-1}) \neq \bar{0},$$

где $\bar{w}$ — корень многочлена $\bar{F}(x)$. Тогда МП ЛРП $u \in L_R(F)^*$ однозначно восстанавливается по последовательности v .

В случае, когда известна последовательность u_0 , можно отказаться от некоторых ограничений на выбор многочлена $g(x)$.

Теорема 17. Пусть $F(x) \in R[x]$ — такой МП многочлен степени m , что $\bar{F}(x) = x^m \ominus bx \ominus c$ и $\deg g(x) \leq m-1$. Тогда МП ЛРП $u \in L_R(F)^*$ однозначно восстанавливается по последовательностям u_0 , v .

Доказательство теорем 16, 17 сводится к указанию алгоритмов восстановления последовательностей $u_0, u_1, \dots, u_{n-2}, u_{n-1}$. При этом используется ряд важных дополнительных свойств МП-рекуррент и МП-многочленов, которые приводятся в следующем разделе.

Некоторые свойства МП-рекуррент.

Многочлен $F(x)$ имеет корень θ в расширении Галуа $S = GR(q^n, p^n)$, $q = p^m$, кольца R (см. [1]). Кольцо S содержит подмножество $\Gamma(S) = Q = \{\alpha \in S : \alpha^q = \alpha\}$, и любой элемент $\xi \in S$ однозначно

представляется в виде суммы

$$\xi = \xi_0 + p\xi_1 + \dots + p^{n-1}\xi_{n-1}, \quad \xi_s = \gamma_s(\xi) \in \Gamma(S). \quad (16)$$

Алгебра Q с операциями, определяемыми условиями (3), есть поле, содержащее в качестве подполя поле $\Gamma(R)$.

Пусть

$$\text{Tr}(x) = \text{Tr}_R^S(x) = \sum_{\sigma \in \text{Aut}(S/R)} \sigma(x)$$

— функция *след* из S в R ,

$$\text{tr}(x) = \text{tr}_{\Gamma(R)}^Q(x) = \sum_{\tau \in \text{Aut}(Q/\Gamma(R))} \tau(x) = \sum_{i=0}^{m-1} x^{p^i}$$

— функция *след* из Q в $\Gamma(R)$.

Теорема 18 (см. [19, 1]). *Для любой ЛРП $u \in L_R(F)$ существует единственная такая константа $\xi \in S$, что*

$$u(i) = \text{Tr}_R^S(\xi\theta^i), \quad i \geq 0. \quad (17)$$

Семейство $L_R(F)$ есть в точности множество всех последовательностей вида (17). При условии (17) и является МП ЛРП тогда и только тогда, когда $\xi_0 = \gamma_0(\xi) \neq 0$.

При этом справедливы соотношения

$$u_0(i) \stackrel{p}{\equiv} \text{tr}(\xi_0\omega^i), \quad \text{где } w = \gamma_0(\theta), \quad (18)$$

$$u_1(i) \stackrel{2}{\equiv} \text{tr}(\xi_1\omega^i) + i \text{tr}(\xi_0\nu\omega^i) + \varkappa(\xi_0\omega^i), \quad (19)$$

где $\nu = w^{-1}\theta_1$,

$$\varkappa(x) = \sum_{\substack{k_0+\dots+k_{m-1}=p \\ 0 \leq k_i \leq p-1, i=0,\dots,m-1}} \frac{1}{k_0! \cdot \dots \cdot k_{m-1}!} x^{k_0+k_1p+\dots+k_{m-1}p^{m-1}}. \quad (20)$$

Положим $\tau_t = (p^m - 1)p^t$ для $t \in \overline{0, n-1}$.

