Math-Net.Ru

Общероссийский математический портал

В. Л. Куракин, Полиномиальные преобразования линейных рекуррентных последовательностей над кольцом $\mathbf{Z}_{p^2}$, *Дискрет. матем.*, 1999, том 11, выпуск 2, 40–65

DOI: <https://doi.org/10.4213/dm373>

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: 44.207.124.84

26 апреля 2023 г., 17:52:40

Полиномиальные преобразования линейных рекуррентных последовательностей над кольцом $\mathbb{Z}_{p^2}$

© 1999 г. В. Л. Куракин

Дается верхняя оценка ранга (степени минимального многочлена) последовательности

$$v(i) = \Phi(u(i), u(i+1), \dots, u(i+s-1))$$

над кольцом $R = \mathbb{Z}_{p^2}$, где u — линейная рекуррентная последовательность (ЛРП) над кольцом R с абсолютно неприводимым характеристическим многочленом $F(x) \in R[x]$ и $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$. В частном случае, когда $\bar{u}$ — ЛРП максимального периода над полем $\bar{R} = R/pR = GF(p)$ и $\Phi(x) \in R[x]$ — многочлен от одной переменной степени не выше $p-1$, найдено точное значение ранга ЛРП $v(i) = \Phi(u(i))$ над кольцом R .

Получена также верхняя оценка ранга последовательности

$$v(i) = \Phi(u_1(i), \dots, u_s(i))$$

над кольцом R , где u_t — ЛРП над кольцом R с абсолютно неприводимым характеристическим многочленом $F_t(x) \in R[x]$, $t = 1, \dots, s$, и $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$. В случае, когда числа $m_1, \dots, m_s$ попарно взаимно просты, $\bar{u}_t$ — ЛРП максимального периода над полем $\bar{R}$ и степень многочлена $\Phi(x_1, \dots, x_s)$ по переменной x_t меньше, чем $\min\{p, m_t, (p-2)m_t/(p-1) + 1\}$, $t = 1, \dots, s$, найдено точное значение ранга ЛРП v над кольцом R .

1. Введение

В работе изучаются минимальные многочлены и ранги (степени минимальных многочленов) последовательностей над кольцом $R = \mathbb{Z}_{p^2}$, полученных в результате полиномиальных преобразований одной или нескольких линейных рекуррентных последовательностей (ЛРП) над кольцом R .

Вначале рассматриваются полиномиальные преобразования одной рекуррентной последовательности. Пусть u — ЛРП над кольцом R с характеристическим многочленом $F(x) \in R[x]$ степени m таким, что $\bar{F}(x)$ — неприводимый многочлен над полем $\bar{R} = R/pR = GF(p)$. Тогда для последовательности

$$v(i) = \Phi(u(i), u(i+1), \dots, u(i+s-1)), \quad i \geq 0,$$

где $\Phi(x_1, \dots, x_s)$ — многочлен степени n над кольцом R , доказана следующая оценка ранга над кольцом R :

$$\text{rank}_R v \leq \sum_{k=0}^n \binom{m+k-1}{k}. \quad (1)$$

Эта оценка достижима при $n \leq p-1$. Найден также характеристический многочлен ЛРП v над кольцом R .

В частном случае, когда $\bar{u}$ — ЛРП максимального периода над полем $\bar{R}$ и

$$\Phi(x) = c_0 + c_1 x + \dots + c_{p-1} x^{p-1} \in R[x]$$

— многочлен от одной переменной степени не выше $p-1$, найдено точное значение ранга ЛРП $v(i) = \Phi(u(i))$, $i \geq 0$, над кольцом R :

$$\text{rank}_R v = \sum_{k \in \mathcal{L}} \binom{m+k-1}{k}, \quad (2)$$

где $\mathcal{L} = \{k \in \{0, 1, \dots, p-1\} : c_k \neq 0\}$. Найден минимальный многочлен и аннулятор ЛРП v над кольцом R .

Далее рассматриваются полиномиальные преобразования нескольких рекуррентных последовательностей. Пусть

$$v(i) = \Phi(u_1(i), \dots, u_s(i)), \quad i \geq 0,$$

где u_t — ЛРП над кольцом R с характеристическим многочленом $F_t(x) \in R[x]$ степени m_t таким, что $\bar{F}_t(x)$ — неприводимый многочлен над полем $\bar{R}$, $t = 1, \dots, s$, и $\Phi(x_1, \dots, x_s)$ — многочлен степени n над кольцом R . Если

$$\Phi(x_1, \dots, x_s) = \sum_{k_1, \dots, k_s \geq 0} c_{k_1, \dots, k_s} x_1^{k_1} \dots x_s^{k_s},$$

то обозначим через Φ^* следующий многочлен над полем рациональных чисел $\mathbf{Q}$:

$$\Phi^*(x_1, \dots, x_s) = \sum_{k_1, \dots, k_s \geq 0} c_{k_1, \dots, k_s}^* \binom{x_1 + k_1 - 1}{k_1} \dots \binom{x_s + k_s - 1}{k_s},$$

где

$$c_{k_1, \dots, k_s}^* = \begin{cases} 1, & \text{если } c_{k_1, \dots, k_s} \neq 0, \\ 0, & \text{если } c_{k_1, \dots, k_s} = 0. \end{cases}$$

Тогда доказанная в этой статье оценка ранга ЛРП v над кольцом R имеет вид

$$\text{rank}_R v \leq \Phi^*(m_1, \dots, m_s). \quad (3)$$

Найден также характеристический многочлен ЛРП v над кольцом R .

При дополнительных предположениях последняя оценка достижима. Пусть числа $m_1, \dots, m_s$ попарно взаимно просты, $\bar{u}_t$ — ЛРП максимального периода над полем $\bar{R}$ и степень d_t многочлена $\Phi(x_1, \dots, x_s)$ по переменной x_t меньше, чем

$$M_t = \min\{p, m_t, (p-2)m_t/(p-1) + 1\}, \quad t = 1, \dots, s$$

(последнее условие, в частности, выполняется, если $d_t \leq 1$, $t = 1, \dots, s$, т. е. многочлен $\Phi(x_1, \dots, x_s)$ свободен от квадратов). Тогда

$$\text{rank}_R v = \Phi^*(m_1, \dots, m_s). \quad (4)$$

Найден также минимальный многочлен и аннулятор ЛРП v над кольцом R .

Для последовательностей над полем ранги и минимальные многочлены полиномиальных преобразований последовательностей изучались ранее рядом авторов. Произведение последовательностей над полем исследовалось в [11, 13]. Последовательность вида

$$v(i) = \Phi(u(i), \dots, u(i + s - 1))$$

над конечным полем рассматривалась в [1, 3, 6, 7]. Ранг и минимальный многочлен последовательности $v(i) = \Phi(u(i))$ над конечным полем изучались в [2, 5, 8, 9, 12]. Последовательность вида

$$v(i) = \Phi(u_1(i), \dots, u_s(i))$$

над конечным полем исследовалась в [4, 5, 6, 10] в предположении, что многочлен Φ свободен от квадратов. Перечисленные результаты можно найти также в книге [18]. Результаты данной статьи являются обобщениями указанных результатов на последовательности над кольцом $\mathbf{Z}_{p^2}$. Кроме того, в случае последовательностей над полем $GF(p)$ формула (4) обобщает результат работы [10] на более широкий класс многочленов Φ . Оценки и точные формулы для рангов линейных рекуррент над полем $GF(p)$ формулируются в дальнейшем как следствия.

Структура статьи следующая. Во втором параграфе вводятся необходимые понятия, связанные с кольцами Галуа и линейными рекуррентными последовательностями. В параграфах 3, 4, 5, 6 доказываются соотношения (1), (2), (3) и (4) соответственно.

2. Линейные рекурренты над кольцом $\mathbf{Z}_{p^2}$ и их представление функцией след

Пусть p — простое число, $R = \mathbf{Z}_{p^2}$ — примарное кольцо вычетов, $\bar{R} = R/pR = GF(p)$ — поле вычетов кольца R , R^∞ — множество последовательностей над кольцом R . Образ элемента $a \in R$ при действии естественного эпиморфизма $R \rightarrow \bar{R}$ будем обозначать $\bar{a}$. Если

$$F(x) = \sum c_k x^k \in R[x]$$

и $u = (u(0), u(1), \dots) \in R^\infty$, то введем обозначения

$$\bar{F}(x) = \sum \bar{c}_k x^k \in \bar{R}[x]$$

и $\bar{u} = (\bar{u}(0), \bar{u}(1), \dots) \in \bar{R}^\infty$.

