Math-Net.Ru

Общероссийский математический портал

Д. Н. Былков, А. А. Нечаев, Алгоритм восстановления ЛРП над кольцом $R = \mathbf{Z}_{p^n}$ по линейному усложнению ее старшей координатной последовательности, *Дискрет. матем.*, 2010, том 22, выпуск 4, 104–120

DOI: <https://doi.org/10.4213/dm1122>

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: 54.209.52.79

26 апреля 2023 г., 17:11:24

Алгоритм восстановления ЛРП над кольцом $R = \mathbb{Z}_{p^n}$ по линейному усложнению ее старшей координатной последовательности

© 2010 г. Д. Н. Былков, А. А. Нечаев

В работе рассматриваются псевдослучайные последовательности v над полем $\mathbb{Z}_p$, которые получаются умножением старшей координатной последовательности линейной рекуррентной последовательности (ЛРП) максимального периода u над кольцом $\mathbb{Z}_{p^n}$ на некоторый многочлен. Изучаются возможность и способ восстановления u по v . Приводится краткий обзор предшествующих результатов.

Работа выполнена при поддержке программой Президента Российской Федерации поддержки ведущих научных школ, проект НШ 8.2010.10.

1. Основные понятия и результаты

Будем обозначать единицу кольца $R = \mathbb{Z}_{p^n}$ через e . Пусть $F(x) \in R[x]$ — многочлен максимального периода (МП-многочлен) степени m , то есть унитарный (со старшим коэффициентом e) многочлен степени m с максимально возможным при данном m периодом $T(F) = p^{n-1}(p^m - 1)$ [2]. Обозначим через $L_R(F)$ множество всех линейных рекуррент над R с характеристическим многочленом $F(x)$, а через $L_R^*(F)$ — подмножество линейных рекуррент $u \in L_R(F)$ периода $T(u) = T(F)$, то есть линейных рекуррентных последовательностей максимального периода (МП ЛРП).

Пусть $\bar{R} = R/pR$ — поле вычетов кольца R . Для любых элемента $a \in R$, многочлена $A(x) \in R[x]$ и последовательности $u \in R^{(1)}$ через $\bar{a}$, $\bar{F}(x)$, $\bar{u}$ обозначим образы этих объектов при естественном эпиморфизме $R \rightarrow \bar{R}$. Тогда

$$L_R^*(F) = \{u \in L_R(F) : \bar{u} \neq \bar{0}\}.$$

Положим

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

Известно, что каждый элемент $a \in R$ однозначно представляется в виде

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

называемом p -ичным разложением элемента a . Будем говорить, что $\delta_s: R \rightarrow \delta(R)$, $s \in \overline{0, n-1}$, — координатные функции на кольце R . Зададим на множестве $\delta(R)$ операции $\oplus$, $\otimes$, полагая для произвольных $a, b \in \delta(R)$

$$a \oplus b = \delta_0(a + b),$$

$$a \otimes b = \delta_0(ab).$$

Алгебра $(\delta(R), \oplus, \otimes)$ есть поле из p элементов. Если не возникает двусмысленности толкования, знак $\otimes$ в формулах может опускаться.

В соответствии со сказанным выше, каждой последовательности $u \in L_R^*(F)$ можно сопоставить последовательности $u_0, \dots, u_{n-1}$ над $\delta(R)$, получающиеся из p -ичного разложения знаков последовательности u :

$$u(i) = u_0(i) + pu_1(i) + \dots + p^{n-1}u_{n-1}(i),$$

$$u_s(i) \in \overline{0, p-1}, \quad s \in \overline{0, n-1}, \quad i \geq 0. \quad (2)$$

Каждую последовательность u_{n-1} можно рассматривать как линейную рекурренту над полем $P = \delta(R)$. Эта последовательность имеет период τ_{n-1} , и по ней однозначно восстанавливается последовательность u [1, 2, 3].

Здесь решается следующая более общая задача. Пусть $g(x) \in P[x]$ — ненулевой многочлен. Можно ли восстановить последовательность u по последовательности

$$v = g(x) \otimes u_{n-1} = g(x)u_{n-1}? \quad (3)$$

Основной результат данной статьи составляет следующая теорема.

Теорема 1. Пусть $F(x) \in R[x]$ — МП-многочлен степени m и $g(x) \in P[x]$ — многочлен степени M такой, что

$$(\bar{g}(x), \bar{F}(x)) = \bar{e}. \quad (4)$$

Тогда для любой МП ЛРП $u \in L_R(F)^*$ существует алгоритм, восстанавливающий рекурренту u по последовательности v

- (а) однозначно при $p > 2$ или $p = n = 2$;
- (б) не более чем в двух вариантах при $p = 2, n > 2$.

При фиксированном p этот алгоритм использует $O(p^n m^p)$ знаков последовательности v , расположенных на отрезке длины $(p^m - 1)p^{n-1} + m$. Для его реализации требуется $O(n(p^n + M + m)t^p)$ операций поля P и $O(n(M + m^p)t)$ операций кольца R .

Этот результат является решением частного случая более общей задачи о восстановлении ЛРП $u \in L_R(F)$ по последовательности $v \in \mathbf{Z}_p^\infty$ вида

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

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

Требуется указать классы характеристических многочленов $F(x)$ и функций Ψ таких, что возможно восстановление исходной ЛРП u по последовательности v .

Первые результаты в этом направлении были опубликованы в работах [1, 3], где рассматривался случай, когда $\Psi(x_1, \dots, x_m) = \Psi(x_1)$ есть функция, зависящая только от одного знака исходной последовательности. В этом случае получены достаточные условия возможности восстановления u по v и предъявлены алгоритмы вычисления начального вектора $u[\bar{0}, m - 1]$ по последовательности v . Часть этих результатов представлена ниже.

Теорема 2 ([3]). Пусть $F(x) \in \mathbf{Z}_{p^n}[x]$ — МП многочлен степени m , $u \in L_R(F)^*$ — МП ЛРП. Тогда начальный вектор ЛРП u однозначно восстанавливается по отрезку последовательности u_{n-1} длины $N = (p^m - 1)p^{n-1}$ со сложностью $O(mp^n)$ операций поля P .

Несколько позже появилась серия зарубежных публикаций [6, 7, 8, 9]. В этих работах также рассматривается случай $\Psi(x_1, \dots, x_m) = \Psi(x_1)$ и доказывается лишь принципиальная возможность восстановления исходной ЛРП, без предъявления алгоритмов восстановления. Кроме того, в этих работах накладываются весьма существенные ограничения как на выбор характеристического многочлена, так и на выбор функции усложнения.

