Math-Net.Ru

Общероссийский математический портал

А. С. Кузьмин, А. А. Нечаев, Восстановление линейной рекурренты максимального периода над кольцом Галуа по ее старшей координатной последовательности, *Дискрет. матем.*, 2011, том 23, выпуск 2, 3–31

DOI: <https://doi.org/10.4213/dm1137>

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: 54.92.164.108

26 апреля 2023 г., 05:53:32

Восстановление линейной рекурренты максимального периода над кольцом Галуа по ее старшей координатной последовательности

© 2011 г. А. С. Кузьмин, А. А. Нечаев

Рассматривается псевдослучайная последовательность w над полем $GF(q)$, $q = p^r$, получающаяся из ЛРП u максимального периода над кольцом Галуа $R = GR(q^n, p^n)$ путем выделения знаков старших разрядов в некотором координатном представлении элементов кольца. Выдвигается гипотеза о возможности восстановления последовательности u по последовательности w . Доказано, что такое восстановление возможно при некоторых ограничениях на выбор координатного представления. В частности, оно возможно всегда, если $R = \mathbb{Z}_{p^n}$, а так же если w — старшая координатная последовательность в p -адическом разложении последовательности u над произвольным кольцом Галуа.

Работа выполнена по заказу Академии криптографии Российской Федерации.

1. Введение

Пусть $R = GR(q^n, p^n)$ — кольцо Галуа мощности q^n и характеристики p^n , где p — простое число, $q = p^r$, $\bar{R} = R/pR = GF(q)$ — поле вычетов кольца R . Для каждого элемента $a \in R$ положим $\bar{a} = \mu(a)$, где $\mu: R \rightarrow \bar{R}$ — естественный эпиморфизм. Подмножество $K \subseteq R$ назовем координатным, если $0 \in K$ и ограничение эпиморфизма μ на K есть биекция, то есть если $0 \in K$ и для каждого элемента $a \in R$ существует единственный элемент $\kappa(a) \in K$ такой, что $\bar{a} = \overline{\kappa(a)}$. В таком случае (см. [5]) каждый элемент $a \in R$ однозначно представляется в виде

$$a = \kappa_0(a) + p\kappa_1(a) + \dots + p^{n-1}\kappa_{n-1}(a), \quad \kappa_t(a) \in K, \quad t = 0, 1, \dots, n-1.$$

Назовем функцию $\kappa_t: R \rightarrow K$ t -й координатной функцией (в координатном множестве K), а разложение (1) — разложением элемента a в координатном множестве K (K -разложением a). Очевидно, при введенных обозначениях координатное множество K удовлетворяет условию $K = \kappa_0(R)$.

Важнейшим примером координатного множества является p -адическое координатное множество

$$\Gamma(R) = \{\alpha \in R: \alpha^q = \alpha\}.$$

Будем записывать $\Gamma(R)$ -разложение элемента $a \in R$ в виде

$$a = \gamma_0(a) + p\gamma_1(a) + \dots + p^{n-1}\gamma_{n-1}(a), \quad \gamma_t(a) \in \Gamma(R), \quad t \in \{0, 1, \dots, n-1\}, \quad (1.1)$$

и называть (1.1) p -адическим координатным разложением элемента a . Соответственно будем называть и координатные функции $\gamma_t: R \rightarrow \Gamma(R)$, $t \in \{0, 1, \dots, n-1\}$.

В случае, когда $R = GR(p^n, p^n) = \mathbf{Z}_{p^n}$, представляет интерес также p -ичное координатное множество

$$\delta(R) = \{0, 1, \dots, p-1\},$$

которому соответствует разложение

$$a = \delta_0(a) + p\delta_1(a) + \dots + p^{n-1}\delta_{n-1}(a), \quad (1.2)$$

где $\delta_t(a) \in \{0, 1, \dots, p-1\}$, $t \in \{0, 1, \dots, n-1\}$. Заметим, что

$$\Gamma(\mathbf{Z}_{p^n}) = \{0, 1, 2^{p^{n-1}}, \dots, (p-1)^{p^{n-1}}\}$$

и равенство $\Gamma(\mathbf{Z}_{p^n}) = \{0, 1, \dots, p-1\}$ выполняется тогда и только тогда, когда либо $n = 1$, либо $p = 2$.

Пусть $u: \mathbf{N}_0 \rightarrow R$ — последовательность элементов кольца R :

$$u = (u(0), u(1), \dots, u(i), \dots).$$

Определим произведение последовательности u на многочлен

$$A(x) = \sum_{s \geq 0} a_s x^s \in R[x]$$

как последовательность $v = A(x)u$ с общим членом

$$v(i) = \sum_{s \geq 0} a_s u(i+s).$$

Последовательность u называется линейной рекуррентной последовательностью (ЛРП) порядка m , если она аннулируется каким-либо унитарным (со старшим коэффициентом e) многочленом степени m , называемым характеристическим многочленом ЛРП u . Характеристический многочлен наименьшей возможной степени называется минимальным многочленом ЛРП, а его степень — рангом ЛРП.

Если u — ЛРП ранга m над кольцом R , то ее период $T(u)$ удовлетворяет неравенству $T(u) \leq (q^m - 1)p^{n-1}$ и при условии $T(u) = (q^m - 1)p^{n-1}$ говорят, что u есть ЛРП максимального периода (u есть МП ЛРП) над R [17].

Рассматривая K -координатное разложение знаков ЛРП u

$$\begin{aligned} u(i) &= w_0(i) + pw_1(i) + \dots + p^{n-1}w_{n-1}(i), \\ w_t(i) &= \kappa_t(u(i)) \in K, \quad t = 0, 1, \dots, n-1, \end{aligned} \quad (1.3)$$

сопоставляем последовательности u координатные последовательности $w_0, \dots, w_{n-1}$ над полем K .

Разложение последовательности u в координатном множестве $\Gamma(R)$ будем записывать в виде

$$\begin{aligned} u(i) &= u_0(i) + pu_1(i) + \dots + p^{n-1}u_{n-1}(i), \\ u_t(i) &= \gamma_t(u(i)) \in \Gamma(R), \quad t \in \{0, 1, \dots, n-1\}. \end{aligned} \quad (1.4)$$

Наша основная цель состоит в продвижении доказательства гипотезы о том, что справедлива следующая теорема.

Теорема 1. Последовательность w_n однозначно восстанавливается по последовательности w_{n-1} при произвольном координатном множестве K .

В случае, когда $R = \mathbf{Z}_{p^n}$, $K = \{0, 1, \dots, p-1\}$, эта теорема (и некоторые ее обобщения на последовательности более сложного вида) уже доказана (см. [3, 9, 12, 19, 22–28]).

Здесь доказательство теоремы 1 будет приведено для случая, когда R — произвольное кольцо Галуа, u — произвольная МП ЛРП над R и координатное множество K удовлетворяет некоторым ограничениям, которые мы сейчас сформулируем.

Пусть

$$\Gamma(R) = \{\alpha_0 = 0, \alpha_1, \dots, \alpha_{q-1}\}.$$

Тогда для любого многочлена $\psi(x) \in R[x]$ такого, что $\psi(0) = 0$, $\psi(x) \equiv x \pmod{pR}$, множество

$$K = \psi(\Gamma(R)) = \{\psi(\alpha_0), \dots, \psi(\alpha_{q-1})\}$$

есть, очевидно, также координатное множество. Обратно, справедливо следующее утверждение.

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

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

Доказательство. Мы упорядочим элементы множества K следующим образом:

$$K = \{a_0, \dots, a_{q-1}\}, \quad \bar{a}_s = \bar{\alpha}_s, \quad s \in \{0, q, \dots, q-1\}.$$

Теперь набор неизвестных коэффициентов искомого многочлена

$$\psi_K(x) = l_0 + l_1x + \dots + l_{q-1}x^{q-1}$$

вычисляется как единственное решение системы линейных уравнений

$$\sum_{t=0}^{q-1} l_t \alpha_s^t = a_s, \quad s \in \{0, 1, \dots, q-1\}.$$

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 $t \in \mathbf{N}$

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

и назовем индексом нелинейности $\text{ind } a$ 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 по условию интерполяционный многочлен любого координатного множества K удовлетворяет соотношениям

$$\deg \psi_K(x) \leq q-1, \quad q = p^r,$$

поэтому

$$1 \leq \text{ind } \psi_K(x) \leq (p-1)r. \quad (1.5)$$

Основным результатом данной работы является следующая теорема.

Теорема 2. *Если интерполяционный многочлен координатного множества K удовлетворяет условию*

$$\text{ind } \psi_K(x) \leq (p-1), \quad (1.6)$$

то последовательность и однозначно восстанавливается по последовательности w_{n-1} из K -координатного разложения (1.3). В частности, эта последовательность однозначно восстанавливается по старшей координатной последовательности u_{n-1} из p -адического разложения (1.4).

Так как для кольца $R = \mathbf{Z}_{p^n}$ справедливо равенство $q = p$, то есть $r = 1$, ввиду (1.5) справедливо следующее утверждение.

Следствие 1. *Для любого координатного множества K кольца $R = \mathbf{Z}_{p^n}$ любая МП ЛРП и над R однозначно восстанавливается по старшей координатной последовательности w_{n-1} из K -координатного разложения (1.3).*

Ранее в [26] теорема 2 была доказана для частного случая, когда $R = GR(2^{rn}, 2^n)$, $K = \Gamma(R)$, и многочлен $F(x)$ удовлетворяет условию $\deg \Phi(x) > 0$, где $\Phi(x)$ определяется из (2.1).

2. Основные свойства МП ЛРП

Здесь мы приведем известные результаты, необходимые для доказательства теоремы 2.

2.1. Описания МП ЛРП

Будем называть унитарный многочлен $F(x) \in R[x]$ реверсивным, если существует параметр $t \in \mathbf{N}$ такой, что $F(x) \mid x^t - e$. Последнее условие равносильно условию $F(0) \in R^*$ (см. [17]). Наименьший из таких параметров t называется периодом многочлена $F(x)$ и обозначается через $T(F)$. Известно, что если $\deg F(x) = m$, то $T(F) \leq \tau p^{n-1}$, где $\tau = q^m - 1$. Если $T(F) = \tau p^{n-1}$, то $F(x)$ называют многочленом максимального периода (МП многочленом) над кольцом Галуа R .

Пусть $L_R(F)$ есть совокупность всех ЛРП над R с характеристическим многочленом $F(x) \in R[x]$. Обозначим через $\overset{F}{\equiv}$ отношение сравнимости по модулю многочлена $F(x)$ на $R[x]$ и через $\bar{F}(x)$ — образ этого многочлена при естественном эпиморфизме $R[x] \rightarrow \bar{R}[x]$.

Теорема 3 ([4, 5, 12]). *Реверсивный многочлен $F(x) \in R[x]$ степени m есть МП многочлен тогда и только тогда, когда $T(\bar{F}) = \tau$ и*

$$x^\tau \overset{F}{\equiv} e + p\Phi(x), \quad \deg \Phi(x) < m, \quad (2.1)$$

где

$$\begin{aligned} \bar{\Phi}(x) &\neq 0, & p > 2 \text{ или } p = n = 2, \\ \bar{\Phi}(x) &\notin \{0, \bar{e}\}, & p = 2 < n. \end{aligned} \quad (2.2)$$

Если $F(x)$ есть МП многочлен, и $\tau_s = \tau p^s$, то для любой ЛРП $u \in L_R(F)$ равносильны следующие утверждения:

- (а) u — ЛРП максимального периода, то есть $T(u) = T(F)$;
- (б) в разложении (1.3) $w_0 \neq 0$;
- (в) в разложении (1.3) $T(w_s) = \tau_s$ для некоторого $s \in \{0, 1, \dots, n-1\}$;
- (г) в разложении (1.3) $T(w_s) = \tau_s$ для каждого $s \in \{0, 1, \dots, n-1\}$.

Всюду далее $F(x)$ есть МП многочлен степени m . В таком случае $F(x)$ имеет корень θ в расширении Галуа $S = GR(q^{mn}, p^n)$ кольца R , $S = R[\theta]$ и группа $\text{Aut}(S/R)$ автоморфизмов кольца S над R есть циклическая группа порядка m : $\text{Aut}(S/R) = \langle \rho \rangle$ (см. [10, 16]). Обозначим через $L_R^*(F)$ подмножество всех ЛРП из $L_R(F)$, которые имеют период $T(F)$.

Функция

$$\text{Tr}(x) = \text{Tr}_R^S(x) = x + \rho(x) + \dots + \rho^{m-1}(x)$$

на S называется функцией след из S на R . Она задает эпиморфизм модулей $\text{Tr}: {}_R S \rightarrow {}_R R$ [10, 16].