Унитарный многочлен $F(x) \in R[x]$ называется абсолютно неприводимым, или многочленом Галуа [16], если $\bar{F}(x)$ — неприводимый над полем $\bar{R}$ многочлен.

Произведением многочлена

$$F(x) = c_m x^m + \dots + c_1 x + c_0 \in R[x]$$

на последовательность $u \in R^\infty$ назовем последовательность $v = F(x)u \in R^\infty$ с элементами

$$v(i) = c_m u(i+m) + \dots + c_1 u(i+1) + c_0 u(i), \quad i \geq 0.$$

Если $F(x)u = 0$, то говорят, что многочлен $F(x)$ аннулирует последовательность u . Множество многочленов, аннулирующих последовательность u , образует идеал кольца $R[x]$, который называется аннулятором последовательности u и обозначается $\text{Ann}(u)$. Если $\text{Ann}(u)$ содержит унитарный многочлен $F(x)$, то последовательность u называется линейной рекуррентной последовательностью (ЛРП) над кольцом R , а многочлен $F(x)$ ее характеристическим многочленом. Если $F(x) \in R[x]$ — унитарный многочлен, то через $L_R(F)$ обозначается множество линейных рекуррентных последовательностей над кольцом R с характеристическим многочленом $F(x)$. Характеристический многочлен ЛРП u наименьшей степени называется минимальным многочленом ЛРП u , а его степень рангом ЛРП u над кольцом R и обозначается $\text{rank}_R u$. Минимальный многочлен $\mu(x)$ линейной рекуррентной последовательности над полем P определяется однозначно условием

$$\text{Ann}(u) = (\mu(x)) = \mu(x)P[x].$$

Для последовательностей над кольцами минимальный многочлен определен, в общем случае, неоднозначно. Например, последовательность $u = (2, 2, 2, \dots)$ над кольцом $\mathbf{Z}_4$ имеет два минимальных многочлена, $x - 1$ и $x - 3$.

Биномиальной последовательностью (порядка 0) над полем P с корнем $\xi \in P$ называется последовательность $c\xi^i$, $i \geq 0$, где $c \in P^*$ — ненулевая константа. Минимальный многочлен такой последовательности равен $x - \xi$. Как известно [14, 15], минимальный многочлен суммы линейных рекуррент с попарно взаимно простыми минимальными многочленами равен произведению минимальных многочленов этих последовательностей. Поэтому по представлению последовательности в виде суммы биномиальных последовательностей с попарно различными корнями можно найти ее минимальный многочлен. Именно, если

$$u(i) = c_1 \xi_1^i + \dots + c_N \xi_N^i, \quad \xi_j \neq \xi_k, \quad j \neq k, \quad c_j \neq 0, \quad j = 1, \dots, N,$$

то минимальный многочлен ЛРП u над полем P равен $(x - \xi_1) \dots (x - \xi_N)$.

Пусть $S = GR(q^2, p^2)$, $q = p^m$, — расширение Галуа степени m кольца Галуа $R = \mathbf{Z}_{p^2} = GR(p^2, p^2)$ (см. [16]). Кольцо S состоит из q^2 элементов, имеет характеристику p^2 и поле вычетов $\bar{S} = S/pS = GF(q)$. Если $G(x) \in R[x]$ — произвольный многочлен Галуа степени m , то $S \cong R[x]/G(x)$. С другой стороны, всякий многочлен Галуа $F(x) \in R[x]$ степени m имеет в кольце S в точности m корней. Если $\xi \in S$ — корень многочлена Галуа $F(x)$, то, согласно теореме 8 из [16], любая ЛРП $u \in L_R(F)$ представляется в виде

$$u(i) = \text{Tr}_R^S(a\xi^i), \quad i \geq 0, \quad (5)$$

где $a \in S$ — константа, однозначно определяемая начальным вектором

$$u(0, m-1) = (u(0), \dots, u(m-1))$$

ЛРП u , а Tr_R^S — функция след из кольца S в кольцо R , определяемая равенством

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

Здесь $\text{Aut}(S/R)$ — группа автоморфизмов кольца S над R . Функция след является линейным над R отображением. Обратно, каждая ЛРП u , представляющаяся в виде (5), принадлежит $L_R(F)$.

Обозначим

$$\Gamma(S) = \{\beta \in S: \beta^q = \beta\}$$

p -адическое координатное множество кольца S . Согласно [16], это множество замкнуто относительно умножения и состоит из $q = p^m$ элементов, попарно не сравнимых по модулю pS . Множество $\Gamma(S)$ содержит в качестве подмножества p -адическое координатное множество $\Gamma(R) = \{\beta \in R: \beta^p = \beta\}$ кольца R , причем $\Gamma(R) = \Gamma(S) \cap R$.

Каждый элемент $a \in S$ однозначно представляется в виде

$$a = a_0 + pa_1, \quad a_0, a_1 \in \Gamma(S),$$

называемом p -адическим разложением элемента a . Элементы

$$a_i = \gamma_i(a) \in \Gamma(S), \quad i = 0, 1,$$

называются p -адическими координатами элемента a . Определим на множестве $\Gamma(S)$ операцию

$$\alpha \oplus \beta = \gamma_0(\alpha + \beta), \quad \alpha, \beta \in \Gamma(S).$$

Тогда $(\Gamma(S), \oplus, \cdot)$ — поле из q элементов, а $\Gamma(R)$ — его подполе из p элементов.

Пользуясь p -адическим разложением элементов кольца S , можно в явном виде описать автоморфизмы группы $\text{Aut}(S/R)$. Как показано в следствии 1 теоремы 7 в [16], группа $\text{Aut}(S/R)$ является циклической группой порядка m , которая порождается автоморфизмом Фробениуса σ_0 . Действие автоморфизма Фробениуса на произвольном элементе $x \in S$ с p -адическим разложением $x = x_0 + px_1$ определяется равенством

$$\sigma_0(x) = x_0^p + px_1^p. \quad (6)$$

Если $F(x)$ — многочлен Галуа степени m над кольцом R с корнем $\xi \in S$, то, согласно следствию 2 теоремы 7 из [16], многочлен $F(x)$ имеет в кольце S в точности m различных корней

$$\xi, \sigma_0(\xi), \dots, \sigma_0^{m-1}(\xi)$$

и разлагается над S на линейные множители

$$F(x) = (x - \xi)(x - \sigma_0(\xi)) \dots (x - \sigma_0^{m-1}(\xi)).$$

В следующем предложении в явном виде описывается правая часть представления (5) линейной рекурренты над кольцом R в виде функции след.

Предложение 1. Пусть $F(x) \in R[x]$ — многочлен Галуа степени m с корнем $\xi \in S$, и последовательность $u \in L_R(F)$ представляется функцией след по формуле (5), то есть

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

Пусть элементы $a, \xi \in S$ имеют p -адические разложения $a = a_0 + pa_1$ и $\xi = \xi_0 + p\xi_1$. Тогда

$$u(i) = \sum_{r=0}^{m-1} (a_0^{p^r} + pa_1^{p^r} + pi(a_0\xi_0^{-1}\xi_1)^{p^r})(\xi_0^i)^{p^r}, \quad i \geq 0. \quad (7)$$

Доказательство. Ясно, что

$$\begin{aligned} u(i) &= \text{Tr}_R^S(a\xi^i) = \sum_{\sigma \in \text{Aut}(S/R)} \sigma(a)\sigma(\xi)^i \\ &= \sum_{r=0}^{m-1} \sigma_0^r(a)\sigma_0^r(\xi)^i = \sum_{r=0}^{m-1} (a_0^{p^r} + pa_1^{p^r})(\xi_0^{p^r} + p\xi_1^{p^r})^i. \end{aligned}$$

Возводя в степень i и пользуясь тем, что характеристика кольца R равна p^2 , находим, что

$$\begin{aligned} u(i) &= \sum_{r=0}^{m-1} (a_0^{p^r} + pa_1^{p^r})((\xi_0^{p^r})^i + pi(\xi_0^{p^r})^{i-1}\xi_1^{p^r}) \\ &= \sum_{r=0}^{m-1} (a_0^{p^r} + pa_1^{p^r} + pi(a_0\xi_0^{-1}\xi_1)^{p^r})(\xi_0^i)^{p^r}, \end{aligned}$$

что совпадает с (7).

3. Полиномиальные преобразования одной рекурренты

Пусть $F(x)$ — многочлен Галуа степени m над кольцом $R = \mathbb{Z}_{p^2}$, $u \in L_R(F)$ и $\Phi(x_1, \dots, x_s)$ — многочлен степени n над кольцом R . В этом параграфе находится верхняя оценка ранга последовательности

$$v(i) = \Phi(u(i), \dots, u(i+s-1)), \quad i \geq 0,$$

над кольцом R .