Лемма 5 (см. [3]). *Для $t \in \overline{0, n-1}$ верны соотношения*

$$\begin{aligned} x^{\tau_t} &\stackrel{F}{\equiv} e + p^{t+1}\Phi_{t+1}(x), \quad \deg \Phi_{t+1}(x) < m, \quad \overline{\Phi}_{t+1}(x) \neq 0; \\ \text{если } p > 2, \text{ то } \Phi_{t+1}(x) &\stackrel{p^t}{\equiv} \Phi_t(x) \quad \text{для } t \geq 1. \end{aligned} \quad (21)$$

Последовательность $u^{(s)} = \Phi_s(x)u$, $s \in \overline{1, n-1}$, называется s -й производной последовательностью ЛРП u . Заметим, что из (21) следует, что многочлен Φ_s однозначно определяется лишь по модулю p^{n-s} , и лишь по этому модулю однозначно определяется последовательность $u^{(s)}$. Для удобства будем считать, что многочлен $\Phi_s \in R[x]$ каким либо образом выбран и зафиксирован, и соответственно выбрана ЛРП $u^{(s)}$.

Положим $\mu^{(s)} = \Phi_s(\theta)$. Из соотношений (21) и теоремы 18 следуют равенства

$$u^{(s)}(i) = \text{Tr}(\xi \mu^{(s)} \theta^i), \quad (22)$$

$$\text{если } p > 2, \text{ то } u_0^{(t)} = u_0^{(1)} \text{ при } t \geq 1; \quad u_1^{(t)} = u_1^{(2)} \text{ при } t \geq 2. \quad (23)$$

Для $s \geq 2$, $t \in \overline{0, s-2}$ положим

$$u_{s,t} = (x^{\tau_0} \ominus e)^{p^{s-1}-p^t} u_s. \quad (24)$$

Лемма 6 (см. [3]). Пусть $F(x) \in \mathbb{Z}_p[x]$ — МП многочлен, $u \in L_R(F)^*$. Тогда:

1) Для $s \geq 1$ выполнены соотношения

$$(x^{\tau_{s-1}} \ominus e) u_s = u_0^{(s)}. \quad (25)$$

2) Если $R = \mathbb{Z}_p$, $p \geq 3$, то для $s \geq 2, t \in \overline{0, s-2}$

$$u_{s,t} = \left(u_0^{(1)}\right)^{p-1} \otimes u_{t+1} \oplus \frac{1}{2} \left(\left(u_0^{(1)}\right)^{p-1} \ominus u_0^{(1)} \right) \oplus z_{s,t}, \quad (26)$$

где

$$z_{s,t} = \begin{cases} \left(u_0^{(1)}\right)^{p-1} \otimes (\bar{\Phi}_1(x)^2 \otimes u_0), & \text{если } p = 3, t = 0, s > 2, \\ (\bar{\Phi}_1(x))^2 \otimes u_0, & \text{если } p = 3, t = 0, s = 2, \\ 0 & \text{в остальных случаях.} \end{cases} \quad (27)$$

Лемма 7 ([5]). 1) Для всех $s \in \overline{1, n-1}, k \in \overline{1, p-1}$ справедливо равенство

$$(x^{\tau_{s-1}} \ominus e)^k \otimes u_s^k = k! \left(u_0^{(1)}\right)^k. \quad (28)$$

2) Для всех $s \in \overline{2, n-1}, k \in \overline{1, p-1}$ справедливо равенство

$$(x^{\tau_{s-1}} \ominus e)^{k-1} \otimes u_s^k = k! \left(u_0^{(1)}\right)^{k-1} u_s \oplus \frac{k-1}{2} \left(u_0^{(1)}\right)^k. \quad (29)$$

3) Для всех $i \in \mathbb{N}_0$, $s \in \overline{1, n-1}$ справедливо равенство

$$u_s \left(i + \frac{\tau_s}{2} \right) = \begin{cases} \ominus u_s(i), & \text{если } \|u(i)\| \geq s, \\ \ominus 1 \ominus u_s(i), & \text{если } \|u(i)\| < s. \end{cases} \quad (30)$$

Лемма 8. Если $u \in L_{\overline{R}}(\overline{F}) \setminus \{0\}$, то матрица

$$A = \begin{pmatrix} u(\overline{i_1, i_1 + m - 1}) \\ \dots \\ u(\overline{i_m, i_m + m - 1}) \end{pmatrix} \quad (31)$$

обратима тогда и только тогда, когда система элементов $w^{i_1}, \dots, w^{i_m}$ линейно независима над $\overline{R}$.