Теорема 4 ([16]). Для любой ЛРП $u \in L_R(F)$ существует единственная константа $\xi \in S$ такая, что

$$u(i) = \text{Tr}(\xi \theta^i), \quad i \geq 0. \quad (2.3)$$

При этом u есть МП ЛРП тогда и только тогда, когда $\bar{\xi} \neq 0$, то есть $\bar{u} \neq 0$.

2.2. Производные последовательности

Доказательство теоремы 2 основывается на следующих свойствах координатных последовательностей w_t и функций $\gamma_t(\text{Tr}(x))$, $t \in \{0, 1, \dots, n-1\}$.

Лемма 1 ([5]). Для $t \in \{0, 1, \dots, n-1\}$ справедливы следующие соотношения:

$$x^{\tau_t} \stackrel{F}{\equiv} e + p^{t+1} \Phi_{t+1}(x), \quad \deg \Phi_{t+1}(x) < m, \quad \bar{\Phi}_{t+1}(x) \neq 0. \quad (2.4)$$

При этом, если $p = 2 < n$, то

$$\bar{\Phi}_2(x) \stackrel{F}{\equiv} \bar{\Phi}_1^2(x) + \bar{\Phi}_1(x), \quad \Phi_{t+1}(x) \stackrel{2^t}{\equiv} \Phi_t(x), \quad t \geq 2; \quad (2.5)$$

если $p \geq 3$, то

$$\Phi_{t+1}(x) \stackrel{p^t}{\equiv} \Phi_t(x), \quad t \geq 1. \quad (2.6)$$

Введем обозначения

$$u^{(t)} = \Phi_t(x)u, \quad w_s^{(t)} = \kappa_s(u^{(t)}), \quad t \in \{0, 1, \dots, n-1\}. \quad (2.7)$$

Будем называть последовательность $u^{(t)}$ из (2.7) t -й производной последовательности u . Заметим, что из (2.4) многочлен Φ_t определяется однозначно лишь по модулю p^{n-t} и лишь по этому модулю однозначно определяется последовательность $u^{(t)}$. Мы,

для удобства, будем считать, что многочлен $\Phi_t \in R[x]$ каким-либо образом выбран и зафиксирован, и соответственно выбрана ЛРП $u^{(t)}$.

Ввиду (2.4), многочлен $\Phi_t(x)$ взаимно прост с $F(x)$, поэтому $u^{(t)} \in L_R^*(F)$, и, ввиду (2.5), (2.6), справедливы следующие соотношения: если $p = 2$, то

$$\begin{aligned} w_0^{(t)} &= w_0^{(2)}, & t \geq 2, \\ w_1^{(t)} &= w_1^{(3)}, & t \geq 3; \end{aligned} \quad (2.8)$$

если $p > 2$, то

$$\begin{aligned} w_0^{(t)} &= w_0^{(1)}, & t \geq 2, \\ w_1^{(t)} &= w_1^{(2)}, & t \geq 2. \end{aligned} \quad (2.9)$$

Определим операции $\oplus$ и $\otimes$ на координатном множестве K правилами

$$\forall \alpha, \beta \in K: \quad \alpha \oplus \beta = \kappa_0(\alpha + \beta), \quad \alpha \otimes \beta = \kappa_0(\alpha \cdot \beta). \quad (2.10)$$

Тогда $(K, \oplus, \otimes) = GF(q)$ — поле и биекция $\mu: K \rightarrow \bar{R}$ есть изоморфизм полей.

В частности, мы можем задать структуры полей на координатных множествах $\Gamma(R)$ и $\Gamma(S)$. Для этого надо в (2.10) выбрать $K = \Gamma(R)$ (или $K = \Gamma(S)$) и использовать в качестве κ_0 координатную функцию γ_0 . При этом поле $P = \Gamma(R) = GF(q)$ естественным образом превращается в подполе поля $Q = \Gamma(S) = GF(q^m)$. Далее обозначения Q и P используются без оговорок.

Эти рассуждения позволяют вывести из (2.16) следующее представление с помощью функции след младшей координатной последовательности $u_0^{(t)}$:

$$u_0^{(t)}(i) = \text{tr}(\xi_0^{(t)} \theta_0^i), \quad i \geq 0, \quad (2.11)$$

где

$$\text{tr}(x) = \text{tr}_P^Q(x) = x \oplus x^q \oplus \dots \oplus x^{q^{m-1}}$$

— след из поля Q в подполе P .

2.3. Эквивалентные формулировки задачи

Задача равносильна восстановлению координатных последовательностей $u_0, \dots, u_{n-1}$ из (1.4). Из очевидных соотношений

$$\begin{aligned} u &\equiv u_0 + pu_1 + \dots + p^{s-1}u_{s-1} \\ &\equiv w_0 + pw_1 + \dots + p^{s-1}w_{s-1} \pmod{p^s}, \quad s \in \{1, \dots, n-1\}, \end{aligned} \quad (2.12)$$

следует, что для любого $s \in \{1, \dots, n-1\}$ восстановление комплекта последовательностей $u_0, \dots, u_{s-1}$ равносильно восстановлению комплекта последовательностей $w_0, \dots, w_{s-1}$.

Из (2.7) видно, что для любых $t \in \{0, 1, \dots, n-1\}$ и $s \in \{0, 1, \dots, n-1\}$ комплект последовательностей $w_0^{(t)}, \dots, w_s^{(t)}$ однозначно определяется по комплекту $w_0, \dots, w_s$. Обратно, так как существуют многочлены $\Phi^{(t)}(x) \in R[x]$ со свойствами

$$\Phi^{(t)}(x)\Phi_t(x) \equiv e \pmod{F(x)}, \quad t \in \{0, 1, \dots, n-1\}, \quad (2.13)$$

то из (2.7) следуют равенства

$$u = \Phi^{(t)}(x)u^{(t)}, \quad t \in \{0, 1, \dots, n-1\}. \quad (2.14)$$

Следовательно, комплект $w_0, \dots, w_s$ однозначно определяется по комплекту $w_0^{(t)}, \dots, w_s^{(t)}$.

Таким образом, задача равносильна задаче восстановления последовательностей $w_0^{(t)}, w_1^{(t)}, \dots, w_{s-1}^{(t)}$ для некоторого $t \in \mathbb{N}$.

С другой стороны, для восстановления ЛРП u нам достаточно найти коэффициент ξ в представлении (2.3). Последняя задача равносильна восстановлению коэффициентов $\xi_0, \dots, \xi_{n-1}$ в разложении

$$\xi = \xi_0 + p\xi_1 + \dots + p^{n-1}\xi_{n-1}, \quad \xi_s \in \Gamma(S). \quad (2.15)$$

Из (2.7) следует, что

$$u^{(t)}(i) = \text{Tr}(\xi^{(t)}\theta^i), \quad i \geq 0, \quad \xi^{(t)} = \xi\Phi_t(\theta). \quad (2.16)$$

При этом, согласно (2.14), $\xi = \xi^{(t)}\Phi^{(t)}(\theta)$, и восстановление набора $\xi_0, \dots, \xi_{s-1}$ равносильно восстановлению $\xi_0^{(t)}, \dots, \xi_{s-1}^{(t)}$.

3. Однозначное восстановление последовательности w_0

Основной метод, используемый далее для восстановления последовательности u по ее старшей координатной последовательности w_{n-1} , мы называем методом сечений координатных последовательностей.

Определим умножение элементов $\alpha \in K$ на элементы $\bar{r} \in \bar{R}$ равенством

$$\bar{r}\alpha = x_0(r\alpha).$$

Тогда K есть $\bar{R}$ -алгебра, и мы можем умножать любую последовательность над K на многочлен из $\bar{R}[x]$, а также рассматривать любую периодическую последовательность ω над K как ЛРП над полем $\bar{R}$.

Назовем сечением координатной последовательности w_s из (1.3) результат произведения этой последовательности на некоторый многочлен из $\bar{R}[x]$, который представляет собой последовательность, более простую, чем w_s . Первый важный пример такого сечения дает следующая лемма.

Лемма 2. Для $s \geq 1$ справедливо равенство

$$(x^{\tau_{s-1}} - \bar{e})w_s = w_0^{(s)}. \quad (3.1)$$

Доказательство. Из теоремы 3 (г) следует, что

$$(x^{\tau_{s-1}} - e)w_r = 0, \quad r \in \{0, 1, \dots, s-1\}.$$

Поэтому

$$(x^{\tau_{s-1}} - e)u \equiv p^s(x^{\tau_{s-1}} - e)w_s \pmod{p^{s+1}}.$$

Согласно (2.4) и (2.7)

$$(x^{\tau_{s-1}} - e)u = p^s\Phi_s(x)w \equiv p^s w_0^{(s)} \pmod{p^{s+1}}.$$

Сопоставляя правые части двух последних сравнений, получаем (3.1).

Предложение 2. При любом координатном множестве K последовательность w_0 однозначно восстанавливается по последовательности w_{n-1} .

Доказательство. Из (3.1) получаем равенство

$$w_0^{(n-1)} = (x^{\tau_{n-2}} - \bar{e})w_{n-1},$$

и из (2.14) находим, что

$$w_0 = \kappa_0(u) = \bar{\Phi}^{(n-1)}(x)w_0^{(n-1)}. \quad (3.2)$$

Заметим, что при $n = 2$ этим завершается восстановление всей последовательности u . Поэтому всюду далее предполагается, что $n \geq 3$.

4. Восстановление ЛРП u в случае $p > 2$

Алгоритм, вытекающий из доказательства предложения 2, однозначно восстанавливает последовательность w_0 , а значит, и последовательности $u_0, u_0^{(1)}$ (см. раздел 2.3). Остается доказать, что при условии теоремы 2 последовательности $u_s, s \in \{1, \dots, n-2\}$, восстанавливаются однозначно по $u_0^{(1)}, w_{n-1}$. Для этого нам потребуется несколько дополнительных результатов.

4.1. Функция переноса и связанные с ней сечения

Назовем функцией переноса в координатном множестве K функцию $\Delta = \Delta_K: K \times K \rightarrow K$ на поле $(K, \oplus, \otimes)$, определяемую равенством

$$\Delta(x, y) = \kappa_1(x + y).$$

Заметим, что по определению $0 \in K$, поэтому $\Delta(x, 0) = \Delta(0, y) = 0$. С этой функцией связаны следующие продуктивные в ряде случаев сечения.

Лемма 3. При любом $p \geq 2$ справедливы соотношения

$$(x^{\tau_{s-2}} - \bar{e})w_s = w_1^{(s-1)} \oplus \Delta(w_{s-1}, w_0^{(s-1)}), \quad s \geq 2. \quad (4.1)$$

Доказательство. Согласно (2.4) и (2.7),

$$\begin{aligned} (x^{\tau_{s-2}} - e)u &= p^{s-1}\Phi_{s-1}(x)u = p^{s-1}u^{(s-1)} \\ &\equiv p^{s-1}w_0^{(s-1)} + p^s w_1^{(s-1)} \pmod{p^{s+1}}. \end{aligned} \quad (4.2)$$

С другой стороны, по теореме 3 (г)

$$(x^{\tau_{s-2}} - e)u \equiv p^{s-1}(x^{\tau_{s-2}} - e)(w_{s-1} + pw_s) \pmod{p^{s+1}}; \quad (4.3)$$

согласно лемме 2 и определению функции Δ_K

$$\begin{aligned} (x^{\tau_{s-2}} - e)w_{s-1} &= (w_{s-1} \oplus w_0^{(s-1)}) - w_{s-1} \\ &\equiv w_{s-1} + w_0^{(s-1)} - p\Delta_K(w_{s-1}, w_0^{(s-1)}) - w_{s-1} \\ &\equiv w_0^{(s-1)} - p\Delta_K(w_{s-1}, w_0^{(s-1)}) \pmod{p^2}. \end{aligned} \quad (4.4)$$

Подставляя правую часть (4.4) в правую часть (4.3), получаем, что

$$(x^{\tau_{s-2}} - e)u \equiv p^{s-1}w_0^{(s-1)} + p^s((x^{\tau_{s-2}} - e)w_s - \Delta_K(w_{s-1}, w_0^{(s-1)})) \pmod{p^{s+1}}. \quad (4.5)$$

Теперь, сравнивая правые части соотношений (4.5) и (4.2), приходим к равенству (4.1). Лемма доказана.

