А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев, Свойства линейных и полилинейных рекуррент над кольцами Галуа (I), *Тр. по дискр. матем.*, 1998, том 2, 191–222

Труды по дискретной математике. Том 2, стр. 191–222
(Под. ред. В. Я. Козлова и др.)
Научное издательство «ТВП», 1998 г.

СВОЙСТВА ЛИНЕЙНЫХ И ПОЛИЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦАМИ ГАЛУА (I)

А. С. КУЗЬМИН, В. Л. КУРАКИН, А. А. НЕЧАЕВ

Предлагаемая работа является продолжением статьи тех же авторов «Псевдослучайные и полилинейные последовательности» [8]. В работе рассматриваются новые проблемы, связанные с оценками рангов координатных последовательностей линейных и полилинейных рекуррент над кольцами Галуа и с изучением распределений знаков на циклах линейных рекуррент над кольцами вычетов.

В первой части (раздел 1) впервые публикуется полное изложение математического аппарата для исследования алгебраических свойств координатных последовательностей линейных рекуррент над кольцами Галуа, в основе которого лежат метод сечений и понятие формальной полиномиальной дистанции. Используя разработанный математический аппарат, удалось существенно усилить нижние оценки рангов координатных последовательностей линейных рекуррент максимального периода над кольцом вычетов $\mathbb{Z}_{p^n}$, полученные ранее в работах А. А. Нечаева, Z. D. Dai, D. Gollmann, и обобщить их на произвольные примарные кольца вычетов. Принципиальным продвижением является получение нижних оценок рангов координатных последовательностей для более широких классов законов рекурсии.

Во второй части статьи (разделы 2 и 3), которая будет опубликована в третьем томе «Трудов по дискретной математике», с использованием оценок сумм характеров с полиномиальными аргументами будут усилены оценки частот появления элементов в линейных рекуррентах над кольцом $\mathbb{Z}_{p^2}$, рассмотрены некоторые вопросы теории полилинейных рекуррентных последовательностей над полями и кольцами Галуа и получены оценки рангов координатных последовательностей k-максимальной рекурренты над примарным кольцом вычетов $\mathbb{Z}_{p^n}$.

СОДЕРЖАНИЕ

Раздел 1. СТРОЕНИЕ И ОЦЕНКИ РАНГОВ КООРДИНАТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦАМИ ВЫЧЕТОВ

§ 1. СТРОЕНИЕ КООРДИНАТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦАМИ ВЫЧЕТОВ

1.1. Функции переноса и сечения координатных последовательностей. Рассмотрим некоторые свойства линейных рекуррентных последовательностей максимального периода (ЛРПМП) над примарным кольцом вычетов и их координатных последовательностей.

Пусть $R = \mathbb{Z}_{p^n}$ — кольцо вычетов целых чисел по модулю p^n, e — единица кольца R, $G(x) = x^m - \sum_{j=0}^{m-1} g_j x^j$ — многочлен максимального периода над кольцом R (см. [7], [8]). Обозначим через $L_R(G)$ множество всех линейных рекуррент над кольцом R с характеристическим многочленом $G(x)$, и пусть u есть ЛРПМП из $L_R(G)$. Знаки $u(i)$, $i \geqslant 0$, последовательности u однозначно представляются в виде

$$u(i) = \sum_{t=0}^{n-1} u_t(i) p^t, \qquad 0 \leqslant u_t(i) < p, \quad t = 0, \ldots, n-1, \quad i \geqslant 0. \tag{1.1.1}$$

Последовательность u_t знаков $u_t(i)$, $i \geqslant 0$, рассматриваемую как линейную рекурренту над полем $\mathbf{GF}(p)$, будем называть t-й координатной последовательностью ЛРП u.

Положим $\tau_t = p^t(p^m - 1)$ для $t = 0, \ldots, n-1$. Для произвольного многочлена $G(x)$ из кольца $R[x]$ через $\overline{G}(x)$ будем обозначать его образ по модулю p. В [8], [9] показано, что для многочлена максимального периода справедливы соотношения:

$$x^{\tau_t} - e \equiv p^{t+1} \Phi^{(t+1)}(x) \pmod{G(x)}, \qquad t = 0, \ldots, n-1, \tag{1.1.2}$$

$$\Phi^{(t)}(x) \not\equiv 0 \pmod{p}, \quad \deg \Phi^{(t)}(x) < m,$$

причем

$$\begin{aligned} &\text{если } p \geqslant 3,\ t \geqslant 1, \text{ то } \quad \Phi^t(x) \equiv \Phi^{(t+1)}(x) \pmod{p^t}, \\ &\text{если } p = 2, \text{ то } \quad \Phi^{(t)}(x) \equiv \Phi^{(t+1)}(x) \pmod{2^{t-1}}, \qquad t \geqslant 2, \\ &\qquad\qquad 4\Phi^{(2)}(x) \equiv 4\Big(\Phi^{(1)}(x) + \big(\Phi^{(1)}(x)\big)^2\Big) \pmod{G(x)}. \end{aligned} \tag{1.1.3}$$

Заметим, что многочлен $\Phi^{(t)}(x)$ однозначно определен только по модулю $p^n - t$. Для произвольного многочлена $H(x) = \sum_{k=0}^{l} h_k x^k$ над кольцом R определим операцию умножения последовательности u на многочлен $H(x)$ по правилу: $w = H(x)u$, где $w(i) = \sum_{k=0}^{l} h_k u(i+k)$ для $i \geqslant 0$.

Для $t = 1, \ldots, n-1$ последовательность $u^{(t)} = \Phi^{(t)}(x)u$ будем называть t-й производной последовательностью ЛРП u (см. [9]).

Из свойств многочленов $\Phi^{(t)}(x)$, $t = 1, \dots, n-1$, вытекает, что

$$\begin{aligned} &u_0^{(1)} = u_0^{(t)} \quad \text{для} \quad p \geqslant 3, \quad t \geqslant 1, \qquad u_1^{(2)} = u_1^{(t)} \quad \text{для} \quad p \geqslant 3, \quad t \geqslant 2, \\ &u_0^{(2)} = u_0^{(t)} \quad \text{для} \quad p = 2, \quad t \geqslant 2, \qquad u_1^{(3)} = u_1^{(t)} \quad \text{для} \quad p = 2, \quad t \geqslant 3. \end{aligned} \tag{1.1.4}$$

В силу свойств ЛРП максимального периода над конечными полями существует такое натуральное $\varkappa$, что $u_0^{(1)} = x^{\varkappa} u_0$, причем $x^{\varkappa} \equiv \overline{\Phi}^{(1)}(x) \pmod{\overline{G}(x)}$.

При исследовании ЛРП над кольцом R важную роль играют свойства арифметических операций в p-ичной системе счисления, в частности, вид функции переноса в старшие разряды при сложении чисел. При проведении выкладок без дополнительных оговорок будем использовать запись элементов кольца $\mathbb{Z}_{p^n}$ в виде p-целых рациональных чисел. Напомним, что рациональное число $r \in \mathbb{Q}$ называется p-целым, если $r = \frac{a}{b}$, где $a, b \in \mathbb{Z}$, $(b, p) = 1$. Множество $\mathbb{Z}_{(p)}$ p-целых рациональных чисел есть подкольцо поля $\mathbb{Q}_p$ p-адических чисел, причем $\mathbb{Q}_p / p^n \mathbb{Q}_p = \mathbb{Z}_{p^n}$. Это замечание позволяет говорить о вычетах p-целых чисел по модулю p^n и умножать эти числа на элементы кольца $\mathbb{Z}_{p^n}$.

Пусть функция $\Delta(x, y)$ определена на множестве $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ равенством

$$\Delta(x, y) = \begin{cases} 0, & \text{если} \quad x + y < p, \\ 1, & \text{если} \quad x + y \geqslant p. \end{cases} \tag{1.1.5}$$

Очевидно, что функция $\Delta(x, y)$ может быть задана полиномом над полем $\mathbb{Z}_p$, причем

$$\Delta(x, y) = \sum_{0 < \alpha < p, 0 < \beta < p} c_{\alpha,\beta} x^{\alpha} y^{\beta}. \tag{1.1.6}$$

Более точно вид функции $\Delta(x, y)$ описывает следующая лемма.

ЛЕММА 1.1.1. *Пусть функция $\Delta(x, y)$ определена на множестве $\mathbb{Z}_p$ условиями* (1.1.5), *тогда коэффициенты из представления* (1.1.6) *функции $\Delta(x, y)$ в виде полинома над $\mathbb{Z}_p$ удовлетворяют соотношениям:*

1) $c_{\alpha,\beta} = c_{\beta,\alpha}$ *для любых* $\alpha, \beta \in \{0, \dots, p-1\}$,

2) *если* $\alpha + \beta > p$, *то* $c_{\alpha,\beta} = 0$,

3) *для* α *и* β *таких, что* $\alpha + \beta \leqslant p$, $\alpha > 0$, $\beta > 0$,

$$c_{\alpha,\beta} = (-1)^{\alpha+\beta} \frac{(\alpha + \beta - 1)!}{\alpha!\, \beta!} q_{p-\alpha-\beta}, \tag{1.1.7}$$

где последовательность $q_0, q_1, \dots$ над полем рациональных чисел задается рекуррентным соотношением

$$\sum_{s=0}^{r} q_s \binom{r}{s} \frac{1}{r + 1 - s} = 1, \qquad q_0 = 1, \quad q_1 = \frac{1}{2}.$$

Доказательство. Первое свойство коэффициентов $c_{\alpha,\beta}$ очевидно. Из определения функции $\Delta(x, y)$ следует, что

$$\Delta(x, y) = \sum_{\substack{0 < k, j < p \\ j + k \geqslant p}} \prod_{\substack{\alpha = 0 \\ \alpha \neq k}}^{p-1} (x \ominus \alpha) \prod_{\substack{\beta = 0 \\ \beta \neq j}}^{p-1} (y \ominus \beta).$$

(Через $\oplus$, $\ominus$, $\otimes$ будем обозначать операции сложения, вычитания и умножения в поле $\mathbb{Z}_p$.) Преобразуя правую часть этого равенства, получаем

$$\Delta(x,y)=\sum_{\substack{0<k,j<p\\ j+k\geqslant p}}\sum_{t=1}^{p-1}\sum_{s=1}^{p-1}x^s y^t\binom{p-1}{s}\binom{p-1}{t}(-k)^{p-1-s}(-j)^{p-1-t}.$$

Отсюда с учетом соотношения $\binom{p-1}{j}\equiv(-1)^j \pmod p$ вытекает, что

$$\Delta(x,y)=\sum_{t=1}^{p-1}\sum_{s=1}^{p-1}x^s y^t\sum_{\substack{0<k,j<p\\ j+k\geqslant p}}k^{p-1-s}j^{p-1-t}$$

и коэффициент $c_{s,t}$ определяется равенством

$$c_{s,t}=\sum_{\substack{0<k,j<p\\ j+k\geqslant p}}k^{p-1-s}j^{p-1-t}. \tag{1.1.8}$$

Рассмотрим коэффициент $c_{s,t}$ при условии $s+t>p$. Пусть $s+t=p+l$, $l>0$, тогда

$$c_{s,t}=\sum_{k=1}^{p-1}k^{p-1-s}\sum_{j=p-k}^{p-1}j^{p-1-t}=\sum_{k=1}^{p-1}k^{p-1-s}\sum_{j=1}^{k}(-j)^{p-1-t}.$$

Для подходящих констант $d_0,d_1,\ldots,d_{p-t}$ из поля $\mathbf{GF}(p)$ выполняется равенство

$$\sum_{j=1}^{k}j^{p-1-t}=\sum_{i=0}^{p-t}d_i k^i.$$

Отсюда вытекает, что

$$c_{s,t}=(-1)^{p-1-t}\sum_{k=1}^{p-1}k^{p-1-s}\sum_{i=0}^{p-t}d_i k^i=(-1)^{p-1-t}\sum_{i=0}^{s-l}d_i\sum_{k=1}^{p-1}k^{p-1-s+i}=0,$$

так как сумма $\sum_{k=1}^{p-1}k^{p-1-s+i}$ отлична от нуля только при условии $s=i$, а внешняя сумма берется в пределах от 0 до $s-l$.

Равенство (1.1.7) выводится из (1.1.8). Доказательство носит технический характер и проводится индукцией по значению $s+t$ с использованием соотношений

$$c_{s,0}=c_{0,t}=0\quad\text{для всех}\quad s,t\in\{0,1,\ldots,p-1\},$$

$$c_{p-1-s,p-1-t}=(-1)^t\left(\sum_{k=0}^{t}\binom{t}{k}(-1)^k c_{p-1-s,p-1-k}+\binom{t}{p-1-s}\right).$$

Лемма доказана.

В. Н. Сачковым и В. Л. Куракиным было замечено, что последовательность чисел $q_0,q_1,q_2,\ldots$ (за исключением q_1) совпадает с хорошо известной в комбинаторике последовательностью чисел Бернулли.

СЛЕДСТВИЕ 1.1.2. *В условиях леммы* 1.1.1 *при* $p \geqslant 3$ *коэффициенты функции* $\Delta(x,y)$ *удовлетворяют равенствам:*

$$\begin{aligned} &c_{\alpha,\beta} = \frac{(-1)^{\alpha}}{\alpha} \quad \textit{для} \quad \alpha+\beta = p, \\ &c_{\alpha,\beta} = \frac{(-1)^{\alpha+1}}{2} \quad \textit{для} \quad \alpha+\beta = p-1, \\ &c_{\alpha,\beta} = 0 \quad \textit{для} \quad \alpha+\beta \not\equiv 0 \pmod 2, \quad \alpha = \beta < p-1. \end{aligned} \tag{1.1.9}$$

Значения указанных коэффициентов получаются непосредственно из соотношения (1.1.7). Отметим, что коэффициенты $c_{p-1,1}$, $c_{p-2,2}$ и $c_{p-2,1}$ легко вычисляются из равенства (1.1.8) с использованием формул суммы арифметической прогрессии и суммы квадратов первых n натуральных чисел (см. [1]).

Для многочленов из кольца $\mathbf{GF}(p)[x,y]$ определим преобразование Λ по правилу: для многочлена $f(x,y) \in \mathbf{GF}(p)[x,y]$ положим

$$\Lambda\big(f(x,y)\big) = f(x+y,y) \ominus f(x,y).$$

ЛЕММА 1.1.3. *Для функции* $\Delta(x,y) = \sum_{\substack{0<\alpha<p \\ 0<\beta<p}} c_{\alpha,\beta} x^{\alpha} y^{\beta}$ *при любом* r, $0 < r < p$, *имеет место равенство*

$$\begin{aligned} \Lambda^{r}\big(\Delta(x,y)\big) = &\sum_{\substack{0<\alpha<p-r \\ r<\beta<p \\ \alpha+\beta\leqslant p}} c_{\alpha,\beta} x^{\alpha} y^{\beta} \sum_{k=0}^{r} \binom{r+1}{k} (-1)^{k} (r+1-k)^{\beta} \\ &+ \sum_{\beta=r+1}^{p} y^{\beta} \frac{(-1)^{\beta}}{\beta} q_{p-\beta} \sum_{k=0}^{r} \binom{r+1}{k} (-1)^{k} (r+1-k)^{\beta}. \end{aligned}$$

В этой статье лемма 1.1.3 в полном объеме использоваться не будет. Нам понадобится более простое утверждение, которое может быть доказано независимо от леммы 1.1.3 на основе следствия 1.1.2.