Значительную часть этих результатов обобщает следующая теорема.

Теорема 3. Пусть $p > 2$, $F(x) \in \mathbf{Z}_{p^n}[x]$ — МП многочлен, $u \in L_R(F)^*$ — МП ЛРП. Пусть также функция

$$\psi(x_0, \dots, x_{n-1}) = x_{n-1}^k \oplus c_{k-1}x_{n-1}^{k-1} \oplus \psi'(x_0, \dots, x_{n-1})$$

удовлетворяет следующим условиям.

- (1) Если $k = 1$, то функция $\psi'(x_0, \dots, x_{n-1})$ не зависит от переменной x_{n-1} и

$$\deg \psi'_{x_{n-2}} \leq p - 2.$$

- (2) Если $k > 1$, то $\deg \psi'_{x_{n-1}} \leq k - 2$ и выполняется хотя бы одно из условий

(а) k нечетно, $n \geq 4$,

(б) $2c_{k-1} \neq k$.

(в) $(k, p - 1) = 1$.

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

В дальнейшем мы будем свободно пользоваться тем, что изоморфизм полей $(P, \oplus, \otimes) \rightarrow (\bar{R}, +, \cdot)$ задается соответствием $a \rightarrow \bar{a}$, а также тем, что координатное множество P можно рассматривать как $\bar{R}$ -алгебру, если определить умножение элементов множества P на элементы множества $\bar{R}$ условием

$$\forall r \in R, \quad a \in P: \quad \bar{r}a = \delta_0(ra). \quad (6)$$

При этом очевидным образом определяется умножение любой последовательности над полем P на многочлен из $\bar{R}[x]$ и, в частности, последовательность (3) можно представить в виде

$$v = \bar{g}(x)u_{n-1}. \quad (7)$$

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

2. Некоторые свойства МП-рекуррент

Многочлен $F(x)$ имеет корень θ в расширении Галуа $S = GR(q^n, p^n)$, $q = p^m$, кольца R (см. [2]). Кольцо S содержит подмножество

$$\Gamma(S) = Q = \{\alpha \in S : \alpha^q = \alpha\},$$

называемое координатным множеством Тейхмюллера, и любой элемент $\xi \in S$ однозначно представляется в виде суммы

$$\xi = \xi_0 + p\xi_1 + \dots + p^{n-1}\xi_{n-1}, \quad \xi_s = \gamma_s(\xi) \in \gamma(S). \quad (8)$$

Алгебра $(Q, \oplus, \otimes)$ с операциями, определяемыми условиями

$$\forall \alpha, \beta \in Q \quad \alpha \oplus \beta = \gamma_0(\alpha + \beta), \quad \alpha \otimes \beta = \gamma_0(\alpha\beta) \quad (9)$$

есть поле, содержащее в качестве подполя поле $(\gamma(R), \oplus, \otimes)$.

Пусть

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

— функция след из S в R ;

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

— функция след из Q в $\gamma(R)$.

Теорема 4 ([2, 10]). Для любой ЛРП $u \in L_R(F)$ существует единственная константа $\xi \in S$ такая, что

$$u(i) = \text{Tr}_R^S(\xi \theta^i), \quad i \geq 0. \quad (10)$$

Семейство $L_R(F)$ есть в точности множество всех последовательностей вида (10). При условии (10) и есть МП ЛРП тогда и только тогда, когда $\xi_0 = \gamma_0(\xi) \neq 0$.

При этом справедливы следующие соотношения:

$$u_0(i) \stackrel{p}{\equiv} \text{tr}(\xi_0 \omega^i), \quad \omega = \theta_0 = \gamma_0(\theta), \quad (11)$$

если $p = 2$, то

$$u_1(i) \stackrel{2}{\equiv} \text{tr}(\xi_1 \omega^i) + i \text{tr}(\xi_0 \nu \omega^i) + \kappa(\xi_0 \omega^i), \quad (12)$$

где

$$\nu = \theta_0^{-1} \theta_1, \quad \kappa(x) = \sum_{0 \leq s < t \leq m-1} \bigoplus x^{2^s + 2^t}.$$

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

Лемма 1 ([4]). Для $t \in \overline{0, n-1}$ верны следующие соотношения:

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

если $p = 2$, то

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

если $p > 2$, то

$$\Phi_{t+1}(x) \stackrel{p^t}{\equiv} \Phi_t(x), \quad t \geq 1. \quad (13)$$

Последовательность $u^{(s)} = \Phi_s(x)u$, $s \in \overline{1, n-1}$, называется s -й производной последовательностью ЛРП u . Заметим, что из (13) многочлен Φ_s однозначно определяется лишь по модулю p^{n-s} , и лишь по этому модулю однозначно определяется последовательность $u^{(s)}$. Для удобства будем считать, что многочлен $\Phi_s \in R[x]$ каким либо образом выбран и зафиксирован, и соответственно выбрана ЛРП $u^{(s)}$.

Положим $\mu^{(s)} = \Phi_s(\theta)$. Из соотношений (13) и теоремы 4 следуют равенства

$$u^{(s)}(i) = \text{Tr}(\xi \mu^{(s)} \theta^i), \quad (14)$$

$$u_0^{(t)} = u_0^{(2)}, \quad t \geq 2; \quad u_1^{(t)} = u_1^{(3)}, \quad t \geq 3; \quad (15)$$

$$\mu_0^{(2)} = \mu_0^{(1)} \oplus \mu_0^{(1)2}, \quad \mu_1^{(t)} = \mu_1^{(3)}, \quad t \geq 3. \quad (16)$$

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

$$u_{s,t} = (x^{\tau_0} - \bar{e})^{p^{s-1}-p^t} u_s. \quad (17)$$

Лемма 2 ([4]). *Верны следующие соотношения:*

$$(x^{\tau_{s-1}} - \bar{e})u_s = u_0^{(s)}, \quad s \geq 1, \quad (18)$$

если $R = \mathbf{Z}_{2^n}$, то

$$(x^{\tau_{s-2}} - \bar{e})u_s = u_1^{(s-1)} \oplus u_{s-1}u_0^{(s-1)}, \quad s \geq 2. \quad (19)$$

