

ВОССТАНОВЛЕНИЕ ПОЛИНОМИАЛЬНО УСЛОЖНЁННОЙ ЛИНЕЙНОЙ РЕКУРРЕНТЫ МАКСИМАЛЬНОГО ПЕРИОДА НАД КОЛЬЦОМ ГАЛУА ПО СТАРШЕЙ КООРДИНАТНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Е. М. Серебряков

Центр специальных разработок, г. Москва, Россия

E-mail: ryback_casey@mail.ru

Рассматриваются усложнения линейной рекуррентной последовательности (ЛРП) максимального периода над кольцом Галуа $\text{GR}(q^n, p^n)$ с помощью некоторого многочлена $E(x)$ над этим кольцом, а также приводится алгоритм восстановления исходной рекурренты по старшей координатной последовательности полиномиально усложнённой ЛРП.

Ключевые слова: ЛРП максимального периода, полиномиальное усложнение, старшая координатная последовательность, восстановление начального вектора.

Введение

В криптографии актуальным остается вопрос о восстановлении линейной рекуррентной последовательности максимального периода (в частности, её начального отрезка) над кольцом Галуа по её старшей координатной последовательности. Ранее рядом авторов исследовалась старшая координатная последовательность u_{n-1} ЛРП максимального периода u и приводились соответствующие алгоритмы восстановления u по u_{n-1} . А. А. Нечаевым предложен алгоритм восстановления ЛРП максимального периода u над кольцом вычетов $R = \mathbb{Z}_{2^n}$ по её старшей координатной последовательности, впоследствии А. С. Кузьминым приведён алгоритм восстановления ЛРП максимального периода u над кольцом $R = \mathbb{Z}_{p^n}$ для произвольного $p \geq 3$.

В ряде работ отечественных [1, 2] и зарубежных авторов [3–6] уже исследовалась возможность восстановления усложнённой последовательности, причём усложнения задавались с помощью «инъективных отображений», то есть отображений, которые допускают однозначное восстановление исходной ЛРП по её усложнению.

Цель этой работы — для полиномиального усложнения ЛРП максимального периода u над кольцом Галуа $\text{GR}(q^n, p^n)$ произвольным многочленом $E(x) \in R[x]$ степени $k \geq 1$ построить алгоритм восстановления начального отрезка исходной рекурренты по значениям старшей координатной последовательности усложнённой ЛРП.

1. Постановка задачи

Всюду далее $R = \text{GR}(q^n, p^n)$ — кольцо Галуа характеристики p^n , состоящее из q^n элементов, где $n \in \mathbb{N}$, p простое, $q = p^r$. Согласно [7], множество pR всех делителей нуля есть идеал кольца R . Обозначим через $\bar{R} = R/pR = \text{GF}(q)$ поле вычетов кольца R . Эпиморфизм $\varphi : R \rightarrow \bar{R}$, действующий по правилу $\varphi(a) = \bar{a}$ для всех $a \in R$, естественным образом можно продолжить на кольцо многочленов $R[x]$. Образ любого многочлена $F(x) \in R[x]$ при таком эпиморфизме будем обозначать через $\bar{F}(x) \in \bar{R}[x]$. Подмножество K кольца R называется *координатным множеством* кольца R , если

его элементы образуют полную систему вычетов по модулю идеала pR . Примером координатного множества является p -адическое координатное множество (координатное множество Тейхмюллера) $\Gamma(R) = \{\alpha \in R : \alpha^q = \alpha\}$. Для $R = \text{GR}(p^n, p^n) = \mathbb{Z}_{p^n}$ ещё одним интересным примером координатного множества является p -ичное координатное множество $\delta(R) = \{0, 1, \dots, p-1\}$. Известно [8], что любой элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + pa_1 + \dots + p^{n-1}a_{n-1}, \quad (1)$$

где $a_t \in K, t = 0, 1, \dots, n-1$. Для всех $t \in \{0, \dots, n-1\}$ определим функции $\gamma_t^K : R \rightarrow K$ следующим образом: $\gamma_t^K(a) = a_t$, где a_t определяется равенством (1).

Функция γ_t^K называется t -й координатной функцией в координатном множестве K . Естественным образом введём на множестве K операции, положив для любых $a, b \in K$

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

Тогда $(K; \oplus, \otimes) = \text{GF}(q)$ — поле, изоморфное $\bar{R}$, причём изоморфизм $\psi : K \rightarrow \bar{R}$ задаётся соотношением $\psi(a) = \bar{a}$, где $a \in K$. Изоморфизм ψ также естественным образом продолжается на множество всех последовательностей K^∞ над множеством K . Образ любой последовательности $v \in K^\infty$ при таком изоморфизме будем обозначать через $\bar{v} \in \bar{R}^\infty$. Стоит отметить, что по последовательности $\bar{v} \in \bar{R}^\infty$ можно однозначно восстановить последовательность $v \in K^\infty$.

В качестве результата умножения многочлена $F(x) = \sum_{r \geq 0} f_r x^r \in R[x]$ на последовательность $u \in R^\infty$ определим последовательность $v = F(x)u$ из множества R^∞ , знаки которой определяются следующим образом:

$$v(i) = \sum_{r \geq 0} f_r u(i+r), \quad i \geq 0.$$

Пусть $F(x) \in R[x]$ — многочлен максимального периода, имеющий степень m и период $T(F) = (q^m - 1)p^{n-1}$ [9]. Обозначим $L_R(F) = \{u \in R^\infty : F(x)u = (0)\}$ множество последовательностей, аннулируемых многочленом $F(x)$. Из работы [9] известно, что период любой рекурренты из $L_R(F)$ удовлетворяет неравенству $T(u) \leq (q^m - 1)p^{n-1}$. Последовательность с периодом $T(u) = (q^m - 1)p^{n-1}$ назовём ЛРП максимального периода (МП).

Пусть всюду далее $u \in L_R(F)$ — ЛРП максимального периода. Для любого многочлена $E(x) = \sum_{j=0}^k e_j x^j \in R[x]$ определим последовательность $z = E(u) \in R^\infty$ со знаками

$$z(i) = \sum_{j=0}^k e_j u(i)^j \text{ для всех } i \geq 0. \text{ Последовательность } E(u) \text{ назовём полиномиальным}$$

усложнением рекурренты u с помощью многочлена $E(x)$ над кольцом R .

Для любой ЛРП $v \in R^\infty$ определим последовательность $v_t = \gamma_t^K(v) = (\gamma_t^K(v(0)), \gamma_t^K(v(1)), \dots)$, которая называется t -й координатной последовательностью рекурренты v в координатном множестве K . Последовательность v_t является ЛРП над K , так как она периодическая. Последовательность v_{n-1} назовём старшей координатной последовательностью ЛРП v .

В данной работе будем решать следующую задачу: по известной старшей координатной последовательности $z_{n-1} = \gamma_{n-1}^K(z)$ полиномиально усложнённой рекурренты восстановить исходную ЛРП максимального периода u . Отметим, что в работе [10]

эта задача решена для произвольного кольца Галуа $R = \text{GR}(q^n, p^n)$ и координатного множества K с некоторыми естественными ограничениями при $E(x) = x$.

Усложнения ЛРП u можно задавать с помощью функций $\Psi : R^n \rightarrow K$ следующим образом:

$$v(i) = \Psi(u_0(i), \dots, u_{n-1}(i)).$$

Такие отображения индуцируют отображения семейств последовательностей $\hat{\Psi} : L_R(F) \rightarrow K^\infty$, которые называются «сжимающими отображениями». Как уже отмечалось, некоторые из таких отображений позволяют однозначно восстановить исходную ЛРП по её усложнению. Поставленную задачу можно свести к отображениям такого вида с помощью следующей леммы.

Лемма 1. Знак координатной последовательности полиномиально усложнённой ЛРП $z = E(u)$ представляется в виде $z_t(i) = \Psi(u_0(i), \dots, u_t(i))$, $i \geq 0$, $t \in \{1, \dots, n-1\}$, где

$$\Psi(x_0, x_1, \dots, x_t) = E'(x_0)x_t + \eta(x_0, x_1, \dots, x_{t-1}), \quad \eta(x_0, x_1, \dots, x_{t-1}) \in K[x_0, x_1, \dots, x_{t-1}].$$

Доказательство. Рассмотрим $E(x)$ над кольцом $R/p^{t+1}R$, где $x \equiv x_0 + px_1 + \dots + p^t x_t \pmod{p^{t+1}}$:

$$E(x) \equiv \sum_{s=0}^{p^{t+1}} e_s \left(\sum_{j=0}^t p^j x_j \right)^s = \sum_{s=0}^k e_s \sum_{j_0+\dots+j_t=s} \frac{s!}{j_0! \dots j_t!} p^{j_1+2j_2+\dots+tj_t} x_0^{j_0} \dots x_t^{j_t}.$$

В этой сумме нас интересуют ненулевые слагаемые при p^t . Очевидно, что этому условию удовлетворяют лишь те слагаемые, у которых либо $j_t = 0$, либо $j_t = 1$, $j_0 = s-1$, $j_1 = \dots = j_{t-1} = 0$. Разбивая таким образом по j_t внутреннюю сумму на две части, $\Psi(x_0, \dots, x_t)$ можно представить в виде

$$\Psi(x_0, \dots, x_t) = \sum_{s=0}^k e_s \left(sp^t x_0^{s-1} x_t + \sum_{j_0+\dots+j_{t-1}=s} \frac{s!}{j_0! \dots j_{t-1}!} p^{j_1+2j_2+\dots+(t-1)j_{t-1}} x_0^{j_0} \dots x_{t-1}^{j_{t-1}} \right).$$

Значит, $\gamma_t^K(\Psi(x_0, \dots, x_t)) = E'(x_0)x_t + \eta(x_0, \dots, x_{t-1})$. ■

Заметим, что в [2] доказана принципиальная возможность восстановления исходной рекурренты, усложнённой с помощью функции $\Psi(x_0, \dots, x_{n-1})$, полученной в лемме 1, однако нет конструктивного алгоритма восстановления.