СЛЕДСТВИЕ 1.1.4. *В условиях леммы* 1.1.3 *выполняется соотношение*

$$\Lambda^{p-2}\big(\Delta(x,y)\big) = y^{p-1}x \oplus \frac{1}{2}(y^{p-1} \ominus y). \tag{1.1.10}$$

Заметим, что в силу свойств преобразования Λ для доказательства следствия 1.1.4 достаточно знать только коэффициенты $c_{p-1,1}$, $c_{p-2,2}$ и $c_{p-2,1}$.

Используя результаты следствий 1.1.2 и 1.1.4, можно получить ряд свойств координатных последовательностей ЛРПМП над примарным кольцом вычетов $R = \mathbb{Z}_{p^n}$.

Для пары значений s и t, $1 \leqslant t+1 < s < n$, введем последовательности

$$v_{s,t} = (x^{\tau_0} \ominus \epsilon)^{p^{s-1}-p^{t}} u_s.$$

ЛЕММА 1.1.5. *Координатные последовательности линейной рекурренты и максимального периода над кольцом* $R = \mathbb{Z}_{p^n}$ *удовлетворяют следую-*

щим соотношениям. Если $p = 2$, *то*

$$v_{s,0} = \begin{cases} u_1^{(1)} \oplus u_0^{(1)} \otimes u_1 & \text{для} \quad s = 2, \\ x^{\varkappa} \otimes u_0^{(2)} \oplus u_0^{(2)} \otimes (u_1^{(1)} \oplus u_0^{(1)} \otimes u_1) & \text{для} \quad s = 3, \\ u_0^{(2)} \otimes (x^{\varkappa} \otimes u_0^{(2)} \oplus u_1^{(1)} \oplus u_0^{(1)} \otimes u_1) & \text{для} \quad s \geqslant 4; \end{cases} \tag{1.1.11}$$

$$v_{s,1} = \begin{cases} u_1^{(2)} \oplus u_0^{(2)} \otimes u_2 & \text{для} \quad s = 3, \\ u_0^{(2)} \otimes (u_1^{(2)} \oplus u_2) & \text{для} \quad s \geqslant 4; \end{cases} \tag{1.1.12}$$

и при $t \geqslant 2$

$$v_{s,t} = \begin{cases} u_1^{(3)} \oplus u_0^{(2)} \otimes u_{t+1} & \text{для} \quad s = t+2, \\ u_0^{(2)} \otimes (u_1^{(3)} \oplus u_{t+1}) & \text{для} \quad s > t+2. \end{cases} \tag{1.1.13}$$

Если $p \geqslant 3$, *то*

$$\begin{aligned} (x^{\tau_{s-1}} \ominus e) \otimes u_s &= u_0^{(1)}, \\ (x^{\tau_{s-2}} \ominus e) \otimes u_s &= u_1^{(s-1)} \oplus \Delta\big(u_{s-1}; u_0^{(1)}\big), \end{aligned} \tag{1.1.14}$$

и для $0 \leqslant t < s-1$

$$v_{s,t} = \big(u_0^{(1)}\big)^{p-1} \otimes u_{t+1} \oplus \frac{(u_0^{(1)})^{p-1} \ominus u_0^{(1)}}{2} \oplus \xi(p,s,t), \tag{1.1.15}$$

где

$$\xi(p,s,t) = \begin{cases} (u_0^{(1)})^{p-1} \otimes ((\overline{\Phi}^{(1)}(x))^2 \otimes u_0), & \text{если} \quad p = 3,\ t = 0,\ s > 2, \\ (\overline{\Phi}^{(1)}(x))^2 \otimes u_0, & \text{если} \quad p = 3,\ t = 0,\ s = 2, \\ 0 & \text{в остальных случаях.} \end{cases} \tag{1.1.16}$$

Доказательство. Первое равенство (1.1.14) следует из сравнения $(x^{\tau_{s-1}} - e)u \equiv p^s \Phi^{(s)}(x) u \equiv p^s u^{(s)} \pmod{p^{s+1}}$ и свойств (1.1.4) производных последовательностей ЛРП u.

Очевидно, что для любых $a, b \in \{0, 1, \ldots, p-1\}$ справедливо равенство $(a \oplus b) - b = a - p\Delta(a; b)$. Следовательно, с учетом первого равенства в (1.1.14) для $i = 0, 1, 2, \ldots$ получаем

$$u_{s-1}(i + \tau_{s-2}) - u_{s-1}(i) \equiv u_0^{(s-1)}(i) - p\Delta\big(u_{s-1}(i); u_0^{(s-1)}(i)\big) \pmod{p^2},$$

и второе равенство в (1.1.14) вытекает из сравнения

$$(x^{\tau_{s-2}} - e)u \equiv p^{s-1} u^{(s-1)} \pmod{p^{s+1}}.$$

Докажем (1.1.15). Из (1.1.14) следует равенство $v_{s,s-2} = (x^{\tau_{s-2}} - e)^{p-2} \otimes (u_1^{(s-1)} \oplus \Delta(u_{s-1}; u_0^{(1)}))$, и поскольку период $T(u_0^{(1)})$ последовательности $u_0^{(1)}$ равен значению τ_0 и $\tau_0 \mid \tau_{s-2}$, ввиду (1.1.14) имеем $(x^{\tau_{s-2}} - e)^{p-2} \otimes \Delta(u_{s-1}; u_0^{(1)}) = \Lambda^{p-2}(\Delta(u_{s-1}; u_0^{(1)}))$. Отсюда в силу (1.1.10) получаем

$$v_{s,s-2} = \big(u_0^{(1)}\big)^{p-1} \otimes u_{s-1} \oplus \frac{(u_0^{(1)})^{p-1} \ominus u_0^{(1)}}{2} \oplus (x^{\tau_{s-2}} - e)^{p-2} \otimes u_1^{(s-1)}, \tag{1.1.17}$$

а так как

$$(x^{\tau_{s-2}}-e)^{p-2}\otimes u_1^{(s-1)}=\begin{cases}(\overline{\Phi}^{(1)}(x))^2\otimes u_0, & \text{если}\quad p=3,\ s=2,\\ 0 & \text{в остальных случаях,}\end{cases}$$

то соотношение (1.1.15) в случае $t=s-2$ доказано. Доказательство равенства (1.1.15) в общем случае проводится индукцией по параметру t с использованием соотношений

$$\begin{aligned}v_{s,t-1}&=(x^{\tau_0}-e)^{p^t-p^{t-1}}\otimes v_{s,t}\\&=\big(u_0^{(1)}\big)^{p-1}\otimes\big((x^{\tau_0}-e)^{p^t-p^{t-1}}\otimes u_{t+1}\big)\\&=\big(u_0^{(1)}\big)^{p-1}\otimes u_t\oplus\frac{(u_0^{(1)})^{p-1}\ominus u_0^{(1)}}{2}\oplus\big(u_0^{(1)}\big)^{p-1}\\&\quad\otimes\big((x^{\tau_{t-1}}-e)^{p-2}\otimes u_1^{(t)}\big),\end{aligned}\tag{1.1.18}$$

$$\big(u_0^{(1)}\big)^{p-1}\otimes\big((x^{\tau_{t-1}}-e)^{p-2}\otimes u_1^{(t)}\big)=\begin{cases}(u_0^{(1)})^{p-1}\otimes((\overline{\Phi}^{(1)}(x))^2\otimes u_0), & \text{если}\quad p=3,\ t=0,\\ 0 & \text{в остальных случаях.}\end{cases}$$

Если определить последовательность $\xi(p,s,t)$ соотношением (1.1.16), равенство (1.1.15) следует из (1.1.17) и (1.1.18).

Соотношения (1.1.11)–(1.1.13) доказываются аналогично. Лемма доказана.

Формулы (1.1.11)–(1.1.15) описывают аналитические зависимости между знаками координатных последовательностей ЛРПМП в определенных тактах. Эти соотношения, как будет видно из дальнейшего изложения, являются своеобразным математическим аппаратом при исследовании аналитических и статистических свойств ЛРПМП над примарными кольцами вычетов.

1.2. Минимальные многочлены координатных последовательностей и их корни. Особое значение при исследовании свойств ЛРП имеют минимальные многочлены этих последовательностей, т. е. характеристические многочлены наименьшей возможной степени. Разложение минимального многочлена на неприводимые множители определяет строение псевдослучайной последовательности. В работах зарубежных авторов (см., например, [18]–[20]) степень минимального многочлена называется линейной сложностью, причем предлагается рассматривать линейную сложность как один из параметров, характеризующих близость псевдослучайной последовательности к случайной равновероятной последовательности. В данной работе в соответствии с [8] степень минимального многочлена будем называть рангом последовательности.

Рассмотрим закономерности строения минимальных многочленов координатных последовательностей ЛРПМП u. Обозначим через $\mu_s(x)$ минимальный многочлен s-й координатной последовательности u_s, $s=0,\dots,n-1$, ЛРП u. Напомним, что $\tau_s=(p^m-1)p^s$, $s=0,\dots,n-1$.

В [9] показано, что для $s=0,\dots,n-1$ существует система таких попарно взаимно простых сепарабельных многочленов $g(x),g_{s,1}(x),\dots,g_{s,p^s-1}(x)$ над

$\mathbf{GF}(p)$, что

$$\mu_s(x) = g(x)^{p^{s-1}+1} g_{s,1}(x)^{p^{s-1}} \times \cdots \times g_{s,p^{s-1}}(x), \tag{1.2.1}$$

$$g(x) \equiv G(x) \pmod p, \quad \prod_{k=1}^{p^{s-1}} g_{s,k}(x) \mid x^{\tau_0} - e.$$

Заметим, что разложение (1.2.1) отличается от традиционного разложения многочлена в произведение неприводимых сомножителей. Многочлены $g_{s,k}(x)$, $k = 1, \ldots, p^{s-1}$, в общем случае являются произведениями различных неприводимых над $\mathbf{GF}(p)$ многочленов.

УТВЕРЖДЕНИЕ 1.2.1. *Для $s = 0, \ldots, n-1$, $k < s$ многочлены $g_{s,1}(x), \ldots, g_{s,p^k-1}(x)$ из разложения* (1.2.1) *минимального многочлена $\mu_s(x)$ ЛРП u_s однозначно определяются $k+1$ младшими координатными последовательностями $u_0, \ldots, u_k$ ЛРП u. При этом в случае $m \geqslant 3$ имеют место равенства:*

$$g_{s,j}(x) = g_{t,j}(x) \quad \textit{для} \quad t \geqslant s+1, \quad j \in \{1, \ldots, (p-1)p^{s-2} - 2\}, \tag{1.2.2}$$

где $s \geqslant 4$ при $p = 2$, $s \geqslant 3$ при $p = 3$, $s \geqslant 2$ при $p \geqslant 5$.

Доказательство. Из определения производных последовательностей ЛРПМП u из $L_R(G)$ следует, что знаки последовательности $(x^{\tau_0} - e)u_s$ определяются только знаками последовательностей $u_0, \ldots, u_{s-1}, u_0^{(1)}, \ldots, u_{s-1}^{(1)}$, а так как $u^{(1)} \equiv \Phi^{(1)}(x)u$, то, в конечном итоге, последовательность $(x^{\tau_0} - e)u_s$ и ее минимальный многочлен определяются последовательностями $u_0, \ldots, u_{s-1}$. Отсюда, с учетом соотношений (1.1.11)–(1.1.16), из леммы 1.1.5 и разложения (1.2.1) многочлена $\mu_s(x)$ получаем первое утверждение.

Рассмотрим закономерности строения многочленов $g_{s,j}(x)$ при различных s. Пусть $2 \leqslant s < t \leqslant n-1$ и $p \geqslant 3$. Тогда в силу леммы 1.1.5

$$v_{t,s-1} = (x^{\tau_0} - e)^{p^{t-1} - p^{s-1}} u_t = \left(u_0^{(1)}\right)^{p-1} u_s + w,$$

где w — рекуррента над $\mathbf{GF}(p)$ периода τ_0. Найдем такое натуральное r, что $(x^{\tau_0} - e)^r u_s = (x^{\tau_0} - e)^r v_{t,s-1}$.

Очевидно, что для этого достаточно найти r, удовлетворяющее условию $(x^{\tau_0} - e)^r (u_s \ominus (u_0^{(1)})^{p-1} u_s) = 0$.

Из леммы 1.1.5 получаем:

$$(x^{\tau_0} - e)^{p^{s-2}} u_s = u_1^{(s-1)} \oplus \Delta\left(u_0^{(1)}; u_{s-1}\right), \tag{1.2.3}$$

$$(x^{\tau_0} - e)^{p^{s-2}} \left(\left(u_0^{(1)}\right)^{p-1} u_s\right) = \left(u_0^{(1)}\right)^{p-1} u_1^{(s-1)} \oplus \Delta\left(u_0^{(1)}; u_{s-1}\right). \tag{1.2.4}$$

Из (1.2.3) и (1.2.4) с учетом равенств (1.1.14) следует соотношение

$$(x^{\tau_0} - e)^{p^{s-2}+2} \left(\left(u_0^{(1)}\right)^{p-1} u_s\right) = (x^{\tau_0} - e)^{p^{s-2}+2} u_s. \tag{1.2.5}$$

Если $p = 2$, то те же рассуждения с использованием леммы 1.1.5 при $t > s \geqslant 4$ приводят к равенству

$$(x^{\tau_0} - e)^{2^{t-1} - 2^{s-1} + 2^{s-2} + 2} u_t = (x^{\tau_0} - e)^{2^{s-2}+2} u_s. \tag{1.2.6}$$

Заметим, что из (1.2.5), (1.2.6) вытекает совпадение минимальных многочленов последовательностей $(x^{\tau_0}-\epsilon)^{p^{t-1}-p^{s-1}+p^{s-2}+2}u_t$ и $(x^{\tau_0}-\epsilon)^{p^{s-2}+2}u_s$. Поскольку минимальные многочлены этих последовательностей получаются из $\mu_s(x)$ и $\mu_t(x)$ отбрасыванием многочленов $g_{s,j}(x)$ и $g_{t,j}(x)$ с номерами $j \geqslant p^{s-1}-p^{s-2}-1$ и соответствующим понижением степени остальных делителей, в силу однозначности представления многочленов $\mu_s(x), s=1,\ldots,n-1$, в виде (1.2.1) получаем равенства (1.2.2).

З а м е ч а н и е 1.2.2. Из доказанного утверждения не следует, что многочлены $g_{s,j}(x)$ и $g_{t,j}(x)$, $t \geqslant s+1$, $j > (p-1)p^{s-2}-2$, будут различаться. Например, при условии $\Phi^{(1)}(x) \equiv \Phi^{(1)}(0) \pmod p$ совпадают все многочлены $g_{t,(p-1)p^{s-2}-1}(x)$, $t \geqslant s$.

Утверждение 1.2.1 позволяет сводить изучение минимальных многочленов координатных последовательностей ЛРППМП над примарными кольцами вычетов к изучению минимальных многочленов координатных последовательностей с меньшими номерами. Так, построив (например, с использованием вычислительной техники) разложение (1.2.1) для минимального многочлена $\mu_s(x)$, сразу же можно выписать часть сомножителей в разложениях (1.2.1) минимальных многочленов $\mu_t(x)$ для $t > s$. В частности, за счет описания вида некоторых сомножителей в (1.2.1) могут быть получены нижние оценки рангов соответствующих координатных последовательностей.

Дальнейшие исследования строения минимальных многочленов координатных последовательностей ЛРППМП над примарным кольцом вычетов $R = \mathbb{Z}_{p^n}$ связаны с описанием корней многочленов $g_{s,k}(x)$, $s=0,\ldots,n-1$, $k=1,\ldots,p^{s-1}$.

Чтобы упростить чтение статьи, приведем необходимые для дальнейшего изложения результаты из [7], [9], [12].