В случае последовательностей над конечным полем верхняя оценка ранга такой последовательности известна [7, 18]. В нашем контексте ее можно сформулировать как верхнюю оценку ранга ЛРП $\bar{v}$ над полем $\bar{R} = GF(p)$. Обозначим через $\left\{ \begin{smallmatrix} m \\ k \end{smallmatrix} \right\}_p$ число размещений k одинаковых шаров по m различным ящикам при условии, что в каждый ящик попадает не более $p-1$ шаров. Согласно [19],

$$\left\{ \begin{smallmatrix} m \\ k \end{smallmatrix} \right\}_p = \sum_{j \geq 0} (-1)^j \binom{m}{j} \binom{m+k-pj-1}{m-1}, \quad k \geq 0.$$

Справедливы неравенства

$$\binom{m}{k} \leq \left\{ \begin{smallmatrix} m \\ k \end{smallmatrix} \right\}_p \leq \binom{m+k-1}{k},$$

поскольку в левой части находится число размещений k одинаковых шаров по m различным ящикам при условии, что в каждый ящик попадает не более одного шара, а в правой части число размещений k шаров по m ящикам без ограничений на число шаров в ящиках. Заметим также, что

$$\begin{aligned} \left\{ \begin{smallmatrix} m \\ k \end{smallmatrix} \right\}_p &= \binom{m+k-1}{k} \text{ при } k = 0, 1, \dots, p-1, \\ \left\{ \begin{smallmatrix} m \\ k \end{smallmatrix} \right\}_2 &= \binom{m+k-1}{k} \text{ при } p = 2, k \geq 0. \end{aligned}$$

При введенных обозначениях верхняя оценка ранга ЛРП $\bar{v}$ над полем $\bar{R}$ выглядит следующим образом:

$$\text{rank}_{\bar{R}} \bar{v} \leq \sum_{k=0}^n \left\{ \begin{matrix} m \\ k \end{matrix} \right\}_p.$$

Эта оценка будет доказана ниже в предложении 2. Понятно, что для ранга ЛРП v над кольцом R оценка может только увеличиться. Мы докажем, что для ранга ЛРП v над кольцом R верна аналогичная оценка, в которой $\left\{ \begin{matrix} m \\ k \end{matrix} \right\}_p$ заменяется на $\binom{m+k-1}{k}$.

Теорема 1. Пусть $u \in L_R(F)$, где $F(x) \in R[x]$ — многочлен Галуа степени $m \geq 1$. Пусть

$$v(i) = \Phi(u(i), \dots, u(i+s-1)), \quad i \geq 0,$$

где $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$ — многочлен степени $n \geq 1$ и $\Phi(0, \dots, 0) = 0$. Тогда

$$\text{rank}_R v \leq \sum_{k=1}^n \binom{m+k-1}{k}, \quad (8)$$

а если $\bar{u} = 0$, то

$$\text{rank}_R v \leq m. \quad (9)$$

Доказательство. Рассмотрим вначале случай, когда $\bar{u} \neq 0$. Последовательность v есть сумма последовательностей вида

$$w(i) = u(i+i_1) \dots u(i+i_k), \quad i_1, \dots, i_k \geq 0, \quad k = 1, \dots, n. \quad (10)$$

Пусть ЛРП u представляется функцией след по формуле (5). В силу (7)

$$w(i) = \prod_{t=1}^k \sum_{r=0}^{m-1} (a_0^{p^r} + p a_1^{p^r} + p(i+i_t)(a_0 \xi_0^{-1} \xi_1)^{p^r}) \xi_0^{p^{r_t}(i+i_t)}.$$

Перемножая k сумм, получим, что

$$w(i) = \sum_{r_1, \dots, r_k=0}^{m-1} \prod_{t=1}^k (a_0^{p^{r_t}} + p a_1^{p^{r_t}} + p(i+i_t)(a_0 \xi_0^{-1} \xi_1)^{p^{r_t}}) \xi_0^{p^{r_t}(i+i_t)}.$$

Так как $\bar{u} \neq 0$, то $a_0 \neq 0$. Следовательно,

$$w(i) = \sum_{r_1, \dots, r_k=0}^{m-1} (a_0 \xi_0^i)^{p^{r_1} + \dots + p^{r_k}} \xi_0^{i_1 p^{r_1} + \dots + i_k p^{r_k}} \prod_{t=1}^k (1 + p(a_0^{-1} a_1)^{p^{r_t}} + p(i+i_t)(\xi_0^{-1} \xi_1)^{p^{r_t}}).$$

Так как характеристика кольца S равна p^2 , то, перемножая k скобок, получим, что

$$w(i) = \sum_{r_1, \dots, r_k=0}^{m-1} (a_0 \xi_0^i)^{p^{r_1} + \dots + p^{r_k}} \xi_0^{i_1 p^{r_1} + \dots + i_k p^{r_k}} \times \left(1 + p \sum_{t=1}^k ((a_0^{-1} a_1)^{p^{r_t}} + i_t (\xi_0^{-1} \xi_1)^{p^{r_t}}) + p i \sum_{t=1}^k (\xi_0^{-1} \xi_1)^{p^{r_t}} \right). \quad (11)$$

Произвольное слагаемое этой суммы есть последовательность вида

$$z(i) = c(1 + pb + pi\eta)\theta^i, \quad i \geq 0, \quad (12)$$

где

$$c = a_0^{p^{r_1} + \dots + p^{r_k}} \xi_0^{i_1 p^{r_1} + \dots + i_k p^{r_k}}, \quad \theta = \xi_0^{p^{r_1} + \dots + p^{r_k}},$$

$$b = \sum_{t=1}^k ((a_0^{-1} a_1)^{p^{r_t}} + i_t (\xi_0^{-1} \xi_1)^{p^{r_t}}), \quad \eta = \sum_{t=1}^k (\xi_0^{-1} \xi_1)^{p^{r_t}}.$$

Эта последовательность z аннулируется многочленом $x - \xi_{r_1, \dots, r_k}$, где

$$\xi_{r_1, \dots, r_k} = \theta(1 + p\eta) = \xi_0^{p^{r_1} + \dots + p^{r_k}} \left(1 + p \sum_{t=1}^k (\xi_0^{-1} \xi_1)^{p^{r_t}} \right).$$

Действительно, при $i \geq 0$

$$\begin{aligned} ((x - \xi_{r_1, \dots, r_k})z)(i) &= z(i+1) - \xi_{r_1, \dots, r_k} z(i) = z(i+1) - \theta(1 + p\eta)z(i) \\ &= c(1 + pb + p(i+1)\eta)\theta^{i+1} - \theta(1 + p\eta)c(1 + pb + pi\eta)\theta^i \\ &= c\theta^{i+1}(1 + pb + p(i+1)\eta - (1 + p\eta)(1 + pb + pi\eta)) = 0. \end{aligned} \quad (13)$$

Следовательно, последовательность (11) аннулируется многочленом

$$G_k(x) = \prod_{\xi_{r_1, \dots, r_k}} (x - \xi_{r_1, \dots, r_k}), \quad (14)$$

где произведение берется по всем различным элементам $\xi_{r_1, \dots, r_k}$, когда $r_1, \dots, r_k \in \{0, 1, \dots, m-1\}$. Степень многочлена $G_k(x)$ равна числу различных элементов среди элементов $\xi_{r_1, \dots, r_k}$, $r_1, \dots, r_k \in \{0, 1, \dots, m-1\}$. Следовательно, степень многочлена $G_k(x)$ не превосходит числа мультимножеств (множеств с повторяющимися элементами)

$$\langle r_1, \dots, r_k \rangle, \quad r_1, \dots, r_k \in \{0, 1, \dots, m-1\},$$

то есть, числа k -мультимножеств над m -множеством. Число таких мультимножеств, как известно, равно $\binom{m+k-1}{k}$, поэтому

$$\deg G_k(x) \leq \binom{m+k-1}{k}.$$

Докажем, что $G_k(x) \in R[x]$ (согласно своему определению $G_k(x) \in S[x]$). В силу следствия 3 теоремы 7 из [16] кольцо R совпадает с множеством элементов кольца S , инвариантных относительно действия автоморфизма Фробениуса σ_0 . Поэтому достаточно доказать, что коэффициенты многочлена $G_k(x)$ инвариантны относительно действия автоморфизма Фробениуса. Это эквивалентно равенству

$$\prod_{\xi_{r_1, \dots, r_k}} (x - \xi_{r_1, \dots, r_k}) = \prod_{\xi_{r_1, \dots, r_k}} (x - \sigma_0(\xi_{r_1, \dots, r_k})). \quad (15)$$