Опишем явный вид функции переноса Δ_K . Из определения интерполяционного многочлена координатного множества K следуют соотношения

$$\begin{aligned} \psi_K(x) &= x + p\lambda_K(x), & \lambda_K(x) &\in R[x], \\ \deg \lambda_K(x) &\leq q-1, & \text{ind } \lambda_K(x) &\leq \text{ind } \psi_K(x) \end{aligned} \quad (4.6)$$

Очевидно, что условие $K = \Gamma(R)$ эквивалентно выполнению равенству $\lambda_K(x) = 0$.

Лемма 4 ([5]). Для любых $x, y \in K$ справедливы соотношения

$$\varkappa_1(\gamma_0(x)) \stackrel{p}{\equiv} -\lambda_K(\gamma_0(x)) \stackrel{p}{\equiv} -\lambda_K(x), \quad (4.7)$$

$$\Delta_K(x, y) \stackrel{p}{\equiv} \sum_{s=1}^{p-1} (-1)^s \frac{1}{s} (x^s y^{(p-s)})^h + \lambda_K(x) + \lambda_K(y) - \lambda_K(x+y), \quad (4.8)$$

где $h = p^{r-1}$.

Доказательство. По определению функций ψ_K и λ_K , справедливы равенства

$$\varkappa_0(\gamma_0(x)) = \psi_K(\gamma_0(x)) = \gamma_0(x) + p\lambda_K(\gamma_0(x)).$$

Отсюда, пользуясь сравнением

$$\gamma_0(x) \stackrel{p^2}{\equiv} \varkappa_0(\gamma_0(x)) + p\varkappa_1(\gamma_0(x)),$$

вытекающим из определения координатных функций $\varkappa_i$, получаем, что

$$p(\lambda_K(\gamma_0(x)) + \varkappa_1(\gamma_0(x))) \stackrel{p^2}{\equiv} 0,$$

откуда и следует (4.7).

Докажем (4.8) сначала для случая, когда $K = \Gamma(R)$. Нетрудно заметить, что для любого $c \in R$ справедливы соотношения

$$c^q \stackrel{p^2}{\equiv} \gamma_0(c)^q = \gamma_0(c),$$

и потому

$$c - c^q \stackrel{p^2}{\equiv} p\gamma_1(c).$$

Следовательно, для любых $\alpha, \beta \in \Gamma(R)$ справедливы соотношения

$$p\gamma_1(\alpha + \beta) \stackrel{p^2}{\equiv} \alpha + \beta - (\alpha + \beta)^q = - \sum_{i=1}^{q-1} \binom{q}{i} \alpha^i \beta^{q-i}.$$

Отсюда, пользуясь тем, что $\binom{q}{i} \stackrel{p^2}{\equiv} 0$, если $q = p^r > p$ и i не делится на $h = p^{r-1}$, а также используя формулу Люка

$$\binom{q}{hs} \stackrel{p^2}{\equiv} \binom{p}{s}$$

(см. теорему 4.71 в [1]), получаем, что

$$p\gamma_1(\alpha + \beta) \stackrel{p^2}{\equiv} - \sum_{s=1}^{p-1} \binom{p}{s} (\alpha^s \beta^{p-s})^h,$$

откуда

$$\gamma_1(\alpha + \beta) \stackrel{p}{\equiv} \sum_{s=1}^{p-1} (-1)^s \frac{1}{s} (\alpha^s \beta^{p-s})^h = \mathfrak{S}(\alpha, \beta). \quad (4.9)$$

Для случая $K = \Gamma(R)$ формула (4.8) доказана.

Для произвольного координатного множества K и любых $x, y \in K$ справедливы равенства

$$\begin{aligned} x &= \psi_K(\alpha) = \alpha + p\lambda_K(\alpha), \\ y &= \psi_K(\beta) = \beta + p\lambda_K(\beta) \end{aligned}$$

при подходящих $\alpha, \beta \in \Gamma(R)$. Тогда

$$\begin{aligned} \Delta_K(x, y) &= \kappa_1((\alpha + p\lambda_K(\alpha)) + (\beta + p\lambda_K(\beta))) \\ &\stackrel{p}{\equiv} \kappa_1(\alpha + \beta) + \lambda_K(\alpha) + \lambda_K(\beta). \end{aligned} \quad (4.10)$$

Так как

$$\begin{aligned} \kappa_1(\alpha + \beta) &\stackrel{p}{\equiv} \kappa_1(\gamma_0(\alpha + \beta) + p\gamma_1(\alpha + \beta)) \\ &\stackrel{p}{\equiv} \kappa_1(\gamma_0(\alpha + \beta)) + \gamma_1(\alpha + \beta), \end{aligned}$$

в силу (4.7)

$$\kappa_1(\alpha + \beta) \stackrel{p}{\equiv} \gamma_1(\alpha + \beta) - \lambda_K(\alpha + \beta).$$

Подставляя полученное выражение в (4.10) и пользуясь (4.9), получаем, что

$$\begin{aligned} \Delta_K(x, y) &\stackrel{p}{\equiv} \mathfrak{S}(\alpha + \beta) + \lambda_K(\alpha) + \lambda_K(\beta) - \lambda_K(\alpha + \beta) \\ &\stackrel{p}{\equiv} \mathfrak{S}(x + y) + \lambda_K(x) + \lambda_K(y) - \lambda_K(x + y). \end{aligned}$$

Лемма доказана.

Для произвольной функции $f(x, y) \in R[x, y]$ пусть

$$\Lambda(f(x, y)) = f(x + y, y) - f(x, y). \quad (4.11)$$

Очевидно, Λ есть линейное преобразование модуля $R[x, y]_{R[y]}$, причем, если $f(x, y) \neq 0$, то

$$\begin{aligned} \deg_x \Lambda(f(x, y)) &< \deg_x f(x, y), \\ \text{ind}_x \Lambda(f(x, y)) &< \text{ind}_x f(x, y). \end{aligned} \quad (4.12)$$

Лемма 5. Если $p > 2$, то справедливо сравнение

$$\Lambda^{p-2}(\Delta_K(x, y)) \stackrel{p}{\equiv} \left(xy^{p-1} - \frac{y^p}{2} \right)^h - \Lambda^{p-1}(\lambda_K(x)), \quad h = p^{r-1}. \quad (4.13)$$

Доказательство. Из (4.8), пользуясь тем, что $\Lambda^{p-2}(x^s) = 0$ для $s < p - 2$ и

$$\lambda_K(x) - \lambda_K(x + y) = -\Lambda(\lambda_K(x)),$$

получаем, что

$$\Lambda^{p-2}(\Delta_K(x, y)) \stackrel{p}{\equiv} \Lambda^{p-2}(B(x))^h + \Lambda^{p-1}(\lambda_K(x)),$$

где

$$B(x, y) = -x^{p-1}y + \frac{1}{2}x^{p-2}y^2.$$

Индукцией по $i \in \{0, 1, \dots, p-2\}$ несложно получить, что

$$\Lambda^i(B(x, y)) = (a_i x^{p-i-1} y^{i+1} + b_i x^{p-i-2} y^{i+2}) + C_i(x, y), \quad (4.14)$$

где $\deg_x C_i(x, y) < p - 2 - i$, $i \in \{0, \dots, p-2\}$,

$$\begin{aligned} a_0 &= -1, & a_{i+1} &= (p - i - 1)a_i; \\ b_0 &= \frac{1}{2}, & b_{i+1} &= \binom{p-i-1}{2} a_i + (p-i-2)b_i. \end{aligned} \quad (4.15)$$

Отсюда при $i = p - 2$ получается (4.13). Лемма доказана.

Лемма 6. Если $\text{ind } \psi_K(x) \leq p - 1$, в частности, если $R = \mathbf{Z}_{p^n}$, то для любых $x, y \in K$ при условии $p > 2$ справедливо соотношение

$$\Lambda^{p-2}(\Delta_K(x, y)) \stackrel{p}{\equiv} (xy^{p-1})^h + c(y), \quad (4.16)$$

где $c(y)$ не зависит от x ; при условии $p = 2$ справедливо соотношение

$$\Delta_K(x, y) \stackrel{2}{\equiv} (xy)^h. \quad (4.17)$$

Доказательство. При условии $\text{ind}_x \psi_K(x) \leq p - 1$ ввиду (4.6) справедливо неравенство $\text{ind}_x \lambda_K(x) \leq p - 1$, и многочлен $\Lambda^{p-1}(\lambda_K(x))$ не зависит от x ввиду (4.12). Теперь при $p > 2$ (4.16) следует из (4.13).

Если $p = 2$, то из (4.8) ввиду условия $\text{ind}_x \lambda_K(x) \leq p - 1 = 1$ следует соотношение

$$\Delta_K(x, y) \stackrel{2}{\equiv} (xy)^h + c,$$

где $c = \Lambda(\lambda_K(x))$ — константа. Подставляя в последнее сравнение $x = 0$, получаем $c \stackrel{2}{\equiv} 0$, то есть справедливо (4.17).

Этот результат позволяет в случае $p > 2$ построить следующее, более “эффективное” сечение последовательности w_s .

Лемма 7. Если $p > 2$ и $\text{ind}_x \psi_K(x) \leq p - 1$, то при $s \geq 2$

$$(x^{\tau_{s-2}} - \bar{e})^{p-1} w_s = (w_{s-1}(w_0^{(1)})^{p-1})^h \oplus d_s(w_0), \quad (4.18)$$

где $d_s(w_0)$ — известная функция, зависящая только от w_0 .

Доказательство. При $p > 2$ ввиду (2.9) сечения (4.1) имеют при $s \geq 2$ вид

$$(x^{\tau_{s-2}} - \bar{e})w_s = \Delta_K(w_{s-1}, w_0^{(1)}) \oplus w_1^{(s-1)}. \quad (4.19)$$

Отсюда получаем, что

$$(x^{\tau_{s-2}} - \bar{e})^2 w_s = (x^{\tau_{s-2}} - \bar{e})\Delta_K(w_{s-1}, w_0^{(1)}) \oplus g_s, \quad (4.20)$$

где $g_s = (x^{\tau_{s-2}} - \bar{e})w_1^{(s-1)}$ и согласно (3.1)

$$g_s = g_s(w_0) = \begin{cases} w_0^{(1)(1)} = \bar{\Phi}_1(x)\bar{\Phi}_1(x)w_0, & s = 2; \\ 0, & s \geq 3. \end{cases} \quad (4.21)$$

Заметим, что $x^{\tau_{s-2}}w_0^{(1)} = w_0^{(1)}$, и, согласно (3.1), $x^{\tau_{s-2}}w_{s-1} = w_{s-1} \oplus w_0^{(1)}$. Поэтому

$$(x^{\tau_{s-2}} - \bar{e})\Delta_K(w_{s-1}, w_0^{(1)}) = \Lambda(\Delta_K)(w_{s-1}, w_0^{(1)}),$$

и из (4.20) следует равенство

$$(x^{\tau_{s-2}} - \bar{e})^2 w_s = \Lambda(\Delta_K)(w_{s-1}, w_0^{(1)}) \oplus g_s(w_0). \quad (4.22)$$

Если $p = 3$, то $\Lambda(\Delta_K) = \Lambda^{p-2}(\Delta_K)$, и с учетом (4.16) равенство (4.22) превращается в (4.18), где $d_s(w_0) = c(w_0^{(1)}) \oplus g_s(w_0)$.

Если $p > 3$, то используя (4.22) получаем цепочку равенств

$$\begin{aligned} (x^{\tau_{s-2}} - \bar{e})^{p-1} w_s &= (x^{\tau_{s-2}} - \bar{e})^{p-3} (\Lambda(\Delta_K)(w_{s-1}, w_0^{(1)}) \oplus g_s(w_0)) \\ &= (x^{\tau_{s-2}} - \bar{e})^{p-3} (\Lambda(\Delta_K)(w_{s-1}, w_0^{(1)})) \\ &= \Lambda^{p-2}(\Delta_K)(w_{s-1}, w_0^{(1)}). \end{aligned}$$

Теперь, опять с использованием (4.16), получившееся равенство превращается в (4.18), где $d_s(w_0) = c(w_0^{(1)})$.

4.2. Алгоритм восстановления ЛРП и

Так как $u_0^{(1)}$ — МП ЛРП периода τ_0 над полем P , имеющая представление через след вида (2.11), можно выбрать набор тактов $J_1 = \{j_1 < j_2 < \dots < j_m\} \subset \{0, 1, \dots, \tau_0 - 1\}$ так, что система элементов $\theta_0^{j_1}, \dots, \theta_0^{j_m}$ линейно независима над полем P и элементы $u_0^{(1)}(j_1), \dots, u_0^{(1)}(j_m)$ обратимы в P . В таком случае из $w_0^{(1)} \stackrel{P}{\equiv} u_0^{(1)}$ следуют условия:

(J_1) координаты вектора $w_0^{(1)}[J_1] = (w_0^{(1)}(j_1), \dots, w_0^{(1)}(j_m))$ обратимы в поле K ;

(J_2) система элементов $\theta^{j_1}, \dots, \theta^{j_m}$ линейно независима над кольцом R , то есть является базисом модуля ${}_R S$.