Существует расширение Галуа кольца R, над которым многочлен $G(x)$ раскладывается на линейные множители. Пусть S — минимальное по мощности кольцо с таким свойством, тогда S есть кольцо Галуа из p^{mn} элементов характеристики p^n (см. [12]). Обозначим через $\mathrm{Aut}\,(S/R)$ группу автоморфизмов кольца S над кольцом R. Тогда функция Tr_R^S, определяемая на S равенством

$$\mathrm{Tr}_R^S(x) = \sum_{\rho \in \mathrm{Aut}\,(S/R)} \rho(x),$$

отображает S на R и называется «следом» из S в R (см. [9]).

Пусть θ — корень многочлена $G(x)$ в кольце S, тогда для ЛРППМП u из $L_R(G)$ существует такой единственный элемент $a \in S$, что

$$u(i) = \mathrm{Tr}_R^S(a\theta^i) \quad \text{для всех} \quad i = 0,1,2,\ldots. \tag{1.2.7}$$

Для произвольного элемента $x \in R$ через $\delta_t(x)$, $t=0,\ldots,n-1$, будем обозначать t-й разряд p-ичного представления элемента x. Отсюда по определению координатных последовательностей получаем

$$u_t(i) = \delta_t\big(\mathrm{Tr}_R^S(a\theta^i)\big), \qquad i \geqslant 0. \tag{1.2.8}$$

Таким образом, задача изучения строения координатных последовательностей ЛРП и их минимальных многочленов сводится к изучению свойств

функций $\delta_t(\mathrm{Tr}_R^S x)$, $t = 0, \ldots, n-1$, осуществляющих отображение кольца S в $\mathbb{Z}_p$. При этом будет использоваться ряд свойств колец Галуа, доказательство которых можно найти, например, в [9]. Пусть $\Gamma(S) = \{x \in S\colon\ x^{p^m} = x\}$, т. е. $\Gamma(S)$ состоит из корней многочлена $x^{p^m} - x$. Множество $\Gamma(S)$ образует полную систему представителей классов вычетов кольца S по модулю pS, и для произвольного элемента $a \in S$ однозначно определено разложение

$$a = \sum_{s=0}^{n-1} p^s \gamma_s(a), \qquad \gamma_s(a) \in \Gamma(S), \quad s = 0, \ldots, n-1, \tag{1.2.9}$$

которое будем называть p-адическим разложением элемента a. Для $s = 0, \ldots, n-1$ элемент $\gamma_s(a)$ из (1.2.9) будем называть s-м разрядом p-адического разложения элемента a. Отметим, что при $p \geqslant 3$ функции δ_s и γ_s на элементах кольца R различны, а при $p = 2$ совпадают.

Множество $\Gamma(S)$ замкнуто относительно операции умножения в кольце S. Введем на множестве $\Gamma(S)$ операцию сложения $\oplus$ по правилу: для $a, b \in \Gamma(S)$ положим $a \oplus b = \gamma_0(a+b)$, тогда $(\Gamma(S), \oplus, \cdot)$ — поле из p^m элементов.

Введенное p-адическое разложение элементов кольца S позволяет более просто описать функцию Tr_R^S. Как показано в [9], справедливо равенство

$$\mathrm{Tr}_R^S(x) = \sum_{k=0}^{m-1} \sum_{s=0}^{n-1} p^s \big(\gamma_s(x)\big)^{p^k}. \tag{1.2.10}$$

Отсюда вытекает, что основным моментом в изучении функций $\delta_t(\mathrm{Tr}_R^S x)$, $t = 0, \ldots, n-1$, является описание разрядов p-ичного разложения суммы элементов из $\Gamma(S)$ при условии, что эта сумма лежит в кольце R. Доказательство этих результатов сопряжено с большим объемом вычислений и сопровождается громоздкими выкладками. В силу указанных причин, а также учитывая, что, в основном, доказательство носит технический характер, а само описание вида функций $\delta_t(\mathrm{Tr}_R^S x)$, $t = 0, \ldots, n-1$, является промежуточным результатом при изучении ЛРП над примарным кольцом R, ограничимся только формулировками результатов и ссылками на опубликованные доказательства.

Для краткости вместо $a \equiv b \pmod{p^l}$ будем писать $a \overset{p^l}{\equiv} b$.

Для любых натуральных $K, M \in \mathbb{N}$ определим множество

$$I_p(M,K) = \big\{(i_1, \ldots, i_M)\colon\ i_k = 0, \ldots, p-1,\ k = 1, \ldots, M,\ i_1 + \cdots + i_M = K\big\} \tag{1.2.11}$$

и полином $\omega_M^{(K)}(\overline{x}) = \omega_M^{(K)}(x_1, \ldots, x_M)$ над кольцом R:

$$\omega_M^{(K)}(\overline{x}) = \sum_{(i_1,\ldots,i_M) \in I_p(M,K)} \prod_{k=1}^{M} \frac{1}{i_k!} x_k^{i_k}. \tag{1.2.12}$$

Мощность множества $I_p(M,K)$ обозначим $\left\{{K \atop M}\right\}$, причем, согласно [14], имеет место равенство

$$\left\{{K \atop M}\right\} = \sum_{t \geqslant 0} (-1)^t \binom{M}{t} \binom{K + M - pt - 1}{M - 1}. \tag{1.2.13}$$

ТЕОРЕМА 1.2.3 (см. [9]). *Пусть* $\overline{a} = (a_1, \ldots, a_M)$ — *такой набор элементов из* $\Gamma(S)$, *что* $(a_1^p, \ldots, a_M^p) = (a_{\pi(1)}, \ldots, a_{\pi(M)})$ *для некоторой подстановки* $\pi \in \mathfrak{S}_M$. *Тогда элемент* $\sigma = \sum_{j=1}^{M} a_j$ *принадлежит кольцу* R *и для каждого целого* t, $0 \leqslant t < \log_p M(p-1)$, *существуют полиномы* $\varkappa_t^{(M)}(x_1, \ldots, x_M)$ *и* $\rho_t^{(M)}(x_1, \ldots, x_M)$ *над* R, *имеющие степень, строго меньшую* p^t, *и удовлетворяющие соотношениям*

$$\gamma_t(\sigma) \overset{p}{\equiv} \omega_M^{(p^t)}(\overline{a}) + \rho_t^{(M)}(\overline{a}), \tag{1.2.14}$$

$$\delta_t(\sigma) \overset{p}{\equiv} \omega_M^{(p^t)}(\overline{a}) + \varkappa_t^{(M)}(\overline{a}). \tag{1.2.15}$$

Включение $\sigma \in R$ вытекает из того, что элемент σ инвариантен относительно всех автоморфизмов группы $\mathrm{Aut}\,(S/R)$. Доказательство формул (1.2.14) и (1.2.15) проводится индукцией по параметру t одновременно для всех $M > \frac{p^t}{p-1}$ и всех наборов $(a_1, \ldots, a_M)$, удовлетворяющих условиям теоремы (см. [9]).

ТЕОРЕМА 1.2.4 ([9]). *Для каждого* $s = 0, \ldots, n-1$ *такого, что* $p^s < m(p-1)$, *существует полином* $\eta_s(x_{0,0}, \ldots, x_{0,m-1}, \ldots, x_{s,m-1})$ *над кольцом* R, *имеющий степень, строго меньшую* p^s, *и удовлетворяющий соотношению*

$$\begin{aligned}\delta_s\bigl(\mathrm{Tr}_R^S(x)\bigr) \overset{p}{\equiv} \omega_M^{(p)}\bigl(\gamma_0(x), \ldots, \gamma_0(x)^{p^{m-1}}\bigr) \\ + \eta_s\bigl(\gamma_0(x), \ldots, \gamma_0(x)^{p^{m-1}}, \ldots, \gamma_s(x)^{p^{m-1}}\bigr).\end{aligned} \tag{1.2.16}$$

Доказательство основано на представлении функции $\mathrm{Tr}_R^S(x)$ в виде суммы

$$\mathrm{Tr}_R^S(x) = \sum_{t=0}^{n-1} p^t \mathrm{Tr}_R^S(\gamma_t(x))$$

и проводится индукцией по параметру s с использованием теоремы 1.2.3 и свойств функций переноса при сложении чисел в p-ичной системе счисления (см. [9]).

Вернемся к изучению свойств минимальных многочленов $\mu_s(x)$ координатных последовательностей ЛРПМП u из $L_R(G)$.

Из результатов работы [9] следует, что поле $\overline{S} = S/pS = \mathbf{GF}\,(p^m)$ есть минимальное поле разложения многочлена $g(x) \equiv G(x) \pmod p$ над полем $\overline{R} = \mathbf{GF}\,(p)$, а его корень $\overline{\theta} = \overline{\gamma_0(\theta)}$ есть примитивный элемент поля.

ТЕОРЕМА 1.2.5. *При условии* $1 \leqslant s < \log_p m(p-1)$ *корнями многочлена* $g_{s,p^s-1}(x)$ *из разложения* (1.2.1) *многочлена* $\mu_s(x)$ *являются все элементы поля* $\mathbf{GF}\,(p^m)$ *вида*

$$\overline{\theta}^{i_0 + i_1 p + \cdots + i_{m-1} p^{m-1}}, \qquad (i_0, \ldots, i_{m-1}) \in I_p(m, p^s), \tag{1.2.17}$$

и справедливо неравенство

$$\mathrm{rank}\, u_s \geqslant m(p^{s-1}+1) + \left\{\begin{matrix} p^s \\ m \end{matrix}\right\}. \tag{1.2.18}$$

Доказательство. Из (1.2.8), (1.2.16) для $i \geqslant 0$ следует равенство

$$u_s(i) \stackrel{p}{\equiv} \omega_M^{(p^s)}\bigl(\gamma_0(a\theta^i), \ldots, \gamma_0(a\theta^i)^{p^{m-1}}\bigr) + \eta_s\bigl(\gamma_0(a\theta^i), \ldots, \gamma_0(a\theta^i)^{p^{m-1}}, \ldots, \gamma_s(a\theta^i)^{p^{m-1}}\bigr).$$

Зададим вспомогательные последовательности $v^{(s)}$ и $w^{(s)}$ над полем $\Gamma(S)$ по правилу

$$v^{(s)}(i) = \gamma_0\Bigl(\omega_M^{(p^s)}\bigl(\gamma_0(a\theta^i), \ldots, \gamma_0(a\theta^i)^{p^{m-1}}\bigr)\Bigr), \qquad i \geqslant 0;$$
$$w^{(s)}(i) = \gamma_0\Bigl(\eta_s\bigl(\gamma_0(a\theta^i), \ldots, \gamma_0(a\theta^i)^{p^{m-1}}, \ldots, \gamma_s(a\theta^i)^{p^{m-1}}\bigr)\Bigr), \qquad i \geqslant 0.$$

Тогда $u_s \stackrel{p}{\equiv} v^{(s)} + w^{(s)}$, и для доказательства первого утверждения теоремы достаточно доказать следующие свойства последовательностей $v^{(s)}$ и $w^{(s)}$:

а) все элементы вида

$$\overline{\theta}^{i_0 + i_1 p + \cdots + i_{m-1}p^{m-1}}, \qquad (i_0, \ldots, i_{m-1}) \in I_p(m, p^s),$$

являются простыми корнями минимального многочлена $\mu_{\overline{v}^{(s)}}(x)$ ЛРП $\overline{v}^{(s)}$ над полем $\overline{S}$;

b) ни один из элементов (1.2.17) не является корнем минимального многочлена $\mu_{\overline{w}^{(s)}}(x)$ ЛРП $\overline{w}^{(s)}$.

Из (1.2.12) следует, что

$$v^{(s)}(i) = \bigoplus_{(i_0, \ldots, i_{m-1}) \in I_p(m, p^s)} \gamma_0\Biggl(a^{\sum_{t=0}^{m-1} i_t p^t} \prod_{t=0}^{m-1} \frac{1}{i_t!}\Biggr)\Bigl(\gamma_0(\theta)^{\sum_{t=0}^{m-1} i_t p^t}\Bigr)^i,$$

где $\oplus$ — операция сложения в поле $\Gamma(S)$. Поскольку $\gamma_0(a) \neq 0$, для любого набора $(i_0, \ldots, i_{m-1})$ имеем

$$\gamma_0\Biggl(a^{\sum_{t=0}^{m-1} i_t p^t} \prod_{t=0}^{m-1} \frac{1}{i_t!}\Biggr) \neq 0.$$

Кроме того, так как $\overline{\theta}$ — примитивный элемент поля $\overline{S}$, то для различных наборов $(i_0, \ldots, i_{m-1})$ и $(i'_0, \ldots, i'_{m-1})$ из $I_p(m, p^s)$ элементы $\overline{\theta}^{\sum_{t=0}^{m-1} i_t p^t}$ и $\overline{\theta}^{\sum_{t=0}^{m-1} i'_t p^t}$ различны. Поэтому

$$\mu_{\overline{v}^{(s)}}(x) = \prod_{(i_0, \ldots, i_{m-1}) \in I_p(m, p^s)} \Bigl(x - \overline{\theta}^{\sum_{t=0}^{m-1} i_t p^t}\Bigr),$$

и свойство а) доказано.

Рассмотрим последовательность $w^{(s)}$. Для $t = 0, \ldots, n-1$, $j = 0, \ldots, m-1$, обозначим через $w_{t,j}^{(s)}$ последовательность над $\Gamma(S)$ вида

$$w_{t,j}^{(s)}(i) = \gamma_t(a\theta^i)^{p^j}, \qquad i \geqslant 0.$$

Тогда

$$w^{(s)} = \gamma_0\Big(\eta_s\big(w^{(s)}_{0,0},\dots,w^{(s)}_{0,m-1},\dots,w^{(s)}_{s,m-1}\big)\Big). \tag{1.2.19}$$

Опишем характеристический многочлен последовательности $w^{(s)}_{t,j}$.

Индукцией по t несложно выводится соотношение $\theta^{p^t\,p^{t+1}} \equiv \gamma_0(\theta)^{p^t}$, из которого при введенных обозначениях получаются равенства

$$\begin{aligned} w^{(s)}_{t,j}(i+p^t) &= \gamma_t(a\theta^{i+p^t})^{p^j} = \gamma_t\big(a\theta^i\gamma_0(\theta)^{p^t}\big)^{p^j} \\ &= \gamma_t(a\theta^i)^{p^j}\gamma_0(\theta)^{p^{t+j}} = \gamma_0(\theta)^{p^{t+j}} w^{(s)}_{t,j}(i). \end{aligned}$$

Отсюда вытекает, что $(x-\overline{\theta}^{p^j})^{p^t}$ — характеристический многочлен ЛРП $\overline{w}^{(s)}_{t,j}$. Так как по теореме 1.2.4 степень многочлена $\eta_s(x_{0,0},\dots,x_{0,m-1},\dots,x_{s,m-1})$ строго меньше p^s, то из (1.2.19) и известных результатов о корнях характеристических многочленов линейных рекуррент, получаемых в виде полиномов от линейных рекуррент над полями (см., например, [28], [30]), следует, что все корни многочлена $\mu_{\overline{w}^{(s)}}(x)$ имеют вид

$$\overline{\theta}^{p^{j_1}+p^{j_2}+\dots+p^{j_r}}, \qquad j_1,\dots,j_r = 0,\dots,m-1, \quad r < p^s.$$

Следовательно, выполняется свойство b) и справедливо первое утверждение теоремы.

Неравенство (1.2.18) является очевидным следствием условия

$$\operatorname{rank} u_s = \deg\mu_s(x) \geqslant \deg g(x)^{p^{s-1}+1} + \deg\mu_{\overline{w}^{(s)}}(x)$$

и равенств (1.2.11), (1.2.13). Теорема доказана.