В левой части все сомножители $x - \xi_{r_1, \dots, r_k}$ различны и, так как σ_0 — автоморфизм, в правой части все сомножители $x - \sigma_0(\xi_{r_1, \dots, r_k})$ различны. Значит, для доказательства (15) достаточно проверить, что

$$\sigma_0(\xi_{r_1, \dots, r_k}) = \xi_{r'_1, \dots, r'_k}$$

для некоторых $r'_1, \dots, r'_k \in \{0, 1, \dots, m-1\}$. Действительно, так как $\xi_0, \xi_1 \in \Gamma(S)$, $\xi_0^{p^m} = \xi_0$, $\xi_1^{p^m} = \xi_1$, и элемент

$$\begin{aligned} \sigma_0(\xi_{r_1, \dots, r_k}) &= \sigma_0 \left(\xi_0^{p^{r_1} + \dots + p^{r_k}} + p \xi_0^{p^{r_1} + \dots + p^{r_k}} \sum_{t=1}^k (\xi_0^{-1} \xi_1)^{p^{r_t}} \right) \\ &= (\xi_0^{p^{r_1} + \dots + p^{r_k}})^p + p (\xi_0^{p^{r_1} + \dots + p^{r_k}})^p \sum_{t=1}^k ((\xi_0^{-1} \xi_1)^{p^{r_t}})^p \end{aligned}$$

совпадает с элементом $\xi_{r_1 \oplus 1, \dots, r_k \oplus 1}$, где $\oplus$ в данном случае обозначает сложение по модулю m . Таким образом, мы доказали, что $G_k(x) \in R[x]$.

Из определения (14) следует, что многочлен $G_k(x)$ не зависит от набора $i_1, \dots, i_k$. Поэтому многочлен $G_k(x)$ аннулирует последовательность (10) при любых неотрицательных $i_1, \dots, i_k$. Следовательно, многочлен

$$G(x) = G_1(x) \dots G_n(x)$$

аннулирует последовательность v . Поскольку

$$\deg G(x) = \sum_{k=1}^n \deg G_k(x) \leq \sum_{k=1}^n \binom{m+k-1}{k},$$

отсюда вытекает оценка (8).

Пусть теперь $\bar{u} = 0$. Тогда $u = pu_1$, где $\bar{u}_1 \in L_{\bar{R}}(\bar{F})$. В этом случае элементы последовательности (10) равны 0 при $k \geq 2$. Следовательно,

$$v(i) = c_0 u(i) + c_1 u(i+1) + \dots + c_{s-1} u(i+s-1), \quad i \geq 0,$$

и многочлен $F(x) = G_1(x)$ аннулирует ЛРП v . Отсюда вытекает соотношение (9). Заметим, что в этом случае ЛРП v аннулируется также многочленом

$$G(x) = G_1(x) \dots G_n(x),$$

и верна оценка (8).

Следствие 1. В условиях теоремы 1 многочлен

$$G(x) = G_1(x) \dots G_n(x)$$

является характеристическим многочленом ЛРП v . Здесь

$$G_k(x) = \prod_{\xi_{r_1, \dots, r_k}} (x - \xi_{r_1, \dots, r_k}) \in R[x], \quad k = 1, \dots, n,$$

где произведение берется по всем различным элементам

$$\xi_{r_1, \dots, r_k}, \quad r_1, \dots, r_k \in \{0, 1, \dots, m-1\},$$

причем

$$\xi_{r_1, \dots, r_k} = \xi_0^{p^{r_1} + \dots + p^{r_k}} \left(1 + p \sum_{t=1}^k (\xi_0^{-1} \xi_1)^{p^{r_t}} \right)$$

и $\xi = \xi_0 + p\xi_1$ — корень многочлена $F(x)$ в кольце Галуа $S = GR(q^2, p^2)$, $q = p^m$.

Следствие 2. В условиях теоремы 1 последовательность

$$w(i) = u(i + i_1) \dots u(i + i_k), \quad i_1, \dots, i_k \geq 0, \quad k \geq 1,$$

аннулируется многочленом $G_k(x)$. При этом

$$\text{rank}_R w \leq \deg G_k(x) \leq \binom{m+k-1}{k}.$$

На основе доказательства теоремы 1 легко вывести известную оценку ранга ЛРП $\bar{v}$ над полем $\bar{R}$. Одновременно это позволит частично описать аннулятор ЛРП v над кольцом R . Для целого неотрицательного числа a , имеющего p -ичное разложение

$$a = a_0 + pa_1 + \dots + p^m a_m, \quad 0 \leq a_r \leq p-1,$$

назовем p -ичным весом, или просто весом числа a величину

$$w(a) = a_0 + a_1 + \dots + a_m.$$

Легко увидеть, что количество чисел $d \in \{1, \dots, p^m - 1\}$ веса $w(d) = k$ равно $\left\{ \begin{smallmatrix} m \\ k \end{smallmatrix} \right\}_p$.

Предложение 2. В условиях теоремы 1 справедлива оценка

$$\text{rank}_{\bar{R}} \bar{v} \leq \sum_{k=1}^n \left\{ \begin{smallmatrix} m \\ k \end{smallmatrix} \right\}_p.$$

Многочлен

$$h(x) = \prod_{\bar{\xi}_0^d} (x - \bar{\xi}_0^d),$$

где произведение берется по всем различным элементам $\bar{\xi}_0^d$ таким, что

$$d \in \{1, \dots, p^m - 1\}, \quad w(d) \leq n,$$

является характеристическим многочленом ЛРП $\bar{v}$ над полем $\bar{R}$.

Доказательство. Вначале заметим, что многочлен $h(x)$ не имеет кратных корней и вместе с корнем $\bar{\xi}_0^d$ обладает корнем $(\bar{\xi}_0^d)^p$. Поэтому $h(x) \in \bar{R}[x]$.

Последовательность $\bar{v}$ есть сумма последовательностей вида

$$\bar{w}(i) = \bar{u}(i + i_1) \dots \bar{u}(i + i_k), \quad i_1, \dots, i_k \geq 0, \quad k = 1, \dots, n.$$

В силу (11)

$$w(i) = \sum_{r_1, \dots, r_k=0}^{m-1} (\bar{a}_0 \bar{\xi}_0^i)^{p^{r_1} + \dots + p^{r_k}} \bar{\xi}_0^{i_1 p^{r_1} + \dots + i_k p^{r_k}}, \quad i \geq 0.$$

Обозначим через d число из отрезка $\{1, \dots, p^m - 1\}$, сравнимое с числом $p^{r_1} + \dots + p^{r_k}$ по модулю $p^m - 1$. Тогда $\bar{\xi}_0^{p^{r_1} + \dots + p^{r_k}} = \bar{\xi}_0^d$ и $w(d) \leq k$. Таким образом, последовательность $\bar{w}$ есть сумма биномиальных последовательностей с корнями $\bar{\xi}_0^d$, где $d \in \{1, \dots, p^m - 1\}$, $w(d) \leq k$. Значит, последовательность $\bar{v}$ есть сумма биномиальных последовательностей с корнями $\bar{\xi}_0^d$, где $d \in \{1, \dots, p^m - 1\}$, $w(d) \leq n$. Так как биномиальная последовательность $c \bar{\xi}_0^{di}$ с корнем $\bar{\xi}_0^d$ аннулируется многочленом $x - \bar{\xi}_0^d$, то последовательность $\bar{v}$ аннулируется многочленом $h(x)$. Так как количество чисел $d \in \{1, \dots, p^m - 1\}$ веса $w(d) = k$ равно $\left\{ \begin{smallmatrix} m \\ k \end{smallmatrix} \right\}_p$,

$$\deg h(x) \leq \sum_{k=1}^n \left\{ \begin{smallmatrix} m \\ k \end{smallmatrix} \right\}_p,$$

откуда вытекает требуемая оценка ранга ЛРП $\bar{v}$.

Пусть $H(x) \in R[x]$ — произвольный унитарный многочлен над кольцом R такой, что $\bar{H}(x) = h(x)$.

Следствие 3. В условиях теоремы 1 справедливо включение

$$\text{Ann } v \supseteq (G(x), pH(x)).$$

Доказательство. По следствию 1 $G(x)$ — характеристический многочлен ЛРП v над кольцом R . Следовательно, $G(x) \in \text{Ann } v$. По предложению 2 $\bar{H}(x)$ — характеристический многочлен ЛРП $\bar{v}$ над полем $\bar{R}$. Следовательно, $pH(x)v = 0$ и значит, $pH(x) \in \text{Ann } v$. Отсюда вытекает, что $\text{Ann } v \supseteq (G(x), pH(x))$.