Доказательство леммы 8 легко проводится с помощью [20].

Лемма 9. Пусть сохраняются обозначения предыдущей леммы и для чисел $d, s_1, \dots, s_{d-1} \in \mathbb{N}$ справедливы неравенства $1 \leq s_1 < \dots < s_{d-1} \leq m - 1$. Тогда для произвольного набора d -грамм $\vec{\alpha}_1, \dots, \vec{\alpha}_m \in \overline{R}^d$ числа $i_1, \dots, i_m$, удовлетворяющие следующим двум условиям:

1) справедливы равенства

$$u[i_j, i_j + s_1, \dots, i_j + s_{d-1}] = \vec{\alpha}_j, \quad j \in \overline{1, m}, \quad (32)$$

2) система $w^{i_1}, \dots, w^{i_m}$ линейно независима,

найдутся в том и только в том случае, когда

$$\text{rank} \{ \vec{\alpha}_1, \dots, \vec{\alpha}_m \} = d. \quad (33)$$

Доказательство. Пусть A — матрица вида (31). Обозначим $\vec{\alpha}_j = (\alpha_j^{(0)}, \dots, \alpha_j^{(d-1)})$, $j \in \overline{1, m}$. Так как u — МП ЛРП, то на цикле u встречаются все m -граммы (кроме нулевой). Поэтому можно выбрать $i_1, \dots, i_m$ так, чтобы выполнялись условия

1) $u[i_j, i_j + s_1, \dots, i_j + s_{d-1}] = \vec{\alpha}_j$, $j \in \overline{1, m}$,

2) $\text{rank} \{ A_t^\downarrow, t \in \overline{0, m-1} \setminus \{0, s_1, \dots, s_{d-1}\} \} = m - d$,

где $A_t^\downarrow$ — t -й столбец матрицы A . Положим $\beta_t^\downarrow = (\alpha_1^{(t)}, \dots, \alpha_m^{(t)})^T$, $t \in \overline{0, d-1}$. По теореме о ранге матрицы ранг системы строк $\{ \vec{\alpha}_1, \dots, \vec{\alpha}_m \}$ равен рангу системы столбцов $\beta = \{ \beta_0^\downarrow, \dots, \beta_{d-1}^\downarrow \}$. Из выбора матрицы A следует, что для всех $t \in \overline{0, d-1}$ справедливы равенства $\beta_t^\downarrow = A_{s_t}^\downarrow$, где $s_0 = 0$. Поэтому $\text{rank}(A) = m$, если и только если $\text{rank}(\beta) = \text{rank} \{ \vec{\alpha}_1, \dots, \vec{\alpha}_m \} = d$.

Для завершения доказательства леммы 9 остаётся воспользоваться леммой 8. $\square$

Алгоритмы восстановления начального заполнения ЛРП u по последовательности v

Как уже отмечалось, доказательство теоремы 16 состоит в поэтапном восстановлении разрядов ЛРП u .

Заметим, что если для некоторых $0 < j \leq n-1$ и $s < n-1$ нам удалось восстановить последовательность $u^{(s)} \pmod{p^j}$, то по ней легко восстанавливается последовательность $u \pmod{p^j}$, и наоборот. Достаточно при условии (21) выбрать многочлен $\Phi^{(s)}(x)$ так, что

$$\Phi^{(s)}(x)\Phi_s(x) \equiv e \pmod{F(x)}. \quad (34)$$

Тогда

$$u \equiv \Phi^{(s)}(x)u^{(s)} \pmod{p^j}. \quad (35)$$

Однозначное восстановление последовательности u_0 .