Отметим, что теорема 1.2.5 справедлива для любой ЛРПМП над примарным кольцом вычетов $R = \mathbb{Z}_{p^n}$ независимо от многочлена $G(x)$ и начального вектора рекурренты. В случае $p = 2$ оценки $\operatorname{rank} u_s$ приобретают наиболее простой вид:

$$\operatorname{rank} u_s \geqslant m(2^{s-1}+1) + \binom{m}{2^s},$$

при этом многочлен $\omega_m^{(2^s)}(\overline{x})$ есть элементарная симметрическая функция степени 2^s от m переменных.

Ограничение $1 \leqslant s < \log_p m(p-1)$ на номер изучаемой координатной последовательности при больших значениях p является существенным. Поэтому представляет интерес задача уточнения строения координатных последовательностей ЛРПМП хотя бы для отдельных классов многочленов максимального периода над кольцом R.

Условие $1 < \log_p m(p-1)$ выполняется для всех $m \geqslant 2$, и, следовательно, для произвольной ЛРПМП порядка $m \geqslant 2$ над кольцом R теорема 1.2.5 справедлива, по крайней мере, для первой координатной последовательности. Отметим, что в [34] получено полное описание строения минимального многочлена первой координатной последовательности ЛРПМП над произвольным кольцом Галуа.

§ 2. ОЦЕНКИ РАНГОВ КООРДИНАТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛРП МАКСИМАЛЬНОГО ПЕРИОДА НАД ПРИМАРНЫМ КОЛЬЦОМ ВЫЧЕТОВ $\mathbb{Z}_{p^n}$

Описание строения координатных последовательностей ЛРП максимального периода над кольцом $R = \mathbb{Z}_{p^n}$ позволяет дать оценки их рангов. Если вид минимального многочлена $\mu_s(x)$ известен полностью, то из равенства $\operatorname{rank} u_s = \deg \mu_s(x)$ получаем точное значение ранга последовательности u_s. Выявление отдельных свойств делителей $g_{s,k}(x)$, $k = 1, \ldots, p^{s-1}$, многочленов $\mu_s(x)$, $s = 1, \ldots, n-1$, дает возможность получить, соответственно, верхние или нижние оценки $\operatorname{rank} u_s$.

Заметим, что при выводе верхних и нижних оценок применяются различные подходы: для получения нижних оценок необходимо доказать, что определенный многочлен делит $g_{s,k}(x)$ для некоторого k, а для получения верхних оценок достаточно показать, что для каждого $k = 1, \ldots, p^{s-1}$ все неприводимые делители многочленов $g_{s,k}(x)$ принадлежат некоторым фиксированным множествам, и чем меньше мощности этих множеств, тем точнее верхние оценки приближаются к истинному значению $\operatorname{rank} u_s$.

2.1. Полиномиальная дистанция. Верхние оценки рангов. Исследования рангов координатных последовательностей ЛРПМП над кольцом $R = \mathbb{Z}_{p^n}$ начнем с определения верхних границ для значений $\operatorname{rank} u_s = \deg \mu_s(x)$, $s = 1, \ldots, n-1$.

Пусть $F(x)$ — многочлен максимального периода из кольца $R[x]$ степени m, $g(x) \equiv F(x) \pmod p$ — многочлен максимального периода над полем $\overline{R} = \mathbf{GF}(p)$, θ — корень $F(x)$ в расширении S кольца R, $\overline{\theta}$ — корень многочлена $g(x)$ в его поле разложения $\mathbf{GF}(p^m)$. Если многочлен $h(x) \in \overline{R}[x]$ раскладывается над $\mathbf{GF}(p^m)$ на линейные множители, то *полиномиальной дистанцией* от многочлена $g(x)$ до $h(x)$ будем называть величину

$$\rho(g,h) = \max\left\{w_p(k)\colon\ 0 < k < p^m,\ h(\overline{\theta}^k) = 0\right\}, \tag{2.1.1}$$

где $w_p(k)$ — вес числа k в p-ичном представлении: если $k = \sum_{s\geqslant 0} k_s p^s$, $0 \leqslant k_s \leqslant p-1$, то $w_p(k) = \sum_{s\geqslant 0} k_s$. Если $h(\overline{\theta}^k) \neq 0$ при всех k, $0 < k < p^m$, то полагаем $\rho(g,h) = +\infty$.

Под полиномиальной дистанцией $\rho(g,v)$ от $g(x)$ до произвольной последовательности v над $\mathbf{GF}(p)$ будем понимать полиномиальную дистанцию от $g(x)$ до минимального многочлена последовательности v.

Отметим ряд свойств полиномиальной дистанции. Если π_1, π_2 — две ЛРП над полем $\mathbf{GF}(p)$, то справедливы неравенства

$$\begin{aligned} \rho(g, \pi_1 + \pi_2) &\leqslant \max\left\{\rho(g,\pi_1), \rho(g,\pi_2)\right\}, \\ \rho(g, \pi_1 \cdot \pi_2) &\leqslant \rho(g,\pi_1) + \rho(g,\pi_2). \end{aligned} \tag{2.1.2}$$

Из теоремы 1.2.5 непосредственно вытекает, что для координатных последовательностей ЛРПМП $u \in L_R(F)$ при условии $p^s \leqslant m(p-1)$ выполняются равенства

$$\rho(g, u_s) = \rho(g, \mu_s) = p^s, \qquad s = 0, \ldots, n-1. \tag{2.1.3}$$

Будем говорить, что последовательность v над полем $P = \mathbf{GF}(p)$ выражается через последовательности $v_1, \ldots, v_r$, если она представляется в виде суммы произведений этих последовательностей с коэффициентами из P:

$$v = \sum c_{i_1 \cdots i_r} \prod_{j=1}^{r} v_j^{i_j}, \tag{2.1.4}$$

где сумма берется по векторам $(i_1, \ldots, i_r)$ из множества $\mathbb{N}_0^{(r)}$, а выражение в правой части равенства (2.1.4) будем называть полиномиальным представлением последовательности v.

Введем понятие формальной полиномиальной дистанции $\overline{\rho}^*(g, v)$ от многочлена $g(x)$ до представления (2.1.4) последовательности v, полагая:

a) $\overline{\rho}^*(g, v) = p^s$, если v является s-й координатной последовательностью некоторой ЛРПМП из $L_R(F)$,

b) $\overline{\rho}^*(g, v) = \overline{\pi}_p(\alpha_1)\overline{\rho}^*(g, v_1) + \cdots + \overline{\pi}_p(\alpha_r)\overline{\rho}^*(g, v_r)$, если $v = cv_1^{\alpha_1} \times \cdots \times v_r^{\alpha_r}$, где $v_1, \ldots, v_r$ — различные последовательности из пункта a), c — обратимый элемент поля $\mathbf{GF}(p)$, а значения $\pi_p(\alpha_j)$, $j = 1, \ldots, r$, определяются по α_j, $j = 1, \ldots, r$, условиями

$$\overline{\pi}_p(x) = \begin{cases} x, & \text{если} \quad x \leqslant p-1, \\ 1 + ((x-1) \bmod (p-1)), & \text{если} \quad x \geqslant p \geqslant 3, \\ 1, & \text{если} \quad x \geqslant p = 2, \end{cases}$$

c) $\overline{\rho}^*(g, v) = \max\{\overline{\rho}^*(g, v_1), \ldots, \overline{\rho}^*(g, v_r)\}$, если $v = c_1 v_1 + \cdots + c_r v_r$, где $v_1, \ldots, v_r$ — последовательности из пунктов a), b), $c_1, \ldots, c_r$ — обратимые элементы $\mathbf{GF}(p)$,

d) $\overline{\rho}^*(g, v) = 0$, если $v = 0$,

e) $\overline{\rho}^*(g, v) = +\infty$ в остальных случаях.

Формальной полиномиальной дистанцией $\overline{\rho}(g, v)$ от многочлена $g(x)$ до последовательности v будем называть минимум значений $\overline{\rho}^*(g, v)$ по всем различным представлениям последовательности v.

Очевидно, что для формальной полиномиальной дистанции (ФПД) выполняются свойства (2.1.2) и имеет место неравенство

$$\overline{\rho}(g, v) \geqslant \rho(g, v).$$

Определим функцию $\pi_p(x)$ следующими условиями:

$$\pi_p(x) = \begin{cases} x, & \text{если} \quad x \leqslant p-1, \\ 1 + ((x-1) \bmod (p-1)), & \text{если} \quad x \geqslant p \geqslant 3, \\ 1 + [x \bmod 2], & \text{если} \quad x \geqslant p = 2. \end{cases}$$

ЛЕММА 2.1.1. ***Пусть*** $F(x)$ — ***многочлен максимального периода над кольцом*** $R = \mathbb{Z}_{p^n}$ ***степени*** m, u — ***ЛРПМП из*** $L_R(F)$ ***и*** $A = \sum_{j=r}^{s-2} A_j p^j$, $0 \leqslant A_j < p$, $A_r > 0$. ***Тогда*** s***-я координатная последовательность*** u_s ***удовлетворяет соотношению***

$$(x^{\tau_0} - e)^A u_s = \frac{(-1)^{A+s-r}}{A_r} \prod_{k=0}^{s-2} A_k! \prod_{j=r}^{s-2} u_{j+1}^{p-1-A} u_{r+1} \alpha \oplus \beta, \tag{2.1.5}$$

где последовательность α задается условиями

$$\alpha = \begin{cases} u_0^{(1)\pi_p(A)}, & \text{если} \quad p \geqslant 3 \text{ или } p = 2,\ A = 1, \\ u_0^{(2)}, & \text{если} \quad p = 2,\ A \text{ — четное}, \\ u_0^{(2)} u_0^{(1)}, & \text{если} \quad p = 2,\ A \text{ — нечетное},\ A \geqslant 3, \end{cases}$$

при этом справедливы неравенства

$$\overline{\rho}\left(g, \prod_{j=r}^{s-2} u_{j+1}^{p-1-A} u_{r+1} \alpha\right) = p^s - pA + \pi_p(A), \quad \overline{\rho}(g, \beta) < p^s - pA + \pi_p(A).$$

Доказательство. Пусть $p \geqslant 3$ и k — номер наибольшего ненулевого коэффициента A_t, $t = r, \ldots, s-2$; тогда из определения производных последовательностей ЛРПМП и свойств функции переноса при сложении чисел в p-ичной системе счисления следует

$$(x^{\tau_k} - e)u_s = (-1)^{s-k-1} u_{s-1}^{p-1} u_{s-2}^{p-1} \cdots u_{k+1}^{p-1} u_0^{(1)} \oplus \xi \oplus \eta, \tag{2.1.6}$$

где ξ выражается через $u_0^{(1)}, u_{k+1}, \ldots, u_{s-1}$, а в полиномиальном представлении последовательности η ни одно из слагаемых не может быть выражено только через последовательности $u_0^{(1)}, u_{k+1}, \ldots, u_{s-1}$; при этом

$$\begin{aligned} &\overline{\rho}(g, (x^{\tau_k} - e)u_s) = p^s - p^{k+1} + 1, \\ &\overline{\rho}(g, \xi) \leqslant p^s - 2(p^{k+1} - 1), \\ &\overline{\rho}(g, \eta) \leqslant p^s - p(p^{k+1} - 1). \end{aligned} \tag{2.1.7}$$

Заметим, что при умножении любой последовательности на многочлен $x^{\tau_k} - e$ ее ФПД уменьшается не менее, чем на $p^{k+1} - 1$, а на максимальной ФПД от $g(x)$ в последовательности $(x^{\tau_k} - e)u_{s-1}^{p-1} u_{s-2}^{p-1} \cdots u_{k+1}^{p-1} u_0^{(1)}$ находится единственное слагаемое $(p-1)u_{s-1}^{p-1} u_{s-2}^{p-1} \cdots u_{k+1}^{p-2} u_0^{(1)^2}$. Это выводится из (1.1.14), (2.1.6) и свойств операций поля $\mathbf{GF}(p)$, если для знаков последовательностей $u_{k+1}, \ldots, u_{s-1}$ использовать равенство (2.1.6) в виде

$$u_t(i + \tau_k) = u_t(i) \oplus u_{t-1}^{p-1}(i) u_{t-2}^{p-1}(i) \cdots u_{k+1}^{p-1}(i) u_0^{(1)}(i) \oplus \omega_{t,k}(i), \qquad i \geqslant 0,$$

где $\overline{\rho}(g, \omega_{t,k}) < p^t - p^{k+1} + 1$ для $t = k+1, \ldots, s-1$.

Следовательно,

$$\begin{aligned} (x^{\tau_k} - e)^{A_k} u_s = (-1)^{s-k-1} \prod_{t=1}^{A_k - 1} (p-t) u_{s-1}^{p-1} u_{s-2}^{p-1} \cdots u_{k+1}^{p-A_k} u_0^{(1)^{A_k}} \\ \oplus \xi^{(k)} \oplus \eta^{(k)}, \end{aligned} \tag{2.1.8}$$

где последовательности $\xi^{(k)}$ и $\eta^{(k)}$ получены по тем же правилам, что и последовательности ξ и η в (2.1.6), причем

$$\begin{aligned} &\overline{\rho}\left(g, u_{s-1}^{p-1} u_{s-2}^{p-1} \cdots u_{k+1}^{p-A_k} u_0^{(1)^{A_k}}\right) = p^s - A_k(p^{k+1} - 1), \\ &\overline{\rho}\left(g, \xi^{(k)}\right) \leqslant p^s - (A_k + 1)(p^{k+1} - 1), \\ &\overline{\rho}\left(g, \eta^{(k)}\right) \leqslant p^s - A_k(p^{k+1} - 1) - (p-1)(p^{k+1} - 1). \end{aligned} \tag{2.1.9}$$

Пусть $A_{k-1} = \cdots = A_{l+1} = 0$, $A_l > 0$, $k > l$. Тогда, умножая (2.1.8) последовательно на многочлены $x^{\tau_l} - e$, получаем

$$\begin{aligned}(x^{\tau_k} - e)^{A_k}(x^{\tau_l} - e)^{A_l} u_s = (-1)^{s-l-1} \prod_{t=1}^{A_k}(p-t) \prod_{t=1}^{A_l - 1}(p-t) \\ \times u_{s-1}^{p-1} \cdots u_{k+1}^{p-A_k-1} u_k^{p-1} \cdots u_{l+1}^{p-A_l} u_0^{(1)^{A_k+A_l}} \\ \oplus \xi^{(l)} \oplus \eta^{(l)},\end{aligned} \tag{2.1.10}$$

где $\xi^{(l)}$ выражается через $u_0^{(1)}, u_{l+1}, \ldots, u_{s-1}$, а в полиномиальном представлении последовательности $\eta^{(l)}$ ни одно из слагаемых не может быть выражено только через последовательности $u_0^{(1)}, u_{l+1}, \ldots, u_{s-1}$, причем

$$\begin{aligned}&\overline{\rho}\big(g, u_{s-1}^{p-1} \cdots u_{k+1}^{p-A_k-1} u_k^{p-1} \cdots u_{l+1}^{p-A_l} u_0^{(1)^{A_k+A_l}}\big) \\ &\qquad = p^s - A_k p^{k+1} - A_l p^{l+1} + \pi_p(A_k + A_l), \\ &\overline{\rho}\big(g, \xi^{(l)}\big) \leqslant p^s - A_k p^{k+1} - A_l p^{l+1} + \pi_p(A_k + A_l + 1) - p^{l+1}, \\ &\overline{\rho}\big(g, \eta^{(l)}\big) \leqslant p^s - A_k p^{k+1} - A_l p^{l+1} - (p-1)(p^{l+1} - 1) + \pi_p(A_k + A_l - 1).\end{aligned} \tag{2.1.11}$$