В теореме 1 на многочлен Φ накладывалось условие $\Phi(0, \dots, 0) = 0$. Если это условие не выполняется, получаем следующий результат.

Предложение 3. Пусть $u \in L_R(F)$, где $F(x) \in R[x]$ — многочлен Галуа степени $m \geq 1$. Пусть

$$v(i) = \Phi(u(i), \dots, u(i + s - 1)), \quad i \geq 0,$$

где $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$ — многочлен степени $n \geq 0$. Тогда многочлен

$$(x - e)G(x) = (x - e)G_1(x) \dots G_n(x),$$

где многочлены $G_k(x)$ определены в следствии 1, является характеристическим многочленом ЛРП v , и

$$\text{rank}_R v \leq \sum_{k=0}^n \binom{m + k - 1}{k}.$$

Аналогичным образом в случае $\Phi(0, \dots, 0) \neq 0$ переформулируются предложение 2 и следствие 3.

Замечание 1. Отметим, что в поле $GF(p)$ выполняется тождество $x^p = x$, и потому при исследовании полиномиальных преобразований последовательностей над этим полем можно считать, что степень многочлена $\bar{\Phi}(x_1, \dots, x_s)$ по каждой переменной не превосходит $p - 1$. Аналогично в кольце R выполняется тождество $x^{p^2} = x^p$, поэтому можно считать, что степень многочлена $\Phi(x_1, \dots, x_s)$ по каждой переменной не превосходит $p^2 - 1$. (Хотя теорема 1 и последующие результаты доказываются без этих предположений.) Если степень многочлена Φ по некоторой переменной больше $p^2 - 1$, то многочлен Φ полезно заменить многочленом меньшей степени по этой переменной, воспользовавшись тождеством $x^{p^2} = x^p$. Если при этом степень n многочлена Φ уменьшится, то уменьшится и оценка ранга ЛРП v .

Поясним сказанное на примере. Пусть $R = \mathbf{Z}_9$, $s = 1$, $\Phi(x) = x^{17}$. Тогда

$$\begin{aligned} v(i) &= u(i)^{17} = u(i)^9 u(i)^8 = u(i)^3 u(i)^8 = u(i)^9 u(i)^2 = u(i)^5, \\ \bar{v}(i) &= \bar{u}(i)^5 = \bar{u}(i)^3 \bar{u}(i)^2 = \bar{u}(i) \bar{u}(i)^2 = \bar{u}(i)^3 = \bar{u}(i). \end{aligned}$$

Ранги последовательностей v и $\bar{v}$ удовлетворяют соотношениям

$$\text{rank}_R v \leq \sum_{k=1}^5 \binom{m+k-1}{k}, \quad \text{rank}_{\bar{R}} \bar{v} = \text{rank}_{\bar{R}} \bar{u} = m.$$

4. Замена элементов линейной рекурренты

Рассмотрим частный случай, когда многочлен $\Phi(x) \in R[x]$ зависит от одной переменной:

$$v(i) = \Phi(u(i)), \quad i \geq 0.$$

При условии, что $\bar{u}$ — ЛРП максимального периода над полем $\bar{R}$ и $\deg \Phi \leq p - 1$, мы найдем точное значение ранга ЛРП v над кольцом R . Поскольку $x^{p^2} = x^p$ в кольце R , заведомо можно считать, что $\deg \Phi(x) \leq p^2 - 1$. Накладываемое нами ограничение $\deg \Phi(x) \leq p - 1$, таким образом, сужает класс рассматриваемых полиномиальных преобразований кольца R .

В случае последовательностей над конечным полем точная формула для ранга ЛРП v известна, см., например, [2, 8, 9, 18]. В наших обозначениях результат этих работ можно сформулировать как формулу для ранга последовательности $\bar{v}$ над полем $\bar{R}$: если

$$\Phi(x) = c_{p-1}x^{p-1} + \dots + c_1x + c_0$$

и $\bar{\mathcal{L}} = \{k \in \{0, 1, \dots, p-1\} : \bar{c}_k \neq 0\}$, то

$$\text{rank}_{\bar{R}} \bar{v} = \sum_{k \in \bar{\mathcal{L}}} \binom{m+k-1}{k}.$$

Понятно, что ранг ЛРП v над кольцом R может только увеличиться. Мы покажем, что величина $\text{rank}_R v$ вычисляется по аналогичной формуле.

Теорема 2. Пусть $u \in L_R(F)$, где $F(x)$ — многочлен Галуа над кольцом $R = \mathbf{Z}_{p^2}$ степени $m \geq 2$, причем $\bar{u}$ — ЛРП максимального периода над полем $\bar{R} = GF(p)$.

Пусть

$$v(i) = \Phi(u(i)), \quad i \geq 0,$$

где $\Phi(x) = c_{p-1}x^{p-1} + \dots + c_1x + c_0 \in R[x]$.

Тогда

$$\text{rank}_R v = \sum_{k \in \mathcal{L}} \binom{m+k-1}{k},$$

где $\mathcal{L} = \{k \in \{0, 1, \dots, p-1\} : c_k \neq 0\}$.

Доказательство. В силу следствия 2, последовательность $u(i)^k$, $k = 1, \dots, p-1$, аннулируется многочленом $G_k(x)$, определенным в следствии 1. Будем использовать обозначения из следствия 1. Так как $\bar{u}$ — ЛРП максимального периода над полем $\bar{R}$, то ξ_0 — примитивный элемент поля $\Gamma(S) = GF(p^m)$. Так как $k \in \{1, \dots, p-1\}$, при различных мультимножествах

$$\langle r_1, \dots, r_k \rangle, \quad r_t \in \{0, 1, \dots, m-1\},$$

числа $p^{r_1} + \dots + p^{r_k}$ будут различными числами из отрезка $\{1, \dots, p^m - 1\}$. Поэтому элементы $\xi_0^{p^{r_1} + \dots + p^{r_k}}$ будут различными. Следовательно, и элементы $\xi_{r_1, \dots, r_k}$ будут различными. Отсюда вытекает, что в случае, когда $\bar{u}$ — ЛРП максимального периода, справедливо равенство

$$G_k(x) = \prod_{\langle r_1, \dots, r_k \rangle} (x - \xi_{r_1, \dots, r_k}), \quad (16)$$

где произведение берется по всем различным мультимножествам

$$\langle r_1, \dots, r_k \rangle, \quad r_1, \dots, r_k \in \{0, 1, \dots, m-1\}.$$

Степень многочлена $G_k(x)$ равна числу таких мультимножеств, то есть

$$\deg G_k(x) = \binom{m+k-1}{k}.$$

При этом

$$\text{rank}_R u^k \leq \deg G_k(x) = \binom{m+k-1}{k}.$$

В силу [2, 8, 9, 18]

$$\text{rank}_{\bar{R}} \bar{u}^k = \binom{m+k-1}{k},$$

поэтому

$$\text{rank}_R u^k = \binom{m+k-1}{k},$$

и многочлен $G_k(x)$ является минимальным многочленом ЛРП u^k над кольцом R . Из этих рассуждений также следует, что $G_k(x)$ — минимальный многочлен ЛРП pu^k над R . Поэтому $G_k(x)$ — минимальный многочлен ЛРП $c_k u^k$ над кольцом R для любого $k \in \mathcal{L}$.

Докажем, что многочлены $x - e, G_1(x), \dots, G_{p-1}(x)$ попарно взаимно просты. Так как $\bar{\xi}_0$ — примитивный элемент поля $\bar{S}$, при $1 \leq k < l \leq p-1$ любые два корня

$$\begin{aligned} \bar{\xi}_{r_1, \dots, r_k} &= \bar{\xi}_0^{p^{r_1} + \dots + p^{r_k}}, & r_1, \dots, r_k &\in \{0, 1, \dots, m-1\}, \\ \bar{\xi}_{r'_1, \dots, r'_l} &= \bar{\xi}_0^{p^{r'_1} + \dots + p^{r'_l}}, & r'_1, \dots, r'_l &\in \{0, 1, \dots, m-1\}, \end{aligned}$$

соответственно многочленов $\bar{G}_k(x)$ и $\bar{G}_l(x)$ различны. Поэтому многочлены $\bar{G}_k(x)$ и $\bar{G}_l(x)$ взаимно просты над полем $\bar{R}$. Кроме того, из условия $m \geq 2$ вытекает, что $\bar{\xi}_{r_1, \dots, r_k} \neq \bar{e}$ для любого $k \in \{1, \dots, p-1\}$. Поэтому многочлены $\bar{G}_k(x)$ и $x - \bar{e}$ взаимно просты над полем $\bar{R}$. Из (2.1) в [17] теперь следует, что многочлены $x - e, G_1(x), \dots, G_{p-1}(x)$ попарно взаимно просты над кольцом R .