если $R = \mathbf{Z}_{2^n}$ и $t \geq 1$, то

$$u_{s,t} = \begin{cases} u_0^{(2)}u_{t+1} \oplus u_1^{(t+1)}, & s = t+2, \\ u_0^{(2)}(u_{t+1} \oplus u_1^{(t+1)}), & s > t+2, \end{cases} \quad (20)$$

$$u_{s,0} = \begin{cases} u_0^{(1)}u_1 \oplus u_1^{(1)}, & s = 2, \\ u_0^{(2)}(u_0^{(1)}u_1 \oplus u_1^{(1)}) \oplus \bar{\Phi}_1(x)u_0^{(2)}, & s = 3, \\ u_0^{(2)}(u_0^{(1)}u_1 \oplus u_1^{(1)} \oplus \bar{\Phi}_1(x)u_0^{(2)}), & s > 4. \end{cases} \quad (21)$$

Если $R = \mathbf{Z}_{p^n}$, $p \geq 3$, то

$$(x^{\tau_0/2} \ominus e) \otimes u_1 \stackrel{p}{\equiv} \ominus u_0^{p-1} \ominus \frac{1}{2}u_0^{(1)} \quad (22)$$

и для $s \geq 2$, $t \in \overline{0, s-2}$

$$u_{s,t} = (u_0^{(1)})^{p-1} \otimes u_{t+1} \oplus \frac{1}{2}((u_0^{(1)})^{p-1} \ominus u_0^{(1)}) \oplus z_{s,t}, \quad (23)$$

где

$$z_{s,t} = \begin{cases} (u_0^{(1)})^{p-1} \otimes (\bar{\Phi}_1(x)^2 \otimes u_0), & p = 3, t = 0, s > 2, \\ (\bar{\Phi}_1(x))^2 \otimes u_0, & p = 3, t = 0, s = 2; \\ 0 & \text{в противном случае.} \end{cases} \quad (24)$$

Лемма 3. Пусть выполнены условия теоремы 4, тогда t -й разряд p -ичного разложения ЛРП u может быть представлен в виде

$$u_t(i) \equiv \text{tr}_{\gamma(R)}^Q(\xi_t w^i) + h_t(\xi_0, \dots, \xi_{t-1}, i), \quad (25)$$

где

$$w = \gamma_0(\theta), \quad \xi_s = \gamma_s(\xi), \quad s \in \overline{0, t},$$

и h_t — некоторое отображение $Q^t \times \mathbf{N}_0$ в Q .

Доказательство. Верно сравнение

$$u(i) \stackrel{p^{t+1}}{\equiv} \sum_{j=0}^t u_j(i) p^j.$$

Найдем представление знака ЛРП $u \pmod{p^{t+1}}$ при помощи функции след:

$$\begin{aligned} u(i) \stackrel{p^{t+1}}{\equiv} \text{Tr}(\xi \theta^i) \stackrel{p^{t+1}}{\equiv} \text{Tr} \left(\sum_{j=0}^t \xi_j p^j \sum_{s=0}^t \gamma_s(\theta^i) p^s \right) \\ \stackrel{p^{t+1}}{\equiv} p^t \text{Tr}(\xi_t w^i) + p^t \text{Tr} \left(\sum_{j=0}^{t-1} \xi_j \gamma_{t-j}(\theta^i) \right) + \text{Tr} \left(\sum_{k=0}^{t-1} p^k \sum_{j=0}^k \xi_j \gamma_{k-j}(\theta^i) \right). \end{aligned}$$

Отсюда, с учетом соотношения $\text{Tr}_R^S(x) \equiv \text{tr}(x)$ для $x \in \gamma(R)$, получаем (25), где

$$h_t(\xi_0, \dots, \xi_{t-1}, i) = \sum_{j=0}^{t-1} \text{tr}(\xi_j \gamma_{t-j}(\theta^i)) \oplus \gamma_t \left(\text{Tr} \left(\sum_{k=0}^{t-1} p^k \sum_{j=0}^k \xi_j \gamma_{k-j}(\theta^i) \right) \right). \quad (26)$$

3. Восстановление ЛРП u по последовательности v

Доказательство теоремы 1 состоит в поэтапном восстановлении разрядов ЛРП u , что равносильно последовательному восстановлению коэффициентов $\xi_0, \dots, \xi_{n-1}$ в разложении (8) коэффициента ξ из (10).

Заметим, что если для некоторых $j \leq n-1$ и $r < n-1$ удалось восстановить последовательность $u^{(r)} \pmod{p^j}$, то по ней легко восстанавливается последовательность $u \pmod{p^j}$, и наоборот. Достаточно при условии (13) выбрать многочлен $\Phi^{(r)}(x)$ так, что

$$\Phi^{(r)}(x) \Phi_r(x) \equiv e \pmod{F(x)}. \quad (27)$$

Тогда

$$u \equiv \Phi^{(r)}(x) u^{(r)} \pmod{p^j}. \quad (28)$$

3.1. Однозначное восстановление последовательности u_0

Предложение 1. Последовательность u_0 однозначно вычисляется по последовательности v .

Доказательство. Из (18) получаем, что

$$(x^{\tau_{n-2}} - \bar{e})u_{n-1} = u_0^{(n-2)}.$$

Умножая обе части этого равенства на известный многочлен $\bar{\Phi}^{(n-2)}(x)$ и учитывая (28), получаем равенства

$$u_0 = \bar{\Phi}^{(n-2)}(x)u_0^{(n-2)} = \bar{\Phi}^{(n-2)}(x)(x^{\tau_{n-2}} - \bar{e})u_{n-1}.$$

Умножая обе части получившегося равенства на известный многочлен $g(x)$ и используя (7), получаем равенство

$$\bar{g}(x)u_0 = \bar{\Phi}^{(n-2)}(x)(x^{\tau_{n-2}} - \bar{e})v. \quad (29)$$

Так как согласно (11) u_0 есть ЛРП над полем $\bar{R}$ с минимальным многочленом $\bar{F}(x)$ и выполняется условие (4), то по известной из (29) последовательности $\bar{g}(x)u_0$ можно однозначно найти последовательность u_0 , а значит и элемент ξ_0 из (11).

3.2. Однозначное восстановление u_{n-1} по известным последовательностям $v, u_0, \dots, u_{n-2}$

Предложение 2. По известным последовательностям $u_0, \dots, u_{n-2}$ и v ЛРП u_{n-1} восстанавливается однозначно.