Продолжая аналогичную процедуру, в случае $p \geqslant 3$ приходим к окончательному выражению

$$\begin{aligned}(x^{\tau_0} - e)^A u_s = (-1)^{s-r-1} \frac{1}{p - A_r} \prod_{\substack{k=r \\ A_k \neq 0}}^{s-2} \prod_{t=1}^{A_k}(p-t) \\ \times \prod_{j=r}^{s-2} u_{j+1}^{p-1-A_j} u_{r+1} (u_0^{(1)})^{\pi_p(A)} \oplus \xi^{(r)} \oplus \eta^{(r)},\end{aligned} \tag{2.1.12}$$

при этом

$$\begin{aligned}&\overline{\rho}\Big(g, \prod_{j=r}^{s-2} u_{j+1}^{p-1-A_j} u_{r+1} (u_0^{(1)})^{\pi_p(A)}\Big) = p^s - pA + \pi_p(A), \\ &\overline{\rho}\big(g, \xi^{(r)}\big) \leqslant p^s - pA + \pi_p(A+1) - p^{r+1}, \\ &\overline{\rho}\big(g, \eta^{(r)}\big) \leqslant p^s - pA + \pi_p(A-1) - (p-1)(p^{r+1} - 1).\end{aligned} \tag{2.1.13}$$

Для доказательства леммы в этом случае остается заметить, что при любом $r = 0, \ldots, s-2$ справедливы неравенства

$$\pi_p(A-1) - (p-1)(p^{r+1} - 1) < \pi_p(A), \quad \pi_p(A+1) - p^{r+1} < \pi_p(A). \tag{2.1.14}$$

Первое неравенство вытекает из условий

$$\pi_p(A-1) - \pi_p(A) < p - 1 < (p-1)(p^{r+1} - 1),$$

а второе — из условий

$$\pi_p(A+1) - \pi_p(A) \leqslant 1 < p^{r+1}.$$

Заметим, что при $p = 2$ в силу свойств функции переноса в двоичной системе счисления последовательности $\xi^{(t)}$, $t = 0, \dots, s-1$, равны нулю. С учетом этого замечания доказательство соотношения (2.1.5) при $p = 2$ для четных значений A полностью повторяет разобранный случай $p \geqslant 3$ с заменой $u_0^{(1)}$ на $u_0^{(2)}$. Рассмотрим случай $p = 2$, A — нечетное число. Для четного числа $A' = A - 1$ справедливо равенство (2.1.12) с заменой $u_0^{(1)}$ на $u_0^{(2)}$, если $A' \neq 0$, и равенство (2.1.6), если $A' = 0$. Если $A' = 0$, то (2.1.5) следует непосредственно из (2.1.6). Если $A' \neq 0$, то, умножая обе части (2.1.12) на $x^{\tau_0} - e$ и учитывая, что $u_0^{(1)} \neq u_0^{(2)}$ при $p = 2$, приходим к равенству

$$(x^{\tau_0} - e)^A u_s = \prod_{j=0}^{s-2} u_{j+1}^{p-1-A_j} u_1 (u_0^{(2)})^{\pi_p(A')} u_0^{(1)} \oplus \eta^{(0)},$$

и в силу (2.1.13) получаем

$$\begin{aligned} \overline{\rho}\Big(g, \prod_{j=1}^{s-2} u_{j+1}^{p-1-A_j} u_1 \big(u_0^{(2)}\big)^{\pi_p(A')} u_0^{(1)}\Big) &= p^s - pA' + \pi_p(A') - 1 \\ &= p^s - pA + \pi_p(A), \\ \overline{\rho}\big(g, \eta^{(0)}\big) &\leqslant p^s - pA' + \pi_p(A' - 1) - (p-1)(p^{r+1} - 1) - 1. \end{aligned}$$

Справедливость неравенств

$$\overline{\rho}\big(g, \eta^{(0)}\big) < p^s - pA + \pi_p(A)$$

для A вытекает из неравенств (2.1.14) для A'.

Теперь (2.1.5) следует из равенств

$$\prod_{\substack{k=r \\ A_k \neq 0}}^{s-2} \prod_{t=1}^{A_k} (p-t) \frac{1}{p - A_r} = \prod_{k=0}^{s-2} (-1)^{A_k} A_k! (-A_r)^{-1} = \frac{(-1)^{A-1}}{A_r} \prod_{k=0}^{s-2} A_k!.$$

Лемма доказана.

ТЕОРЕМА 2.1.2. *Пусть $F(x)$ — многочлен максимального периода над кольцом $R = \mathbb{Z}_{p^n}$ степени m, и — ЛРПМП из $L_R(F)$. Тогда для рангов координатных последовательностей u_s, $s = 0, \dots, n-1$, выполняются неравенства*

$$\operatorname{rank} u_s \leqslant \sum_{k=0}^{p^{s-1}} (1+k) \sum_{t=d_0(k),\, t \in V}^{d_1(k)} \binom{t}{m}, \tag{2.1.15}$$

где $V = \{n \in \mathbb{N}\colon n \equiv 0 \pmod{p-1}$ или $n \equiv 1 \pmod 2\}$,

$$d_1(k) = p^s - pk + \pi_p(k), \quad d_0(k) = p^s - p(k+1) + \pi_p(k+1) + 1.$$

Доказательство. Из (1.1.14) следует, что для $s = 1, \dots, n-1$, $A = 1, \dots, p^{s-1}$ минимальный многочлен последовательности $(x^{\tau_0} - e)^A u_s$ имеет вид

$$g(x)^{p^{s-1}+1-A} g_{s,1}(x)^{p^{s-1}-A} \cdots g_{s,p^{s-1}-A}(x). \tag{2.1.16}$$

С другой стороны, из неравенства

$$\overline{\rho}(g,(x^{\tau_0}-e)^A u_s) \leqslant p^s - pA + \pi_p(A) \tag{2.1.17}$$

вытекает, что элементы поля $\mathbf{GF}(p^m)$ вида $\overline{\theta}^{\sum_{j=0}^{m-1} i_j p^j}$,

$$\sum_{j=0}^{m-1} i_j > p^s - pA + \pi_p(A), \qquad 0 \leqslant i_j < p,$$

не являются корнями минимального многочлена последовательности $(x^{\tau_0} - e)^A u_s$. Поэтому если элемент $\overline{\theta}^{\sum_{j=0}^{m-1} i_j p^j}$, $\sum_{j=0}^{m-1} i_j = d$, является корнем многочлена $\mu_s(x)$, то его кратность не больше $k+1$, где k — наибольшее целое число, удовлетворяющее условию $d \leqslant p^s - pk + \pi_p(k)$. Используя введенные в формулировке теоремы обозначения, получаем верхние оценки рангов координатных последовательностей ЛРП u:

$$\operatorname{rank} u_s \leqslant \sum_{k=0}^{p^{s-1}} (1+k) \sum_{t=d_0(k)}^{d_1(k)} \binom{t}{m}. \tag{2.1.18}$$

В [4] показано, что при $p \geqslant 5$ корни многочленов $\mu_s(x)$, $s = 0, \ldots, n-1$, являются решениями уравнения

$$(x^{\tau_0/2} \oplus e)(x^{\tau_0/(p-1)} \ominus e) = 0.$$

Элемент $\overline{\theta}^{\sum_{j=0}^{m-1} i_j p^j}$, $\sum_{j=0}^{m-1} i_j = d$, $0 \leqslant i_j < p$, удовлетворяет уравнению $x^{\tau_0/(p-1)} \ominus e = 0$ в том и только том случае, когда $d \equiv 0 \pmod{(p-1)}$, а уравнению $x^{\tau_0/2} \oplus e = 0$ — в том и только том случае, когда $d \not\equiv 0 \pmod 2$. Следовательно, при $p \geqslant 5$ верхняя оценка ранга координатных последовательностей ЛРПММП u может быть уточнена за счет отбрасывания в (2.1.18) слагаемых, соответствующим тем значениям t, вычеты которых по модулю $p-1$ принадлежат множеству $\{2, 4, \ldots, p-3\}$.

Следствие 2.1.3. *В условиях теоремы* 2.1.2 *для* $s = 1, \ldots, n-1$ *многочлены* $g_{s,j}(x)$, $j = 1, \ldots, p^{s-1}$, *из разложения* (1.2.1) *минимального многочлена* $\mu_s(x)$ *s-й координатной последовательности ЛРПММП и удовлетворяют условиям*

$$\overline{\rho}(g, g_{s,j}) \leqslant p^s - kp + \pi_p(k), \qquad k + j = p^{s-1}. \tag{2.1.19}$$

Этот факт является очевидным следствием (2.1.16), (2.1.17).

2.2. Нижние оценки рангов. Уточнения для классов многочленов. Рассмотренный подход позволяет не только дать нетривиальные верхние оценки рангов координатных последовательностей ЛРПММП над примарными кольцами вычетов, но и уточнить нижние оценки рангов, полученные в § 1.

В [7], [21] для некоторых классов многочленов максимального периода над R получены нижние оценки рангов координатных последовательностей

ЛРПМП, улучшающие (1.2.18). Из этих результатов следует, что возможность улучшения оценок рангов зависит от свойств конкретных многочленов максимального периода, в частности, от свойств многочленов $\Phi^{(s)}(x)$, $s = 1, 2$.

Пусть $F(x)$ — многочлен максимального периода степени m над кольцом $R = \mathbb{Z}_{p^n}$; u — ЛРПМП из $L_R(F)$; $\overline{\theta}$ — корень многочлена $g(x) \equiv F(x) \pmod p$ в его поле разложения $\mathbf{GF}(p^m)$.

Лемма 2.2.1. *Пусть u есть ЛРПМП из $L_R(F)$ и $p^r \leqslant m(p-1)$. Тогда последовательность*

$$v = \prod_{t=0}^{r-1} u_t^{\alpha}, \qquad 0 \leqslant \alpha_t \leqslant p-1, \quad t = 0, \ldots, n-1, \quad r < n,$$

удовлетворяет равенству

$$v(i) = \prod_{t=0}^{r-1} \alpha_t!\, w_m^{(k)}\bigl(a\overline{\theta}^i, \ldots, (a\overline{\theta}^i)^{p^{m-1}}\bigr) \oplus \xi(i), \qquad i \geqslant 0,$$

где $k = \sum_{t=0}^{r-1} \alpha_t p^t$, $\rho(g, \xi) < k$.

Доказательство. Из теоремы 1.2.5 следует, что знаки ЛРП u_t могут быть представлены в виде

$$u_t(i) = w_m^{(p_t)}\bigl(a\overline{\theta}^i, \ldots, (a\overline{\theta}^i)^{p^{m-1}}\bigr) \oplus \lambda_t(i), \qquad i \geqslant 0, \tag{2.2.1}$$

где $\overline{\rho}(g, \lambda_t) < p^t$.

Из определения $w_m^{(K)}(x_1, \ldots, x_m)$ вытекает, что в этом многочлене коэффициент при $x_1^{s_1} \cdots x_m^{s_m}$, $s_1 + \cdots + s_m = K$, $0 \leqslant s_j < p$, сравним по модулю p с деленным на $K!$ коэффициентом при $x_1^{s_1} \cdots x_m^{s_m}$, $s_1 + \cdots + s_m = K$, целочисленного полинома $(x_1 + \cdots + x_m)^K$. Отсюда несложно получить, что произведение полиномов $w_m^{(K)}(x_1, \ldots, x_m)$ и $w_m^{(L)}(x_1, \ldots, x_m)$ представляется в виде

$$w_m^{(K)}(x_1, \ldots, x_m) w_m^{(L)}(x_1, \ldots, x_m) = c w_m^{(K+L)}(x_1, \ldots, x_m) \oplus \eta_{K+L}(x_1, \ldots, x_m),$$

где степень полинома $\eta_{K+L}(x_1, \ldots, x_m)$ строго меньше $K + L$, а коэффициент c определяется сравнением

$$c \equiv \frac{(K+L)!}{K!\, L!} \pmod p.$$

Следовательно, в силу теоремы Люка [25] выполняются соотношения

$$w_m^{(p^t)}(x_1, \ldots, x_m)^{\alpha_t} \equiv a_t!\, w_m^{(\alpha_t p^t)}(x_1, \ldots, x_m) \oplus \eta_{\alpha_t p^t}(x_1, \ldots, x_m),$$

где $\deg \eta_{\alpha_t p^t}(x_1, \ldots, x_m) < \alpha_t p^t$, и

$$\prod_{t=0}^{r-1} w_m^{(p^t)}(x_1, \ldots, x_m)^{\alpha_t} \equiv \prod_{t=0}^{r-1} \alpha_t!\, w_m^{(k)}(x_1, \ldots, x_m) \oplus \eta_k(x_1, \ldots, x_m), \tag{2.2.2}$$

где $k = \sum_{t=0}^{r-1} \alpha_t p^t$, $\deg \eta_k(x_1, \ldots, x_m) < k$.

Легко видеть, что лемма 2.2.1 является непосредственным следствием (2.2.1) и (2.2.2), причем в силу условия $p^r \leqslant m(p-1)$ значения полиномиальной дистанции и формальной полиномиальной дистанции от многочлена $g(x)$ до последовательности v совпадают. Лемма доказана.

Для $s = 1, \ldots, n-1$ обозначим через $\overline{\Phi^{(s)}(x)}$ вычет многочлена $\Phi^{(s)}(x)$ по модулю p и положим $\varkappa_s = \overline{\Phi^{(s)}(\overline{\theta})}$. Будем говорить, что натуральное число k принадлежит множеству $I_p^*(m, L)$, если $k = k_0 + k_1 p + \cdots + k_{m-1}p^{m-1}$, $k_j \in \{0, 1, \ldots, p-1\}$, и $(k_0, k_1, \ldots, k_{m-1}) \in I_p(m, L)$.

ТЕОРЕМА 2.2.2. *Если и есть ЛРПМП из $L_R(F)$, $\deg F(x) = m$, $\overline{\theta}$ — корень многочлена $g(x) \equiv F(x) \pmod p$ в его поле разложения $\mathbf{GF}(p^m)$, то корнями многочлена $g_{s,t}(x)$ из разложения (1.2.1) минимального многочлена $\mu_s(x)$ координатной последовательности u_s являются все элементы поля $\mathbf{GF}(p^m)$ вида*

$$\overline{\theta}^{\sum_{j=0}^{m-1} r_j p^j}, \qquad 0 \leqslant r_j < p, \quad \sum_{j=0}^{m-1} r_j = p^s - pk + \pi_p(k) \leqslant m(p-1), \quad k = p^{s-1} - t, \tag{2.2.3}$$

удовлетворяющие условиям

$$\sum_{(j_0,\ldots,j_{m-1}) \in I_p(m, \pi_p(k))} \prod_{t=0}^{m-1} \binom{r_t}{j_t} \varkappa_1^{\sum_{s=0}^{m-1} j_s p^s} \neq 0, \text{ если } p \geqslant 3 \text{ или } p = 2, \ k = 1,$$

$$\sum_{0 \leqslant s < m} r_s \varkappa_2^{p^s} \neq 0, \quad \text{если} \quad p = 2, \ k_0 \equiv 0 \pmod p,$$

$$\sum_{\substack{0 \leqslant j,\, l < m \\ j \neq l}} r_j r_l \varkappa_1^{2^l} \varkappa_1^{2^{j+1}} \neq 0, \quad \text{если} \quad p = 2, \ k \geqslant 3, \ k \equiv 1 \pmod p.$$

Доказательство. Пусть $p \geqslant 3$. Из леммы 2.1.1 следует, что последовательность $w_{s,k}$, задаваемая условиями

$$w_{s,k} = (x^{\tau_0} - \epsilon)^k u_s, \qquad s = 1, \ldots, n-1,$$
$$k = \sum_{t=r}^{s-2} k_t p^t, \qquad 0 \leqslant k_t < p, \quad t = r, \ldots, s-2, \quad k_r > 0,$$

представляется в виде

$$w_{s,k} = \frac{(-1)^{k+s-r}}{k_r} \prod_{l=0}^{s-2} k_l! \prod_{j=r}^{s-2} u_{j+1}^{p-1-k_j} u_{r+1} u_0^{(1)^q} \oplus \beta, \tag{2.2.4}$$

где $q = \pi_p(k)$, $\overline{\rho}(g, \beta) < p^s - pk + \pi_p(k)$.