2. Сечения

Одним из подходов к изучению свойств координатных последовательностей является метод сечений. Определим умножение элемента $\alpha \in K$ на элемент $\bar{r} \in \bar{R}$ равенством $\bar{r}\alpha = \gamma_0^K(r\alpha)$. Тогда K есть $\bar{R}$ -алгебра и можно умножать любую последовательность над K на многочлен из $\bar{R}[x]$, а также рассматривать любую периодическую последовательность w над K как ЛРП над полем $\bar{R}$. Под сечением будем понимать умножение последовательности на некоторый многочлен, в результате чего получается более простая рекуррента. Обозначим $\tau_t = p^t(q^m - 1)$, $t = 0, 1, \dots, n-1$, $\tau_0 = \tau$. В работе [11] доказана следующая лемма.

Лемма 2. Пусть $F(x) \in R[x]$ — многочлен максимального периода. Тогда существуют многочлены $\Phi^{(t+1)}(x) \in R[x]$, $t \in \{0, \dots, n-1\}$, такие, что

$$\begin{aligned} x^{\tau_t} - e &\equiv p^{t+1} \Phi^{(t+1)}(x) \pmod{F(x)}, \quad t \in \{0, \dots, n-1\}, \\ \bar{\Phi}^{(t+1)}(x) &\neq 0, \quad \deg \Phi^{(t+1)}(x) < m, \end{aligned} \tag{2}$$

причём, если $p \geq 3$, $t \geq 1$, то $\Phi^{(t)}(x) \equiv \Phi^{(t+1)}(x) \pmod{p^{t+1}}$.

Очевидно, что многочлены $\Phi^{(t)}(x)$, где $t \in \{1, \dots, n\}$, определены неоднозначно, поэтому выберем их и зафиксируем. Последовательность $u^{(t)} = \Phi^{(t)}(x)u$ назовём *t-й производной последовательностью* рекурренты u . Нетрудно видеть, что $u^{(t)}$ — ЛРП максимального периода [8]. В работе [11] также доказано, что

$$\begin{aligned} u_0^{(1)} &= u_0^{(t)}, & t \geq 1, \\ u_1^{(2)} &= u_1^{(t)}, & t \geq 2. \end{aligned} \quad (3)$$

Далее считаем, что элементы координатных множеств $K = \{\alpha_1, \dots, \alpha_q\}$ и $\Gamma(R) = \{\beta_1, \dots, \beta_q\}$ упорядочены так, что $\alpha_t \equiv \beta_t \pmod{p}$, $t = 0, \dots, q-1$.

Известно [12], что существует единственный многочлен $\Psi_K(x) = \psi_{q-1}x^{q-1} + \dots + \psi_1x + \psi_0 \in R[x]$, такой, что $\Psi_K(\beta_t) = \alpha_t$, $t \in \{0, \dots, q-1\}$, при этом $\Psi_K(x) \equiv x \pmod{p}$ и $\psi_0 = 0$. Многочлен $\Psi_K(x)$ называется *интерполяционным многочленом* координатного множества K . Обозначим через

$$\Psi_K^*(x) = \psi_{q-1}^*x^{q-1} + \dots + \psi_1^*x \in R[x]$$

такой многочлен, что $\Psi_K(x) = x + p\Psi_K^*(x)$.

Пусть $F(x_1, \dots, x_k) \in R[x_1, \dots, x_k]$. Тогда через $\frac{\partial F}{\partial x_j}$ будем обозначать формальную частную производную многочлена F по переменной x_j для всех $j \in \{1, \dots, k\}$. Эти производные являются многочленами из $R[x_1, \dots, x_k]$. Через $\frac{\partial F}{\partial x_j}(a_1, \dots, a_k)$ будем обозначать значение частной производной в точке $(a_1, \dots, a_k) \in R^k$. В работе [12] доказана следующая лемма.

Лемма 3. Для любого $F(x_1, \dots, x_k) \in R[x_1, \dots, x_k]$ существует такой многочлен $F^*(x_1, \dots, x_k)$, что $F(x_1, \dots, x_k)^q = F(x_1^q, \dots, x_k^q) + pF^*(x_1, \dots, x_k)$, и для любых $a_1, \dots, a_k \in K$

$$\begin{aligned} \gamma_1^K(F(a_1, \dots, a_k)) &\equiv -F^*(a_1, \dots, a_k) + \sum_{i=1}^k \frac{\partial F}{\partial x_i}(a_1, \dots, a_k) \Psi_K^*(a_i) - \\ &\quad - \Psi_K^*(F(a_1, \dots, a_k)) \pmod{p}, \end{aligned} \quad (4)$$

в частности, для любых $a, b \in K$

$$\gamma_1^K(a+b) \equiv \sum_{j=1}^{p-1} \frac{1}{j!(p-j)!} a^{hj} b^{h(p-j)} + \Psi_K^*(a) + \Psi_K^*(b) - \Psi_K^*(a+b) \pmod{p}. \quad (5)$$

Для любого $s \in \{1, \dots, n\}$ обозначим $b^{(s)} = E'(u)u^{(s)} \in R^\infty$, где $E'(x)$ — производная многочлена $E(x)$. Пусть также $b_t^{(s)} = \gamma_t^K(b^{(s)})$, $s \in \{1, \dots, n\}$, $t = 0, 1$. Исследуем некоторые свойства последовательности $b^{(s)}$. Так как $b_0^{(s)}(i+\tau) = b_0^{(s)}(i)$ для всех $i \geq 0$, то $T(b_0^{(s)}) \mid \tau$ для всех $s \in \{1, \dots, n\}$.

Лемма 4. При всех $t \in \{2, \dots, n+1\}$ для координатной последовательности $b_1^{(t-1)} = \gamma_1^K(E'(u)u^{(t-1)})$ верно следующее равенство:

$$\begin{aligned} b_1^{(t-1)} &\equiv E'(u_0)\Psi_K^*(u_0^{(t-1)}) - \Psi_K^*(E'(u_0)u_0^{(t-1)}) - E'_*(u_0)u_0^{(t-1)} + \\ &\quad + E''(u_0)\Psi_K^*(u_0)u_0^{(t-1)} + E''(u_0)u_0^{(t-1)}u_1 + E'(u_0)u_1^{(t-1)} \pmod{p}, \end{aligned} \quad (6)$$

где $E'_*(x) \in R[x]$ — такой многочлен, что $E'(x)^q = E'(x^q) + pE'_*(x)$; $E''(x)$ — производная многочлена $E'(x)$.

Доказательство. Обозначим $v = E'(u)$, $w = u^{(t-1)}$, $v_j = \gamma_j^K(v)$, $w_j = \gamma_j^K(w)$, $j = 0, 1$. Тогда имеем

$$\begin{aligned} b_1^{(t-1)} &= \gamma_1^K(vw) = \gamma_1^K((v_0 + pv_1)(w_0 + pw_1)) = \\ &= \gamma_1^K(v_0w_0 + p(v_1w_0 + v_0w_1)) \equiv \gamma_1^K(v_0w_0) + v_1w_0 + v_0w_1 \pmod{p}. \end{aligned} \quad (7)$$

Заметим, что

$$v_0w_1 \equiv E'(u_0)u_1^{(t-1)} \pmod{p}. \quad (8)$$

Найдём $\gamma_1^K(v_0w_0)$. Возьмём в условиях леммы 3 в качестве $F(x_1, x_2)$ многочлен $x_1x_2 \in R[x_1, x_2]$, тогда из равенства (4) имеем

$$\begin{aligned} \gamma_1^K(v_0w_0) &\equiv w_0\Psi_K^*(v_0) + v_0\Psi_K^*(w_0) - \Psi_K^*(v_0w_0) \equiv \\ &\equiv u_0^{(t-1)}\Psi_K^*(E'(u_0)) + E'(u_0)\Psi_K^*(u_0^{(t-1)}) - \Psi_K^*(E'(u_0)u_0^{(t-1)}) \pmod{p}. \end{aligned} \quad (9)$$