Лемма 10. *Последовательность u_0 однозначно вычисляется по последовательности v .*

Для доказательства леммы 10 нам потребуется ряд вспомогательных утверждений. Через y будем обозначать последовательность, знаки которой заданы равенствами $y(i) = i \cdot u_0^{(1)}(i)$.

Лемма 11. *Справедливо равенство*

$$\begin{aligned} \frac{1}{k!} \left((-e)^k x^{\frac{\tau_0}{2}} \oplus e \right) \left((x^{\tau_0} \ominus e)^{p^{n-2}-1} (x^{\tau_{n-2}} \ominus e)^{k-1} u_{n-1}^k \ominus y \oplus \frac{k!}{2} \left(u_0^{(1)} \right)^k \right) = \\ = \left(u_0^{(1)} \right)^{k-1}. \end{aligned}$$

Доказательство. Построим вспомогательную последовательность u' :

$$\begin{aligned} u' &= (x^{\tau_0} \ominus e)^{p^{n-2}-1} (x^{\tau_{n-2}} \ominus e)^{k-1} u_{n-1}^k = \\ &= (x^{\tau_0} \ominus e)^{p^{n-2}-1} \left(k! \left(u_0^{(1)} \right)^{k-1} u_{n-1} \oplus \frac{k-1}{2} \left(u_0^{(1)} \right)^k \right) = \\ &= k! \left(u_0^{(1)} \right)^{k-1} u_1 \oplus \frac{k!}{2} \left(u_0^{(1)} \right)^{k-1} \ominus \frac{k!}{2} \left(u_0^{(1)} \right)^k \oplus k! \left(u_0^{(1)} \right)^{k-1} z_{n-2,0}. \end{aligned}$$

Отсюда получаем, что знаки последовательности $u'' = u' \ominus y \oplus \frac{k!}{2} \left(u_0^{(1)} \right)^k$ имеют вид

$$u''(i) = k! \left(u_0^{(1)} \right)^{k-1} (\text{tr}(\xi_1 w^i) \oplus \varkappa(\xi_0 w^i) \oplus z_{n-2,0}(i)) \oplus \frac{k!}{2} \left(u_0^{(1)} \right)^{k-1}.$$

Несложно заметить, что справедливы равенства

$$\mathrm{tr}(\xi_1 w^{i+\frac{\tau_0}{2}}) = \ominus \mathrm{tr}(\xi_1 w^{i+\frac{\tau_0}{2}}), \quad z_{n-2,0}(i + \frac{\tau_0}{2}) = \ominus z_{n-2,0}(i).$$

Покажем, что $\varkappa(\xi_0 w^{i+\frac{\tau_0}{2}}) = \ominus \varkappa(\xi_0 w^i)$. Действительно, из формулы (20) следует, что показатель степени у каждого из мономов нечетный. Поэтому справедливы равенства

$$\varkappa(\xi_0 w^{i+\frac{\tau_0}{2}}) = \varkappa(\xi_0 w^i w^{\frac{\tau_0}{2}}) = \varkappa(\ominus \xi_0 w^{i+\frac{\tau_0}{2}}) = \ominus \varkappa(\xi_0 w^i).$$

Отсюда получаем утверждение леммы. $\square$

Воспользовавшись леммой 11, можно по последовательности v найти последовательность

$$g(x) \left(u_0^{(1)} \right)^{k-1}. \quad (36)$$

Если $k = 2$, то по последовательности $g(x)u_0$ последовательность u_0 определяется однозначно.

Далее будем рассматривать случай $k > 2$.

Лемма 12. Пусть $\ell \in L_{\mathbb{Z}_p}(\overline{F})^*$, $\ell(i) \stackrel{p}{\equiv} \mathrm{tr}(aw^i)$, где $a \in \Gamma(S) \setminus \{0\}$. Тогда для любого $t \in \overline{2, p-1}$ последовательность ℓ^t представляется в виде

$$\ell^t = \ell' \oplus \ell'',$$

где $\ell'(i) \stackrel{p}{\equiv} \mathrm{tr}(a^t w^{ti})$, а ℓ'' — ЛРП, минимальный многочлен которой взаимно прост с минимальным многочленом последовательности ℓ' .