Доказательство. Пусть

$$F(x) = x^m - f_{m-1}x^{m-1} - \dots - f_0,$$

тогда

$$u_{n-1}(i+m) = \sum_{j=0}^{m-1} \bar{f}_j u_{n-1}(i+j) \oplus \lambda(i), \quad (30)$$

где знаки $\lambda(i)$ находятся однозначно по известным последовательностям $u_0, \dots, u_{n-2}$ из равенства

$$\lambda(i) = \delta_{n-1} \left(\sum_{s=0}^{m-1} f_s \sum_{t=0}^{n-2} 2^t u_t(i+s) \right).$$

Из (30) следует, что

$$\bar{F}(x)u_{n-1} = \lambda.$$

Так как $\bar{g}(x)$ и $\bar{F}(x)$ взаимно просты, существуют многочлены $\bar{h}(x), \bar{b}(x)$ такие, что

$$\bar{h}(x)\bar{g}(x) = e + \bar{b}(x)\bar{F}(x).$$

Отсюда следует, что

$$\bar{h}(x)v = \bar{h}(x)\bar{g}(x)u_{n-1} = u_{n-1} \oplus \bar{b}(x)\lambda.$$

Следовательно,

$$u_{n-1} = \bar{h}(x)v \ominus \bar{b}(x)\lambda.$$

3.3. Восстановление промежуточных последовательностей

Дальнейшее изложение разбивается на две части: случай $p > 2$ и $p = 2$.

3.3.1. Восстановление последовательностей $u_1, \dots, u_{n-2}$ по u_0 и v в случае $p > 2$

Предложение 3. Пусть $p > 2$, $t \geq 0$, тогда по последовательностям $u_0, \dots, u_t$ и v однозначно вычисляется ЛРП u_{t+1} .

Доказательство. По условию, известна последовательность $u \pmod{p^{t+1}}$, а значит, и коэффициент $\xi \pmod{p^{t+1}}$. Из леммы 3 следует, что последовательность u_{t+1} определяется значениями $\xi_0, \dots, \xi_{t+1}$. Покажем, что по известным значениям $\xi_0, \dots, \xi_t$ и последовательности v можно определить величину ξ_{t+1} , а значит, и последовательность u_{t+1} .

Вычислим

$$v' = (x^{\tau_0} - \bar{e})p^{n-2-p^t}v.$$

Тогда, согласно (17),

$$v' = (x^{\tau_0} - \bar{e})p^{n-2-p^t} \bar{g}(x)u_{n-1} = \bar{g}(x)u_{n-1,t}. \quad (31)$$

Подставляя сюда вместо $u_{n-1,t}$ правую часть выражения (23) (при $s = n-1$) и вычитая из получившегося выражения для v' известные последовательности, зависящие только от u_0 , получаем последовательность

$$v'' = \bar{g}(x)((u_0^{(1)})^{p-1}u_{t+1}).$$

Из леммы 3 следует, что i -й знак последовательности u_{t+1} представляется в виде (25):

$$u_{t+1}(i) \stackrel{p}{\equiv} \text{tr}(\xi_{t+1}w^i) + h_{t+1}(\xi_0, \dots, \xi_t, i).$$

Вычитая из v'' известную, по условию леммы, последовательность $g(x) \otimes (u_0^{(1)})^{p-1} \otimes h_{t+1}$, зависящую только от $\xi_0, \dots, \xi_t$, получаем последовательность

$$y = \bar{g}(x)((u_0^{(1)})^{p-1} \otimes z), \quad (32)$$

где последовательность $z \in L_P(\bar{F})$ удовлетворяет условию

$$z(i) \stackrel{p}{\equiv} \text{tr}(\xi_{t+1}w^i). \quad (33)$$

Нашей задачей является вычисление коэффициента ξ_{t+1} , что, очевидно, равносильно вычислению последовательности z . Так как последовательности z и $u_0^{(1)}$ суть МП рекурренты с характеристическим многочленом $\bar{F}(x)$, то найдется число $k \in \mathbb{N}_0$ такое, что $z = x^k u_0^{(1)}$.

Заметим, что согласно (14)

$$u_0^{(1)}(i) = \text{tr}(\mu_0^{(1)}\xi_0 w^i),$$

а значит,

$$z(i) = \text{tr}(\mu_0^{(1)}\xi_0 w^k w^i) \quad (34)$$

и, согласно (33),

$$\xi_{t+1} = \mu_0^{(1)} \xi_0 w^k.$$

Таким образом, задача вычисления коэффициента ξ_{t+1} сводится в задаче нахождения значения w^k в (34). Нам потребуется следующее утверждение.

Лемма 4. Пусть $l \in L_P(\bar{F})^*$, $l(i) \equiv \text{tr}(aw^i)$, где $a \in \gamma(S) \setminus \{0\}$. Тогда для любого $k \in \mathbf{N}_0$ последовательность $l^{p^{-1}}(x^k l)$ представляется в виде

$$l^{p^{-1}}(x^k l) = l' \oplus l'',$$

где $l'(i) = \text{tr}(a^p w^k w^{pi})$, $a l''$ есть ЛРП, минимальный многочлен которой взаимно прост с $\bar{F}(x)$.

Доказательство. Знаки ЛРП l описываются равенствами

$$l(i) = \text{tr}(aw^i) = \sum_{j=0}^{m-1} (aw^i)^{p^j}.$$

Возведем последнее равенство в степень $p-1$:

$$l(i)^{p-1} = \sum_{\substack{s_0 + \dots + s_{m-1} = p-1 \\ s_0, \dots, s_{m-1} \in \mathbf{0}, p-1}} \frac{(p-1)!}{s_0! \dots s_{m-1}!} (aw^i)^{s_0 + ps_1 + \dots + p^{m-1}s_{m-1}}.$$

Тогда i -й знак последовательности $l^{p^{-1}}(x^k l)$ имеет вид

$$\sum_{\substack{j \in \mathbf{0}, m-1 \\ s_0 + \dots + s_{m-1} = p-1 \\ s_0, \dots, s_{m-1} \in \mathbf{0}, p-1}} \frac{(p-1)!}{s_0! \dots s_{m-1}!} (aw^k w^i)^{p^j} (aw^i)^{s_0 + ps_1 + \dots + p^{m-1}s_{m-1}} \quad (35)$$