Так как $E'(x) = \sum_{j=1}^k je_jx^{j-1}$, то

$$\begin{aligned} v = E'(u) &\equiv \sum_{j=1}^k je_j(u_0 + pu_1)^{j-1} \equiv \sum_{j=1}^k je_ju_0^{j-1} + pu_1 \sum_{j=2}^k j(j-1)e_ju_0^{j-2} \equiv \\ &\equiv E'(u_0) + pE''(u_0)u_1 \pmod{p^2}. \end{aligned} \quad (10)$$

Теперь, используя соотношения (10) и взяв в (4) в качестве $F(x_1, \dots, x_k)$ многочлен $E'(x)$, получаем

$$\begin{aligned} v_1 &\equiv \gamma_1^K(E'(u_0)) + E''(u_0)u_1 \equiv \\ &\equiv -E'_*(u_0) + E''(u_0)\Psi_K^*(u_0) - \Psi_K^*(E'(u_0)) + E''(u_0)u_1 \pmod{p}. \end{aligned} \quad (11)$$

Умножая (11) на $w_0 = u_0^{(t-1)}$, находим

$$\begin{aligned} v_1w_0 &\equiv -E'_*(u_0)u_0^{(t-1)} + E''(u_0)\Psi_K^*(u_0)u_0^{(t-1)} - \Psi_K^*(E'(u_0))u_0^{(t-1)} + \\ &\quad + E''(u_0)u_0^{(t-1)}u_1 \pmod{p}. \end{aligned} \quad (12)$$

Подставляя (8), (9) и (12) в соотношение (7), получаем (6). ■

Для $r, t \in \mathbb{N}$ обозначим

$$\delta(r = t) = \begin{cases} 1, & \text{если } r = t, \\ 0, & \text{если } r \neq t. \end{cases}$$

Обозначим $h = p^{r-1}$. Перейдём к построению сечений координатных последовательностей.

Теорема 1. Для координатных последовательностей ЛРП $z = E(u)$ справедливы следующие соотношения:

для $t = 1, \dots, n-1$

$$(x^{\tau_{t-1}} - e)z_t \equiv E'(u)u_0^{(t)} \pmod{p}; \quad (13)$$

для $t = 2, \dots, n-1$

$$(x^{\tau_{t-2}} - e)z_t \equiv \gamma_1^K(z_{t-1} + b^{(t-1)}) + \frac{1}{2}\delta(t=2)E''(u)(u_0^{(t-1)})^2 \pmod{p}; \quad (14)$$

для $j = 1, \dots, p-1, t = 1, \dots, n-1$

$$(x^{\tau_{t-1}} - e)^j z_t^j \equiv j! \left(b_0^{(t)}\right)^j \equiv j! \left(E'(u_0)u_0^{(t)}\right)^j \pmod{p}; \quad (15)$$

для $j = 1, \dots, p-1, t = 1, \dots, n-1$

$$(x^{\tau_{t-1}} - e)^{j-1} z_t^j \equiv j! z_t \left(b_0^{(t)}\right)^{j-1} + \frac{j-1}{2} j! \left(b_0^{(t)}\right)^j \pmod{p}; \quad (16)$$

для $t = 2, \dots, n-1$

$$\begin{aligned} (x^\tau - e)^{p^{t-1}-p^{t-2}} z_t &\equiv \left(z_{t-1} \left(b_0^{(t-1)}\right)^{p-1}\right)^h + \frac{p-2+2^{h-1}}{2^h} \left(b_0^{(t-1)}\right)^{ph} - \\ &- \sum_{s=p-1}^{q-1} \psi_s^* \sum_{\substack{j_1+\dots+j_p=s, \\ j_1 \geq 0, j_2 > 0, \dots, j_p > 0}} \frac{s!}{j_1! \dots j_p!} z_{t-1}^{j_1} \left(b_0^{(t-1)}\right)^{s-j_1} + \xi(p, t) \pmod{p}, \end{aligned} \quad (17)$$

где

$$\xi(p, t) = \begin{cases} E'(u_0)\Phi^{(1)}(x)u_0^{(1)} + E''(u_0) \left(u_0^{(1)}\right)^2, & \text{если } p=3, t=2, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Доказательство. Докажем равенство (13). Учитывая, что $T(u_t) = \tau_t$ [8], по лемме 1 получим $T(z_t) \mid \tau_t$. Тогда

$$(x^{\tau_{t-1}} - e)z \equiv p^t(x^{\tau_{t-1}} - e)z_t \pmod{p^{t+1}}. \quad (18)$$

С другой стороны, из соотношения (2) следует, что $(x^{\tau_{t-1}} - e)u \equiv p^t u_0^{(t)} \pmod{p^{t+1}}$, или

$$u(i + \tau_{t-1}) \equiv u(i) + p^t u_0^{(t)}(i) \pmod{p^{t+1}}. \quad (19)$$

Теперь, используя равенство (19), имеем для всех $i \geq 0$

$$\begin{aligned} (x^{\tau_{t-1}} - e)z(i) &= z(i + \tau_{t-1}) - z(i) \equiv \sum_{j=0}^k e_j (u(i + \tau_{t-1})^j - u(i)^j) \equiv \\ &\equiv \sum_{j=0}^k j e_j u(i)^{j-1} p^t u_0^{(t)}(i) = p^t E'(u(i))u_0^{(t)}(i) \pmod{p^{t+1}}. \end{aligned} \quad (20)$$

Сравнивая соотношения (18) и (20), получаем равенство (13).

Докажем равенство (14). Используя (2), получаем

$$(x^{\tau_{t-2}} - e)u = p^{t-1}u^{(t-1)} \equiv p^{t-1}u_0^{(t-1)} + p^t u_1^{(t-1)} \pmod{p^{t+1}}.$$

Тогда для всех $i \geq 0$

$$\begin{aligned} u(i + \tau_{t-2})^j &\equiv \left(u(i) + p^{t-1}u_0^{(t-1)}(i) + p^t u_1^{(t-1)}(i)\right)^j \equiv u(i)^j + j u(i)^{j-1} \left(p^{t-1}u_0^{(t-1)}(i) + \right. \\ &\quad \left. + p^t u_1^{(t-1)}(i)\right) + \binom{j}{2} u(i)^{j-2} \left(p^{t-1}u_0^{(t-1)}(i) + p^t u_1^{(t-1)}(i)\right)^2 \equiv u(i)^j + \\ &\quad + j u(i)^{j-1} \left(p^{t-1}u_0^{(t-1)}(i) + p^t u_1^{(t-1)}(i)\right) + \delta(t=2) \binom{j}{2} u(i)^{j-2} p^t (u_0^{(t-1)}(i))^2 \pmod{p^{t+1}}. \end{aligned} \quad (21)$$

Используя соотношение (21), получаем

$$\begin{aligned}
(x^{\tau_{t-2}} - e)z(i) &= z(i + \tau_{t-2}) - z(i) \equiv \sum_{j=0}^k e_j (u(i + \tau_{t-2})^j - u(i)^j) \equiv \\
&\equiv \sum_{j=0}^k e_j \left[ju(i)^{j-1} (p^{t-1}u_0^{(t-1)}(i) + p^t u_1^{(t-1)}(i)) + \delta(t=2) \binom{j}{2} u(i)^{j-2} p^t u_0^{(t-1)}(i)^2 \right] \equiv \quad (22) \\
&\equiv p^{t-1} E'(u(i)) u_0^{(t-1)}(i) + p^t E'(u(i)) u_1^{(t-1)}(i) + \frac{1}{2} \delta(t=2) p^t E''(u(i)) (u_0^{(t-1)}(i))^2 \pmod{p^{t+1}}.
\end{aligned}$$

С другой стороны, используя соотношения $T(z_t) \mid \tau_t$ для всех $t \in \{0, \dots, n-1\}$ и равенство $z_t(i + \tau_{t-1}) = \gamma_0^K(z_t(i) + E'(u(i))u^{(t)}(i))$, вытекающее из (13), получаем

$$\begin{aligned}
(x^{\tau_{t-2}} - e)z(i) &\equiv (x^{\tau_{t-2}} - e)(p^{t-1}z_{t-1}(i) + p^t z_t(i)) \equiv \\
&\equiv p^{t-1}(z_{t-1}(i + \tau_{t-2}) - z_{t-1}(i)) + p^t(x^{\tau_{t-2}} - e)z_t(i) \equiv \quad (23) \\
&\equiv p^{t-1}(\gamma_0^K(z_{t-1}(i) + E'(u(i))u^{(t-1)}(i)) - z_{t-1}(i)) + p^t(x^{\tau_{t-2}} - e)z_t(i) \pmod{p^{t+1}}.
\end{aligned}$$

Сравнивая (23) с соотношением (22), получаем

$$\begin{aligned}
&p(x^{\tau_{t-2}} - e)z_t \equiv \\
&\equiv E'(u)u_0^{(t-1)} + pE'(u)u_1^{(t-1)} + \frac{1}{2}\delta(t=2)pE''(u)(u_0^{(t-1)})^2 - \gamma_0^K(z_{t-1} + E'(u)u^{(t-1)}) + z_{t-1} \equiv \\
&\equiv p\gamma_1^K(z_{t-1} + E'(u)u^{(t-1)}) + \frac{1}{2}\delta(t=2)pE''(u)(u_0^{(t-1)})^2 \pmod{p^2}.
\end{aligned}$$

В итоге $(x^{\tau_{t-2}} - e)z_t \equiv \gamma_1^K(z_{t-1} + E'(u)u^{(t-1)}) + \frac{1}{2}\delta(t=2)E''(u)(u_0^{(t-1)})^2 \pmod{p}$, что и требовалось доказать.