Теперь для восстановления ЛРП u достаточно найти вектор

$$u[J_1] = (u(j_1), \dots, u(j_m)). \quad (4.23)$$

Действительно, по этому вектору можно однозначно восстановить константу ξ в представлении (2.3), решая систему линейных уравнений

$$\begin{aligned} \text{Tr}(\xi \theta^{j_1}) &= u(j_1), \\ &\dots \\ \text{Tr}(\xi \theta^{j_m}) &= u(j_m), \end{aligned} \quad (4.24)$$

которая имеет единственное решение ввиду условия $(J_1 2)$.

Для восстановления вектора (4.23) воспользуемся разложением (1.3), из которого следует равенство

$$u[J_1] = w_0[J_1] + p w_1[J_1] + \dots + p^{n-2} w_{n-2}[J_1] + p^{n-1} w_{n-1}[J_1]. \quad (4.25)$$

Векторы $w_{n-1}[J_1], w_0[J_1]$ нам уже известны. Построим по ним последовательно векторы $w_{n-2}[J_1], \dots, w_1[J_1]$.

Как отмечено в разделе 2.3, по известной последовательности w_0 однозначно строится $w_0^{(1)}$. Пусть

$$I_*^{(1)} = \{J_1 \in \mathbf{N}_0 : w_0^{(1)}(j) \neq 0\}.$$

Используя операции в поле $(K, \oplus, \otimes)$, соотношение (4.18) можно переписать в виде

$$w_{s-1}(w_0^{(1)})^{p-1} = ((x^{\tau_{s-2}} - \bar{e})^{p-1} w_s \ominus d_s(w_0))^p, \quad s \in \{n-1, \dots, 2\}. \quad (4.26)$$

Отсюда, пользуясь определением $I_*^{(1)}$, получаем что для $s \in \{n-1, \dots, 2\}$ и $j \in I_*^{(1)}$ справедливы равенства

$$\begin{aligned} w_{s-1}(j) &= (w_0^{(1)}(j))^{p-1} \ominus \\ &\otimes \left(\sum_{i=0}^{p-1} (-1)^i \binom{p-1}{i} w_s(j + i \tau_{s-2}) \ominus d_s(w_0(j)) \right)^p, \quad j \in I_*^{(1)}. \end{aligned} \quad (4.27)$$

Заметим, что

$$J_1 + l \tau_0 \subset I_*^{(1)}, \quad l \in \mathbf{N}_0.$$

Поэтому нетрудно увидеть, что равенства (4.27) позволяют при $n \geq 3$ по известным отрезкам $w_{n-1}[J_1], w_{n-1}[J_1 + \tau_0], \dots, w_{n-1}[J_1 + (p^{n-2} - 1)\tau_0]$ последовательности w_{n-1} восстановить последовательно $w_{n-2}[J_1], w_{n-2}[J_1 + \tau_0], \dots, w_{n-2}[J_1 + (p^{n-3} - 1)\tau_0]; \dots; w_2[J_1], w_2[J_1 + \tau_0], \dots, w_2[J_1 + (p-1)\tau_0]$; и, наконец, отрезок $w_1[J_1]$. Отсюда получается отрезок (4.25) и искомая ЛРП u .

5. Восстановление ЛРП u по последовательности w_{n-1} в случае $p = 2$

Как и в разделе 4, мы считаем, что последовательность w_0 уже восстановлена и, соответственно, известна последовательность $w_0^{(n-2)}$. Для восстановления остальных координатных последовательностей мы не можем применить здесь подход, который оказывается

эффективным при $p > 2$ и состоит в переходе от сечения (4.1) к сечению (4.20), а затем — к сечению (4.18). Причина в том, что в случае $p = 2$ уже сечение (4.20) вырождается в сечение (3.1) и не дает способа выразить w_{s-1} через w_s . Поэтому мы вынуждены работать непосредственно с сечением (4.1), используя тот факт, что вид его в случае $p = 2$ упрощается. Интересно отметить, что наши доказательства различны для случаев $q > 2$ и $q = 2$.

5.1. Восстановление последовательности w_1 в q вариантах

Здесь по-прежнему предполагается, что $n \geq 3$ (см. конец раздела 3). По найденной уже последовательности $w_0^{(n-2)}$ можно построить множество

$$I_0^{(n-2)} = \{i \in \mathbf{N}_0 : w_0^{(n-2)}(i) = 0\} = \{i \in \mathbf{N}_0 : u_0^{(n-2)}(i) = 0\}. \quad (5.1)$$

Заметим, что равенство (4.1) при $s = n - 1$ дает при $n \geq 3$

$$(x^{\tau_{n-3}} - \bar{e})w_{n-1} = w_1^{(n-2)} \oplus \Delta_K(w_{n-2}, w_0^{(n-2)}). \quad (5.2)$$

Так как для всех $i \in I_0^{(n-2)}$ выполняется равенство

$$\Delta_K(w_{n-2}(i), w_0^{(n-2)}(i)) = \Delta_K(w_{n-2}(i), 0) = 0,$$

из (5.2) следует, что

$$w_1^{(n-2)}(i) = w_{n-1}(i + \tau_{n-3}) \ominus w_{n-1}(i), \quad i \in I_0^{(n-2)}. \quad (5.3)$$

Таким образом, последовательность $w_1^{(n-2)}$ однозначно определена в тактах, принадлежащих множеству $I_0^{(n-2)}$.

Положим $\tilde{R} = R/4R = GR(q^2, 4)$ и обозначим через $\tilde{K}, \tilde{F}, \tilde{u}, \dots$ образы $K, F, u, \dots$ при естественном эпиморфизме $R \rightarrow \tilde{R}$. Аналогично, полагая $\tilde{S} = S/4S$, образ произвольного $\alpha \in S$ при эпиморфизме $S \rightarrow \tilde{S}$ обозначим через $\tilde{\alpha}$. В этих обозначениях, согласно результатам раздела 2.3, мы можем утверждать, что нам известны знаки

$$u_0^{(n-2)}(i) \equiv w_0^{(n-2)}(i) \pmod{2}, \quad i \in \mathbf{N}_0,$$

и знаки

$$\tilde{u}^{(n-2)}(i) = \tilde{w}_0^{(n-2)}(i) + 2\tilde{w}_1^{(n-2)}(i), \quad i \in I_0^{(n-2)}.$$

Отсюда нам известны знаки $u_1^{(n-2)}(i)$, $i \in I_0^{(n-2)}$.

Лемма 8. *Существует ровно q различных ЛРП $\tilde{z} \in L_{\tilde{R}}(\tilde{F})$ таких, что*

$$\tilde{z}_0 = \tilde{u}_0^{(n-2)}, \quad \tilde{z}_1(i) = \tilde{u}_1^{(n-2)}(i), \quad i \in I_0^{(n-2)}. \quad (5.4)$$

Множество всех таких ЛРП есть множество $L^{(n-2)}$ всех последовательностей

$$\tilde{z}^{(d)} = (e + 2d)\tilde{u}^{(n-2)}, \quad d \in P. \quad (5.5)$$

Доказательство. Согласно (2.3), последовательность $\tilde{u}^{(n-2)}$ удовлетворяет условию

$$\tilde{u}^{(n-2)}(i) = \text{Tr}_{\tilde{R}}(\tilde{\xi}^{(n-2)}\tilde{\theta}^i), \quad i \in \mathbf{N}_0, \quad (5.6)$$

где

$$\tilde{\xi}^{(n-2)} = \tilde{\xi}_0^{(n-2)} + 2\tilde{\xi}_1^{(n-2)}.$$

В силу предложения 2, нам известны константы ξ_0 и $\xi_0^{(n-2)}$. Для описания всех возможных последовательностей $\tilde{z} \in L_{\tilde{R}}(\tilde{F})$, имеющих заданные значения $\tilde{z}(i) = \tilde{u}^{(n-2)}(i)$ в тактах $i \in I_0^{(n-2)}$, нам нужно описать соответствующие значения константы $\xi_1^{(n-2)}$. Для этого мы имеем систему уравнений

$$\text{Tr}(\tilde{\xi}^{(n-2)}\tilde{\theta}^i) = \tilde{u}^{(n-2)}(i), \quad i \in I_0^{(n-2)}, \quad (5.7)$$

в которой правая часть известна. Выделяя здесь в явном виде неизвестное $\xi_1^{(n-2)}$, получаем, что

$$2 \text{Tr}(\tilde{\xi}_1^{(n-2)}\tilde{\theta}^i) = \tilde{u}^{(n-2)}(i) - \text{Tr}(\tilde{\xi}_0^{(n-2)}\tilde{\theta}^i), \quad i \in I_0^{(n-2)}. \quad (5.8)$$

Так как, ввиду (2.16),

$$\tilde{u}^{(n-2)}(i) \equiv \text{Tr}(\tilde{\xi}_0^{(n-2)}\tilde{\theta}^i) \pmod{2},$$

известная правая часть системы уравнений (5.8) имеет вид

$$\tilde{u}^{(n-2)}(i) - \text{Tr}(\tilde{\xi}_0^{(n-2)}\tilde{\theta}^i) = 2\tilde{c}_i,$$

где $c_i \in \Gamma(R)$, $i \in I_0^{(n-2)}$. Теперь, пользуясь очевидным соотношением

$$2 \text{Tr}(\tilde{\xi}_1^{(n-2)}\tilde{\theta}^i) \equiv 2 \text{tr}(\xi_1^{(n-2)}\theta_0^i) \pmod{2},$$

можно утверждать, что элемент $\xi_1^{(n-2)}$ есть решение системы уравнений (5.7) тогда и только тогда, когда он есть решение системы линейных уравнений

$$\text{tr}(x\theta_0^i) = c_i, \quad i \in I_0^{(n-2)} \quad (5.9)$$

над полем $\mathcal{Q}$. Эта система совместна по построению. Для описания множества всех ее решений преобразуем ее. Рассмотрим однородное линейное уравнение над $\mathcal{Q}$:

$$\text{tr}(\xi_0^{(n-2)}y) = 0. \quad (5.10)$$

Так как $\xi_0^{(n-2)} \neq 0$, множество $H^{(n-2)}$ решений этого уравнения есть подпространство размерности $r-1$ пространства $\mathcal{Q}_P$. Из определения множества $I_0^{(n-2)}$ и формулы (2.11) следует, что $H^{(n-2)} \setminus 0$ есть множество всех различных элементов вида θ^i , $i \in I_0^{(n-2)}$. Поэтому система (5.9) равносильна системе

$$\text{tr}(x\delta) = c(\delta), \quad \delta \in H^{(n-2)}, \quad (5.11)$$

где $c(0) = 0$, и если $\delta \in H^{(n-2)} \setminus 0$, то $c(\delta) = c_i$ для $i \in I_0^{(n-2)}$ такого, что $\delta = \theta^i$. Множество решений ассоциированной с (5.11) системы однородных линейных уравнений

$$\text{tr}(x\delta) = 0, \quad \delta \in H^{(n-2)}, \quad (5.12)$$

есть одномерное подпространство, ортогональное к подпространству $H^{(n-2)}$ размерности $r - 1$. Так как по построению $\xi_0^{(n-2)}$ — ненулевое решение системы (5.12), пространство всех ее решений есть $\xi_0^{(n-2)} P < Q_P$.

По построению истинное значение $\xi_1^{(n-2)}$ есть некоторое частное решение уравнения (5.11), поэтому множество всех решений этого уравнения есть

$$D^{(n-2)} = \{\xi_1^{(n-2)} \oplus \xi_0^{(n-2)} d : d \in P\}.$$

Итак, множество различных ЛРП $\tilde{z} \in L_{\tilde{R}}(\tilde{F})$, удовлетворяющих условию (5.4) есть множество $L^{(n-2)}$ всех последовательностей вида

$$\tilde{z}^{(d)}(i) = \text{Tr}((\xi_0^{(n-2)} + 2(\xi_1^{(n-2)} + \xi_0^{(n-2)} \tilde{d}))\tilde{\theta}^i), \quad i \in \mathbb{N}_0, \quad d \in P.$$

Нетрудно видеть, что

$$\tilde{z}^{(d)}(i) = \text{Tr}((e + p\tilde{d})(\xi_0^{(n-2)} + p\xi_1^{(n-2)})\tilde{\theta}^i) = (e + p\tilde{d}) \text{Tr}(\xi^{(n-2)}\tilde{\theta}^i),$$

то есть, верно (5.5).