Период последовательности $l^{p^{-1}}(x^k l)$, очевидно, делит $\tau_0 = p^m - 1$, и так как это — последовательность над полем из p элементов, то ее минимальный многочлен над полем P есть некоторое произведение попарно различных унитарных неприводимых многочленов, степени которых делят m , а сама последовательность представляется в виде суммы

$$(l^{p^{-1}}(x^k l))(i) = \sum_{t \in C} \text{tr}(b_t \omega^{ti}), \quad (36)$$

где C — множество минимальных представителей p -циклотомических классов, на которые разбивается множество $\overline{0, p^m - 2}$. Слагаемые вида $b w^i$ появляются в (35) в точности при условии, что

$$s_0 + ps_1 + \dots + p^j(s_j + 1) + \dots + p^{m-1}s_{m-1} \equiv^{p^{m-1}} 1.$$

Последнее условие выполняется тогда и только тогда, когда

$$j = m-1, s_0 = \dots = s_{m-2} = 0, s_{m-1} = p-1,$$

следовательно,

$$b_1 = a^{p^m} (w^k)^{p^{m-1}} = a(w^k)^{p^{m-1}}.$$

Отсюда и из свойства функции след $\text{tr}(x^p) = \text{tr}(x)$ получаем утверждение леммы.

Вернемся к равенству (32). Применяя лемму 4 к последовательностям $u_0^{(1)}$ и z получаем равенство

$$(u_0^{(1)})^{p-1} \otimes z = l' \oplus l'',$$

где $l'(i) = \text{tr}((\mu_0^{(1)} \xi_0)^p w^k w^{ip})$, а l'' есть ЛРП, минимальный многочлен которой взаимно прост с $\bar{F}(x)$. Следовательно,

$$\begin{aligned} y(i) &= (\bar{g}(x)l' \oplus \bar{g}(x)l'')(i) \\ &= \text{tr}((\mu_0^{(1)} \xi_0)^p w^k g(w^p) w^{pi}) \oplus (\bar{g}(x)l'')(i). \end{aligned}$$

В силу выбора последовательностей l' и l'' , из последовательности y можно найти последовательность $\bar{g}(x)l'$. Так как $g(w^p) \neq 0$, то $\bar{g}(x)l' \neq 0$ и по этой последовательности можно вычислить w^k , то есть найти u_{t+1} . Предложение 3 доказано.

3.3.2. Восстановление двух вариантов последовательности u_1 по u_0 и v в двоичном случае

Заметим, что если $p = n = 2$, то последовательность $u_1 = u_{n-1}$ восстанавливается однозначно по предложению 2.

Предложение 4. Если $p = 2$, $n \geq 2$, то последовательность u_1 вычисляется по последовательности v не более чем в двух вариантах.

Доказательство. В связи со сказанным выше можно считать, что нам известны последовательность v , многочлен $g(x)$ и последовательность u_0 , то есть коэффициент ξ_0 . В таком случае можно вычислить последовательность

$$v' = (x^{\tau_0} - \bar{e})^{2^{n-2}-1} v,$$

которая по определению имеет вид

$$v' = \bar{g}(x)u_{n-1,0},$$

где последовательность $u_{n-1,0}$ описывается соотношениями (21) (при $s = n - 1$). Рассмотрим два случая.

Пусть $n = 3$. Тогда, согласно (21),

$$u_{n-1,0} = u_{2,0} = u_0^{(1)}u_1 \oplus u_1^{(1)}.$$

Отсюда, пользуясь соотношениями (11), (12), (14), получаем, что

$$\begin{aligned} u_{2,0} &= \text{tr}(\mu_0^{(1)} \xi_0 \omega^i) (\text{tr}(\xi_1 \omega^i) \oplus i \text{tr}(\xi_0 v \omega^i) \oplus \kappa(\xi_0 \omega^i)) \\ &\quad \oplus \text{tr}(\gamma_1 (\xi \mu^{(1)}) \omega^i) \oplus i \text{tr}(\gamma_0 (\xi \mu^{(1)}) v \omega^i) \oplus \kappa(\gamma_0 (\xi \mu^{(1)}) \omega^i). \end{aligned} \quad (37)$$

Заметим, что

$$\text{tr}(\gamma_1 (\xi \mu^{(1)}) \omega^i) = \text{tr}((\xi_1 \mu_0^{(1)}) \omega^i) \oplus \text{tr}((\xi_0 \mu_1^{(1)}) \omega^i). \quad (38)$$

Теперь нетрудно видеть, что

$$u_{2,0} = u'_{2,0} \oplus u''_{2,0},$$

где

$$u'_{2,0}(i) = \text{tr}(\mu_0^{(1)} \xi_0 \omega^i) \text{tr}(\xi_1 \omega^i) \oplus \text{tr}((\xi_1 \mu_0^{(1)}) \omega^i) \quad (39)$$

и $u''_{2,0}$ — сумма тех слагаемых из разложения (37)–(38), которые определяются известными константами $\xi_0, \mu^{(1)}, v$, то есть известная последовательность.

Вычитая из известной последовательности v' известную последовательность $\bar{g}(x)u''_{2,0}$, находим последовательность

$$v'' = \bar{g}(x)u'_{2,0}. \quad (40)$$

Далее в этом доказательстве потребуется следующее утверждение.

Лемма 5. *Последовательность (39) есть сумма последовательностей*

$$u'_{2,0} = y \oplus z, \quad (41)$$

где y — ЛРП над P с характеристическим многочленом $\bar{F}(x)$ вида

$$y = \text{tr}(h(\xi_1)\omega^i), \quad h(\xi_1) = (\mu_0^{(1)} \xi_1 \xi_0)^{2^{m-1}} \oplus \mu_0^{(1)} \xi_1; \quad (42)$$

z — ЛРП над P , характеристический многочлен которой в $\bar{R}[x]$ взаимно прост с $\bar{F}(x)$.

Доказательство. Период последовательности (39), очевидно, делит $\tau_0 = 2^m - 1$, и так как это — последовательность над полем из 2-х элементов, ее минимальный многочлен над полем $\bar{R}$ есть некоторое произведение попарно различных унитарных неприводимых многочленов, степени которых делят m , а сама последовательность представляется в виде суммы

$$u'_{2,0}(i) = \sum_{k \in C} \text{tr}(h_k \omega^{ki}), \quad (43)$$

где C — множество минимальных представителей 2-циклотомических классов, на которые разбивается множество $\overline{0, 2^m - 2}$. Очевидно, остается показать, что коэффициент h_1 из (43) равен $h(\xi_1)$.