Докажем сравнение (15). Для всех $i \geq 0$ и $s \in \overline{1, p-1}$, используя соотношение (13) и условие $T(b_0) \mid \tau_{t-1}$, имеем

$$\begin{aligned}
(x^{\tau_{t-1}} - e)z_t^s(i) &\equiv z_t^s(i + \tau_{t-1}) - z_t^s(i) \equiv (z_t(i) + b_0^{(t)}(i))^s - z_t^s(i) \equiv \\
&\equiv \sum_{j=0}^{s-1} \binom{s}{j} z_t^j(i) (b_0^{(t)}(i))^{s-j} \equiv g(z_t(i), b_0^{(t)}(i)) \pmod{p}, \quad (24)
\end{aligned}$$

где $g(x, y) \in K[x, y]$; $\deg_x g \leq s-1$; $\deg_y g \leq s$.

Поэтому нетрудно видеть, что для любого $s \in \{1, \dots, p-1\}$ при $l > s$

$$(x^{\tau_{t-1}} - e)^l z_t^s \equiv 0 \pmod{p}.$$

Используя (24), методом математической индукции покажем, что для всех $j \in \{1, \dots, p-1\}$ и $s \in \{1, \dots, j\}$ выполняется

$$\begin{aligned}
&(x^{\tau_{t-1}} - e)^s z_t^j \equiv j(j-1) \dots (j-s+1) z_t^{j-s} (b_0^{(t)})^s + \\
&+ \frac{s}{2} j(j-1) \dots (j-s) z_t^{j-s-1} (b_0^{(t)})^{s+1} + g^{(s)}(z_t, b_0^{(t)}) \pmod{p}, \quad (25)
\end{aligned}$$

где $g^{(s)}(x, y) \in K[x, y]$; $\deg_x g^{(s)}(x, y) \leq j-s-2$.

Проверим основание индукции при $s=1$. Имеем

$$(x^{\tau_{t-1}} - e)z_t^j \equiv (z_t + b_0^{(t)})^j - z_t^j \equiv j z_t^{j-1} b_0^{(t)} + \frac{j(j-1)}{2} z_t^{j-2} (b_0^{(t)})^2 + g^{(1)}(z_t, b_0^{(t)}) \pmod{p},$$

где $\deg_x g^{(1)}(x, y) \leq j-3$.

Пусть равенство (25) верно для s , проверим его справедливость для $s + 1$. Имеем

$$\begin{aligned} (x^{\tau_{t-1}} - e)^{s+1} z_t^j &\equiv j(j-1) \dots (j-s+1) \left(b_0^{(t)}\right)^s \left((j-s) z_t^{j-s-1} b_0^{(t)} + \right. \\ &\quad \left. + \frac{(j-s)(j-s-1)}{2} z_t^{j-s-2} \left(b_0^{(t)}\right)^2 + g_1^{(s+1)}(z_t, b_0^{(t)})\right) + \\ &\quad + \frac{s}{2} j(j-1) \dots (j-s) \left(b_0^{(t)}\right)^{s+1} \left((j-s-1) z_t^{j-s-2} b_0^{(t)} + \right. \\ &\quad \left. + g_2^{(s+1)}(z_t, b_0^{(t)})\right) + g^{(s+1)}(z_t, b_0^{(t)}) \pmod{p}, \end{aligned}$$

где $\deg_x g_1^{(s+1)} \leq j-s-3$; $\deg_x g_2^{(s+1)} \leq j-s-3$; $\deg_x g^{(s+1)} \leq j-s-3$.

Сгруппируем слагаемые с одинаковыми степенями z_t :

$$\begin{aligned} (x^{\tau_{t-1}} - e)^{s+1} z_t^j &\equiv j(j-1) \dots (j-s) z_t^{j-(s+1)} \left(b_0^{(t)}\right)^{s+1} + \\ &\quad + \frac{s+1}{2} j(j-1) \dots (j-s-1) z_t^{j-s-2} \left(b_0^{(t)}\right)^{s+2} + \hat{g}^{(s+1)}(z_t, b_0^{(t)}) \pmod{p}. \end{aligned}$$

Таким образом, сравнение (25) верно. Подставляя в него $s = k-1$ и $s = k$, получаем сравнения (15) и (16) соответственно.

Докажем сравнение (17). Напомним, что $b^{(t)} = E'(u)u^{(t)}$, $b_r^{(t)} = \gamma_r^K(b^{(t)})$, $r \in \{0, 1\}$, $t \in \{1, \dots, n\}$. Тогда $b_0^{(t)} \equiv E'(u_0)u_0^{(t)} \pmod{p}$. Используя равенство (14), получаем

$$(x^{\tau_{t-2}} - e)z_t \equiv \gamma_1^K(z_{t-1} + b_0^{(t-1)}) + b_1^{(t-1)} + \frac{1}{2}\delta(t=2)E''(u_0)\left(u_0^{(t-1)}\right)^2 \pmod{p}. \quad (26)$$

Рассмотрим последовательное $(p-2)$ раза умножение $(x^{\tau_{t-2}} - e)$ на последовательность $\gamma_1^K(z_{t-1} + b_0^{(t-1)})$. Из (5) имеем $\gamma_1^K(z_{t-1} + b_0^{(t-1)}) \equiv A + D \pmod{p}$, где

$$A = \sum_{j=1}^{p-1} \frac{1}{j!(p-j)!} z_{t-1}^{jh} \left(b_0^{(t-1)}\right)^{(p-j)h}, \quad D = \Psi_K^*(z_{t-1}) + \Psi_K^*(b_0^{(t-1)}) - \Psi_K^*(z_{t-1} + b_0^{(t-1)}).$$

Используя (25), методом математической индукции докажем, что для всех $s \in \{1, \dots, p-2\}$ верно

$$\begin{aligned} (x^{\tau_{t-2}} - e)^s A &\equiv \frac{(p-1)^h \dots (p-s)^h}{(p-1)!} z_{t-1}^{(p-s-1)h} \left(b_0^{(t-1)}\right)^{(s+1)h} + \\ &\quad + \frac{(s+2^{h-1})(p-2)^h \dots (p-s-1)^h}{2^h(p-2)!} z_{t-1}^{(p-s-2)h} \left(b_0^{(t-1)}\right)^{(s+2)h} + \\ &\quad + g^{(s)}(z_{t-1}, b_0^{(t-1)}) \pmod{p}, \end{aligned} \quad (27)$$

где $g^{(s)}(x, y) \in K[x, y]$; $\deg_x g^{(s)} \leq (p-s-3)h$.

Пользуясь тем, что характеристика поля K делит h , и используя сравнение (25) при $s = 1$ и $k = j$, $j \in \{1, \dots, p-1\}$, получаем для всех $i \geq 0$

$$\begin{aligned} (x^{\tau_{t-2}} - e)z_{t-1}^{jh}(i) &\equiv z_{t-1}(i + \tau_{t-2})^{jh} - z_{t-1}(i)^{jh} \equiv (z_{t-1}(i + \tau_{t-2})^j - z_{t-1}(i)^j)^h \equiv \\ &\equiv ((x^{\tau_{t-2}} - e)z_{t-1}^j(i))^h \equiv j^h z_{t-1}(i)^{(j-1)h} b_0^{(t-1)}(i)^h + \\ &\quad + \frac{j^h(j-1)^h}{2^h} z_{t-1}(i)^{(j-2)h} b_0^{(t-1)}(i)^{2h} + g(z_{t-1}(i), b_0^{(t-1)}(i)) \pmod{p}, \end{aligned} \quad (28)$$

где $g(x, y) \in K[x, y]$; $\deg_x g \leq (j-3)h$.