Доказательство. Знаки ЛРП ℓ описываются равенствами

$$\ell(i) \stackrel{p}{\equiv} \mathrm{tr}(aw^i) = \sum_{j=0}^{m-1} (aw^i)^{p^j}.$$

Возведём последнее равенство в степень t :

$$\ell(i)^t \stackrel{p}{\equiv} \sum_{\substack{s_0 + \dots + s_{m-1} = t \\ s_0, \dots, s_{m-1} \in \overline{0, t}}} \frac{t!}{s_0! \dots s_{m-1}!} (aw^i)^{s_0 + ps_1 + \dots + p^{m-1}s_{m-1}}. \quad (37)$$

Период последовательности ℓ^t , очевидно, делит $\tau_0 = p^m - 1$. Так как это последовательность над полем $\mathbb{Z}_p$ из p элементов и $(p, \tau_0) = 1$, то

ее минимальный многочлен над $\mathbb{Z}_p$ есть некоторое произведение попарно различных унитарных неприводимых многочленов, степени которых делят m , а сама последовательность представляется в виде суммы

$$(\ell^t)(i) \stackrel{p}{\equiv} \sum_{s \in C} \text{tr}(b_s \omega^{ti}), \quad (38)$$

где C — множество минимальных представителей p -циклотомических классов, на которые разбивается множество $\overline{0, p^m - 2}$. Слагаемые вида $b\omega^{ti}$ появляются в (37) в точности при условии

$$s_0 + ps_1 + \dots + p^{m-1}s_{m-1} \stackrel{p^m-1}{\equiv} t.$$

Последнее условие выполняется тогда и только тогда, когда

$$s_0 = t, \quad s_1 = \dots = s_{m-1} = 0,$$

следовательно, $b_t = a^t$. Отсюда получаем утверждение леммы. $\square$

По лемме 12 последовательность $\left(u_0^{(1)}\right)^{k-1}$ можно представить в виде суммы $\left(u_0^{(1)}\right)^{k-1} = l' \oplus l''$, где $(M_{l'}(x), M_{l''}(x)) = e$, и справедливы равенства

$$l'(i) \stackrel{p}{\equiv} \text{tr}(\xi_0^{k-1} w^{(k-1)i}), \quad i \in \mathbb{N}_0.$$

Отсюда имеем:

$$g(x) \left(u_0^{(1)}\right)^{k-1} = g(x)l' \oplus g(x)l''.$$

В силу соотношения $(M_{l'}(x), M_{l''}(x)) = e$ из последней суммы можно выделить последовательность $g(x)l'$, знаки которой имеют вид

$$l'(i) \stackrel{p}{\equiv} \text{tr} \left(\xi_0^{k-1} g(w^{k-1}) w^{(k-1)i} \right).$$

Так как по условию теоремы 16 выполнено соотношение $g(w^{k-1}) \neq 0$, то по последовательности $g(x)l'$ однозначно определяется элемент ξ_0^{k-1} .

Проводя аналогичные рассуждения для последовательности

$$\frac{1}{k!} (x^{\tau_{s-1}} \ominus e)^k \otimes v = g(x) \left(u_0^{(1)}(i)\right)^k,$$

можно однозначно определить элемент ξ_0^k . Отсюда вычисляется ξ_0 , а значит, и последовательность u_0 .

Несложно увидеть, что если выполнены условия п. 2 теоремы 15, то по последовательности $g(x) \left(u_0^{(1)}(i)\right)^k$ однозначно находится элемент ξ_0 .

Восстановление последовательностей $u_{n-1}, \dots, u_1$.