Для этого достаточно показать, что в разложении последовательности $u'_{2,0}$ в сумму биномиальных последовательностей коэффициент при последовательности ω^i равен $h(\xi_1)$. Из (39) следует, что

$$u'_{2,0}(i) = \sum_{r_0, r_1 \in \overline{0, m-1}} (\mu_0^{(1)} \xi_0)^{2^{r_0}} (\xi_1)^{2^{r_1}} \omega^{(2^{r_0} + 2^{r_1})i} \oplus \sum_{r \in \overline{0, m-1}} (\mu_0^{(1)} \xi_1)^{2^r} \omega^{2^r i} \quad (44)$$

Нетрудно видеть, что после приведения подобных членов в правой части последнего равенства коэффициент h_1 при ω^i есть сумма коэффициентов, соответствующих значениям $(r_0, r_1) = (m-1, m-1)$, $r = 0$. Отсюда следует, что $h_1 = h(\xi_1)$.

Заметим теперь, что известная ЛРП v' однозначно представляется в виде суммы

$$v''(i) = \text{tr}(\eta \omega^i) \oplus z'(i), \quad (45)$$

где z' — ЛРП, минимальный многочлен которой взаимно прост с $\bar{F}$. При этом из (40) и леммы 5 следуют равенства

$$g(x)z = z', \quad (g(x)y)(i) = \text{tr}(\eta \omega^i).$$

Из последнего в силу (42) вытекает уравнение относительно ξ_1 :

$$h(\xi_1)g(\omega) = \eta. \quad (46)$$

Возводя обе части этого уравнения в квадрат, получаем равносильное уравнение

$$(\mu_0^{(1)}\xi_1)^2 \oplus \mu_0^{(1)}\xi_0\xi_1 = \alpha,$$

где $\alpha = (\eta g(\omega)^{-1})^2$, нормируя которое, получаем уравнение

$$\xi_1^2 \oplus \beta_1\xi_1 \oplus \beta_2 = 0, \quad \beta_1 = (\mu_0^{(1)})^{-1}\xi_0, \quad \beta_2 = (\eta g(\omega)^{-1}(\mu_0^{(1)})^{-1})^2. \quad (47)$$

Это уравнение разрешимо, так как разрешимо уравнение (46), и имеет два решения, так как $\beta_1 \neq 0$. Отсюда следует предложение 4 в рассматриваемом случае.

Рассмотрим теперь второй случай, пусть $n \geq 4$. В этом случае, вычитая из известной последовательности v известные последовательности $\bar{g}(x)\bar{\Phi}_1(x)u_0^{(2)}$ при $n = 4$ и $(\bar{g}(x)u_0^{(2)})(\bar{\Phi}_1(x)u_0^{(2)})$ при $n \geq 5$, согласно (21) получаем последовательность

$$v' = \bar{g}(x)u_{n-1,0}^*, \quad u_{n-1,0}^* = u_0^{(2)}(u_0^{(1)}u_1 \oplus u_1^{(1)}).$$

Отсюда, пользуясь соотношениями (11), (12), (14), получаем равенство

$$\begin{aligned} u_{n-1,0}^*(i) = & \operatorname{tr}(\mu_0^{(2)}\xi_0\omega^i) \operatorname{tr}(\mu_0^{(1)}\xi_0\omega^i)(\operatorname{tr}(\xi_1\omega^i) \oplus i \operatorname{tr}(\xi_0v\omega^i) \oplus \kappa(\xi_0\omega^i)) \\ & \oplus \operatorname{tr}(\mu_0^{(2)}\xi_0\omega^i)(\operatorname{tr}(\gamma_1(\xi\mu^{(1)})\omega^i) \oplus i \operatorname{tr}(\gamma_0(\xi\mu^{(1)})v\omega^i) \oplus \kappa(\gamma_0(\xi\mu^{(1)})\omega^i)). \end{aligned} \quad (48)$$

Теперь, пользуясь (38), нетрудно увидеть, что

$$u_{n-1,0}^* = u'_{n-1,0} \oplus u''_{n-1,0},$$

где

$$u'_{n-1,0}(i) = \operatorname{tr}(\mu_0^{(2)}\xi_0\omega^i) \operatorname{tr}(\mu_0^{(1)}\xi_0\omega^i) \operatorname{tr}(\xi_1\omega^i) \oplus \operatorname{tr}(\mu_0^{(2)}\xi_0\omega^i) \operatorname{tr}((\xi_1\mu_0^{(1)})\omega^i), \quad (49)$$

$u''_{n-1,0}$ — сумма тех слагаемых из разложения (48), которые определяются известными константами $\xi_0, \mu^{(1)}, \mu^{(2)}, v$, то есть известная последовательность.

Вычитая теперь из известной последовательности v' известную последовательность $\bar{g}(x)u''_{n-1,0}$, находим последовательность

$$v'' = \bar{g}(x)u'_{n-1,0}. \quad (50)$$

Для завершения доказательства предложения 4 докажем следующее утверждение.

Лемма 6. Последовательность (49) есть сумма последовательностей

$$u'_{n-1,0} = y + z, \quad (51)$$

где y — ЛРП над P с характеристическим многочленом $\bar{F}(x)$ вида

$$y = \operatorname{tr}(f(\xi_1)\omega^i), \quad (52)$$

где

$$f(\xi_1) = (\mu_0^{(2)}\mu_0^{(1)}\xi_0^2(\xi_1^2 \oplus (\mu_0^{(2)} \oplus \mu_0^{(1)})\xi_0\xi_1 \oplus \mu_0^{(2)}\mu_0^{(1)}\xi_1^2))^{2^{m-2}}, \quad (53)$$

z — ЛРП над P , характеристический многочлен которой в $\bar{R}[x]$ взаимно прост с $\bar{F}(x)$.

Доказательство. Как и при доказательстве леммы 5, получаем, что исследуемая последовательность представляется в виде суммы

$$u'_{n-1,0}(i) = \sum_{k \in C} \text{tr}(f_k \omega^{ki}), \quad (54)$$

где C — множество минимальных представителей 2-циклотомических классов, на которые разбивается множество $\overline{0, 2^m - 2}$. Остается показать, что коэффициент f_1 из (54) равен $f(\xi_1)$.