Таким образом, ЛРП v есть сумма последовательностей $\bar{c}_k u^k$, $k \in \mathcal{L}$, с попарно взаимно простыми минимальными многочленами $G_k(x)$. В силу утверждения 6(б) из [17], произведение указанных минимальных многочленов, то есть многочлен

$$G(x) = \prod_{k \in \mathcal{L}} G_k(x),$$

где $G_0(x) = x - e$, является минимальным многочленом ЛРП v над кольцом R . В частности,

$$\text{rank}_R v = \sum_{k \in \mathcal{L}} \deg G_k(x) = \sum_{k \in \mathcal{L}} \binom{m+k-1}{k}.$$

Следствие 4. В условиях теоремы 2 многочлен

$$G(x) = \prod_{k \in \mathcal{L}} G_k(x)$$

является минимальным многочленом ЛРП v над кольцом R . Здесь $G_0(x) = x - e$ и

$$G_k(x) = \prod_{\langle r_1, \dots, r_k \rangle} (x - \xi_{r_1, \dots, r_k}),$$

где произведение берется по всем различным мультимножествам

$$\langle r_1, \dots, r_k \rangle, \quad r_1, \dots, r_k \in \{0, 1, \dots, m-1\},$$

а элемент $\xi_{r_1, \dots, r_k} \in S$ определен в следствии 1. Аннулятор последовательности v равен

$$\text{Ann}(v) = (G(x), pH(x)),$$

где

$$H(x) = \prod_{k \in \mathcal{L}} G_k(x), \quad \bar{\mathcal{L}} = \{k \in \{0, 1, \dots, p-1\} : \bar{c}_k \neq 0\}. \quad (17)$$

Доказательство. То, что $G(x)$ — минимальный многочлен ЛРП v , было установлено в доказательстве теоремы 2. В силу [17] аннулятор ЛРП v есть идеал вида $(G(x), pH(x))$, где $G(x)$ — произвольный минимальный многочлен ЛРП v , $H(x)$ — произвольный минимальный многочлен ЛРП pv . Последнее эквивалентно тому, что $\bar{H}(x)$ — минимальный многочлен ЛРП $\bar{v}$ и $H(x)$ — унитарный многочлен. В силу [2, 8, 9, 18] этим условиям удовлетворяет многочлен (17).

5. Полиномиальные преобразования нескольких линейных рекуррент, верхняя оценка ранга

Пусть $u_t \in L_R(F_t)$, где $F_t(x)$ — многочлен Галуа над кольцом R степени $m_t \geq 1$, $t = 1, \dots, s$. Рассмотрим последовательность над кольцом R вида

$$v(i) = \Phi(u_1(i), \dots, u_s(i)), \quad i \geq 0,$$

где $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$. Если

$$\Phi(x_1, \dots, x_s) = \sum_{k_1, \dots, k_s \geq 0} c_{k_1, \dots, k_s} x_1^{k_1} \dots x_s^{k_s}, \quad (18)$$

то определим многочлены $\Phi^*(x_1, \dots, x_s)$ и $\bar{\Phi}^*(x_1, \dots, x_s)$ над полем рациональных чисел $\mathbb{Q}$ равенствами

$$\Phi^*(x_1, \dots, x_s) = \sum_{k_1, \dots, k_s \geq 0} c_{k_1, \dots, k_s}^* \binom{x_1 + k_1 - 1}{k_1} \dots \binom{x_s + k_s - 1}{k_s}, \quad (19)$$

$$\bar{\Phi}^*(x_1, \dots, x_s) = \sum_{k_1, \dots, k_s \geq 0} \bar{c}_{k_1, \dots, k_s}^* \binom{x_1 + k_1 - 1}{k_1} \dots \binom{x_s + k_s - 1}{k_s}, \quad (20)$$

где

$$c_{k_1, \dots, k_s}^* = \begin{cases} 1, & \text{если } c_{k_1, \dots, k_s} \neq 0, \\ 0, & \text{если } c_{k_1, \dots, k_s} = 0, \end{cases} \quad (21)$$

$$\bar{c}_{k_1, \dots, k_s}^* = \begin{cases} 1, & \text{если } \bar{c}_{k_1, \dots, k_s} \neq 0, \\ 0, & \text{если } \bar{c}_{k_1, \dots, k_s} = 0. \end{cases} \quad (22)$$

Отметим, что если многочлен Φ свободен от квадратов, то

$$\Phi(x_1, \dots, x_s) = \sum_{0 \leq k_1, \dots, k_s \leq 1} c_{k_1, \dots, k_s} x_1^{k_1} \dots x_s^{k_s}$$

и

$$\Phi^*(x_1, \dots, x_s) = \sum_{0 \leq k_1, \dots, k_s \leq 1} c_{k_1, \dots, k_s}^* x_1^{k_1} \dots x_s^{k_s},$$

то есть многочлен $\Phi^*(x_1, \dots, x_s)$ такой же, как и многочлен, введенный в [10].

Для ЛРП над полем последовательность $\Phi(u_1, \dots, u_s)$ рассматривалась в [4, 5, 6, 10, 18]. Сформулируем следствие одного из результатов работы [10], которое в нашем контексте является формулой для ранга ЛРП $\bar{v}$ над полем $\bar{R}$: если многочлен $\Phi(x_1, \dots, x_s)$ свободен от квадратов, то

$$\text{rank}_{\bar{R}} \bar{v} \leq \bar{\Phi}^*(m_1, \dots, m_s);$$

если при этом $\bar{u}_t$ — ЛРП максимального периода над полем $\bar{R}$, $t = 1, \dots, s$, и числа $m_1, \dots, m_s$ попарно взаимно просты, то

$$\text{rank}_{\bar{R}} \bar{v} = \bar{\Phi}^*(m_1, \dots, m_s).$$

Мы получим аналогичный результат для ранга последовательности v над кольцом R . При этом мы не предполагаем, что многочлен Φ свободен от квадратов. В этом параграфе будет получена верхняя оценка

$$\text{rank}_R v \leq \Phi^*(m_1, \dots, m_s),$$

а в следующем будет доказано, что если числа $m_1, \dots, m_s$ попарно взаимно просты, $\bar{u}_t$ — ЛРП максимального периода над полем $\bar{R}$ и степень многочлена $\Phi(x_1, \dots, x_s)$ по переменной x_t меньше, чем $\min\{p, m_t, (p-2)m_t/(p-1) + 1\}$, $t = 1, \dots, s$, то

$$\text{rank}_R v = \Phi^*(m_1, \dots, m_s).$$

Теорема 3. Пусть $u_t \in L_R(F_t)$, где $F_t(x)$ — многочлен Галуа над кольцом R степени $m_t \geq 1$, $t = 1, \dots, s$, и пусть $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$. Тогда для ранга последовательности

$$v(i) = \Phi(u_1(i), \dots, u_s(i)), \quad i \geq 0,$$

над кольцом R справедлива оценка

$$\text{rank}_R v \leq \Phi^*(m_1, \dots, m_s).$$

Доказательство. Рассмотрим вначале случай, когда $\bar{u}_t \neq 0$, $t = 1, \dots, s$. Пусть ξ_t — корень многочлена $F_t(x)$ в расширении Галуа $S_t = GR(q_t^2, p^2)$, $q_t = p^{m_t}$, кольца R , и пусть

$$u_t(i) = \text{Tr}_R^{S_t}(a_t \xi_t^i), \quad i \geq 0, \quad a_t \in S_t, \quad t = 1, \dots, s. \quad (23)$$

Все элементы a_t , ξ_t принадлежат расширению Галуа $S = GR(q^2, p^2)$ кольца R , где $q = p^{m_1 \dots m_s}$. Пусть p -адические разложения этих элементов имеют вид

$$a_t = a_{t0} + p a_{t1}, \quad \xi_t = \xi_{t0} + p \xi_{t1}, \quad a_{t0}, a_{t1}, \xi_{t0}, \xi_{t1} \in \Gamma(S_t) \subseteq \Gamma(S). \quad (24)$$