Искомая ЛРП u согласно (2.14), удовлетворяет соотношению

$$u = \Phi^{(n-2)}(x)u^{(n-2)}. \quad (5.13)$$

Отсюда, с учетом леммы 8, вытекает следующее утверждение.

Лемма 9. *Существует ровно q различных ЛРП $\tilde{y} \in L_{\tilde{R}}(\tilde{F})$ таких, что*

$$\tilde{y}_0^{(n-2)} = \tilde{u}_0^{(n-2)}, \quad \tilde{y}_1^{(n-2)}(i) = \tilde{u}_1^{(n-2)}(i), \quad i \in I_0^{(n-2)}. \quad (5.14)$$

Множество L всех таких ЛРП есть множество всех последовательностей

$$\tilde{u}^{(d)} = (e + p\tilde{d})\tilde{u}, \quad d \in P. \quad (5.15)$$

Доказательство. ЛРП $\tilde{y} \in L_{\tilde{R}}(\tilde{F})$ удовлетворяет условию (5.14) тогда и только тогда, когда ЛРП $\tilde{z} = \tilde{\Phi}_{n-2}(x)\tilde{y} = \tilde{y}^{(n-2)}$ удовлетворяет условию (5.4), то есть имеет вид (5.5). Таким образом, совокупность L искомых ЛРП $\tilde{y}$ описывается формулой

$$\tilde{y} = \tilde{u}^{(d)} = \tilde{\Phi}^{(n-2)}(x)\tilde{z}^{(d)}, \quad d \in P,$$

и в силу (5.5), (5.13) L есть множество последовательностей (5.15).

В результате проведенных вычислений мы сумели по последовательности w_{n-1} восстановить последовательность $\tilde{u} = u \pmod{4}$ в q вариантах, которые описываются формулой (5.15). При этом истинный вариант соответствует значению $d = 0 \in P$, при любом значении $d \in P$ нулевая P -координатная последовательность ЛРП $\tilde{u}^{(d)}$ является истинной: $\gamma_0(\tilde{u}^{(d)}) = u_0^{(d)} = u_0$, а первая координатная последовательность d -го варианта имеет вид

$$u_1^{(d)} = u_1 \oplus du_0, \quad (5.16)$$

где $\oplus$ — сложение в P . Таким образом, последовательность u_1 восстанавливается в q вариантах. При этом истинный вариант из совокупности (5.16) соответствует значению $d = 0$, но мы не знаем какой именно это вариант.

Для дальнейшего важно отметить, что найденным q вариантам (5.15) последовательности $\tilde{u}$ соответствует единственный вариант $w_0 = \psi_K(u_0)$ нулевой K -координатной последовательности и q вариантов $w_1^{(d)}$ первых K -координатных последовательностей, которые получаются из равенств

$$\tilde{u}^{(d)} = \tilde{w}_0 + 2\tilde{w}_1^{(d)} = (1 + 2d)(\tilde{w}_0 + 2\tilde{w}_1).$$

Таким образом,

$$w_1^{(d)} = w_1 \oplus \hat{d} \odot w_0 = w_1 \oplus \hat{d} w_0, \quad \hat{d} = \psi_K(d), \quad (5.17)$$

в операциях поля $(K, \oplus, \odot)$. Ввиду (5.15), младшие координаты производных последовательностей также связаны соотношениями

$$w_1^{(d)(k)} = w_1^{(k)} \oplus \hat{d} w_0^{(k)}, \quad k = 1, 2, \dots \quad (5.18)$$

Завершение доказательства теоремы 2 осуществляется в следующие два этапа.

5.2. Восстановление 2-адических координатных последовательностей

$u_2, \dots, u_{n-3}$ по w_0, w_1, w_{n-1}

Если $n = 3$, то $n - 1 = 2$ и задача уже решена. Далее в этом разделе полагаем $n \geq 4$.

Допустим, что при произвольном выборе координатного множества K нам известны последовательности w_0, w_1, w_{n-1} . Тогда, как уже отмечалось выше, нам известны последовательности u_0, u_1 и производные последовательности $w_0^{(t)}, w_1^{(t)}$, и можно пытаться рекурсивно вычислять последовательности $w_{n-2}, w_{n-3}, \dots, w_2$, используя при $s \geq 2$ соотношения

$$\Delta_K(w_{s-1}, w_0^{(s-1)}) = (x^{\tau_{s-2}} - \bar{e})w_s \ominus w_1^{(s-1)}, \quad (5.19)$$

вытекающие из (4.1). Так как при $s = 2$ последовательность $w_{s-1} = w_1$ считается известной, нам достаточно использовать эти соотношения при $s \geq 3$, а тогда ввиду (2.8) и условия $p = 2$ они имеют вид

$$\Delta_K(w_{s-1}, w_0^{(2)}) = (x^{\tau_{s-2}} - \bar{e})w_s \ominus w_1^{(s-1)}. \quad (5.20)$$

При условии теоремы 2, согласно лемме 6 (см. (4.10)), в операциях поля $(K, \oplus, \odot)$ справедливо равенство

$$\Delta_K(x, y) = x^h y^h,$$

где $h = q/2$ и уравнение (5.20) при $s \geq 3$ можно переписать в виде

$$w_{s-1}w_0^{(2)} = ((x^{\tau_{s-2}} - \bar{e})w_s \ominus w_1^{(s-1)})^2. \quad (5.21)$$

Теперь мы воспользуемся той же методикой, которая была применена в разделе 4.2.

Так как $w_0^{(2)}$ есть МП ЛРП над полем K , имеющая представление (2.7), и ввиду (2.11) справедливы соотношения

$$w_0^{(2)}(i) \stackrel{2}{=} u_0^{(2)}(i) = \text{tr}(\xi_0^{(2)} \theta_0^i), \quad i \geq 0, \quad (5.22)$$

можно выбрать набор тактов

$$J_2 = \{j_1 < j_2 < \dots < j_m\} \subset \{0, 1, \dots, \tau_0 - 1\}$$

так, чтобы выполнялись условия

(J_2 1) координаты вектора $w_0^{(2)}[J_2] = (w_0^{(2)}(j_1), \dots, w_0^{(2)}(j_m))$ обратимы в поле K ;

(J_2 2) система элементов $\theta^{j_1}, \dots, \theta^{j_m}$ есть базис модуля S_R .

Как и в разделе 4.2, легко показать, что ввиду свойства (J_2 2) для восстановления ЛРП u достаточно найти вектор

$$u[J_2] = (u(j_1), \dots, u(j_m)). \quad (5.23)$$

Для восстановления вектора (5.23) воспользуемся разложением (1.3), из которого следует равенство

$$u[J_2] = w_0[J_2] + pw_1[J_2] + \dots + p^{n-2}w_{n-2}[J_2] + p^{n-1}w_{n-1}[J_2]. \quad (5.24)$$

Векторы $w_{n-1}[J_2], w_1[J_2], w_0[J_2]$ нам уже известны. Построим по ним последовательно векторы $w_{n-2}[J_2], \dots, w_2[J_2]$.

Как отмечено в разделе 2.3, по известной последовательности w_0 однозначно строится $w_0^{(2)}$. Пусть

$$I_*^{(2)} = \{j \in \mathbf{N}_0 : w_0^{(2)}(j) \neq 0\} = \{j \in \mathbf{N}_0 : u_0^{(2)}(j) \neq 0\} \quad (5.25)$$

— множество, дополнительное к $I_0^{(2)}$ в $\mathbf{N}_0$.

Из соотношения (5.21) и определения множества $I_*^{(2)}$ получаем, что для каждого $s \geq 3$ справедливы равенства

$$w_{s-1}(i) = w_0^{(2)}(i)^{-1}((w_s(i + \tau_{s-2}) \ominus w_s(i) \ominus w_1^{(s-1)}(i))^2, \quad i \in I_*^{(2)}. \quad (5.26)$$

Заметим, что $J_2 + l\tau_0 \subset I_*^{(2)}$, $l \in \mathbf{N}_0$, в частности, справедливы равенства

$$w_{s-1}(j + l\tau_1) = w_0^{(2)}(j)^{-1}((w_s(j + l\tau_1 + \tau_{s-2}) \ominus w_s(j + l\tau_1) \ominus w_1^{(s-1)}(j))^2, \quad j \in J_2, \quad l \in \mathbf{N}_0. \quad (5.27)$$

Нетрудно видеть, что эти равенства позволяют при $n \geq 4$ по известным отрезкам $w_{n-1}[J_2], w_{n-1}[J_2 + \tau_1], \dots, w_{n-1}[J_2 + \tau_{n-3}] = w_{n-1}[J_2 + p^{n-4}\tau_1]$ последовательности w_{n-1} восстановить последовательно отрезки $w_{n-2}[J_2], w_{n-2}[J_2 + \tau_1], \dots, w_{n-2}[J_2 + \tau_{n-4}]; \dots; w_3[J_2], w_3[J_2 + \tau_1]$; и, наконец, — отрезок $w_2[J_2]$. Отсюда получается отрезок ЛРП (5.24), а следовательно — и ЛРП u .

Таким образом, с учетом результатов раздела 5.1, мы восстановили последовательность u и ее 2-адические координатные последовательности по старшей координатной последовательности w_{n-1} в q вариантах.

Отметим, что в частных случаях этот результат, независимо от авторов данной работы, был получен А. А. Варфоломеевым при $q = 2$, $K = \{0, 1\}$ и В. Н. Цыпышевым при $q = 2^r$, $K = \Gamma(R)$ (устные сообщения).

5.3. Отсев ложных вариантов последовательностей $w_1^{(d)}$ по последовательности w_{n-1}

Здесь мы полагаем $n \geq 3$. Пользуясь результатами раздела 5.2, по известным последовательностям w_{n-1}, w_0 для каждого варианта первой K -координатной последовательности

$$w_1^{(d)} = w_1 \oplus \hat{d}w_0, \quad d \in P,$$

из (5.17), рассматривая его как истинный, однозначно последовательно восстановим значения $w_{n-2}^{(d)}, \dots, w_2^{(d)}$ оставшихся координатных последовательностей. Получим последовательность

$$u^{(d)} = w_0 + 2w_1^{(d)} + \dots + 2^{n-2}w_{n-2}^{(d)} + 2^{n-1}w_{n-1}.$$

Если рассматриваемый вариант $w_1^{(d)}$ является истинным, то $u^{(d)} \in L_R(F)$. Остается доказать, что справедлива следующая теорема.

Теорема 5. Если $u^{(d)} \in L_R(F)$, то $d = 0$.

Таким образом, если $d \neq 0$, то на некотором такте последовательность $u^{(d)}$ перестанет удовлетворять закону рекурсии, определяемому многочленом F , и при соответствующей проверке будет отсеяна как ложная.

Всюду далее мы полагаем

$$w_0^{(d)} = w_0, \quad w_{n-1}^{(d)} = w_{n-1}.$$

Доказательство теоремы разбивается на два этапа: для $q > 2$ и для $q = 2$.