Выделим в A следующие два слагаемых:

$$A = \frac{1}{(p-1)!} z_{t-1}^{(p-1)h} \left(b_0^{(t-1)}\right)^h + \frac{1}{2(p-2)!} z_{t-1}^{(p-2)h} \left(b_0^{(t-1)}\right)^{2h} + g^{(0)} \left(z_{t-1}, b_0^{(t-1)}\right),$$

где $g^{(0)}(x, y) \in K[x, y]$; $\deg_x g^{(0)} \leq (p-3)h$. Теперь, пользуясь тем, что $T(b_0^{(t-1)})|_{\tau_{t-2}}$, докажем базу индукции, используя (28). Имеем

$$\begin{aligned} (x^{\tau_{t-2}} - e)A &\equiv \frac{1}{(p-1)!} \left(b_0^{(t-1)}\right)^h (x^{\tau_{t-2}} - e) z_{t-1}^{(p-1)h} + \frac{1}{2(p-2)!} \left(b_0^{(t-1)}\right)^{2h} (x^{\tau_{t-2}} - e) z_{t-1}^{(p-2)h} + \\ &+ (x^{\tau_{t-2}} - e) g^{(0)} \left(z_{t-1}, b_0^{(t-1)}\right) \equiv \frac{1}{(p-1)!} \left(b_0^{(t-1)}\right)^h \left((p-1)^h z_{t-1}^{(p-2)h} \left(b_0^{(t-1)}\right)^h + \right. \\ &+ \left. \frac{(p-1)^h (p-2)^h}{2^h} z_{t-1}^{(p-3)h} \left(b_0^{(t-1)}\right)^{2h} + g_1^{(1)} \left(z_{t-1}, b_0^{(t-1)}\right) \right) + \\ &+ \frac{\left(b_0^{(t-1)}\right)^{2h}}{2(p-2)!} \left((p-2)^h z_{t-1}^{(p-3)h} \left(b_0^{(t-1)}\right)^h + g_2^{(1)} \left(z_{t-1}, b_0^{(t-1)}\right) \right) + \hat{g}^{(1)} \left(z_{t-1}, b_0^{(t-1)}\right) \pmod{p}, \end{aligned}$$

где $g_1^{(1)}(x, y), g_2^{(1)}(x, y), \hat{g}^{(1)}(x, y) \in K[x, y]$; $\deg_x g_1^{(1)} \leq (p-4)h$; $\deg_x g_2^{(1)} \leq (p-4)h$; $\deg_x \hat{g}^{(1)} \leq (p-4)h$.

Группируем коэффициенты при одинаковых степенях z_{t-1} :

$$\begin{aligned} (x^{\tau_{t-2}} - e)A &\equiv \frac{(p-1)^h}{(p-1)!} z_{t-1}^{(p-2)h} \left(b_0^{(t-1)}\right)^{2h} + \\ &+ \left(\frac{(p-1)^h (p-2)^h}{2^h (p-1)!} + \frac{(p-2)^h}{2(p-2)!} \right) z_{t-1}^{(p-3)h} \left(b_0^{(t-1)}\right)^{3h} + g^{(1)} \left(z_{t-1}, b_0^{(t-1)}\right) \pmod{p}, \end{aligned}$$

где $g^{(1)}(x, y) \in K[x, y]$; $\deg_x g^{(1)} \leq (p-4)h$.

Пользуясь тем, что h нечётное, получаем

$$\begin{aligned} (x^{\tau_{t-2}} - e)A &\equiv \frac{(p-1)^h}{(p-1)!} z_{t-1}^{(p-2)h} \left(b_0^{(t-1)}\right)^{2h} + \frac{(2^{h-1} + 1)(p-2)^h}{2^h (p-2)!} z_{t-1}^{(p-3)h} \left(b_0^{(t-1)}\right)^{3h} + \\ &+ g^{(1)} \left(z_{t-1}, b_0^{(t-1)}\right) \pmod{p}, \end{aligned}$$

где $g^{(1)}(x, y) \in K[x, y]$; $\deg_x g^{(1)} \leq (p-4)h$.

Используя сравнение (28), проверим шаг индукции:

$$\begin{aligned} (x^{\tau_{t-2}} - e)^{s+1} A &\equiv \frac{(p-1)^h \dots (p-s)^h}{(p-1)!} \left(b_0^{(t-1)}\right)^{(s+1)h} (x^{\tau_{t-2}} - e) z_{t-1}^{(p-s-1)h} + \\ &+ \frac{(s+2^{h-1})(p-2)^h \dots (p-s-1)^h}{2^h (p-2)!} \left(b_0^{(t-1)}\right)^{(s+2)h} (x^{\tau_{t-2}} - e) z_{t-1}^{(p-s-2)h} + \\ &+ (x^{\tau_{t-2}} - e) g^{(s)} \left(z_{t-1}, b_0^{(t-1)}\right) \equiv \frac{(p-1)^h \dots (p-s)^h}{(p-1)!} \left(b_0^{(t-1)}\right)^{(s+1)h} \times \\ &\times \left((p-s-1)^h z_{t-1}^{(p-s-2)h} \left(b_0^{(t-1)}\right)^h + \frac{(p-s-1)^h (p-s-2)^h}{2^h} z_{t-1}^{(p-s-3)h} \left(b_0^{(t-1)}\right)^{2h} + \right. \end{aligned}$$

$$\begin{aligned}
& + g_1^{(s+1)}(z_{t-1}, b_0^{(t-1)}) + \frac{(s + 2^{h-1})(p-2)^h \dots (p-s-1)^h}{2^h(p-2)!} \times \\
& \times \left(b_0^{(t-1)}\right)^{(s+2)h} \left((p-s-2)^h z_{t-1}^{(p-s-3)h} \left(b_0^{(t-1)}\right)^h + \right. \\
& \left. + g_2^{(s+1)}(z_{t-1}, b_0^{(t-1)}) \right) + \hat{g}^{(s+1)}(z_{t-1}, b_0^{(t-1)}) \pmod{p},
\end{aligned}$$

где $g_1^{(s+1)}(x, y), g_2^{(s+1)}(x, y), \hat{g}^{(s+1)}(x, y) \in K[x, y]$; $\deg_x g_1^{(s+1)} \leq (p-s-4)h$; $\deg_x g_2^{(s+1)} \leq (p-s-4)h$; $\deg_x \hat{g}^{(s+1)} \leq (p-s-4)h$.

Раскрывая скобки и группируя коэффициенты при одинаковых степенях z_{t-1} , получаем

$$\begin{aligned}
(x^{\tau_{t-2}} - e)^{s+1} A & \equiv \frac{(p-1)^h \dots (p-s)^h (p-s-1)^h}{(p-1)!} z_{t-1}^{(p-s-2)h} \left(b_0^{(t-1)}\right)^{(s+2)h} + \\
& + \frac{(p-1)^h \dots (p-s-2)^h}{2^h(p-1)!} z_{t-1}^{(p-s-3)h} \left(b_0^{(t-1)}\right)^{(s+3)h} + \\
& + \frac{(s + 2^{h-1})(p-2)^h \dots (p-s-2)^h}{2^h(p-2)!} z_{t-1}^{(p-s-3)h} \left(b_0^{(t-1)}\right)^{(s+3)h} + g^{(s+1)}(z_{t-1}, b_0^{(t-1)}) \pmod{p},
\end{aligned}$$

где $g^{(s+1)}(x, y) \in K[x, y]$; $\deg_x g^{(s+1)} \leq (p-s-4)h$. Отсюда следует справедливость сравнения (27).

Аналогично методом математической индукции доказывается, что для всех $s \in \{1, \dots, p-2\}$

$$(x^{\tau_{t-2}} - e)^s D \equiv - \sum_{r=s+1}^{q-1} \psi_r^* \sum_{\substack{j_1 + \dots + j_{s+2} = r, \\ j_1 \geq 0, j_2 > 0, \dots, j_{s+2} > 0}} \frac{r!}{j_1! \dots j_{s+2}!} z_{t-1}^{j_1} \left(b_0^{(t-1)}\right)^{r-j_1} \pmod{p}. \quad (29)$$

Подставляя $s = p-2$ в равенства (27) и (29) и используя теорему Вильсона, получаем

$$\begin{aligned}
(x^{\tau_{t-2}} - e)^{p-2} A & \equiv \left(z_{t-1} \left(b_0^{(t-1)}\right)^{p-1} \right)^h + \frac{p-2+2^{h-1}}{2^h} \left(b_0^{(t-1)}\right)^q \pmod{p}, \\
(x^{\tau_{t-2}} - e)^{p-2} D & \equiv - \sum_{r=p-1}^{q-1} \psi_r^* \sum_{\substack{j_1 + \dots + j_p = r, \\ j_1 \geq 0, j_2 > 0, \dots, j_p > 0}} \frac{r!}{j_1! \dots j_p!} z_{t-1}^{j_1} \left(b_0^{(t-1)}\right)^{r-j_1} \pmod{p}.
\end{aligned}$$

Таким образом,

$$\begin{aligned}
(x^{\tau_{t-2}} - e)^{p-2} \gamma_1^K \left(z_{t-1} + b_0^{(t-1)} \right) & \equiv \left(z_{t-1} \left(b_0^{(t-1)}\right)^{p-1} \right)^h + \frac{p-2+2^{h-1}}{2^h} \left(b_0^{(t-1)}\right)^{ph} - \\
& - \sum_{r=p-1}^{q-1} \psi_r^* \sum_{\substack{j_1 + \dots + j_p = r, \\ j_1 \geq 0, j_2 > 0, \dots, j_p > 0}} \frac{r!}{j_1! \dots j_p!} z_{t-1}^{j_1} \left(b_0^{(t-1)}\right)^{r-j_1} \pmod{p}. \quad (30)
\end{aligned}$$