Лемма 13. *Если выполнены условия теоремы 16, то по последовательностям u_0, v однозначно восстанавливаются ЛРП $u_{n-1}, u_{n-2}, \dots, u_1$.*

Доказательство. Вычислим

$$v' = (x^{\tau_{n-2}} \ominus e)^{k-1} v.$$

В силу соотношения (29) справедливо равенство

$$v' = g(x) \left(\left(u_0^{(1)} \right)^{k-1} u_{n-1} \right) \oplus \frac{k-1}{2} g(x) \left(u_0^{(1)} \right)^k; \quad (39)$$

вычитая из последнего соотношения известную последовательность, зависящую только от u_0 , получим:

$$v''(i) = \sum_{j=0}^{l-1} \oplus g_j \left(u_0^{(1)}(i+j) \right)^{k-1} u_{n-1}(i+j). \quad (40)$$

Рассмотрим сначала случай $b = c = e$, то есть $\bar{F}(x) = x^m - x - e$. В силу максимальной периода последовательности $u_0^{(1)}$ существует такое i_0 , что

$$u_0^{(1)}[\overline{i_0, i_0 + m - 1}] = \overbrace{(e, -e, e, -e, \dots, (-e)^{l-1})}^l, 0, \dots, 0).$$

Отсюда и из закона рекурсии ЛРП $u_0^{(1)}$ имеем:

$$\begin{cases} u_0^{(1)}[\overline{i_0, i_0 + m - 1}] = (e, -e, e, -e, \dots, (-e)^{l-1}, 0, \dots, 0), \\ u_0^{(1)}[\overline{i_0 + 1, i_0 + m}] = (-e, e, -e, \dots, (-e)^{l-1}, 0, 0, \dots, 0), \\ \dots \\ u_0^{(1)}[\overline{i_0 + l - 1, i_0 + m - l - 2}] = ((-e)^{l-1}, 0, \dots, 0). \end{cases} \quad (41)$$

Воспользовавшись равенствами (40), (41), вычислим значения рекуррент v'' в точках $i_0, \dots, i_0 + l - 1$:

$$v''(i_0 + s) = \sum_{j=s}^{l-1} g_{j-s} (-e)^{j(k-1)} u_{n-1}(i_0 + j), \quad s = 0, \dots, l-1. \quad (42)$$

Равенства (42) можно рассматривать как систему линейных уравнений относительно неизвестных $u_{n-1}(i_0), \dots, u_{n-1}(i_0 + l - 1)$. Нетрудно заметить, что матрица этой системы верхнетреугольная, и так как $g_0 \neq 0$, то система линейных уравнений (42) имеет единственное решение.

Случай $(b, c) = (e, e)$ был выбран исключительно ради удобства изложения. В случае $(b, c) \neq (e, e)$ выберем такт i_0 так, чтобы выполнялись условия $u_0^{(1)}(i_0) \neq 0$, $u_0^{(1)}(i_0 + t) = (-c/b)^t u_0^{(1)}(i_0)$, $t \in \overline{1, l-1}$, $u_0^{(1)}(i_0 + t) = 0$, $t \in \overline{l, m-1}$. Несложно увидеть, что и в этом случае система (42) будет иметь единственное решение.

Выберем $i_1, \dots, i_{m-l}$ так, чтобы выполнялись равенства

$$\begin{cases} u_0^{(1)}[\overline{i_1, i_1 + m - 1}] = (\overbrace{e, 0, \dots, 0}^l, e, \dots, 0), \\ u_0^{(1)}[\overline{i_2, i_2 + m - 1}] = (e, 0, \dots, 0, 0, e, \dots, 0), \\ \dots \\ u_0^{(1)}[\overline{i_{m-l}, i_{m-l} + m - 1}] = (\overbrace{e, 0, \dots, 0}^l, 0, \dots, e). \end{cases} \quad (43)$$

Воспользовавшись равенствами (40), (43), вычислим значения последовательности v'' в точках $i_1, \dots, i_{m-l}$:

$$\begin{aligned} v''(i_1) &= g_0 u_{n-1}(i_1), \\ &\dots \\ v''(i_{m-l}) &= g_0 u_{n-1}(i_{m-l}). \end{aligned} \quad (44)$$

Так как $g_0 \neq 0$, то из равенств (44) однозначно находятся знаки последовательности u_{n-1} в тактах $i_1, \dots, i_{m-l}$.