Тогда, согласно (7),

$$u_t(i) = \sum_{r=0}^{m_t-1} (a_{t0}^{p^r} + p a_{t1}^{p^r} + p i (a_{t0} \xi_{t0}^{-1} \xi_{t1})^{p^r}) (\xi_{t0}^i)^{p^r}, \quad i \geq 0.$$

Так как $\bar{u}_t \neq 0$, то $a_{t0} \neq 0$, и это соотношение можно записать в виде

$$u_t(i) = \sum_{r=0}^{m_t-1} (a_{t0} \xi_{t0}^i)^{p^r} (1 + p (a_{t0}^{-1} a_{t1})^{p^r} + p i (\xi_{t0}^{-1} \xi_{t1})^{p^r}), \quad i \geq 0.$$

Возводя в степень $k \geq 0$, получим, что

$$u_t^k(i) = \sum \frac{k!}{k_0! \dots k_{m_t-1}!} \prod_{r=0}^{m_t-1} ((a_{t0} \xi_{t0}^i)^{p^r} (1 + p (a_{t0}^{-1} a_{t1})^{p^r} + p i (\xi_{t0}^{-1} \xi_{t1})^{p^r}))^{k_r},$$

где сумма берется по всем целым неотрицательным $k_0, \dots, k_{m_t-1}$ таким, что $k_0 + \dots + k_{m_t-1} = k$. Возводя в степень k_r каждую скобку и перемножая m_t скобок,

получим (с учетом того, что характеристика кольца S равна p^2), что

$$u_t^k(i) = \sum_{\substack{k_0 + \dots + k_{m_t-1} = k \\ k_0, \dots, k_{m_t-1} \geq 0}} \frac{k!}{k_0! \dots k_{m_t-1}!} (a_{t0} \xi_{t0}^i)^{k_0 + pk_1 + \dots + p^{m_t-1} k_{m_t-1}} \times \left(1 + p \sum_{r=0}^{m_t-1} k_r (a_{t0}^{-1} a_{t1})^{p^r} + pi \sum_{r=0}^{m_t-1} k_r (\xi_{t0}^{-1} \xi_{t1})^{p^r} \right). \quad (25)$$

Теперь заметим, что последовательность $v = \Phi(u_1, \dots, u_s)$ есть сумма последовательностей $u_1^{k_1} \dots u_s^{k_s}$ с коэффициентами $c_{k_1, \dots, k_s}$. Пользуясь соотношением (25), находим, что

$$u_1^{k_1}(i) \dots u_s^{k_s}(i) = \prod_{t=1}^s \sum_{\substack{k_{t0} + \dots + k_{t,m_t-1} = k_t \\ k_{t0}, \dots, k_{t,m_t-1} \geq 0}} \frac{k_t!}{k_{t0}! \dots k_{t,m_t-1}!} (a_{t0} \xi_{t0}^i)^{k_{t0} + pk_{t1} + \dots + p^{m_t-1} k_{t,m_t-1}} \times \left(1 + p \sum_{r=0}^{m_t-1} k_{tr} (a_{t0}^{-1} a_{t1})^{p^r} + pi \sum_{r=0}^{m_t-1} k_{tr} (\xi_{t0}^{-1} \xi_{t1})^{p^r} \right).$$

Перемножая s сумм, получим, что

$$u_1^{k_1}(i) \dots u_s^{k_s}(i) = \sum_{\substack{k_{t0} + \dots + k_{t,m_t-1} = k_t \\ k_{tr} \geq 0, 1 \leq t \leq s}} \left(\prod_{t=1}^s \frac{k_t!}{k_{t0}! \dots k_{t,m_t-1}!} (a_{t0} \xi_{t0}^i)^{k_{t0} + pk_{t1} + \dots + p^{m_t-1} k_{t,m_t-1}} \right) \times \left(1 + p \sum_{t=1}^s \sum_{r=0}^{m_t-1} k_{tr} (a_{t0}^{-1} a_{t1})^{p^r} + pi \sum_{t=1}^s \sum_{r=0}^{m_t-1} k_{tr} (\xi_{t0}^{-1} \xi_{t1})^{p^r} \right). \quad (26)$$

Каждое слагаемое этой суммы есть последовательность вида

$$z(i) = c(1 + pb + pi\eta)\theta^i, \quad i \geq 0,$$

где b, c, η, θ — некоторые константы, зависящие от набора

$$K = (k_{10}, \dots, k_{1,m_1-1}, \dots, k_{s0}, \dots, k_{s,m_s-1}),$$

в частности,

$$\theta = \prod_{t=1}^s \xi_{t0}^{k_{t0} + pk_{t1} + \dots + p^{m_t-1} k_{t,m_t-1}},$$

$$\eta = \sum_{t=1}^s \sum_{r=0}^{m_t-1} k_{tr} (\xi_{t0}^{-1} \xi_{t1})^{p^r}. \quad (27)$$

Положим

$$\xi_K = \theta(1 + p\eta). \quad (28)$$

В обозначении ξ_K учитывается зависимость от набора K . Как и в (13), устанавливается, что последовательность z аннулируется многочленом $x - \xi_K$. Следовательно, последовательность (26) аннулируется многочленом

$$G_{k_1, \dots, k_s}(x) = \prod_{\xi_K} (x - \xi_K), \quad (29)$$

где произведение берется по всем различным элементам ξ_K , когда наборы

$$K = (k_{10}, \dots, k_{1, m_1-1}, \dots, k_{s0}, \dots, k_{s, m_s-1})$$

удовлетворяют условиям

$$k_{t0} + \dots + k_{t, m_t-1} = k_t, \quad k_{tr} \geq 0, \quad t = 1, \dots, s, \quad r = 0, 1, \dots, m_t - 1.$$

Мы полагаем $G_{0, \dots, 0}(x) = x - e$. Степень многочлена $G_{k_1, \dots, k_s}(x)$ равна числу различных элементов ξ_K и не превосходит числа наборов K , удовлетворяющих указанным условиям. Последняя величина, как известно [19], равна

$$\binom{m_1 + k_1 - 1}{k_1} \dots \binom{m_s + k_s - 1}{k_s}.$$

Следовательно,

$$\deg G_{k_1, \dots, k_s}(x) \leq \binom{m_1 + k_1 - 1}{k_1} \dots \binom{m_s + k_s - 1}{k_s}.$$

Докажем, что $G_{k_1, \dots, k_s}(x) \in R[x]$. Для этого, как и в доказательстве теоремы 1, достаточно проверить, что $\sigma_0(\xi_K) = \xi_{K'}$ для некоторого набора K' , где σ_0 — автоморфизм Фробениуса кольца S над R . Действительно,

$$\sigma_0(\xi_K) = \sigma_0(\theta(1 + p\eta)) = \sigma_0(\theta)(1 + p\sigma_0(\eta)).$$

Так как $\theta \in \Gamma(S)$, то, ввиду (6), $\sigma_0(\theta) = \theta^p$. Кроме того, в силу (6),

$$p\sigma_0(\eta) = p\gamma_0(\eta)^p = p\eta^p.$$

Отсюда

$$\begin{aligned} \sigma_0(\xi_K) &= \theta^p(1 + p\eta^p) \\ &= \prod_{t=1}^s (\xi_{t0}^{k_{t0} + pk_{t1} + \dots + p^{m_t-1}k_{t, m_t-1}})^p \left(1 + p \sum_{t=1}^s \sum_{r=0}^{m_t-1} (k_{tr}(\xi_{t0}^{-1}\xi_{t1})^{p^r})^p \right). \end{aligned}$$

С учетом соотношений $\xi_{t0}^{p^{m_t}} = \xi_{t0}$, $\xi_{t1}^{p^{m_t}} = \xi_{t1}$, $k_{tr}^p \equiv k_{tr} \pmod{p}$, получаем, что $\sigma_0(\xi_K) = \xi_{K'}$ для набора

$$\begin{aligned} K' = (k_{10} + 1 \pmod{m_1}, \dots, k_{1, m_1-1} + 1 \pmod{m_1}, \dots, \\ k_{s0} + 1 \pmod{m_s}, \dots, k_{s, m_s-1} + 1 \pmod{m_s}). \end{aligned}$$

Тем самым мы доказали, что $G_{k_1, \dots, k_s}(x) \in R[x]$. Следовательно, $G_{k_1, \dots, k_s}(x)$ — характеристический многочлен последовательности $u_1^{k_1} \dots u_s^{k_s}$ над кольцом R . Многочлен $G_{0, \dots, 0}(x) = x - e$ является характеристическим многочленом последовательности-константы $\Phi(0, \dots, 0) = c_{0, \dots, 0}$.