Теперь вычислим $(x^{\tau_{t-2}} - e)^{p-2} b_1^{(t-1)}$. С учётом леммы 4 видно, что в соотношении (6) все слагаемые, кроме последних двух, имеют период, делящий τ , поэтому

$$\begin{aligned}
(x^{\tau_{t-2}} - e)^{p-2} b_1^{(t-1)} & \equiv E''(u_0) u_0^{(t-1)} (x^{\tau_{t-2}} - e)^{p-2} u_1 + \\
& + E'(u_0) (x^{\tau_{t-2}} - e)^{p-2} u_1^{(t-1)} \pmod{p}. \quad (31)
\end{aligned}$$

Пользуясь равенствами (3) и соотношениями $T(u_1) \mid \tau_1$ и $(x^\tau - e)u_1 \equiv u_0^{(1)} \pmod{p}$, получаем

$$(x^{\tau_{t-2}} - e)u_1 = \begin{cases} u_0^{(1)}, & \text{если } t = 2, \\ 0, & \text{если } t > 2. \end{cases}$$

Так как $T(u_0^{(1)}) \mid \tau_0$, имеем

$$(x^{\tau_{t-2}} - e)^{p-2}u_1 = \begin{cases} u_0^{(1)}, & \text{если } p = 3, t = 2, \\ 0 & \text{в противном случае.} \end{cases} \quad (32)$$

В итоге из равенств (32) вытекает

$$E''(u_0)u_0^{(t-1)}(x^{\tau_{t-2}} - e)^{p-2}u_1 = \begin{cases} E''(u_0)(u_0^{(1)})^2, & \text{если } p = 3, t = 2, \\ 0 & \text{в противном случае.} \end{cases} \quad (33)$$

Рассмотрим $(x^{\tau_{t-2}} - e)u_1^{(t-1)}$:

$$\begin{aligned} (x^{\tau_{t-2}} - e)u_1^{(t-1)} &\equiv (x^{\tau_{t-2}} - e)\gamma_1^K(u^{(t-1)}) \equiv (x^{\tau_{t-2}} - e)\gamma_1^K(\Phi^{(t-1)}(x)u) \equiv \\ &\equiv (x^{\tau_{t-2}} - e)\gamma_1^K(\Phi^{(1)}(x)u) \equiv (x^{\tau_{t-2}} - e)\gamma_1^K(\Phi^{(1)}(x)(u_0 + pu_1)) \equiv \\ &\equiv (x^{\tau_{t-2}} - e)\gamma_1^K(\Phi^{(1)}(x)u_0 + p\Phi^{(1)}(x)u_1) \equiv (x^{\tau_{t-2}} - e)\gamma_1^K(\Phi^{(1)}(x)u_0) + \\ &\quad + (x^{\tau_{t-2}} - e)(\Phi^{(1)}(x)u_1) \pmod{p}. \end{aligned}$$

Так как период последовательности $\gamma_1^K(\Phi^{(1)}(x)u_0)$ делит τ , то, используя соотношения $T(u_1) \mid \tau_1$ и $(x^\tau - e)u_1 \equiv u_0^{(1)} \pmod{p}$, получаем

$$(x^{\tau_{t-2}} - e)u_1^{(t-1)} \equiv (x^{\tau_{t-2}} - e)\Phi^{(1)}(x)u_1 \equiv \begin{cases} \Phi^{(1)}(x)u_0^{(1)}, & \text{если } t = 2, \\ 0 & \text{в противном случае.} \end{cases} \quad (34)$$

Пользуясь (34) и соотношением $T(u_0^{(1)}) \mid \tau$, получаем

$$E'(u_0)(x^{\tau_{t-2}} - e)^{p-2}u_1^{(t-1)} \equiv \begin{cases} E'(u_0)\Phi^{(1)}(x)u_0^{(1)}, & \text{если } p = 3, t = 2, \\ 0 & \text{в противном случае.} \end{cases} \quad (35)$$

С учётом (33) и (35) равенство (31) примет вид

$$(x^{\tau_{t-2}} - e)^{p-2}b_1^{(t-1)} \equiv \begin{cases} E'(u_0)\Phi^{(1)}(x)u_0^{(1)} + E''(u_0)(u_0^{(1)})^2, & \text{если } t = 2, p = 3, \\ 0 & \text{в противном случае.} \end{cases} \quad (36)$$

Таким образом, с использованием сравнения (26) имеем

$$(x^{\tau_{t-2}} - e)^{p-1}z_t \equiv (x^{\tau_{t-2}} - e)^{p-2}\gamma_1^K(z_t + b_0^{(t-1)}) + (x^{\tau_{t-2}} - e)^{p-2}b_1^{(t-1)} \pmod{p}. \quad (37)$$

Объединяя результаты (30), (36) и (37), получаем

$$\begin{aligned} (x^\tau - e)^{p^{t-1}-p^{t-2}}z_t &\equiv \left(z_{t-1} \left(b_0^{(t-1)}\right)^{p-1}\right)^h + \frac{p-2+2^{h-1}}{2^h} \left(b_0^{(t-1)}\right)^{ph} - \\ &\quad - \sum_{r=p-1}^{q-1} \psi_r^* \sum_{\substack{j_1+\dots+j_p=r, \\ j_1 \geq 0, j_2 > 0, \dots, j_p > 0}} \frac{r!}{j_1! \dots j_p!} z_{t-1}^{j_1} \left(b_0^{(t-1)}\right)^{r-j_1} + \xi(p, t), \end{aligned}$$

где

$$\xi(p, t) = \begin{cases} E'(u_0)\Phi^{(1)}(x)u_0^{(1)} + E''(u_0)(u_0^{(1)})^2, & \text{если } t = 2, p = 3, \\ 0 & \text{в противном случае.} \end{cases}$$

Теорема доказана. ■

3. Алгоритм восстановления

Прежде чем перейти к алгоритму восстановления, приведем еще несколько результатов. Для всех $t \in \mathbb{N}$ обозначим

$$t = \sum_{i \geq 0} \nu_i(t) p^i, \quad \nu_i(t) \in \{0, \dots, p-1\}, \quad w_p(t) = \sum_{i \geq 0} \nu_i(t),$$

$$t = \sum_{i \geq 0} \rho_i(t) q^i, \quad \rho_i(t) \in \{0, \dots, q-1\}, \quad w_q(t) = \sum_{i \geq 0} \rho_i(t),$$

где $\nu_i(t)$ — коэффициент при p^i в p -ичном разложении; $\rho_i(t)$ — коэффициент при q^i в q -ичном разложении; $w_p(t)$ — p -ичный вес числа t ; $w_q(t)$ — q -ичный вес числа t .

Для доказательства основного результата потребуется ещё одна лемма.

Лемма 5 [13]. Пусть $\alpha \in \mathbb{N}$, $k_1, \dots, k_\alpha \in \mathbb{N}_0$, $k = k_1 + \dots + k_\alpha$, ε — максимальная степень простого числа p , делящая полиномиальный коэффициент $\frac{k!}{k_1! \dots k_\alpha!}$. Тогда

$$\text{а) } \varepsilon = \frac{w_p(k_1) + \dots + w_p(k_\alpha) - w_p(k)}{p-1};$$

$$\text{б) } \frac{k!}{k_1! \dots k_\alpha!} \equiv (-p)^\varepsilon \prod_{m \geq 0} \frac{\nu_m(k)!}{\nu_m(k_1)! \dots \nu_m(k_\alpha)!} \pmod{p^{\varepsilon+1}}.$$

Так как $\bar{F}(x) \in \bar{R}[x]$ — примитивный многочлен, то существует корень ω этого многочлена в расширении Галуа $\bar{S} = \text{GF}(q^m)$ поля $\bar{R}$. Известно, что любая последовательность из $L_{\bar{R}}(\bar{F})$ представляется в виде линейной комбинации биномиальных последовательностей с корнями из множества корней многочлена $\bar{F}(x) \in \bar{R}[x]$.

Лемма 6. Пусть $E(x) = \sum_{r=0}^k e_r x^r$ и $\deg \bar{E}(x) = k' \in \{1, \dots, q-1\}$. Тогда последовательность $b_0^{(1)}$ представляется в виде

$$b_0^{(1)} = (s+1)\bar{e}_{s+1}u_0^s \otimes u_0^{(1)} \oplus l, \quad s \in \{0, \dots, k'-1\}, \quad (\mu_l(x), \mu_s(x)) = \bar{e},$$

где $l \in K^\infty$; $\mu_l(x)$ — минимальный многочлен ЛРП l ; $\mu_s(x)$ — минимальный многочлен ЛРП $u_0^s u_0^{(1)}$.