5.3.1. Доказательство теоремы 5 для $q > 2$

Лемма 10. Для $t \in \{2, \dots, n-2\}$ справедливы равенства

$$w_t^{(d)}(i) = w_t(i) \oplus \hat{d}^2 w_0^{(2)}(i), \quad i \in I_*^{(2)}. \quad (5.28)$$

Доказательство. Заметим, что для K -координатных последовательностей любой ЛРП $u \in L_R(F)$ справедливы соотношения (5.21). Поэтому, если $u^{(d)} \in L_R(F)$, то при $s \geq 3$ справедливы соотношения

$$w_{s-1}^{(d)} w_0^{(2)} = ((x^{\tau_{s-2}} - \bar{e})w_s^{(d)} \oplus w_1^{(d)(s-1)})^2. \quad (5.29)$$

При этом, согласно (5.18), для любого $s \geq 3$

$$w_1^{(d)(s-1)} = w_1^{(s-1)} \oplus \hat{d}w_0^{(2)}. \quad (5.30)$$

Подставляя (5.30) в (5.29), получаем, что при $s \geq 3$

$$w_{s-1}^{(d)} w_0^{(2)} = ((x^{\tau_{s-2}} - \bar{e})w_s^{(d)} \oplus w_1^{(s-1)})^2 \oplus (\hat{d}w_0^{(2)})^2. \quad (5.31)$$

Теперь, пользуясь тем, что $w_{n-1}^{(d)} = w_{n-1}$, и следовательно

$$(x^{\tau_{n-3}} - \bar{e})w_{n-1}^{(d)} = (x^{\tau_{n-3}} - \bar{e})w_{n-1},$$

из (5.31) для $s = n - 1$ получаем равенство

$$w_{n-2}^{(d)} w_0^{(2)} = ((x^{\tau_{n-3}} - \bar{e})w_{n-1} \oplus w_1^{(n-2)})^2 \oplus (\hat{d}w_0^{(2)})^2.$$

Используя (5.21) при $s = n - 1$, приходим к равенству

$$w_{n-2}^{(d)} w_0^{(2)} = w_{n-2} w_0^{(2)} \oplus (\hat{d}w_0^{(2)})^2,$$

из которого для всех $i \in I_*^{(2)}$ следуют равенства

$$w_{n-2}^{(d)}(i) = w_{n-2}(i) \oplus \hat{d}^2 w_0^{(2)}(i).$$

Отсюда ввиду условия $I_*^{(2)} + l\tau_0 \subset I_*^{(2)}$, $l \in \mathbf{N}_0$, получаем, что для $n \geq 4$ верны равенства

$$((x^{\tau_{n-4}} - \bar{e})w_{n-2}^{(d)})(i) = ((x^{\tau_{n-4}} - \bar{e})w_{n-2})(i), \quad i \in I_*^{(2)}.$$

Из этих соотношений и (5.29) при $s = n - 3$, с использованием (5.30), получаем, что

$$w_{n-3}^{(d)} w_0^{(2)}(i) = (((x^{\tau_{n-4}} - \bar{e})w_{n-2})(i) \oplus w_1^{(n-2)}(i))^2 \oplus (\hat{d}w_0^{(2)}(i))^2, \quad i \in I_*^{(2)},$$

и, используя (5.21) при $s = n - 2$, приходим к соотношениям

$$w_{n-3}^{(d)}(i) = w_{n-3}(i) \oplus \hat{d}^2 w_0^{(2)}(i), \quad i \in I_*^{(2)}.$$

Теперь нетрудно видеть, что с использованием равенств (5.21), (5.31) последовательно для $s = n - 1, s = n - 2, \dots, s = 3$ и $i \in I_*^{(2)}$ доказываются соотношения

$$\begin{aligned} ((x^{\tau_{s-2}} - \bar{e})w_s^{(d)})(i) &= ((x^{\tau_{s-2}} - \bar{e})w_s)(i), \\ w_{s-1}^{(d)}(i) &= w_{s-1}(i) \oplus \hat{d}^2 w_0^{(2)}(i). \end{aligned} \quad (5.32)$$

Умножая соотношения (5.28) на $w_0^{(2)}(i)$ и пользуясь определением множества $I_*^{(2)}$, получаем, что справедливо следующее утверждение.

Следствие 2. Если $u^{(d)} \in L_R(F)$, то справедливо равенство

$$w_t^{(d)} w_0^{(2)} = w_t w_0^{(2)} \oplus (\hat{d}w_0^{(2)})^2. \quad (5.33)$$

Лемма 11. Если $u^{(d)} \in L_R(F)$ и $d \neq 0$, то справедливо одно из следующих утверждений:

(i) $q = 2$, $d = e$, и в операциях поля P

$$u_0 u_0^{(1)} u_0^{(2)} \oplus u_0^{(1)} u_0^{(2)} = 0; \quad (5.34)$$

(ii) $q > 2$, и для некоторого $a \in P^*$ выполняются соотношения

$$\bar{\Phi}_1(x) = \bar{a}, \quad a^2 \oplus a = b \in P^*, \quad d = a^{-1}. \quad (5.35)$$

Доказательство. Из (4.1) при $s = 2$ получаем, что

$$(x^{\tau_0} - \bar{e})w_2 = w_1^{(1)} \oplus \Delta_K(w_1, w_0^{(1)}), \quad (5.36)$$

и ввиду условия теоремы также

$$(x^{\tau_0} - \bar{e})w_2^{(d)} = w_1^{(d)(1)} \oplus \Delta_K(w_1^{(d)}, w_0^{(1)}) \stackrel{2}{=} w_1^{(d)(1)} \oplus (w_1^{(d)}w_0^{(1)})^h. \quad (5.37)$$

Заметим, что (5.18) при $k = 1$ дает равенство

$$w_1^{(d)(1)} = w_1^{(1)} \oplus \hat{d}w_0^{(1)}.$$

Подставляя правую часть последнего равенства в правую часть (5.37) и используя (5.17), соотношение (5.37) можно записать в виде

$$(x^{\tau_0} - \bar{e})w_2^{(d)} \stackrel{2}{=} w_1^{(1)} \oplus \hat{d}w_0^{(1)} \oplus (w_1w_0^{(1)} \oplus \hat{d}w_0w_0^{(1)})^h. \quad (5.38)$$

С другой стороны, из (5.28) при $t = 2$ и (5.36) получаем равенство

$$\begin{aligned} ((x^{\tau_0} - \bar{e})w_2^{(d)})(i) &= w_1^{(1)}(i) \oplus \Delta_K(w_1(i), w_0^{(1)}(i)) \\ &\stackrel{2}{=} w_1^{(1)}(i) \oplus (w_1(i)w_0^{(1)}(i))^h, \quad i \in I_*^{(2)}. \end{aligned} \quad (5.39)$$

Сравнивая правую часть (5.39) с правой частью (5.38) и пользуясь тем, что оба выражения принадлежат K , получаем равенства

$$(\hat{d}w_0^{(1)}(i)w_0(i))^h \oplus \hat{d}w_0^{(1)}(i) = 0, \quad i \in I_*^{(2)},$$

из которых, используя возведение в квадрат и определение параметра h , получаем равенство

$$\hat{d}w_0^{(1)}(i)(w_0(i) \oplus \hat{d}w_0^{(1)}(i)) = 0, \quad i \in I_*^{(2)}.$$

Последние равенства, записанные в операциях поля $(K, \oplus, \cdot)$, ввиду соотношений

$$\hat{d} \stackrel{2}{=} d, \quad w_0^{(k)} \stackrel{2}{=} u^{(k)} \stackrel{2}{=} u_0^{(k)}, \quad k \in \{0, 1\},$$

можно переписать в виде сравнений

$$du_0^{(1)}(i)(u_0(i) + du_0^{(1)}(i)) \stackrel{2}{=} 0, \quad i \in I_*^{(2)},$$

из которых, уже в операциях поля P , следуют равенства

$$du_0^{(1)}(i)(u_0(i) \oplus du_0^{(1)}(i)) = 0, \quad i \in I_*^{(2)}.$$

Отсюда, умножая обе части на $u_2^{(0)}$ и пользуясь условием $d \neq 0$ и определением (5.25) множества $I_*^{(2)}$, получаем равенство

$$u_0^{(2)}u_0^{(1)}(u_0 \oplus du_0^{(1)}) = 0. \quad (5.40)$$

Рассмотрим две ситуации.

Пусть $v_0 = u_0 \oplus du_0^{(1)}$ — ненулевая последовательность для любого $d \in P^*$. Тогда v_0 есть ЛРП максимального периода $q^m - 1$ над полем P и равенство (5.40) означает, что произведение трех таких ЛРП равно нулю. Последнее невозможно, если $q = 2^l > 2$. Действительно, в этом случае каждая из рассматриваемых ЛРП содержит ровно $q^{m-1} - 1$ нулевых элементов на начальном отрезке длины $q^m - 1$, и потому произведение в левой

части (5.40) есть последовательность, у которой число нулей на указанном отрезке ограничено сверху величиной $3(q^{m-1} - 1) < 4(q^{m-1} - 1) \leq q^m - q$, которая строго меньше, чем $q^m - 1$. Таким образом в рассматриваемом случае $q = 2$, $d = e$ и из (5.40) следует (5.34), то есть справедливо утверждение (i).

Пусть $v_0 = 0$ для некоторого $d \in P^*$. Тогда $u_0^{(1)} = au_0$ для $a = d^{-1} \in P^*$. Отсюда по определениям функции $\Phi_1(x)$ и последовательности $u_0^{(1)}$ в силу леммы 1 следует (5.35).

Покажем, что условие (ii) леммы 11 невыполнимо. Заметим, сразу, что из (5.35) для K -координатных последовательностей ЛРП u следуют соотношения (в операциях поля $(K, \oplus, \odot)$)

$$\begin{aligned} w_0^{(1)} &= \hat{a}w_0, & w_0^{(2)} &= \hat{b}w_0, & \hat{b} &= \hat{a}^2 \oplus \hat{a} \neq 0; \\ I_*^{(2)} &= I_* = \{j \in \mathbb{N}_0: w_0(j) \neq 0\}. \end{aligned} \quad (5.41)$$

Ввиду (5.17), младшие K -координатные последовательности ЛРП $u^{(d)} \in L_R(F)$ имеют вид

$$w_0^{(d)} = w_0, \quad w_1^{(d)} = w_1 \oplus \hat{d}w_0, \quad w_2^{(d)} = w_2 \oplus \delta, \quad (5.42)$$

где последовательность δ над K , согласно (5.28), удовлетворяет условиям

$$\delta(i) = \begin{cases} 0, & n = 3; \\ \hat{d}^2 w_0^{(2)}(i) = (\hat{e} \oplus \hat{d})w_0(i), & n > 3, i \in I_*. \end{cases} \quad (5.43)$$

Рассмотрим разность последовательностей $u^{(d)} - u \in L_R(F)$. Ввиду (5.42), нулевая координатная последовательность этой разности равна нулю, а первая отлична от нуля. Следовательно $u^{(d)} - u = 2u'$, где u' — МП ЛРП из $L_R(F)$. Более того, она удовлетворяет соотношениям

$$\begin{aligned} u' &\stackrel{4}{=} (w_1 \oplus \hat{d}w_0) - w_1 + 2((w_2 \oplus \delta) - w_2) \\ &\stackrel{4}{=} (w_1 \oplus \hat{d}w_0) + w_1 + 2(w_1 \oplus \delta), \end{aligned}$$

и ее 0-я и 1-я K -координатные последовательности имеют вид

$$\begin{aligned} w'_0 &= \hat{d}w_0, \\ w'_1 &= w_1 \oplus \delta \oplus \Delta_K(w_1 \oplus \hat{d}w_0, w_1). \end{aligned} \quad (5.44)$$

Невыполнимость условия (ii) леммы 11 будет доказана, если будет доказано следующее утверждение.

Лемма 12. При сформулированных условиях последовательность w'_1 не может быть первой координатной последовательностью какой-либо МП ЛРП из $L_R(F)$.

Для доказательства этой леммы нам понадобятся еще 2 вспомогательных утверждения.

Лемма 13. При условии теоремы 2 для $p = 2$ справедливо равенство

$$\Delta_K(x, y) \stackrel{2}{=} (xy)^h, \quad (5.45)$$

где $h = 2^{r-1}$.

Доказательство. По условию теоремы, индекс нелинейности интерполяционного многочлена

$$\psi_K(x) = x + \lambda_K(x)$$

координатного множества K не превосходит 1, и, так как $0 \in K$, многочлен $\lambda_K(x)$ имеет вид

$$\lambda_K(x) = \sum_{i \in \{0, 1, \dots, r-1\}} c_i x^{2^i}, \quad (5.46)$$

и потому удовлетворяет тождеству

$$\lambda_K(x + y) = \lambda_K(x) \oplus \lambda_K(y).$$

Теперь (5.45) следует из (4.8) при $p = 2$.

Заметим сразу, что теперь формула (5.44) существенно упрощается:

$$w'_1 = w_1 \oplus \delta \oplus ((w_1 \oplus \hat{d}w_0)w_1))^h = w_1 \oplus \delta \oplus w_1^q \oplus (\hat{d}w_0w_1)^h,$$

и окончательно

$$w'_1 = \delta \oplus (\hat{d}w_0w_1)^h. \quad (5.47)$$

Для того, чтобы доказать, что такая последовательность w'_1 не может быть первой K -координатной последовательностью МП ЛРП $u' \in L_R(F)$, опишем представление последовательности w_1 ЛРП u с помощью функции след. Мы используем представление (2.3) последовательности u и при этом обозначим через $\xi_0, \xi_1, \dots; \theta_0, \theta_1, \dots$ p -адические координаты элементов, соответственно, ξ, θ , а также используем элемент $\eta = \theta_0^{-1}\theta_1 \in \Gamma(S)$.