Применим лемму 2.2.1, положив $\alpha_{t+1} = p - 1 - k_t$ для $t = r+1, \ldots, s-2$ и $\alpha_{r+1} = p - k_r$. Тогда из (2.2.4) получаем

$$w_{s,k}(i) = (-1)^{k+s-r} {k_r}^{-1} \prod_{l=0}^{s-2} k_l! \prod_{t=r}^{s-2} (p-1-k_t)!\,(p-k_r)$$
$$\times\, w_m^{(L)}\big(a\overline{\theta}^i, \ldots, (a\overline{\theta}^i)^{p^{m-1}}\big)\big(u_0^{(1)}(i)\big)^q \oplus \beta', \qquad i \geqslant 0, \tag{2.2.5}$$

где

$$L=\sum_{t=r+1}^{s-2}p^t\alpha_t=\sum_{t=r}^{s-2}p^{t+1}(p-1-k_t)+p^{r+1}=p^s-pk,\qquad \overline{\rho}(g,\beta')<p^s-pk.$$

Так как справедливы сравнения

$$\begin{aligned}k!\,(p-1-k)!&\equiv(-1)^k(p-1)(p-2)\times\cdots\times(p-k)(p-1-k)!\\&\equiv(-1)^k(p-1)!\equiv(-1)^{k+1}\pmod p,\end{aligned}$$

то из (2.2.5) следует соотношение

$$w_{s,k}(i)=w_m^{(L)}\bigl(a\overline{\theta}^i,\dots,(a\overline{\theta}^i)^{p^{m-1}}\bigr)\bigl(u_0^{(1)}(i)\bigr)^q\oplus\beta',\qquad i\geqslant 0. \tag{2.2.6}$$

Последовательность $w_{s,k}$ может быть однозначно представлена в виде суммы двух последовательностей λ_1 и λ_2 со свойствами:

- все неприводимые делители минимального многочлена последовательности λ_1 находятся на полиномиальной дистанции $d_1(k)=p^s-pk+\pi_p(k)$ от многочлена $g(x)$;
- полиномиальная дистанция от $g(x)$ до последовательности λ_2 строго меньше $d_1(k)$.

При $i\geqslant 0$ знаки ЛРП $u_0^{(1)^q}$ удовлетворяют равенству

$$u_0^{(1)}(i)^q=\bigl(\mathrm{tr}_m(a\varkappa_1\overline{\theta}^i)\bigr)^q=\sum_{(j_0,\dots,j_{m-1})\in I_p(m,q)}\frac{q!}{j_0!\cdots j_{m-1}!}(a\varkappa_1\overline{\theta}^i)^{\sum_{s=0}^{m-1}j_sp^s},$$

где $\mathrm{tr}_m(x)=x\oplus x^p\oplus\cdots\oplus x^{p^{m-1}}$ — функция следа из поля $\mathbf{GF}(p^m)$ в поле $\mathbf{GF}(p)$, поэтому из (2.2.6) получаем

$$\begin{aligned}\lambda_1(i)&=\sum_{\substack{i\in I_p^*(m,L)\\ j\in I_p^*(m,q)\\ i_s+j_s<p,\ s=0,\dots,m-1}}\frac{q!\,(a\overline{\theta}^i)^{\sum_{s=0}^{m-1}(i_s+j_s)p^s}}{i_0!\cdots i_{m-1}!\,j_0!\cdots j_{m-1}!}\varkappa_1^{\sum_{s=0}^{m-1}j_sp^s}\\&=\sum_{r\in I_p^*(m,d_1(k))}\frac{q!\,(a\overline{\theta}^i)^{\sum_{s=0}^{m-1}r_sp^s}}{r_0!\cdots r_{m-1}!}\sum_{j\in I_p^*(m,q)}\prod_{t=0}^{m-1}\binom{r_t}{j_t}\varkappa_1^{\sum_{s=0}^{m-1}j_sp^s}.\end{aligned} \tag{2.2.7}$$

Отсюда вытекает, что элемент $\overline{\theta}^r$, $r\in I_p^*(m,d_1(k))$, $d_1(k)\leqslant m(p-1)$, является корнем минимального многочлена ЛРП $w_{s,k}$ в том и только том случае, когда

$$\sum_{j\in I_p^*(m,q)}\prod_{t=0}^{m-1}\binom{r_t}{j_t}\varkappa_1^{\sum_{s=0}^{m-1}j_sp^s}\neq 0. \tag{2.2.8}$$

Из условия $d_1(k)\leqslant m(p-1)$ следует, что для последовательности λ_1 значения полиномиальной дистанции и формальной полиномиальной дистанции совпадают. По определению ЛРП λ_1 ее минимальный многочлен взаимно прост с минимальным многочленом последовательности λ_2. Поэтому (2.2.8) задает условия, при которых $\overline{\theta}^r$, $r\in I_p^*(m,d_1(k))$, $d_1(k)\leqslant m(p-1)$, является корнем

$\mu_s(x)$. Остается заметить, что из (2.2.7) следует, что $\overline{\theta}^r$, $r \in I_p^*(m, d_1(k))$, является простым корнем минимального многочлена ЛРП $w_{s,k}$, т.е. $\overline{\theta}^r$, $r \in I_p^*(m, d_1(k))$, есть корень многочлена $g_{s,j}(x)$, где $j = p^{s-1} - k$.

Пусть $p = 2$. Если $k = 1$, то доказательство условий (2.2.3) полностью совпадает с разобранным выше случаем. Если k — четное число, то доказательство условий (2.2.3) повторяет рассуждения в случае $p \geqslant 3$ с заменой последовательности $u_0^{(1)}$ на $u_0^{(2)}$ и параметра $\varkappa_1$ на $\varkappa_2$. В этом случае (2.2.8) приобретает более простой вид

$$\sum_{0 \leqslant s < m} r_s \varkappa_2^{p^s} \neq 0. \tag{2.2.9}$$

Если k — нечетное число, $k \geqslant 3$, то, согласно лемме 2.2.1, последовательность $w_{s,k}$ удовлетворяет равенству

$$w_{s,k} = u_0^{(1)} u_0^{(2)} u_1 \prod_{j=1}^{s-2} u_{j+1}^{1-k_j} \oplus \beta,$$

где $k = \sum_{t=0}^{s-2} k_t 2^t$, $0 \leqslant k_t \leqslant 1$, $t = 1, \ldots, s-2$, $k_0 = 1$,

$$\overline{\rho}(g, \beta) < d_1(k) = 2^s - 2k + \pi_2(k).$$

Представим последовательность $w_{s,k}$ в виде суммы двух последовательностей λ_1 и λ_2 со свойствами:

- все неприводимые делители минимального многочлена ЛРП λ_1 находятся на полиномиальной дистанции $d_1(k) = 2^s - 2k + \pi_2(k)$ от многочлена $g(x)$;
- $\overline{\rho}(g, \lambda_2) < d_1(k)$.

В силу свойств ЛРППМП над $\mathbb{Z}_{2^n}$ (см. [9]) для $i \geqslant 0$ справедливы соотношения

$$u_0^{(1)}(i) = \mathrm{tr}_m(a\varkappa_1 \overline{\theta}^i), \quad u_0^{(2)}(i) = \mathrm{tr}_m\big(a(\varkappa_1 \oplus \varkappa_1^2)\overline{\theta}^i\big),$$

откуда с учетом леммы 2.2.1 следует

$$\lambda_1(i) = \sum_{r \in I_2^*(m, d_1(k))} (a\overline{\theta}^i)^{\sum_{s=0}^{m-1} r_s p^s} \sum_{\substack{0 \leqslant j, l < m \\ j \neq l}} r_j r_l \varkappa_1^{2^l} (\varkappa_1 \oplus \varkappa_1^2)^{2^j}. \tag{2.2.10}$$

Следовательно, элемент $\overline{\theta}^r$, $r \in I_2^*(m, d_1(k))$, $d_1(k) \leqslant m$, является корнем минимального многочлена ЛРП λ_1 тогда и только тогда, когда

$$\sum_{\substack{0 \leqslant j, l < m \\ j \neq l}} r_j r_l \varkappa_1^{2^l} (\varkappa_1 \oplus \varkappa_1^2)^{2^j} = \sum_{\substack{0 \leqslant j, l < m \\ j \neq l}} r_j r_l \varkappa_1^{2^l} \varkappa_1^{2^{j+1}} \neq 0. \tag{2.2.11}$$

Как и в случае $p \geqslant 3$, справедливы замечания о взаимной простоте минимальных многочленов последовательностей λ_1 и λ_2, а также о кратности корня $\overline{\theta}^r$, $r \in I_2^*(m, d_1(k))$, $d_1(k) \leqslant m$, минимального многочлена ЛРП λ_1. Таким образом, при выполнении условия (2.2.11) элемент $\overline{\theta}^r$, $r \in I_2^*(m, d_1(k))$, $d_1(k) \leqslant m$, является корнем многочлена $g_{s, p^{s-1}-k}(x)$. Теорема доказана.

Доказанная теорема дает возможность для некоторых классов многочленов максимального периода над кольцом $\mathbb{Z}_{p^n}$ описать часть корней минимальных многочленов координатных последовательностей ЛРПМП из $L_R(F)$ и уточнить нижние оценки их рангов.

Будем говорить, что многочлен $F(x)$ максимального периода над кольцом $R = \mathbb{Z}_{p^n}$ удовлетворяет $\{s,t\}$-условию, если степень минимального многочлена над полем $\mathbf{GF}(p)$ элемента $\varkappa_s$ равна t, и $\{s,*\}$-условию, если элементы $\varkappa_s, \varkappa_s^p, \ldots, \varkappa_s^{p^{m-1}}$ линейно независимы над полем $\mathbf{GF}(p)$. Отметим, что выполнение $\{s,*\}$-условия автоматически влечет выполнение $\{s,m\}$-условия. В [9] описан способ построения многочленов максимального периода над примарными кольцами вычетов, удовлетворяющих $\{s,t\}$-условию и $\{s,*\}$-условию.

Утверждение 2.2.3. *Если $F(x)$ — многочлен максимального периода степени m над кольцом $R = \mathbb{Z}_{p^n}$, удовлетворяющий $\{2,1\}$-условию, то для рангов координатных последовательностей u_s, $s = 1, \ldots, n-1$, ЛРПМП и из $L_R(F)$ справедливы неравенства:*

$$\begin{aligned} \operatorname{rank} u_s &\geqslant \sum_{k=0}^{p^{s-1}} (1+k) \left\{ \begin{matrix} d_1(k) \\ m \end{matrix} \right\} \quad \textit{при} \quad p \geqslant 3, \\ \operatorname{rank} u_s &\geqslant \sum_{\substack{k=0 \\ 2 \mid k}}^{2^{s-1}} (1+k) \left\{ \begin{matrix} d_1(k) \\ m \end{matrix} \right\} \quad \textit{при} \quad p = 2, \end{aligned} \tag{2.2.12}$$

где $d_1(k) = p^s - pk + \pi_p(k)$.

Доказательство. Выполнение $\{2,1\}$-условия означает, что параметр $\varkappa_2$ многочлена $F(x)$ является ненулевым элементом поля $\mathbf{GF}(p)$. Поэтому (см., например, [11]) последовательности $u_0^{(2)}$ и u_0 связаны соотношением $u_0^{(2)} = \varkappa_2 u_0$ (напомним, что $\varkappa_1 = \varkappa_2$ для $p \geqslant 3$). Следовательно, в случаях, когда $p \geqslant 3$ или $p = 2$ и A — четное число, равенство (2.1.5) из леммы 2.1.1 может быть записано в виде

$$(x^{\tau_0} - e)^A u_s = c \prod_{j=r}^{s-2} u_{j+1}^{p-1-A_j} u_{\tau+1} u_0^{\pi_p(A)} \oplus \beta,$$

где $\overline{\rho}(g,\beta) < d_1(A)$, а ненулевой коэффициент c имеет вид

$$c = \varkappa_2^{\pi_p(A)} \frac{(-1)^{A+s-\tau}}{A_\tau} \prod_{k=0}^{s-2} A_k!.$$

Отсюда, с учетом леммы 2.2.1 и теоремы 2.2.2, получаем, что корнями многочлена $g_{s,p^{s-1}-k}(x)$ являются все элементы $\overline{\theta}^\tau$, $\tau \in I_p^*(m, d_1(k))$, $d_1(k) \leqslant m(p-1)$, и указанные в формулировке утверждения оценки рангов координатных последовательностей ЛРПМП и вытекают непосредственно из разложения (1.2.1) многочленов $\mu_s(x)$, $s = 1, \ldots, n-1$.

Теорема 2.2.4. *Если $F(x)$ — многочлен максимального периода степени m над кольцом $R = \mathbb{Z}_{p^n}$, удовлетворяющий $\{1,*\}$-условию, то для рангов*

координатных последовательностей u_s, $s = 1, \dots, n-1$, *ЛРПМП* u *из* $L_R(F)$ *справедливы неравенства:*

$$\begin{aligned} \operatorname{rank} u_s &\geqslant \sum_{\substack{k=0 \\ \pi_p(k)=1}}^{p^{s-1}} (1+k)\left\{ \begin{matrix} d_1(k) \\ m \end{matrix} \right\} \quad \textit{при} \quad p \geqslant 3, \\ \operatorname{rank} u_s &\geqslant \sum_{\substack{k=0 \\ 2 \mid k,\ \pi_p(k) < m}}^{2^{s-1}} (1+k)\left\{ \begin{matrix} d_1(k) \\ m \end{matrix} \right\} + 2\left\{ \begin{matrix} 2^s-1 \\ m \end{matrix} \right\} \quad \textit{при} \quad p = 2, \end{aligned} \tag{2.2.13}$$

где $d_1(k) = p^s - pk + \pi_p(k)$.

Доказательство. Пусть $p \geqslant 3$ и k удовлетворяет условиям $d_1(k) = p^s - pk + \pi_p(k) \leqslant m(p-1)$, $\pi_p(k) = 1$. Тогда $I_p^*(m, \pi_p(k)) = I_p^*(m, 1)$, и в силу теоремы 2.2.2 элемент $\overline{\theta}^r$, $r \in I_p^*(m, d_1(k))$, является корнем многочлена $g_{s,p^{s-1}-k}(x)$ в том и только том случае, когда

$$\sum_{0 \leqslant s < m} r_s \varkappa_1^{p^s} \neq 0. \tag{2.2.14}$$

Справедливость (2.2.14) для произвольного $r \in I_p^*(m, d_1(k))$ следует из линейной независимости над $\mathbf{GF}(p)$ элементов $\varkappa_1, \varkappa_1^p, \dots, \varkappa_1^{p^{m-1}}$ ($\{1, *\}$-условие).