Таким образом, мы вычислили знаки рекурренты u_{n-1} в тактах с номерами $\vec{\lambda}_0 = (i_0, i_0 + 1, \dots, i_0 + l - 1, i_1, \dots, i_{m-l})$. Теперь найдём значения последовательностей $u_1, \dots, u_{n-2}$ в наборе точек $\vec{\lambda}_0$.

Положим для $j \in \mathbb{N}$

$$\vec{\lambda}_j = (i_0 + \tau_0 j, \dots, i_0 + l - 1 + \tau_0 j, i_1 + \tau_0 j, \dots, i_{m-l} + \tau_0 j).$$

Так как $T(u_0^{(1)}) = \tau_0$, то равенства (41), (43) выполняются также для набора точек $\vec{\lambda}_j$ при $j = 1, 2, \dots$. Отсюда и из соотношений (42), (44) следует, что знаки последовательности u_{n-1} можно найти в наборе точек $\vec{\lambda}_j$ для $j = 0, 1, 2, \dots$. Подставляя найденные с шагом τ_0 знаки ЛРП u_{n-1} в равенства (26), вычислим знаки рекуррент $u_1, \dots, u_{n-2}$ в наборе точек $\vec{\lambda}_0$.

Докажем линейную независимость системы элементов поля $\Gamma(S)$

$$\alpha = \{w^{i_0}, \dots, w^{i_0+l-1}, w^{i_1}, \dots, w^{i_{m-l}}\}$$

над $\Gamma(R)$. Так как матрица

$$A = \begin{pmatrix} u_0^{(1)}[\overline{i_0, i_0 + m - 1}] \\ \dots \\ u_0^{(1)}[\overline{i_0 + l - 1, i_0 + m - l - 2}] \\ u_0^{(1)}[\overline{i_1, i_1 + m - 1}] \\ \dots \\ u_0^{(1)}[\overline{i_{m-l+1}, i_{m-l+1} + m - 1}] \end{pmatrix} =$$

$$= \begin{pmatrix} e & -e & \dots & (-e)^{l-1} & 0 & 0 & \dots & 0 \\ -e & \dots & (-e)^{l-1} & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ (-e)^{l-2} & (-e)^{l-1} & 0 & \dots & 0 & 0 & \dots & 0 \\ (-e)^{l-1} & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ e & 0 & \dots & 0 & e & 0 & \dots & 0 \\ e & 0 & \dots & 0 & 0 & e & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ e & 0 & \dots & 0 & 0 & 0 & \dots & e \end{pmatrix}$$

обратима, то согласно лемме 8 система элементов α линейно независима. Отсюда следует, что последовательность $u \pmod{p^n}$ однозначно определяется своими значениями в наборе точек λ_0 . $\square$

Доказательство теоремы 15. Если последовательность u_0 известна, то последовательности $u_{n-1}, \dots, u_1$ восстанавливаются по алгоритму, указанному в доказательстве леммы 13.

Если выполнены условия пункта 2 теоремы, то последовательность u_0 восстанавливается по лемме 10, далее переходим к п. 1. $\square$

Автор благодарен рецензенту Ларину М.В. за внимательное прочтение работы, позволившее улучшить ее текст. Автор признателен Серебрякову Е.М. за замечания, позволившие уточнить доказательства.

Список литературы

- [1] Kurakin V.L., Kuzmin A.S., Mikhalev A.V., Nechaev A.A., "Linear recurring sequences over rings and modules", *J. Math. Sci.*, **76**:6 (1995), 2793–2915.
- [2] Кузьмин А.С., Куракин В.Л., Нечаев А.А., "Псевдослучайные и полилинейные последовательности", *Труды по дискретной математике*, **1** (1997), 139–202.
- [3] Кузьмин А. С., Нечаев А.А., "Линейные рекуррентные последовательности над кольцами Галуа", *Алгебра и логика*, **34**:2 (1995), 169–189.