Лемма 14. Если $u \in L_R(F)$ есть МП ЛРП вида (2.3), то при условии (5.46) имеют место соотношения

$$w_0(i) = \text{tr}(\xi_0\theta_0^i), \quad w_1 \stackrel{2}{\equiv} \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4, \quad (5.48)$$

где

$$\alpha_1(i) = i \text{tr}(\eta\xi_0\theta_0^i), \quad \alpha_2(i) = \sum_{0 \leq s < t \leq m-1} \xi_0^{(q^s+q^t)h} (\theta_0^{(q^s+q^t)h})^i, \quad (5.49)$$

$$\alpha_3(i) = \text{tr}(\xi_1\theta_0^i), \quad \alpha_4(i) = \sum_{l=0}^{r-1} c_l \text{tr}(\xi_0^{2^l} (\theta_0^{2^l})^i). \quad (5.50)$$

Доказательство. Согласно теореме 1.5 в [5],

$$u_0(i) \stackrel{2}{\equiv} \text{tr}(\xi_0\theta_0^i), \quad u_1 \stackrel{2}{\equiv} \alpha_1 + \alpha_2 + \alpha_3. \quad (5.51)$$

Теперь заметим, что по определению

$$\begin{aligned} \kappa_0(u) &= \kappa_0(u_0) = u_0 + 2\lambda_K(u_0), \\ 2\kappa_1(u) &\stackrel{4}{\equiv} u - \kappa_0(u) = u - \kappa_0(u_0) \stackrel{4}{\equiv} 2(u_1 + \lambda_K(u_0)). \end{aligned}$$

Таким образом,

$$w_1 = \kappa_1(u) \stackrel{2}{\equiv} u_1 + \lambda_K(u_0).$$

Теперь (5.48) следует из (5.51) и (5.46).

Доказательство леммы 12. Если утверждение леммы ложно, то по лемме 14 для подходящих $\xi'_0 \in \Gamma(S)^*$, $\xi'_1 \in \Gamma(S)$ выполняется соотношение

$$w'_1 \stackrel{2}{\equiv} \alpha'_1 + \alpha'_2 + \alpha'_3 + \alpha'_4, \quad (5.52)$$

где слагаемые в правой части получаются из соответствующих слагаемых в правой части (5.48) заменой констант $\xi_0 \rightarrow \xi'_0$, $\xi_1 \rightarrow \xi'_1$. Заметим также, что параметр $\eta = \theta_0^{-1}\theta_1$ в определениях последовательностей α_1 , α'_1 удовлетворяет условию

$$\bar{\eta} = \bar{\Phi}_1(\theta_0)$$

(для доказательства достаточно подставить $x = \theta$ в сравнение (2.4) при $t = 0$), поэтому, ввиду условия (5.35),

$$\eta = a \in P. \quad (5.53)$$

Возводя обе части соотношения (5.47) в квадрат и подставляя в полученное сравнение соотношения (5.52) и (5.48), получаем, что

$$(\alpha'_1)^2 + (\alpha'_2)^2 + (\alpha'_3)^2 + (\alpha'_4)^2 \stackrel{2}{\equiv} \delta^2 + dw_0(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4).$$

Покажем, что

$$(\alpha'_1)^2 \stackrel{2}{\equiv} dw_0\alpha_1. \quad (5.54)$$

Действительно, ввиду (5.44) параметр ξ' удовлетворяет соотношениям

$$w'_0(i) \stackrel{2}{\equiv} \text{tr}(\xi'_0(\theta_0)^i) \stackrel{2}{\equiv} \text{tr}(d\xi_0(\theta_0)^i).$$

Следовательно, $\xi'_0 = d\xi_0$. В таком случае из (5.49), (5.53) и (5.35) следует, что

$$\begin{aligned} \alpha'_1(i)^2 &= i \text{tr}(a\xi'_0\theta_0^i)^2 = i \text{tr}(\xi_0\theta_0^i)^2; \\ dw_0(i)\alpha_1(i) &= d \text{tr}(\xi_0\theta_0^i)i \text{tr}(a\xi_0\theta_0^i) = i \text{tr}(\xi_0\theta_0^i)^2, \end{aligned}$$

следовательно, верно (5.54). Теперь мы имеем соотношение

$$(\alpha'_2)^2 + (\alpha'_3)^2 + (\alpha'_4)^2 \stackrel{2}{\equiv} \delta^2 + dw_0(\alpha_2 + \alpha_3 + \alpha_4). \quad (5.55)$$

Покажем, что оно невозможно.

Далее нам понадобится следующий хорошо известный результат из общей теории линейных рекуррент над полями (см., например, [15, 12, 2]). Если z — последовательность над полем Q вида

$$z(i) = k_1\rho_1^i \oplus \dots \oplus k_\mu\rho_\mu^i, \quad i \in \mathbb{N}_0, \quad (5.56)$$

где $\rho_1, \dots, \rho_\mu \in Q^*$ — попарно различные элементы, $k_1, \dots, k_\mu \in Q^*$, то будем говорить что последовательность z имеет экспоненциальное представление (5.56) и ρ_j есть корень этого представления с коэффициентом k_j .

Предложение 3. *Если последовательность z имеет экспоненциальное представление, то оно определено однозначно, и при условии (5.56) z есть ЛРП над полем Q с минимальным многочленом*

$$M_z(x) = (x \ominus \rho_1) \dots (x \ominus \rho_\mu).$$

В случае $n = 3$ из (5.43), (5.54), (5.49), (5.50) следует, что

$$dw_0(i)\alpha_2(i) \stackrel{2}{=} \alpha'_2(i)^2 + \alpha'_3(i)^2 + \alpha'_4(i)^2 + dw_0(i)(\alpha_3(i) + \alpha_4(i)),$$

а также

$$\begin{aligned} d \operatorname{tr}(\xi_0(\theta_0)^i) & \sum_{0 \leq s < t \leq m-1} \xi_0^{(q^s+q^t)h} (\theta_0^{(q^s+q^t)h})^i \\ & \stackrel{2}{=} \sum_{0 \leq s < t \leq m-1} (\xi'_0)^{(q^s+q^t)q} (\theta_0^{(q^s+q^t)q})^i + \operatorname{tr}((\xi'_1)^2 (\theta_0^2)^i) + \sum_{l=0}^{r-1} c_l^2 \operatorname{tr}((\xi'_0)^{2^{l+1}} (\theta_0^{2^{l+1}})^i) \\ & + d \operatorname{tr}(\xi_0 \theta_0^i) \left(\operatorname{tr}(\xi_1 \theta_0^i) + \sum_{l=0}^{r-1} c_l \operatorname{tr}(\xi_0^{2^l} (\theta_0^{2^l})^i) \right). \end{aligned} \quad (5.57)$$

Пользуясь определением функции $\operatorname{tr}(x)$ (см. (2.11)), нетрудно получить, что в левой части соотношения (5.57) записана ненулевая ЛРП, имеющая экспоненциальное представление над $\mathcal{Q}$, все корни которого принадлежат множеству $\{\theta_0^{q^k+hq^s+hq^t} : 0 \leq s < t \leq m-1, k \in \{0, \dots, m-1\}\}$, а все корни экспоненциального представления ЛРП из правой части (5.57) принадлежат множеству $\{\theta_0^{q^s+q^t}, \theta_0^{2^l q^k} : 0 \leq s < t \leq m-1, k \in \{0, \dots, m-1\}, l \in \{0, \dots, r\}\}$. Поскольку в случае $q > 2$ указанные множества не пересекаются, соотношение (5.57), а значит и соотношение (5.55), невозможно.

Теперь пусть $n > 3$. Тогда $\delta \neq 0$, однако, согласно (5.43) справедливо равенство $w_0(i)\delta(i) = (e + d)w_0(i)^2$. Поэтому, домножая обе части (5.55) на $w_0(i) = \operatorname{tr}(\xi_0 \theta_0^i)$, получаем

$$\begin{aligned} w_0((\alpha'_2)^2 + (\alpha'_3)^2 + (\alpha'_4)^2) & \stackrel{2}{=} (e + d^2)w_0^3 + dw_0^2(\alpha_2 + \alpha_3 + \alpha_4); \\ dw_0^2\alpha_2 & \stackrel{2}{=} w_0(i)((\alpha'_2)^2 + (\alpha'_3)^2 + (\alpha'_4)^2) + dw_0^2(\alpha_3 + \alpha_4) + (e + d^2)w_0(i)^3; \end{aligned}$$

и

$$\begin{aligned} d \operatorname{tr}(\xi_0^2 (\theta_0^2)^i) & \sum_{0 \leq s < t \leq m-1} \xi_0^{(q^s+q^t)h} (\theta_0^{(q^s+q^t)h})^i \\ & \stackrel{2}{=} \operatorname{tr}(\xi_0 \theta_0^i) \left(\sum_{0 \leq s < t \leq m-1} (\xi'_0)^{(q^s+q^t)q} (\theta_0^{(q^s+q^t)q})^i \right. \\ & \quad \left. + \operatorname{tr}((\xi'_1)^2 (\theta_0^2)^i) + \sum_{l=0}^{r-1} c_l^2 \operatorname{tr}((\xi'_0)^{2^{l+1}} (\theta_0^{2^{l+1}})^i) \right) \\ & \quad + d \operatorname{tr}(\xi_0^2 (\theta_0^2)^i) \left(\operatorname{tr}(\xi_1 \theta_0^i) + \sum_{l=0}^{r-1} c_l \operatorname{tr}(\xi_0^{2^l} (\theta_0^{2^l})^i) \right) + (e + d^2) \operatorname{tr}(\xi_0 \theta_0^i)^3. \end{aligned} \quad (5.58)$$

Отсюда, опять используя определение функции tr , нетрудно вывести, что последовательности в обеих частях соотношения (5.58) имеют экспоненциальные представления над $\mathcal{Q}$.

При условии $m \geq 3$ экспоненциальное представление рекурренты в левой части соотношения (5.57), имеет корень $\rho = \theta_0^{2+hq+hq^2}$ с коэффициентом $\xi_0^{2+hq+hq^2}$, и этот корень не является корнем экспоненциального представления рекурренты из правой части (5.58), поскольку корни последнего принадлежат множеству $\{\theta_0^{q^a+q^s+q^t}, \theta_0^{q^a+2^l q^b}, \theta_0^{2^l q^a+2^l q^b} : a, b \in \{0, \dots, m-1\}, 0 \leq s < t \leq m-1, l \in \{0, \dots, r\}\}$.

Если $m = 2, q > 4$, то есть $h > 2$, то вместо указанного корня достаточно рассмотреть корень $\rho = \theta_0^{h+2+hq}$.

Наконец, если $m = 2, q = 4$ (то есть $r = 2$), то соотношение (5.58) упрощается и дает соотношение

$$\begin{aligned} d \xi_0^{2+2q} \operatorname{tr}(\xi_0^2 (\theta_0^2)^i) (\theta_0^{2+2q})^i \\ \equiv \operatorname{tr}(\xi_0 \theta_0^i) \left((\xi_0')^{1+q} (\theta_0^{1+q})^i + \operatorname{tr}((\xi_1')^2 (\theta_0^2)^i) + \sum_{l=0}^1 c_l^2 \operatorname{tr}((\xi_0')^{2l+1} (\theta_0^{2l+1})^i) \right) \\ + d \operatorname{tr}(\xi_0^2 (\theta_0^2)^i) \left(\operatorname{tr}(\xi_1 \theta_0^i) + \sum_{l=0}^1 c_l \operatorname{tr}(\xi_0^{2l} (\theta_0^{2l})^i) \right) + (e + d^2) \operatorname{tr}(\xi_0 \theta_0^i)^3. \end{aligned} \quad (5.59)$$

Здесь корни экспоненциального представления последовательности из левой части суть θ_0^{3+q} и θ_0^{1+3q} , и они не являются корнями экспоненциального представления последовательности из правой части, которые принадлежат множеству $\{\theta_0^{q^a+2q^b}, \theta_0^{2q^a}, \theta_0^{q^a} : a, b \in \{0, 1\}\}$. Итак, соотношение (5.55) невозможно. Лемма 12 доказана.

Таким образом, условие (ii) леммы 11 невыполнимо, и для случая $q > 2$ теорема 5 доказана.

5.3.2. Доказательство теоремы 5 для $q = 2$

Лемма 15. Если $q = 2$ и $u^{(e)} \in L_R(F)$, то $u_0^{(2)} = u_0$.