Пусть $p = 2$ и k — четное число, $d_1(k) = 2^s - 2k + 1 < m$. Тогда в силу теоремы 2.2.2 элемент $\overline{\theta}^r$, $r \in I_2^*(m, d_1(k))$, является корнем многочлена $g_{s,2^{s-1}-k}(x)$ в том и только том случае, когда

$$\sum_{0 \leqslant s, m} r_s \varkappa_2^{2^s} \neq 0. \tag{2.2.15}$$

По определению имеем $\varkappa_2 = \varkappa_1 \oplus \varkappa_1^2$. Подставляя выражение $\varkappa_2$ через $\varkappa_1$ в (2.2.15), получаем

$$\sum_{0 \leqslant s < m} r_s \varkappa_2^{2^s} = \sum_{0 \leqslant s < m} r_s (\varkappa_1^{2^s} \oplus \varkappa_1^{2^{s+1}}).$$

Так как $d_1(k) = 2^s - 2k + 1 < m$, то в силу линейной независимости над $\mathbf{GF}(2)$ элементов $\varkappa_1, \varkappa_1^2, \dots, \varkappa_1^{2^{m-1}}$ условие (2.2.15) выполняется для всех $r \in I_2^*(m, d_1(k))$.

Если $p = 2$, $k = 1$, то в силу теоремы 2.2.2 элемент $\overline{\theta}^r$, $r \in I_2^*(m, 2^s - 1)$, $2^s - 1 \leqslant m$, является корнем многочлена $g_{s,2^{s-1}-1}(x)$ в том и только том случае, когда

$$\sum_{0 \leqslant s < m} r_s \varkappa_1^{2^s} \neq 0. \tag{2.2.16}$$

Из $\{1, *\}$-условия следует, что (2.2.16) выполняется для всех $r \in I_2^*(m, 2^s - 1)$.

Таким образом, описана часть корней многочленов $g_{s,k}(x)$, $k = 1, \dots, p^{s-1}$, и оценки рангов координатных последовательностей ЛРПМП u, приведенные в формулировке теоремы, вытекают непосредственно из разложения (1.2.1) многочленов $\mu_s(x)$, $s = 1, \dots, n-1$. Теорема доказана.

Утверждение 2.2.3 и теорема 2.2.4 усиливают результаты работ [7], [21] для тех же классов многочленов максимального периода (оценки из работ [7], [21] получаются, если в (2.2.12) и (2.2.13) суммирование проводить только по значениям $k = p^t$, $t = 1, \dots, s-1$). Качественно новый подход к получению нижних оценок рангов координатных последовательностей ЛРПМП дает следующая теорема.

ТЕОРЕМА 2.2.5. *Если $F(x)$ — многочлен максимального периода степени m над кольцом $R = \mathbb{Z}_{p^n}$, удовлетворяющий $\{2, h\}$-условию, $h > p$, то для рангов координатных последовательностей u_s, $s = 1, \dots, n-1$, ЛРПМП и из $L_R(F)$ справедливы неравенства:*

$$\operatorname{rank} u_s \geqslant m(p^{s-1}+1) + \left\{ {p^s \atop m} \right\} + \frac{h-p}{h} \sum_{\substack{k=1 \\ \pi_p(k)=1}}^{p^{s-1}-1} (1+k) \left(\left\{ {d_1(k) \atop m} \right\} - \delta_k \right), \quad (2.2.17)$$

где $d_1(k) = p^s - pk + \pi_p(k) \leqslant m(p-1)$,

$$\delta_k = \begin{cases} 1, & \text{если} \quad m \mid d_1(k),\ \operatorname{tr}_m(\varkappa_2) = 0, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Доказательство. Основная идея доказательства заключается в разбиении элементов поля $\mathbf{GF}(p^m)$ на подмножества таким образом, чтобы в каждом из этих подмножеств присутствовало определенное число корней минимального многочлена $\mu_s(x)$, $s = 1, \dots, n-1$.

Пусть $p \geqslant 3$ и k удовлетворяет условиям $\pi_p(k) = 1$, $d_1(k) = p^s - pk + \pi_p(k) \leqslant m(p-1)$, или $p = 2$ и k — четное число, $d_1(k) = 2^s - 2k + 1 \leqslant m$; тогда в силу теоремы 2.2.2 элемент $\overline{\theta}^r$, $r \in I_p^*(m, d_1(k))$, является корнем многочлена $g_{s,p^{s-1}-k}(x)$ в том и только том случае, когда

$$\sum_{0 \leqslant s < m} r_s \varkappa_2^{p^s} \neq 0, \quad r = \sum_{s=0}^{m-1} r_s p^s, \qquad 0 \leqslant r_s < p \qquad (2.2.18)$$

(при $p \geqslant 3$ имеет место равенство $\varkappa_1 = \varkappa_2$).

Оценим общее число корней многочлена $g_{s,p^{s-1}-k}(x)$ в множестве $\mathfrak{B}_k = \{\overline{\theta}^r,\ r \in I_p^*(m, d_1(k))\}$, не определяя в явном виде, какие конкретно элементы множества $\mathfrak{B}_k$ — корни $g_{s,p^{s-1}-k}(x)$. Для этого достаточно оценить сверху число линеаризованных многочленов

$$M_r(x) = \sum_{s=0}^{m-1} r_s x^{p^s}, \qquad r = \sum_{s=0}^{m-1} r_s p^s \in I_p^*\big(m, d_1(k)\big),$$

корнем которых является $\varkappa_2$.

Будем говорить, что многочлен $M_r(x)$ построен по значению r или по вектору $\overline{r} = (r_0, r_1, \dots, r_{m-1})$.

Если многочлен $M_r(x)$ построен по вектору $\overline{r} = (a, a, \dots, a)$, $a \in \{0, 1, \dots, p-1\}$, то $m \mid d_1(k)$, $M_r(x) = a \operatorname{tr}_m(x)$ и соотношения (2.2.18) эквивалентны условию $\operatorname{tr}_m(\varkappa_2) \neq 0$.

Первичной спецификацией вектора $\overline{r} = (r_0, \dots, r_{m-1})$ с координатами из множества $\{0, 1, \dots, p-1\}$ будем называть набор чисел $(\alpha_0, \alpha_1, \dots, \alpha_{p-1})$, где

α_j $(j=0,\dots,p-1)$ — число координат вектора $\overline{r}$, равных j, и записывать это в виде $[\overline{r}]=[0^{\alpha_0},1^{\alpha_1},\dots,(p-1)^{\alpha_{p-1}}]$, $\alpha_0+\alpha_1+\dots+\alpha_{p-1}=m$ (см. [14]).

Предположим, что $\alpha_j<m$ для $j=0,\dots,p-1$, т. е. координаты вектора $\overline{r}$ принимают хотя бы два различных значения.

Пусть $\varkappa_2$ — корень многочлена $M_r(x)$, а многочлен $M_{r'}(x)$ построен по вектору $\overline{r}'=(r'_0,r'_1,\dots,r'_{m-1})$, $r'=\sum_{s=0}^{m-1}r'_sp^s$, $0\leqslant r'_s<p$, $r'\in I_p^*(m,d_1(k))$, отличающемуся от вектора $\overline{r}$ перестановкой двух различных координат с номерами j и k для некоторых $j,k\in\{0,1,\dots,m-1\}$, $j<k$. В этом случае имеет место равенство

$$M_{r'}(\varkappa_2)-M_r(\varkappa_2)=a\left(\varkappa_2^{p^j}-\varkappa_2^{p^k}\right),$$

где $a=r'_j-r_j=r_k-r'_k$.

Следовательно, $\varkappa_2$ будет корнем многочлена $M_{r'}(x)$ в том и только том случае, когда минимальный многочлен элемента $\varkappa_2$ над полем $\mathbf{GF}(p)$ делит $x^{p^{k-j}}-x$. А это в силу свойств конечных полей эквивалентно условию $h\mid k-j$.

Рассмотрим в множестве $I_p(m,d_1(k))$ подмножество $\mathfrak{M}$ векторов $\overline{r}$ с фиксированной первичной спецификацией $[\overline{r}]=[0^{\alpha_0},1^{\alpha_1},\dots,(p-1)^{\alpha_{p-1}}]$, $\alpha_0+\alpha_1+\dots+\alpha_{p-1}=m$ (см. [14]): $\mathfrak{M}=\{\overline{r}\in I_p(m,d_1(k))$: в векторе $\overline{r}$ ровно α_j координат равны j, $j=0,\dots,p-1\}$.

На векторах множества $\mathfrak{M}$ введем метрику $\mathcal{R}$, положив расстояние $\mathcal{R}(\overline{a},\overline{b})$ между векторами $\overline{a}$ и $\overline{b}$ из $\mathfrak{M}$ равным наименьшему числу транспозиций координат, с помощью которых из вектора $\overline{a}$ можно получить вектор $\overline{b}$. Тогда если $\varkappa_2$ — корень многочлена $M_a(x)$, $\overline{a}\in\mathfrak{M}$, то число многочленов, построенных по векторам из множества

$$\mathfrak{S}(\overline{a})=\left\{\overline{b}\in\mathfrak{M}\colon\ \mathcal{R}(\overline{a},\overline{b})\leqslant 1\right\},$$

корнем которых является $\varkappa_2$, вообще говоря, меньше мощности множества $\mathfrak{S}(\overline{a})$. В частности, если $h=m$, то в $\mathfrak{S}(\overline{a})$ нет ни одного вектора $\overline{b}$, $\overline{b}\neq\overline{a}$, со свойством $M_b(\varkappa_2)=0$.

ЛЕММА 2.2.6. *Если $\mathfrak{M}$ — множество векторов длины m, в каждом из которых ровно α_j координат равны j, $j=0,\dots,p-1$, $\alpha_0+\alpha_1+\dots+\alpha_{p-1}=m$, $\mathfrak{N}$ — подмножество из $\mathfrak{M}$, такое, что любые два вектора из $\mathfrak{N}$ отличаются более чем в двух координатах, то*

$$|\mathfrak{M}|\geqslant|\mathfrak{N}|\bigl(1+\max\{\alpha_j,j=0,\dots,p-1\}\bigr).\tag{2.2.19}$$

Доказательство. Без ограничения общности можно считать, что $\alpha_0=\max\{\alpha_j,j=0,\dots,p-1\}$. Строим все векторы с первичной спецификацией $[0^{\alpha_0+1},1^{\alpha_1},\dots,k^{\alpha_k-1},\dots,(p-1)^{\alpha_{p-1}}]$ и для каждого из них строим α_0^k-множество векторов из $\mathfrak{M}$ мощности α_0+1, заменяя один из нулей на k. В каждом из этих α_0^k-множеств любые два вектора различаются одной транспозицией координат, и, следовательно, α_0^k-множество может содержать не более одного элемента из $\mathfrak{N}$. Аналогичную процедуру выполняем для всех $k=1,\dots,p-1$.

Общее число построенных α_0^k-множеств, $k=1,\dots,p-1$, равно

$$\sum_{k=1}^{p-1}\frac{m!}{\alpha_1!\cdots\alpha_{p-1}!}\,\frac{\alpha_k}{\alpha_0+1}=\frac{m!}{\alpha_1!\cdots\alpha_{p-1}!}\,\frac{m-\alpha_0}{\alpha_0+1}.$$

Очевидно, что каждый вектор из $\mathfrak{N}$ входит ровно в $m-\alpha_0$ различных α_0^k-множеств, $k=1,\dots,p-1$. Поэтому справедливо неравенство

$$(m-\alpha_0)|\mathfrak{N}| \leqslant \frac{m!}{\alpha_1!\cdots\alpha_{p-1}!}\,\frac{m-\alpha_0}{\alpha_0+1},$$

или

$$|\mathfrak{N}| \leqslant \frac{m!}{\alpha_1!\cdots\alpha_{p-1}!}\,\frac{1}{\alpha_0+1},$$

что и завершает доказательство леммы 2.2.6.

Пусть $h=m$. Из леммы 2.2.6 следует, что в множестве $\{M_a(x)\colon \overline{a}\in\mathfrak{M}\}$ не более $|\mathfrak{M}|(1+\max\{\alpha_j, j=0,\dots,p-1\})^{-1}$ многочленов имеют $\varkappa_2$ своим корнем, причем при условии $\alpha_0+\dots+\alpha_{p-1}=m$ справедливо неравенство

$$\bigl(1+\max\{\alpha_j, j=0,\dots,p-1\}\bigr)^{-1} \leqslant \Bigl(1+\frac{m}{p}\Bigr)^{-1}. \tag{2.2.20}$$

Множество $\mathfrak{B}_k$ представляется в виде объединения непересекающихся подмножеств

$$\mathfrak{B}_k = \bigcup\bigl\{\overline{\theta}^T\in\mathfrak{B}_k,\ [\overline{r}]=\bigl[0^{\alpha_0},1^{\alpha_1},\dots,(p-1)^{\alpha_{p-1}}\bigr]\bigr\},$$

где объединение берется по всем таким различным наборам $(\alpha_0,\dots,\alpha_{p-1})$, что $\sum_{j=0}^{p-1}\alpha_j=m$, $\sum_{j=0}^{p-1}\alpha_j j=d_1(k)$. Для каждого из этих подмножеств справедлива лемма 2.2.6, и с учетом (2.2.20) получаем, что в множестве $\mathfrak{B}_k$ не менее чем

$$|\mathfrak{B}_k|\frac{m}{m+p} = |\mathfrak{B}_k|\Bigl(1-\frac{1}{1+m/p}\Bigr)$$

элементов являются корнями многочлена $g_{s,p^s-1-k}(x)$.

Пусть $h<m$. По смыслу параметра h имеем $h\mid m$. Выберем и зафиксируем некоторое α_0-множество $\mathfrak{T}$ из доказательства леммы 2.2.6. Предположим, что $\overline{a}\in\mathfrak{T}$ и $M_a(\varkappa_2)=0$; тогда по построению множества $\mathfrak{T}$ существует такой номер l_a, $l_a\in\{0,\dots,m-1\}$, что для произвольного вектора $\overline{b}$ из $\mathfrak{T}\backslash\{\overline{a}\}$ векторы $\overline{a}$ и $\overline{b}$ отличаются в координатах с номерами l_a и l' для некоторого l', $l'\neq l_a$. При этом, если $M_b(\varkappa_2)=0$, то h делит $l'-l_a$. Следовательно, в множестве $\mathfrak{T}$ существует не более m/h векторов со свойством: $M_b(\varkappa_2)=0$, и общее число векторов множества $\mathfrak{M}$ со свойством $M_b(\varkappa_2)=0$ не превосходит величины

$$\frac{m}{h}\,\frac{|\mathfrak{M}|}{(1+\max\{\alpha_j, j=0,\dots,p-1\})}.$$

Отсюда и из (2.2.20) вытекает, что в множестве $\mathfrak{B}_k$ не менее

$$|\mathfrak{B}_k|\Bigl(1-\frac{m/h}{1+m/p}\Bigr)$$

элементов являются корнями многочлена $g_{s,p^s-1-k}(x)$. Для получения оценок (2.2.17) рангов координатных последовательностей ЛРПМП заметим, что

$$1-\frac{m/h}{1+m/p} > \frac{h-p}{h}.$$

Пусть $p = 2$, $k = 1$, $d_1(k) = 2^s - 1 \leqslant m$. Тогда в силу теоремы 2.2.2 элемент $\overline{\theta}^r$, $r \in I_p^*(m, d_1(1))$, является корнем многочлена $g_{s,p^{s-1}-1}(x)$ в том и только том случае, когда

$$\sum_{0 \leqslant s < m} r_s \varkappa_1^{p^s} \neq 0.$$

Оценка числа корней многочлена $g_{s,p^{s-1}-1}(x)$ в множестве $\mathfrak{B}_1 = \{\overline{\theta}^r,\ r \in I_p^*(m, d_1(1))\}$ получается аналогично рассмотренному выше общему случаю, если во всех выкладках заменить $\varkappa_2$ на $\varkappa_1$ и учесть, что в силу определения параметра $\varkappa_2$ степень минимального многочлена элемента $\varkappa_1$ над полем $\mathbf{GF}(p)$ не меньше степени минимального многочлена элемента $\varkappa_2$ над полем $\mathbf{GF}(p)$.