Для этого достаточно показать, что в разложении последовательности $u'_{n-1,0}$ в сумму биномиальных последовательностей коэффициент при последовательности ω^i равен $f(\xi_1)$. Из (49) следует, что

$$u'_{n-1,0}(i) = \sum_{r_0, r_1, r_2 \in \overline{0, m-1}} (\mu_0^{(2)} \xi_0)^{2^{r_0}} (\mu_0^{(1)} \xi_0)^{2^{r_1}} (\xi_1)^{2^{r_2}} \omega^{(2^{r_0} + 2^{r_1} + 2^{r_2})i} \oplus \sum_{s_0, s_1 \in \overline{0, m-1}} (\mu_0^{(2)} \xi_0)^{2^{s_0}} (\mu_0^{(1)} \xi_1)^{2^{s_1}} \omega^{(2^{s_0} + 2^{s_1})i}. \quad (55)$$

Нетрудно видеть, что после приведения подобных членов в правой части последнего равенства коэффициент f_1 при ω^i есть сумма коэффициентов, соответствующих значениям $(r_0, r_1, r_2) \in \{(m-1, m-2, m-2), (m-2, m-1, m-2), (m-2, m-2, m-1)\}$, $(s_0, s_1) = (m-1, m-1)$. Отсюда $f_1 = f(\xi_1)$.

Теперь, как и в случае $n = 3$, представляя известную ЛРП v'' в виде суммы (45), из (50) и леммы 6 получаем равенства

$$\begin{aligned} g(x)z &= z', \\ (g(x)y)(i) &= \text{tr}(\eta \omega^i). \end{aligned}$$

Из последних равенств ввиду (52) вытекает уравнение относительно ξ_1

$$f(\xi_1)g(\omega) = \eta. \quad (56)$$

Возводя обе части этого уравнения в квадрат и нормируя его, получаем равносильное уравнение

$$(e \oplus \mu_0^{(2)} \mu_0^{(1)}) \xi_1^2 \oplus \beta_1 \xi_1 \oplus \beta_2 = 0, \quad \beta_1 = (\mu_0^{(1)} \oplus \mu_0^{(2)}) \xi_0. \quad (57)$$

Это уравнение разрешимо, так как разрешимо уравнение (56), и имеет не более двух решений, так как $\beta_1 \neq 0$, поскольку $\mu_0^{(1)} \neq 0$ и ввиду (15) $\mu_0^{(1)} \neq \mu_0^{(2)}$. Отсюда следует предложение 4 в случае $n \geq 4$.

Замечание 1. Неоднозначность восстановления последовательности u_1 в двоичном случае, в отличие от случая $p > 2$, объясняется тем, что при $p = 2$ выражения для $u_{s,t}$ существенно отличаются в случаях $t = 0$ и $t > 0$. Поэтому при $t = 0$ нельзя получить простой вид формулы (32), вместо нее приходится пользоваться формулами (44) и (55).

3.3.3. Однозначное восстановление последовательностей $u_2, \dots, u_{n-2}$ по u_0, u_1 и v в двоичном случае

Предложение 5. Пусть $R = \mathbb{Z}_{2^n}$, $t \geq 1$, тогда по последовательностям $u_0, u_1, \dots, u_t, v$ однозначно вычисляется ЛРП u_{t+1} .

Доказательство. Доказательство в значительной части повторяет доказательство предложения 3. Как и там, достаточно показать, что по известным значениям $\xi_0, \dots, \xi_t$ и последовательности v можно определить величину ξ_{t+1} , а значит и последовательность u_{t+1} .

Вычислим

$$v' = (x^{\tau_0} - \bar{e})^{2^{n-2}-2^t} v.$$

Тогда, согласно (17),

$$v' = (x^{\tau_0} - \bar{e})^{2^{n-2}-2^t} \bar{g}(x)u_{n-1} = \bar{g}(x)u_{n-1,t}.$$

Подставляя сюда вместо $u_{n-1,t}$ правую часть выражения (20) (при $s = n-1$) и вычитая из получившегося выражения для v' известные последовательности, зависящие только от u_0 и u_1 , получаем последовательность

$$v'' = \bar{g}(x)(u_0^{(2)}u_{t+1}).$$

Из леммы 3 следует, что i -й знак последовательности u_{t+1} представляется в виде (25)

$$u_{t+1}(i) \stackrel{2}{\equiv} \text{tr}(\xi_{t+1}w^i) + h_{t+1}(\xi_0, \dots, \xi_t, i).$$

Вычитая из v'' известную по условию леммы последовательность $g(x) \otimes u_0^{(2)} \otimes h_{t+1}$, зависящую только от $\xi_0, \dots, \xi_t$, получаем последовательность

$$y = \bar{g}(x)(u_0^{(2)} \otimes z), \quad (58)$$

где последовательность $z \in L_P(\bar{F})$ удовлетворяет условию

$$z(i) \stackrel{2}{\equiv} \text{tr}(\xi_{t+1}w^i). \quad (59)$$

Формулы (58) и (59) получаются соответственно из формул (32) и (33) с заменой p на 2 и $u_0^{(1)}$ на $u_0^{(2)}$, поэтому дальнейшее доказательство этого предложения почти дословно совпадает с доказательством предложения 3.

Первая часть теоремы 1 доказана.

Замечание 2. Допустим, что $u_1^{[1]}$ и $u_1^{[2]}$ — два варианта последовательности u_1 , восстановленные в соответствии с предложением 4, и $u^{[1]}, u^{[2]}$ — соответствующие им варианты последовательности u , полученные по данному алгоритму, $u^{[s]} \in L_R(F)$, $s = 1, 2$ по построению. Один из этих вариантов является истинным. Для отсева ложного варианта мы можем лишь проверить выполнение соотношений

$$g(x)u_{n-1}^{[s]} = v, \quad s = 1, 2.$$

Если одно из этих соотношений не выполняется, то мы восстанавливаем последовательность u однозначно. Мы не можем доказать последнее утверждение, однако проведенные эксперименты для $n = 3, m = 4$ показывают, что оно верно.

4. Оценка сложности алгоритма

В целях упрощения рассуждений рассмотрим случай $p > 2$, случай $p = 2$ рассматривается аналогично. Очевидно, что наибольший вклад в оценку сложности алгоритма вносит этап восстановления промежуточных последовательностей $u_1, \dots, u_{n-2}$. Как уже было сказано при доказательстве предложения 3, решение этой задачи эквивалентно вычислению коэффициентов $\xi_1, \dots, \xi_{n-2}$.