Доказательство. Из определения $b_0^{(1)}$ получаем

$$b_0^{(1)} = \bar{E}'(u_0) \otimes u_0^{(1)} = \sum_{r=0}^{k'-1} \oplus (r+1)\bar{e}_{r+1}u_0^r \otimes u_0^{(1)}.$$

Для доказательства леммы достаточно показать, что для двух разных $r_1, r_2 \in \{0, \dots, k'-1\}$ выполняется $(\mu_{r_1}(x), \mu_{r_2}(x)) = \bar{e}$, где $\mu_{r_i}(x)$ — минимальный многочлен последовательности $u_0^{r_i} u_0^{(1)}$, $i = 1, 2$. Воспользуемся биномиальным представлением линейных рекуррент u_0 и $u_0^{(1)}$:

$$u_0(i) \equiv \sum_{j=0}^{m-1} (\xi \omega^i)^{q^j} \pmod{p}, \quad u_0^{(1)}(i) \equiv \sum_{j=0}^{m-1} (\xi \omega^d \omega^i)^{q^j} \pmod{p},$$

где ω — корень $\bar{F}(x)$ в поле $\bar{S}$; $\xi \in \bar{S}$; $d \in \{0, \dots, \tau-1\}$ — такое, что $x^d \equiv \bar{\Phi}^{(1)}(x) \pmod{\bar{F}(x)}$. Для любого $r \in \{0, \dots, k'-1\}$ представим ЛРП $u_0^r \otimes u_0^{(1)}$ в виде сумм биномиальных последовательностей:

$$u_0^r(i) \otimes u_0^{(1)}(i) \equiv \sum_{\substack{j_0 + \dots + j_{m-1} = r, \\ t \in \{0, \dots, m-1\}}} \frac{r!}{j_0! \dots j_{m-1}!} \xi^{\sum_{\alpha=0}^{m-1} j_\alpha q^\alpha + q^t} \omega^{q^t d} \omega^i \left(\sum_{\alpha=0}^{m-1} j_\alpha q^\alpha + q^t \right) \pmod{p}, \quad i \geq 0.$$

Отсюда следует, что $w_q \left(\sum_{\alpha=0}^{m-1} j_\alpha q^\alpha + q^t \right) = r+1$. Значит, $u_0^r \otimes u_0^{(1)}$ представляется в виде линейной комбинации биномиальных последовательностей с коэффициентами из $\bar{S}$ и корнями вида ω^t , где $t \in \{0, \dots, \tau-1\}$, $w_q(t) = r+1$. Таким образом, множества корней в поле разложения многочленов $\mu_{r_1}(x)$ и $\mu_{r_2}(x)$ не пересекаются при $r_1 \neq r_2$; значит, они взаимно просты. ■

Лемма 7. Пусть знаки последовательности u_0 представляются в виде функции след $u_0(i) \equiv \text{tr}(\xi \omega^i) \pmod{p}$, где $\xi \in \bar{S}$, $i \geq 0$. Тогда для любого $s \in \{0, \dots, q-2\}$ последовательность $u_0^s \otimes u_0^{(1)}$ над координатным множеством K представляется в виде

$$u_0^s \otimes u_0^{(1)} = l_1 \oplus l_2,$$

где $l_1, l_2 \in K^\infty$; $\mu_{l_1}(x)$ — минимальный многочлен последовательности l_1 ; $\mu_{l_2}(x)$ — минимальный многочлен последовательности l_2 ; $l_1 \equiv \text{tr}(\xi^{s+1} \omega^{i(s+1)+d}) \pmod{p}$ и $(\mu_{l_1}(x), \mu_{l_2}(x)) = \bar{e}$.

Доказательство. Из доказательства леммы 6 следует, что для любого $s \in \{0, \dots, q-2\}$ последовательность $u_0^s \otimes u_0^{(1)}$ представляется в виде

$$u_0^s(i) \otimes u_0^{(1)}(i) \equiv \sum_{\substack{j_0+\dots+j_{m-1}=s, \\ t \in \{0, \dots, m-1\}}} \frac{s!}{j_0! \dots j_{m-1}!} \xi^{\sum_{\alpha=0}^{m-1} j_\alpha q^\alpha + q^t} \omega^{q^t d} \omega^{i \left(\sum_{\alpha=0}^{m-1} j_\alpha q^\alpha + q^t \right)} \pmod{p}, \quad i \geq 0.$$

С другой стороны, период последовательности $u_0^s \otimes u_0^{(1)}$ делит $\tau_0 = q^m - 1$. Так как эта последовательность над полем K и q взаимно просто с τ_0 , то её минимальный многочлен $\mu(x)$ есть произведение попарно различных унитарных неприводимых многочленов, степени которых делят m , а сама последовательность представляется в виде суммы

$$u_0^s(i) \otimes u_0^{(1)}(i) \equiv \sum_{r \in C} \text{tr}(a_r \omega^{ri}) \pmod{p}, \quad i \geq 0, \quad (38)$$

где C — множество минимальных представителей q -циклотомических классов, на которые разбивается множество $\{0, \dots, \tau_0 - 1\}$. Слагаемое вида $a \omega^{(s+1)i}$ появляется в (38) при условии

$$q^t + j_0 + qj_1 + \dots + q^{m-1}j_{m-1} = s+1 \pmod{q^m - 1}.$$

Такое возможно тогда и только тогда, когда $t = 0$, $j_0 = s$, $j_1 = \dots = j_{m-1} = 0$. Значит, $a = \xi^{s+1} \omega^d$. ■

Индексом нелинейности ненулевого одночлена lx^t будем называть число $\text{ind } lx^t = w_p(t)$ [10]. Для нулевого многочлена индекс нелинейности положим равным $-\infty$. Индексом нелинейности $\text{ind } \psi(x)$ ненулевого многочлена $\psi(x)$ будем называть максимум индексов нелинейности его мономов. Поскольку интерполяционный многочлен произвольного координатного множества K имеет степень, не превышающую $q-1$, то

$$1 \leq \text{ind } \Psi_K(x) \leq (p-1)r.$$

Отметим, что, согласно [14], многочлен $\bar{E}(x)$ как функция над конечным полем $\bar{R}$ из q элементов может быть представлен многочленом $\tilde{E}(x)$ над этим же полем, степень которого не превышает $q-1$. Поэтому в дальнейшем считаем, что $\deg \bar{E}(x) \leq q-1$.

Получим теперь основной результат.

Теорема 2. Пусть $E(x) = \sum_{s=0}^k e_s x^s \in R[x]$, $u \in L_R(F)$ — ЛРП максимального периода, $z = E(u)$ и выполнены следующие условия:

$$\bar{E}'(x) \text{ не имеет корней в поле } \bar{R}; \quad (39)$$

$$\text{ind } \Psi_K(x) \leq p - 1; \quad (40)$$

существует такое $s \in \{0, \dots, k-1\}$, что $(s+1, q^m - 1) = 1$ и $\bar{e}_{s+1} \neq \bar{0}$.

Тогда по последовательности $z_{n-1} = \gamma_{n-1}^K(E(u))$ однозначно восстанавливается начальный отрезок $u(0), \dots, u(m-1)$.

Доказательство. Приведём конструктивный алгоритм восстановления $u(0), \dots, u(m-1)$ по z_{n-1} .

Э т а п I. Полагая в соотношении (13) $t = n-1$, находим последовательность $b_0^{(1)}$. По условию существует такое $s \in \{0, \dots, k-1\}$, что коэффициент многочлена $\bar{e}_{s+1} \neq \bar{0}$. Согласно лемме 6, ЛРП $b_0^{(1)}$ представляется в виде $b_0^{(1)} = (s+1)\bar{e}_{s+1}u_0^s \otimes u_0^{(1)} \oplus l$, причём минимальный многочлен $\mu_l(x)$ ЛРП l взаимно прост с минимальным многочленом ЛРП $u_0^s \otimes u_0^{(1)}$. Отсюда по известной последовательности $b_0^{(1)}$ однозначно восстанавливается последовательность $u_0^s \otimes u_0^{(1)}$.

Согласно лемме 7, по ЛРП $u_0^s \otimes u_0^{(1)}$ можно восстановить последовательность $\text{tr}(\xi^{s+1}\omega^d\omega^{(s+1)i})$, $i \geq 0$, а по ней ξ^{s+1} . Пользуясь тем, что $(s+1, q^m - 1) = 1$, находим величину ξ . Таким образом, последовательность u_0 восстановлена.

Э т а п II. Поскольку u_0 — ЛРП МП, то последовательность $u_0^{(1)}$ — её сдвиг, и она также является рекуррентной максимального периода с периодом $\tau_0 = q^m - 1$. Тогда существует такое $i_0 \in \mathbb{N}_0$, что $u_0^{(1)}(i_0 + j) \neq 0$ для всех $j \in \{0, \dots, m-1\}$.

Э т а п III. Из условия (40) следует, что $\text{ind } \Psi_K^*(x) \leq p-1$, т.е. $\psi_s^* \neq 0$ только при $w_p(s) \leq p-1$. Согласно лемме 5, полиномиальный коэффициент во внутренней сумме сечения (17) не равен 0 по модулю p при условии $w_p(j_1) + \dots + w_p(j_p) = w_p(s)$. Это возможно только при $j_1 = 0, j_2 = 1, \dots, j_p = 1$. Тогда в двойной сумме в (17) остаются только слагаемые вида $s! \psi_s^* \left(b_0^{(t-1)}\right)^s$.