Теорема 2.2.7. *Если $F(x)$ — многочлен максимального периода степени $m \geqslant 2$ над кольцом $R = \mathbb{Z}_{p^n}$, удовлетворяющий $\{1, *\}$-условию, то для рангов координатных последовательностей u_s, $s = 1, \ldots, n-1$, ЛРПМП и из $L_R(F)$ справедливы неравенства:*

$$\begin{aligned}
\operatorname{rank} u_s \geqslant & \sum_{\substack{k=0 \\ \pi_p(k)=1}}^{p^{s-1}} (1+k) \left\{ \begin{matrix} d_1(k) \\ m \end{matrix} \right\} \\
& + \frac{m}{m+p} \sum_{\substack{k=2 \\ \pi_p(k)=2}}^{p^{s-1}} (1+k) \left\{ \begin{matrix} d_1(k) \\ m \end{matrix} \right\} \quad \textit{при} \quad p \geqslant 3, \\
\operatorname{rank} u_s \geqslant & \sum_{\substack{k=0 \\ \pi_p(k)=1,\ d_1(k)<m}}^{2^{s-1}} (1+k) \left\{ \begin{matrix} d_1(k) \\ m \end{matrix} \right\} \\
& + \frac{m}{m+2} \sum_{\substack{k=3 \\ \pi_p(k)=2,\ d_1(k)<m}}^{2^{s-1}} (1+k) \left\{ \begin{matrix} d_1(k) \\ m \end{matrix} \right\} \quad \textit{при} \quad p = 2,
\end{aligned} \tag{2.2.21}$$

где $d_1(k) = p^s - pk + \pi_p(k)$.

Доказательство. Пусть $p \geqslant 3$ и k удовлетворяет условиям $d_1(k) = p^s - pk + \pi_p(k) \leqslant m(p-1)$, $\pi_p(k) = 2$. Тогда в силу теоремы 2.2.2 элемент $\overline{\theta}^r$, $r \in I_p^*(m, d_1(k))$, является корнем многочлена $g_{s,p^{s-1}-k}(x)$ в том и только том случае, когда

$$\begin{aligned}
& \sum_{(j_0, \ldots, j_{m-1}) \in I_p(m,2)} \prod_{t=0}^{m-1} \binom{r_t}{j_t} \varkappa_1^{\sum_{s=0}^{m-1} j_s p^s} \\
& \qquad = \sum_{s=0}^{m-1} \binom{r_s}{2} \varkappa_1^{2p^s} + \sum_{0 \leqslant s < k < m} r_s r_k \varkappa_1^{p^s + p^k} \neq 0.
\end{aligned} \tag{2.2.22}$$

Рассмотрим два различных вектора $\overline{a}$ и $\overline{b}$ из $I_p(m, d_1(k))$, различающиеся транспозицией двух координат. Без ограничения общности можно считать, что эти векторы отличаются перестановкой двух первых координат. Непосредственно проверяется, что разность коэффициентов (2.2.22), соответству-

ющих этим векторам, имеет вид

$$\left(\binom{r_0}{2} - \binom{r_1}{2}\right)(\varkappa_1^2 \ominus \varkappa_1^{2p}) \oplus \left((r_0 - r_1)(\varkappa_1 \ominus \varkappa_1^p) \sum_{s=2}^{m-1} r_s \varkappa_1^{p^s}\right). \tag{2.2.23}$$

Предположим, что для обоих векторов $\overline{a}$ и $\overline{b}$ коэффициенты (2.2.22) равны нулю, тогда из (2.2.23) в силу $\{1,*\}$-условия получаем

$$\left(\binom{r_0}{2} - \binom{r_1}{2}\right)(\varkappa_1 \oplus \varkappa_1^p) \oplus \left((r_0 - r_1) \sum_{s=2}^{m-1} r_s \varkappa_1^{p^s}\right) = 0.$$

Так как $\overline{a} \neq \overline{b}$, то $r_0 \neq r_1$, и приходим к линейному соотношению между элементами $\varkappa_1, \ldots, \varkappa_1^{p^{m-1}}$. Если существует такой номер j, $2 \leqslant j < m$, что $r_j \neq 0$, то получаем противоречие с $\{1,*\}$-условием.

Рассмотрим случай $r_j = 0$, $2 \leqslant j < m$. В силу $\{1,*\}$-условия необходимо, чтобы выполнялись соотношения $r_0 \neq r_1$, $\binom{r_0}{2} = \binom{r_1}{2}$, $r_0 + r_1 = d_1(k)$. При $r_0 \neq r_1$ сравнение $\binom{r_0}{2} \equiv \binom{r_1}{2} \pmod p$ имеет место только в случае $r_0 + r_1 \equiv 1 \pmod p$, что невозможно, так как $d_1(k) \equiv 2 \pmod p$.

Следовательно, если в условиях теоремы два различных вектора $\overline{a}$ и $\overline{b}$ из $I_p(m, d_1(k))$ различаются перестановкой двух координат, то хотя бы один из элементов $\overline{\theta}^a$ и $\overline{\theta}^b$ является корнем многочлена $g_{s,p^{s-1}-k}(x)$.

Пусть $p = 2$, k — нечетное число, $k \geqslant 3$, $d_1(k) = 2^s - 2k + 2 \leqslant m$, $\pi_2(k) = 2$. Тогда в силу теоремы 2.2.2 элемент $\overline{\theta}^r$, $r \in I_2(m, d_1(k))$, является корнем многочлена $g_{s,p^{s-1}-k}(x)$ в том и только том случае, когда

$$\sum_{\substack{0 \leqslant j,l < m \\ j \neq l}} r_j r_l \varkappa_1^{2^l} \varkappa_1^{2^{j+1}} \neq 0. \tag{2.2.24}$$

Рассмотрим два различных вектора $\overline{a}$ и $\overline{b}$ из $I_2(m, d_1(k))$, различающиеся транспозицией двух координат. Без ограничения общности можно считать, что эти векторы различаются перестановкой двух первых координат, т. е. $\overline{a} = (0, 1, r_2, \ldots, r_{m-1})$, $\overline{b} = (1, 0, r_2, \ldots, r_{m-1})$. Разность коэффициентов (2.2.24), соответствующих этим векторам, имеет вид

$$\sum_{j=2}^{m-1} r_j \big((\varkappa_1 \oplus \varkappa_1^2)^2 \varkappa_1^{2^j} \oplus (\varkappa_1 \oplus \varkappa_1^2) \varkappa_1^{2^{j+1}}\big).$$

Если оба этих коэффициента равны нулю, то

$$\sum_{j=2}^{m-1} r_j (\varkappa_1 \oplus \varkappa_1^2 \oplus \varkappa_1^{2^j}) = 0.$$

Следовательно,

$$(\varkappa_1 \oplus \varkappa_1^2) \sum_{j=2}^{m-1} r_j \oplus \sum_{j=2}^{m-1} r_j \varkappa_1^{2^j} = 0. \tag{2.2.25}$$

Сумма $\sum_{j=2}^{m-1} r_j$ равна $d_1(k) - 1$, поэтому $\sum_{j=2}^{m-1} r_j \equiv 1 \pmod p$, и (2.2.25) задает нетривиальное линейное соотношение между элементами $\varkappa_1, \ldots, \varkappa_1^{2^{m-1}}$, что противоречит $\{1,*\}$-условию.

Следовательно, если в условиях теоремы два различных вектора $\overline{a}$ и $\overline{b}$ из $I_2(m, d_1(k))$ различаются перестановкой двух координат, то хотя бы один из элементов $\overline{\theta}^a$ и $\overline{\theta}^b$ является корнем многочлена $g_{s,2^{s-1}-k}(x)$.

Таким образом, оценки рангов координатных последовательностей ЛРП максимального периода вытекают из леммы 2.2.6 и разложения (1.2.1) многочленов $\mu_s(x)$, $s = 1, \ldots, n-1$. При этом необходимо учесть, что в силу $\{1, *\}$-условия $\mathrm{tr}_m(\varkappa_1) \neq 0$ и элементы $\overline{\theta}^r$, $r \in I_p^*(m, d_1(k))$, $\overline{r} = (a, a, \ldots, a)$, являются корнями многочлена $g_{s,p^{s-1}-k}(x)$. Теорема доказана.

Как видно из доказанных теорем, нижние оценки рангов координатных последовательностей ЛРПМП получены для достаточно широких классов многочленов максимального периода, причем дополнительные условия на многочлен $F(x)$ сформулированы в таком виде, который позволяет легко строить большие классы многочленов максимального периода с необходимыми свойствами (см. [9]).

Использование полученных верхних и нижних оценок рангов координатных последовательностей позволяет достаточно точно оценить порядок величины $\mathrm{rank}\, u_s$, $s = 1, \ldots, n-1$. Например, если $R = \mathbb{Z}_{2^5}$, то $F(x) = x^{20} + x^{19} + 2x^{12} - 2x^{11} + 2x^{10} + x^4 + x^3 + 2x^2 - 1$ является многочленом максимального периода, и для любой ЛРПМП $u \in L_R(F)$ справедливы неравенства

$$1.72 \cdot 10^5 \leqslant \mathrm{rank}\, u_3 \leqslant 4.3 \cdot 10^5,$$
$$9.65 \cdot 10^5 \leqslant \mathrm{rank}\, u_4 \leqslant 4.72 \cdot 10^6.$$

Из приведенных неравенств видно, что верхние и нижние оценки совпадают по порядку.

СПИСОК ЛИТЕРАТУРЫ

1. *Ван-дер-Варден Б. Л.* Алгебра. М.: Наука, 1979, 623 с.
2. *Кнут Д.* Искусство программирования для ЭВМ, т. 2. М.: Мир, 1977, 724 с.
3. *Коробов Н. М.* Тригонометрические суммы и их приложения. М.: Наука, 1989, 240 с.
4. *Кузьмин А. С.* Распределение элементов на циклах линейных рекуррент над кольцами вычетов. — Успехи матем. наук, 1993, т. 47, № 6, с. 213–214.
5. *Кузьмин А. С.* Нижние оценки рангов координатных последовательностей линейных рекуррентных последовательностей над кольцами вычетов целых чисел. — Успехи матем. наук, 1993, т. 48, № 3, с. 193–194.
6. *Кузьмин А. С.* Линейная сложность координатных последовательностей линейных рекуррент над примарными кольцами вычетов. — В сб.: Международная конференция «Современные проблемы теории чисел»: Тезисы докладов. Тула: ТГПУ, 1993, с. 98.
7. *Кузьмин А. С., Нечаев А. А.* Линейные рекуррентные последовательности над кольцом Галуа. — Успехи матем. наук, 1993, т. 48, № 1, с. 167–168.
8. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Псевдослучайные и полилинейные последовательности. — В кн.: Труды по дискретной математике./ Под общей ред. В. Н. Сачкова. Т. 1. М.: ТВП, 1997, с. 139–202.
9. *Кузьмин А. С., Куракин В. Л., Михалев А. В., Нечаев А. А.* Линейные рекурренты над кольцами и модулями. — В сб.: Итоги науки и техники. Алгебра, топология, геометрия (в печати). Англ. перев.: Kuzmin A.S., Kurakin V.L., Mikhalev A.V., Nechaev A.A. Linear recurrences over rings and modules. — J. Math. Sci. (Contemporary Math.) and Its Appl. Thematic Surveys. 1995, v. 76, № 6, p. 2793–2915.

10. *Лаксов Д.* Линейные рекуррентные последовательности над конечными полями. — Математика. (Сб. перев.) Москва, 1968, № 6, с. 145–158.
11. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 2. М.: Мир, 1988, 824 с.
12. *Нечаев А. А.* Код Кердока в циклической форме. — Дискретн. матем., 1989, т. 1, № 4, с. 123–139.
13. *Нечаев А. А.* Линейные рекуррентные последовательности над коммутативными кольцами. — Дискретн. матем., 1991, т. 3, № 4, с. 105–127.
14. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: Наука, 1982, 384 с.
15. *Сидельников В. М.* Оценки для числа появления знаков на отрезке рекуррентной последовательности над конечным полем. — Дискретн. матем., 1991, т. 3, № 2, с. 87–95.
16. *Шпарлинский И. Е.* Распределение дробных долей рекуррентной последовательности. — Матем. заметки, 1981, т. 21, № 6, с. 1588–1591.
17. *Цирлер Н.* Линейные возвратные последовательности. — Кибернетический сборник. Вып. 6. М.: ИЛ, 1963, с. 55–80.
18. *Brynielsson L.* On the linear complexity of combined shift register sequences. — Lect. Notes Comput. Sci., 1985, v. 219, p. 156–160.
19. *Cerlienco L., Mignotte M., Piras F.* Linear recurrent sequences: algebraic and arithmetical properties. — Enseign. Math. (2), 1987, v. 33, № 1–2, p. 67–108.
20. *Chan A. H., Goresky M., Klapper A.* On the linear complexity of feedback register (extended abstract). — Lect. Notes Comput. Sci., 1990, v. 434, p. 563–570.
21. *Dai Z. D., Beth T., Gollmann D.* Lower bounds for the linear complexity of sequences over residue rings. — Lect. Notes Comput. Sci., 1991, v. 473, p. 189–195.
22. *Green B. F. J., Smith J. E. K., Klem Laura.* Empirical tests of an additive random number generator. — J. Ass. Comput. Mach., 1959, v. 6, p. 527–537.
23. *Jansson B.* Random Number Generators. Stockholm: Almqvist and Wiksell, 1966, 206 c.
24. *Kuzmin A. S., Nechaev A. A.* Distribution of elements in linear recurrences of maximal period over $\mathbb{Z}_{p^2}$. — In: Proceedings of the IV International Workshop «Algebraic and Combinatorial Coding Theory» (Novgorod). Sofia: Zakrila, 1994, p. 132–136.
25. *Lucas E.* Théorie des fonctions numériques simplement periodiques. — Amer. J. Math., 1878, v. 1, p. 184–240, 289–321.
26. *MacWilliams F. J., Sloane N. J. A.* Pseudo-random sequences and arrays. — Proc. IEEE, 1976, v. 64, № 11, p. 1715–1729.
27. *Ronse C.* Feedback Shift Registers. Berlin: Springer-Verlag, 1984, 145 c.
28. *Rueppel R. A., Staffelbach O. J.* Products of linear recurring sequences with maximum complexity. — IEEE Trans. Inform. Theory, 1987, v. 33, № 1, p. 126–131.
29. *Webb W. A., Long C. T.* Distribution modulo p of the general linear second order recurrence. — Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. Sez. 8, 1975, v. 58, № 2, p. 92–100.
30. *Zierler N., Mills W. H.* Products of linear recurring sequences. — J. Algebra, 1973, v. 27, № 1, p. 147–157.
31. *Cerlienco L., Piras F.* On the continuous dual of a polynomial bialgebra. — Comm. Algebra, 1991, v. 19, № 10, c. 2707–2727.
32. *Kuzmin A. S., Nechaev A. A.* Linear recurrent sequences over Galois rings. — In: Proceedings of the 2nd International Conference on Algebra. Barnaul, 1991.
33. *Куракин В. Л.* Представления над кольцом $\mathbb{Z}_{p^n}$ линейной рекуррентной последовательности максимального периода над полем $\mathbf{GF}(p)$. — Дискретн. матем., 1992, т. 4, № 4, с. 96–116.
34. *Куракин В. Л.* Первая координатная последовательность линейной рекурренты максимального периода над кольцом Галуа. — Дискретн. матем., 1994, т. 6, № 2, с. 88–100.