Оценим сложность нахождения коэффициента ξ_t , $t \in \overline{1, n-2}$, по уже найденным значениям $\xi_0, \dots, \xi_{t-1}$ и последовательности v . Положим

$$d = m \binom{m+p-2}{m-1}.$$

Ниже будет показано, что ранг последовательности y вида (32) не превышает d . Для того, чтобы найти коэффициент ξ_t нам потребуется вычислить d членов последовательности v' вида

$$v' = (x^{\tau_0} - \bar{e})^{p^{n-2}-p^t} v = (x^{\tau_t} - \bar{e})^{p^{n-2-t}-1} v.$$

Из последнего равенства следует, что для вычисления одного знака рекурренты v' необходимо сложить не более p^{n-t-2} знаков ЛРП v . Поэтому сложность вычисления отрезка $v'[0, d-1]$ можно оценить как $O(p^{n-t-2}d)$ операций поля P . Последовательность v'' вычисляется по формуле

$$v'' = v' - g(x) \left(\frac{1}{2}((u_0^{(1)})^{p-1} - u_0^{(1)}) + z_{s,t} \right),$$

где последовательность $z_{s,t}$ определяется по (24). Для получения отрезка $v''[0, d-1]$ необходимо вычислить $M+d$ знаков последовательности $\frac{1}{2}((u_0^{(1)})^{p-1} - u_0^{(1)}) + z_{s,t}$, зависящей только от рекурренты u_0 , и умножить ее на многочлен $g(x)$. Поэтому сложность вычисления отрезка $v''[0, d-1]$ можно оценить величиной $O(p^{n-t-2}d + Md + m(M+d))$ операций поля P . Отрезок $y[0, d-1]$ вычисляется по формуле

$$y[0, d-1] = v''[0, d-1] - (g(x)((y_0^{(1)})^{p-1} h_t)) [0, d-1].$$

Согласно равенству (26), последовательность h_t равна сумме ЛРП ранга m над полем P и t -й координатной последовательности ЛРП ранга m над кольцом R . Поэтому сложность вычисления одного знака последовательности h_t есть $O(m)$ операций поля P плюс $O(m)$ операций кольца R . Из вышесказанного следует, что сложность вычисления отрезка $y[0, d-1]$ равна $O(d(p^{n-2-t} + m + M))$ операций поля P плюс $O((d+M)m)$ операций кольца R .

Покажем теперь, что ранг ЛРП y не превосходит d и оценим сложность восстановления коэффициента ξ_t по отрезку последовательности y . Сформулируем необходимые для этого определения и факты. Пусть $M, N \in \mathbb{N}$ и

$$I(M, N) = \{(k_0, \dots, k_{M-1}) \in \mathbb{N}^M : k_0 + k_1 + \dots + k_{M-1} = N, \\ k_0, \dots, k_{M-1} \in \overline{0, p-1}\}.$$

Положим

$$\left\{ \begin{matrix} M \\ N \end{matrix} \right\} = |I(M, N)|.$$

Тогда в соответствии с [5]

$$\left\{ \begin{matrix} M \\ N \end{matrix} \right\} = \sum_{s \geq 0} (-1)^s \binom{M}{s} \binom{N + M - ps - 1}{M - 1}$$

и

$$\left\{ \begin{matrix} M \\ N \end{matrix} \right\} = 0, \quad M(p - 1) < N.$$

Согласно равенству (32), ранг последовательности y не превышает ранга рекурренты $((u_0^{(1)})^{p-1} \otimes z)$. В соответствии с разложением (35), линейная сложность последовательности $((u_0^{(1)})^{p-1} \otimes z)$ не превышает

$$m \left\{ \begin{matrix} m \\ p - 1 \end{matrix} \right\} = m \binom{m + p - 2}{m - 1} = d.$$

Домножив отрезок $y[\overline{0, d - 1}]$ на минимальный многочлен $M_{l''}(x)$ последовательности l'' , получим отрезок $(M_{l''} \bar{g}(x) l')[\overline{0, m - 1}]$. Сложность вычисления указанного отрезка оценивается величиной

$$O((\deg M_{l''}(x) - m)m) = O((d - m)m)$$

операций поля P . Так как l' есть ЛРП над полем $\bar{R}$ с минимальным многочленом $\bar{F}(x)$ и выполняются условия

$$(\bar{F}(x), \bar{g}(x)) = (\bar{F}(x), M_{l''}(x)) = e,$$

то по отрезку последовательности $(M_{l''} \bar{g}(x) l')[\overline{0, m - 1}]$ можно однозначно найти коэффициент ξ_t .

Таким образом, сложность вычисления коэффициента ξ_t есть $O(d(p^{n-2-t} + m + M))$ операций поля P и $O((d + M)m)$ операций кольца R . Заметим, что справедливо равенство

$$\binom{m + p - 2}{m - 1} = \binom{m + p - 2}{p - 1}.$$

Если p фиксировано и $m \rightarrow \infty$, то

$$\binom{m + p - 2}{p - 1} = O(m^{p-1}).$$

Отсюда следует справедливость равенства

$$O(d) = O(m^p).$$

Поэтому трудоемкость всего алгоритма восстановления оценивается величиной $O(n(p^n + M + m)m^p)$ операций поля P и $O(n(m^p + M)m)$ операций кольца R . Теорема 1 доказана.

Список литературы

1. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., Linear recurring sequences over rings and modules. *J. Math. Sci.* (1995) **76**, №6, 2793–2915.
2. Кузьмин А. С., Куракин В. Л., Нечаев А. А., Кольца Галуа в приложениях к кодам и рекуррентам. В сб.: *Труды Академии криптографии РФ*. Наука, Москва, 1998.
3. Кузьмин А. С., Нечаев А. А., Линейные рекуррентные последовательности над кольцами Галуа. *Успехи матем. наук* (1993) **48**, №1, 167–168.
4. Кузьмин А. С., Нечаев А. А., Линейные рекуррентные последовательности над кольцами Галуа. *Алгебра и логика* (1995) **34**, №2, 169–189.
5. Сачков В. Н., *Введение в комбинаторные методы дискретной математики*. МЦНМО, Москва, 2004.
6. 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.
7. 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.
8. 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.
9. Xuan-Yong Zhu, Wen-Feng Qi, Further results of compressing maps on primitive sequences over $\mathbf{Z}_{p^n}$. *Math. Comp.* (2008) **77**, 1623–1637.
10. Нечаев А. А., Код Кердока в циклической форме. *Дискретная математика* (1989) **1**, №1, 123–139.

Статья поступила 1.09.2010.

Переработанный вариант поступил 4.11.2010.