- [4] Кузьмин А. С., Нечаев А. А., “Линейные рекуррентные последовательности над кольцами Галуа”, *Успехи матем. наук*, **48**:1 (1993), 167–168.
- [5] Кузьмин А. С., Маршалко Г.Б., Нечаев А. А., “Восстановление линейной рекурренты над примарным кольцом вычетов по ее усложнению”, *Математические вопросы криптографии*, **1**:2 (2010), 31–56.
- [6] Кузьмин А. С., Нечаев А. А., “Восстановление линейной рекурренты максимального периода над кольцом Галуа по ее старшей координатной последовательности”, *Дискретная математика*, **23**:2 (2011), 3–31.
- [7] Былков Д. Н., “Класс усложнений линейных рекуррент над кольцом Галуа, не приводящий к потере информации”, *Проблемы передачи информации*, **46**:3 (2010), 51–59.
- [8] Tian Tian, Wen-Feng Qi, “Injectivity of compressing map on primitive sequences over $Z/(p^e)$ ”, *IEEE Trans. Inf. Theory*, **53**:8 (2007), 2960–2966.
- [9] Xuan-Yong Zhu, Wen-Feng Qi, “Uniqueness of the distribution of zeroes of primitive level sequences over $Z/(p^e)$ ”, *Finite Fields and their Appl.*, **11**:1 (2005), 30–44.
- [10] Xuan-Yong Zhu, Wen-Feng Qi, “Compression mappings on primitive sequences over $Z/(p^e)$ ”, *IEEE Trans. Inf. Theory*, **50**:10 (2004), 2442–2448.
- [11] Xuan-Yong Zhu, Wen-Feng Qi, “Further result of compressing maps on primitive sequences modulo odd prime powers”, *IEEE Trans. Inf. Theory*, **53**:8 (2007), 2985–2990.
- [12] Sun Zhonghua, Qi Wen-Feng, “Injective maps on primitive sequences over $\mathbb{Z}_p$ ”, *Appl. Math. J. Chinese Univ., Ser. B*, **22**:4 (2007), 469–477.
- [13] Былков Д.Н., Нечаев А.А., “Алгоритм восстановления последовательностей, полученных линейным усложнением координатных последовательностей ЛРП над кольцом $R = \mathbb{Z}_{p^n}$ ”, *Дискретная математика*, **22**:4 (2010), 104–120.
- [14] Xuan-Yong Zhu, Wen-Feng Qi, “On the distinctness of modular reductions of maximal length sequences modulo odd prime powers”, *Math. Comput.*, **77**:263 (2008), 1623–1637.
- [15] Qun-Xiong Zheng, Wen-Feng Qi, Tian Tian, “On the distinctness of modular reductions of primitive sequences over $Z/(2^{32}-1)$ ”, *Designs, Codes and Cryptography*, **70** (2014), 359–368.
- [16] Qun-Xiong Zheng, Wen-Feng Qi, Tian Tian, “On the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers”, *IEEE Trans. Inf. Theory*, **59**:1 (2013), 680–690.
- [17] Qun-Xiong Zheng, Wen-Feng Qi, “Further results on the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers”, *IEEE Trans. Inf. Theory*, **59**:6 (2013), 4013–4019.
- [18] Камловский О.В., Кузьмин А.С., “Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа”, *Фунд. и прикл. матем.*, **6**:4 (2000), 1083–1094.
- [19] Нечаев А.А., “Код Кердока в циклической форме”, *Дискретная математика*, **4**:1 (1989), 123–139.
- [20] Глухов М.М., Елизаров В.П., Нечаев А.А., *Алгебра*, **2**, М. : Гелиос, 2003, 336 с.