Доказательство. Из (2.16), (2.11) следуют равенства

$$u_0(i) = \operatorname{tr}(\xi_0 \theta_0^i), \quad u_0^{(1)}(i) = \operatorname{tr}(\xi_0 \varphi_1 \theta_0^i), \quad u_0^{(2)}(i) = \operatorname{tr}(\xi_0 \varphi_2 \theta_0^i) \quad (5.60)$$

где для краткости введены обозначения

$$\varphi_1 = \gamma_0(\Phi_1(\theta)), \quad \varphi_2 = \gamma_0(\Phi_2(\theta)) = \varphi_1^2 \oplus \varphi_1. \quad (5.61)$$

Рассмотрим подпространство $C = (e, \varphi_1, \varphi_2)_P = (e, \varphi_1, \varphi_1^2)_P$ пространства Q_P .

Равенство $\dim C_P = 1$ невозможно, так как тогда $\varphi_1 \in P = \mathbf{Z}_2$ и $\varphi_2 = \varphi_1^2 \oplus \varphi_1 = 0$. Равенство $\dim C_P = 2$, как легко видеть, равносильно соотношению $e + \varphi_1 + \varphi_1^2 = 0$, означающему, что $\varphi_2 = e$, т.е. выполняется нужное равенство $u_0^{(2)} = u_0$.

Пусть $\dim C_P = 3$. Покажем, что это предположение противоречит тождеству (5.34), которое следует из условия доказываемой леммы. Рассмотрим систему линейных уравнений

$$\begin{aligned} \operatorname{tr}(\xi_0 x) &= 0, \\ \operatorname{tr}(\xi_0 \varphi_1 x) &= e, \\ \operatorname{tr}(\xi_0 \varphi_2 x) &= e \end{aligned} \quad (5.62)$$

над полем Q . По предположению, система элементов $\xi_0, \xi_0 \varphi_1, \xi_0 \varphi_2$ линейно независима над P , а значит, существует решение $\alpha \in Q$ системы (5.62). В представлении (2.11), θ_0 — примитивный элемент поля Q и $\alpha \in Q^*$, поэтому $\alpha = \theta_0^j$ для подходящего $j \in \mathbf{N}_0$. Но тогда согласно (5.60)

$$\begin{aligned} u_0(j) &= 0, \quad u_0^{(1)}(j) = e, \quad u_0^{(2)}(j) = e, \\ u_0(j) u_0^{(1)}(j) u_0^{(2)}(j) \oplus u_0^{(1)}(j) u_0^{(2)}(j) &\neq 0, \end{aligned}$$

что противоречит условию (5.34).

Лемма 16. Если $q = 2, u_0^{(2)} = u_0$, и $u^{(e)} \in L_R(F)$, то

$$u^{(e)} = (2^{n-1} - 1)u. \quad (5.63)$$

Доказательство. Мы опять возвращаемся к K -координатной записи последовательностей $u, u^{(e)}$ и к операциям в поле $(K, \oplus, \odot)$. Ввиду условия $u_0^{(2)} = u_0$, справедливо равенство $w_0^{(2)} = w_0$, и, ввиду (5.17), (5.28), имеют место соотношения

$$w_t^{(e)}(i) = w_t(i) \oplus \hat{e}w_0(i), \quad \hat{e} = \psi_K(e), \quad t \in \{1, \dots, n-2\}, \quad i \in I_*, \quad (5.64)$$

где

$$I_* = I_*^{(2)} = \{i \in \mathbf{N}_0 : w_0(i) = \hat{e}\}.$$

В частности, в тактах из множества $J \subseteq I_*$ со свойствами (J1), (J2) из раздела 5.2, $w_0[J] = (\hat{e}, \dots, \hat{e}) \in K^m$. Таким образом, справедливы соотношения

$$\begin{aligned} u(j) &= \hat{e} + 2w_1(j) + \dots + 2^{n-2}w_{n-2}(j) + 2^{n-1}w_{n-1}(j), \\ u^{(e)}(j) &= \hat{e} + 2(w_1(j) \oplus \hat{e}) + \dots + 2^{n-2}(w_{n-2}(j) \oplus \hat{e}) + 2^{n-1}w_{n-1}(j), \end{aligned} \quad (5.65)$$

Заметим теперь, что $K = \{0, \hat{e}\}$. Поэтому

$$w_t(j) + (w_t(j) \oplus \hat{e}) = \hat{e}.$$

Отсюда вытекают соотношения

$$\begin{aligned} u(j) + u^{(e)}(j) &= 2\hat{e} + 2\hat{e} + \dots + 2^{n-2}\hat{e} + 2^{n-1}(w_{n-1}(j) + w_{n-1}(j)) \\ &= 2^{n-1}\hat{e} = 2^{n-1}w_0(j), \quad j \in J. \end{aligned} \quad (5.66)$$

Другими словами,

$$u^{(e)}[J] = -u[J] + 2^{n-1}w_0[J] = -u[J] + 2^{n-1}u[J] = (2^{n-1} - 1)u[J]. \quad (5.67)$$

Так как $u \in L_R(F)$ и ввиду условия (J2) любая ЛРП из $L_R(F)$ однозначно определяется набором значений в тактах множества J , то при условии $u^{(e)} \in L_R(F)$ из (5.67) следует (5.63).

Лемма 17. Если $q = 2$, то для некоторого $t \in \{0, 1, \dots, \tau_1 - 1\}$ выполняются равенства

$$w_0(t) = 0, \quad w_1(t) = \hat{e}. \quad (5.68)$$

Доказательство. Согласно (3.1),

$$w_1(i + \tau_0) = w_1(i) \oplus w_0^{(1)}(i), \quad i \in \mathbf{N}_0,$$

причем $w_0^{(1)} \neq w_0$, так как в (2.7) $\bar{\Phi}_1(x) \neq \bar{e}$. Следовательно, для некоторого $t \in \mathbf{N}_0$ справедливо равенство $(w_0(t), w_0^{(1)}(t)) = (0, \hat{e})$, и либо $(w_0(t), w_1(t)) = (0, \hat{e})$, либо $(w_0(t + \tau_0), w_1(t + \tau_0)) = (0, \hat{e})$.

Лемма 18. ЛРП $u' = (2^{n-1} - 1)u \in L_P(F)$ удовлетворяет условию $w'_{n-1} \neq w_{n-1}$.

Доказательство. Пусть K -координатное разложение последовательности u' имеет вид

$$u' = w'_0 + 2w'_1 + \dots + 2^{n-1}w'_{n-1}, \quad w'_s(i) \in K = \{0, \hat{e}\}.$$

Для параметра t , удовлетворяющего условию (5.68), справедливо равенство $2^{n-1}u(t) = 0$. Отсюда следует, что

$$u'(t) = (2^{n-1} - 1)u(t) = -u(t),$$

и, пользуясь равенствами $w_s(t) + (w_s(t) \oplus \hat{e}) = \hat{e}$, получаем, что

$$-u(t) = 0 + 2\hat{e} + 2^2(w_2(t) \oplus \hat{e}) + \dots + 2^{n-1}(w_{n-1}(t) \oplus \hat{e}).$$

Таким образом, $w'_{n-1}(t) = w_{n-1}(t) \oplus \hat{e}$.

Из сравнения лемм 16 и 18 следует, что если $q = 2, u_0^{(2)} = u_0$, то $u^{(e)} \notin L_R(F)$. Теорема 5 доказана.

Авторы благодарны Д. Н. Былкову за важные замечания, позволившие уточнить формулировку основного результата и некоторые доказательства, и К. А. Жукову, обнаружившему серьезное упущение в первоначальном доказательстве теоремы 5. Мы признательны также Д. А. Пронькину за внимательное прочтение текста рукописи, в результате чего было устранено несколько искажений.

Список литературы

1. Берлекэмп Э., *Алгебраическая теория кодирования*. Мир, Москва, 1971.
2. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, 2. Гелиос АРВ, Москва, 2003.
3. Кузьмин А. С., Нечаев А. А., Построение помехоустойчивых кодов с использованием линейных рекуррент над кольцами Галуа. *Успехи математических наук* (1992) **47**, №5, 183–184.
4. Kuzmin A. S., Nechaev A. A., Linear recurrences over Galois rings. В сб.: *Труды 2-й Межд. конф. по алгебре*, Барнаул, 1991.
5. Кузьмин А. С., Нечаев А. А., Линейные рекуррентные последовательности над кольцами Галуа. *Алгебра и логика* (1995) **3**, №2, 169–189.
6. Кузьмин А. С., Куракин В. Л., Нечаев А. А., Псевдослучайные и полилинейные последовательности. *Труды по дискретной математике* (1997) **1**, 139–202.
7. Кузьмин А. С., Куракин В. Л., Нечаев А. А., Свойства линейных и полилинейных рекуррент над кольцами Галуа. *Труды по дискретной математике* (1998) **2**, 191–222.
8. Кузьмин А. С., Куракин В. Л., Нечаев А. А., Структурные аналитические и статистические свойства линейных и полилинейных рекуррент. *Труды по дискретной математике* (2000) **3**, 155–194.
9. Кузьмин А. С., Маршалко Г. Б., Нечаев А. А., Восстановление линейной рекурренты над примарным кольцом вычетов по ее усложнению. *Математические вопросы криптографии* (2010) **1**, №2, 31–56.
10. Нечаев А. А., Конечные кольца главных идеалов. *Математический сб.* (1973) **91**, №3, 350–366.
11. Нечаев А. А., Линейные рекуррентные последовательности над коммутативными кольцами. *Дискретная математика* (1991) **3**, №4, 107–121.
12. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., Linear recurring sequences over rings and modules. *J. Math. Sci.* (1995) **76**, №6, 2793–2915.

13. Кузьмин А. С., Нечаев А. А., Линейные рекуррентные последовательности над кольцами Галуа. *Успехи математических наук* (1993) **48**, №1, 167–168.
14. Кузьмин А. С., Нижние оценки рангов координатных последовательностей линейных рекуррентных последовательностей над примарными кольцами вычетов. *Успехи математических наук* (1993) **48**, №3, 193–194.
15. Лидл Р., Нидеррайтер Г., *Конечные поля*, 2. Мир, Москва, 1988.
16. Нечаев А. А., Код Кердока в циклической форме. *Дискретная математика* (1989) **1**, №4, 123–139.
17. Нечаев А. А., Цикловые типы линейных подстановок над конечными коммутативными локальными кольцами. *Математический сб.* (1993) **184**, №3, 21–56.
18. Laxton R. R., Anderson J. A., Linear recurrences and maximal length sequences. *Math. Gazette* (1972) **56**, 299–309.
19. Min-Qiang Huang, Zong-Duo Dai, Projective maps of linear recurring sequences with maximal p -adic periods. *Fibonacci Quart.* (1992) **30**, №2, 139–143.
20. Min-Qiang Huang, *Analysis and cryptologic evaluation for primitive sequences over an integer residue ring*, PhD Thesis. Graduate School of USTC, Academia Sinica, Beijing, China, 1988.
21. Xuan-Yong Zhu, Wen-Feng Qi, Uniqueness of the distribution of zeros of primitive level sequences over $\mathbf{Z}_{p^n}$. *Finite Fields Appl.* (2005) **11**, №1, 30–44.
22. Xuan-Yong Zhu, Wen-Feng Qi, Compression mappings on primitive sequences over $\mathbf{Z}_{p^n}$. *IEEE Trans. Inform. Theory* (2004) **50**, №10, 2442–2448.
23. Xuan-Yong Zhu, Wen-Feng Qi, Further result of compressing maps on primitive sequences modulo odd prime powers. *IEEE Trans. Inform. Theory* (2007) **53**, №8, 2985–2990.
24. Tian Tian, Wen-Feng Qi, Injectivity of compressing map on primitive sequences over $\mathbf{Z}_{p^l}$. *IEEE Trans. Inform. Theory* (2007) **53**, №8, 2960–2966.
25. Zong-Duo Dai, Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials. *J. Cryptology* (1992) **5**, №4, 193–207.
26. Weng-Feng Qi, Xuan-Yong Zhu, Compressing maps on primitive sequences over $\mathbf{Z}_{2^n}$ and its Galois extension. *Finite Fields Appl.* (2002) **8**, №4, 570–588.
27. Weng-Feng Qi, *Compressing maps on primitive sequences over $\mathbf{Z}_{2^n}$ and analysis of their derivative sequences*, PhD Thesis. Zhengzhou Inform. Eng. Univ., Zhengzhou, China, 1997.
28. Weng-Feng Qi, Jun-Hui Yang, Jin-Jun Zhou, ML-sequences over rings $\mathbf{Z}_{2^n}$. *Lecture Notes Computer Sci.* (1998) **1514**, 315–325.

Статья поступила 16.04.2010.