Пользуясь тем, что для всех $t \in \{2, \dots, n-1\}$ и $j \in \{0, \dots, m-1\}$ верно $b_0^{(t)}(i_0 + j) = b_0^{(1)}(i_0 + j) = \bar{E}'(u_0(i_0 + j))u_0^{(1)}(i_0 + j) \neq 0$, так как $\bar{E}'(u_0(i_0 + j)) \neq 0$ в силу условия (39) теоремы и $u_0^{(1)}(i_0 + j) \neq 0$ по выбору i_0 , и полагая в сечении (17) последовательно $t = n-1, n-2, \dots, 2$, находим $z_s(i_0 + j)$ для всех $s \in \{1, \dots, n-2\}$ и $j \in \{0, \dots, m-1\}$. Знаки последовательности $\xi(p, t)$ и двойной суммы однозначно вычисляются по известным знакам последовательностей u_0 и $u_0^{(1)}$.

Находим $z_0 = \bar{E}(u_0)$. Таким образом, узнаем значения ЛРП z над кольцом R в тактах $i_0, i_0 + 1, \dots, i_0 + m - 1$.

Э т а п IV. Теперь для каждого $j \in \{0, \dots, m-1\}$ по известным знакам $z_t(i_0 + j)$, $t \in \{1, \dots, n-1\}$, используя результат леммы 1 и условие (39), находим знаки последовательностей $u_t(i_0 + j)$, $t \in \{1, \dots, n-1\}$.

Э т а п V. Начальный вектор $(u(0), \dots, u(m-1))$ вычисляется по известному вектору $(u(i_0), u(i_0 + 1), \dots, u(i_0 + m - 1))$ с использованием закона рекурсии. ■

Заметим, что условие $u_0^{(1)}(i_0 + j) \neq 0$ для всех $j \in \{0, \dots, m-1\}$, введённое на этапе II алгоритма, можно ослабить: для восстановления начального вектора ЛРП u достаточно найти знаки $u(i)$ в тактах $i_1, \dots, i_m$, таких, что система вычетов по модулю $\bar{F}(x)$ многочленов $x^{i_1}, \dots, x^{i_m}$ линейно независима над $\bar{R}$. Поэтому в последова-

тельности $u_0^{(1)}$ достаточно найти m ненулевых значений $u_0^{(1)}(i_j)$, $j = 0, \dots, m-1$, для которых система вычетов по модулю $\bar{F}(x)$ многочленов $x^{i_1}, \dots, x^{i_m}$ линейно независима над $\bar{R}$. При этом на этапе V начальный вектор $(u(0), \dots, u(m-1))$ вычисляется по известному вектору $(u(i_1), u(i_2), \dots, u(i_m))$ следующим образом:

$$(u(0), \dots, u(m-1)) = (u(i_1), u(i_2), \dots, u(i_m))A^{-1},$$

где $A = (S(F)^{i_1}\mathbf{e}, \dots, S(F)^{i_m}\mathbf{e})$; $S(F)$ — сопровождающая матрица многочлена $F(x)$; $\mathbf{e} = (e, 0, \dots, 0)$. Матрица A обратима в указанных условиях.

Следствие 1. Пусть $K = \Gamma(R)$, $E(x) = \sum_{s=0}^k e_s x^s \in R[x]$, $u \in L_R(F)$ — ЛРП максимального периода, $z = E(u)$ и выполнены следующие условия:

- 1) $\bar{E}'(x)$ не имеет корней в поле $\bar{R}$;
- 2) существует такое $s \in \{0, \dots, k-1\}$, что $(s+1, q^m-1) = 1$ и $\bar{e}_{s+1} \neq \bar{0}$.

Тогда по последовательности $z_{n-1} = \gamma_{n-1}^K(E(u))$ однозначно восстанавливается начальный отрезок $u(0), \dots, u(m-1)$.

Следствие 2. Пусть $R = \mathbb{Z}_{p^n}$, K — произвольное координатное множество кольца R , $E(x) = \sum_{s=0}^k e_s x^s \in R[x]$, $u \in L_R(F)$ — ЛРП максимального периода, $z = E(u)$ и выполнены следующие условия:

- 1) $\bar{E}'(x)$ не имеет корней в поле $\bar{R}$;
- 2) существует такое $s \in \{0, \dots, k-1\}$, что $(s+1, q^m-1) = 1$ и $\bar{e}_{s+1} \neq \bar{0}$.

Тогда по последовательности $z_{n-1} = \gamma_{n-1}^K(E(u))$ однозначно восстанавливается начальный отрезок $u(0), \dots, u(m-1)$.

Отметим, что при дополнительных требованиях ограничение (39) на $\bar{E}'(x)$ в условиях теоремы 2 можно ослабить.

Для любого $i \geq 0$ знак производной последовательности можно представить в виде $u_0^{(1)}(i) = \text{tr}(\xi \Phi^{(1)}(\omega) \omega^i) = \text{tr}(\xi \omega^d \omega^i)$, где $d \in \{0, \dots, \tau-1\}$. Найдём такие $d \in \{0, \dots, \tau-1\}$, при которых $\omega^d \in \bar{R}$. Очевидно, что это включение выполняется только при условии $(q^m-1) \mid d(q-1)$. Этому соотношению удовлетворяют только числа вида $d = y(1 + q + \dots + q^{m-1})$, $y \in \{1, \dots, q-1\}$. Для таких d можно воспользоваться свойством линейности функции след и представить рекурренту $u_0^{(1)}$ в виде $u_0^{(1)} = cu_0$, где c — некоторая константа из $\bar{R}$. Таким образом, верно следующее следствие.

Следствие 3. Пусть в условиях теоремы 2 для многочлена максимального периода $F(x) \in R[x]$ определено число $d \in \{0, \dots, \tau-1\}$, такое, что $\bar{\Phi}^{(1)}(x) \equiv x^d \pmod{\bar{F}(x)}$, и выполнены следующие условия:

- 1) существует такое $\bar{r} \in \bar{R}$, что $\bar{E}'(\bar{r}) \neq \bar{0}$;
- 2) d представляется в виде $d = y(1 + q + \dots + q^{m-1})$, $y \in \{1, \dots, q-1\}$;
- 3) $\text{ind } \Psi_K(x) \leq p-1$;
- 4) существует такое $s \in \{0, \dots, k-1\}$, что $(s+1, q^m-1) = 1$ и $\bar{e}_{s+1} \neq \bar{0}$.

Тогда по последовательности $z_{n-1} = \gamma_{n-1}^K(E(u))$ однозначно восстанавливается начальный отрезок $u(0), \dots, u(m-1)$.

Автор выражает благодарность Д. Н. Былкову за помощь в написании статьи и уточнении некоторых результатов.

ЛИТЕРАТУРА

1. Кузьмин А. С., Маршалко Г. Б., Нечаев А. А. Восстановление линейной рекурренты над примарным кольцом вычетов по её усложнению // Математические вопросы криптографии. 2010. Т. 1. № 2. С. 31–56.
2. Былков Д. Н. Класс усложнений линейных рекуррент над кольцом Галуа, не приводящий к потере информации // Проблемы передачи информации. 2010. Т. 46. № 3. С. 51–59.
3. Tian T. and Wen-Feng Q. Injectivity of compressing map on primitive sequences over $\mathbb{Z}/(p^e)$ // IEEE Trans. Inform. Theory. 2007. V. 53. No. 8. P. 2960–2966.
4. Xuan-Yong Z. and Wen-Feng Q. Uniqueness of the distribution of zeros of primitive level sequences over $\mathbb{Z}/(p^e)$ // Finite Fields Their Appl. 2005. V. 11. No. 1. P. 30–44.
5. Xuan-Yong Z. and Wen-Feng Q. Compression mappings on primitive sequences over $\mathbb{Z}/(p^e)$ // IEEE Trans. Inform. Theory. 2004. V. 50. No. 10. P. 2442–2448.
6. Xuan-Yong Z. and Wen-Feng Q. Further result of compressing maps on primitive sequences modulo odd prime powers // IEEE Trans. Inform. Theory. 2007. V. 53. No. 8. P. 2985–2990.
7. Нечаев А. А. Код Кердока в циклической форме // Дискретная математика. 1989. Т. 4. № 1. С. 123–139.
8. Кузьмин А. С., Нечаев А. А. Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и логика. 1995. Т. 3. № 2. С. 169–189.
9. Нечаев А. А. Цикловые типы линейных подстановок над конечными коммутативными локальными кольцами // Математич. сб. 1993. Т. 184. № 3. С. 21–56.
10. Кузьмин А. С., Нечаев А. А. Восстановление линейной рекуррентной последовательности над кольцом Галуа по её старшей координатной последовательности // Дискретная математика. 2011. Т. 23. № 2. С. 3–31.
11. Кузьмин А. С., Куракин В. Л., Нечаев А. А. Псевдослучайные и полилинейные последовательности // Труды по дискретной математике. 1997. Т. 1. С. 139–202.
12. Куракин В. Л. Функция переноса в первый разряд в кольце Галуа // Дискретная математика. 2012. Т. 24. № 2. С. 21–36.
13. Куракин В. Л. Представления над кольцом $\mathbb{Z}_{p^n}$ линейной рекуррентной последовательности максимального периода над полем $\text{GF}(p)$ // Дискретная математика. 1992. Т. 4. № 4. С. 96–116.
14. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. Т. 2. М.: Гелиос, 2003.