Так как последовательность $v = \Phi(u_1, \dots, u_s)$ есть сумма последовательностей $u_1^{k_1} \dots u_s^{k_s}$ с коэффициентами $c_{k_1, \dots, k_s}$, ЛРП v аннулируется многочленом

$$G(x) = \prod_{\substack{k_1, \dots, k_s \geq 0 \\ c_{k_1, \dots, k_s} \neq 0}} G_{k_1, \dots, k_s}(x). \quad (30)$$

Следовательно,

$$\begin{aligned} \text{rank}_R v &\leq \deg G(x) = \sum_{\substack{k_1, \dots, k_s \geq 0 \\ c_{k_1, \dots, k_s} \neq 0}} \deg G_{k_1, \dots, k_s}(x) \\ &\leq \sum_{\substack{k_1, \dots, k_s \geq 0 \\ c_{k_1, \dots, k_s} \neq 0}} \binom{m_1 + k_1 - 1}{k_1} \dots \binom{m_s + k_s - 1}{k_s} = \Phi^*(m_1, \dots, m_s), \end{aligned}$$

что и требовалось доказать.

Рассмотрим теперь случай, когда $\bar{u}_t = 0$ хотя бы для одного $t \in \{1, \dots, s\}$. Можно записать

$$u_t = p^{\varepsilon_t} u'_t, \quad \text{где } \varepsilon_t \in \{0, 1, 2\}, \quad u'_t \in L_R(F_t), \quad \bar{u}'_t \neq 0, \quad t \in \{1, \dots, s\}.$$

Рассмотрим многочлен

$$\tilde{\Phi}(x_1, \dots, x_s) = \Phi(p^{\varepsilon_1} x_1, \dots, p^{\varepsilon_s} x_s).$$

Очевидно, $\tilde{\Phi}^*(m_1, \dots, m_s) \leq \Phi^*(m_1, \dots, m_s)$. При этом

$$v = \Phi(u_1, \dots, u_s) = \Phi(p^{\varepsilon_1} u'_1, \dots, p^{\varepsilon_s} u'_s) = \tilde{\Phi}(u'_1, \dots, u'_s).$$

Пользуясь уже доказанным, получим, что

$$\text{rank } v = \text{rank } \tilde{\Phi}(u'_1, \dots, u'_s) \leq \tilde{\Phi}^*(m_1, \dots, m_s) \leq \Phi^*(m_1, \dots, m_s).$$

Теорема доказана.

Следствие 5. В условиях теоремы 3 многочлен $G(x)$, определяемый соотношениями (30), (29), (28), (27), (24) и (23), является характеристическим многочленом ЛРП v над кольцом R . Справедливо включение

$$\text{Ann}(v) \supset (G(x), pH(x)),$$

где

$$H(x) = \prod_{\substack{k_1, \dots, k_s \geq 0 \\ c_{k_1, \dots, k_s} \neq 0}} G_{k_1, \dots, k_s}(x).$$

Заметим, что если степень многочлена $\Phi(x_1, \dots, x_s)$ по некоторой переменной больше $p^2 - 1$, то эта степень может быть понижена с учетом тождества $x^{p^2} = x^p$ в кольце R (см. замечание 1). Перед применением теоремы 3 полезно добиться того, чтобы степень многочлена Φ по каждой переменной не превосходила $p^2 - 1$.

6. Полиномиальные преобразования нескольких линейных рекуррент, точная формула для ранга

При дополнительных условиях на последовательности $u_1, \dots, u_s$ и на $\Phi(x_1, \dots, x_s)$ удастся получить точную формулу для ранга последовательности $v = \Phi(u_1, \dots, u_s)$ над кольцом R . Вывод этой формулы основывается на следующей лемме.

Лемма 1. Если ξ — примитивный элемент поля $GF(p^m)$ и $\xi^{a-b} \in GF(p)$, где

$$a, b \in \{0, 1, \dots, p^m - 1\}, \quad 0 \leq w(a), w(b) < \min\{m, (p-2)m/(p-1) + 1\}, \quad (31)$$

то $a = b$.

Доказательство. Так как $w(a), w(b) < m$, то $a, b \in \{0, 1, \dots, p^m - 2\}$. По условию $\xi^b = \lambda \xi^a$, $\lambda \in GF(p)^*$. Если $\lambda = 1$, то $a = b$ и все доказано.

Пусть $\lambda \neq 1$. Тогда из равенства $\xi^b = \lambda \xi^a$ следует, что

$$b \equiv (1 + p + \dots + p^{m-1})t + a \pmod{p^m - 1}$$

для некоторого $t \in \{1, \dots, p-2\}$. Тогда

$$w(b) = mt + w(a) - (p-1)c,$$

где c — число переносов, возникающих при сложении чисел $(1 + p + \dots + p^{m-1})t$ и a в p -ичной системе счисления и приведении по модулю $p^m - 1$, когда перенос, возникающий в $(m-1)$ -м разряде, складывается не с m -м, а с нулевым разрядом. Если $c = 0$, то $w(b) = mt + w(a) \geq m$, что противоречит условию (31). Следовательно, $c \geq 1$, то есть при сложении чисел $(1 + p + \dots + p^{m-1})t$ и a в p -ичной системе счисления должны возникать переносы.

Чтобы при сложении с числом $(1 + p + \dots + p^{m-1})t$ возник перенос, к нему нужно добавить число веса не менее $p-t$ (например, число, равное $p-t$). Чтобы возникали последующие переносы, нужно добавлять числа веса не менее $p-t-1$ (например, числа $(p-t-1)p^i$, $i = 1, 2, \dots$). Чтобы возникло $c \geq 1$ переносов, нужно добавить число веса не менее $(p-t) + (p-t-1)(c-1) = (p-t-1)c + 1$. Следовательно,

$$w(a) \geq (p-t-1)c + 1.$$

Пользуясь условием (31), получаем неравенство $(p-t-1)c + 1 < (p-2)m/(p-1) + 1$. Следовательно, число переносов c ограничено величиной

$$c < \frac{(p-2)m}{(p-1)(p-t-1)}.$$

Из этих соотношений следует, что вес числа b удовлетворяет неравенству

$$\begin{aligned} w(b) &= mt + w(a) - (p-1)c \geq mt + (p-t-1)c + 1 - (p-1)c \\ &= mt - ct + 1 > mt - \frac{(p-2)mt}{(p-1)(p-t-1)} + 1. \end{aligned}$$

Обозначим правую часть последнего соотношения через $f(t)$ и найдем минимум функции $f(t)$ при $t \in \{1, \dots, p-2\}$. Производная

$$f'(t) = m \left(1 - \frac{p-2}{(p-t-1)^2} \right) \leq 0$$

при $t \geq 1$, поэтому минимум достигается при $t = p - 2$ и равен

$$f(p - 2) = \frac{p - 2}{p - 1}m + 1.$$

В итоге

$$w(b) > \frac{p - 2}{p - 1}m + 1,$$

что противоречит условию. Значит, случай $\lambda \neq 1$ невозможен.

Теорема 4. Пусть $u_t \in L_R(F_t)$, где $F_t(x)$ — многочлен Галуа над кольцом R степени $m_t \geq 1$, $t = 1, \dots, s$, и пусть $\Phi(x_1, \dots, x_s) \in R[x_1, \dots, x_s]$. Предположим, что выполняются следующие условия:

- (1) $\bar{u}_t$ — ЛРП максимального периода над полем $\bar{R}$, $t = 1, \dots, s$;
- (2) числа $m_1, \dots, m_s$ попарно взаимно просты;
- (3) степень d_t многочлена $\Phi(x_1, \dots, x_s)$ по переменной x_t меньше, чем

$$M_t = \min\{p, m_t, (p - 2)m_t/(p - 1) + 1\}, \quad t = 1, \dots, s.$$

Тогда ранг последовательности

$$v(i) = \Phi(u_1(i), \dots, u_s(i)), \quad i \geq 0,$$

над кольцом R вычисляется по формуле

$$\text{rank}_R v = \Phi^*(m_1, \dots, m_s), \quad (32)$$

где $\Phi^*(x_1, \dots, x_s)$ — многочлен, определяемый соотношениями (18), (19), (21).

Доказательство. Последовательность v есть сумма последовательностей $u_1^{k_1} \dots u_s^{k_s}$ с коэффициентами $c_{k_1, \dots, k_s}$, где $0 \leq k_t < M_t$, $t = 1, \dots, s$. В ходе доказательства теоремы 3 установлено, что последовательность $u_1^{k_1} \dots u_s^{k_s}$ имеет вид (26) и аннулируется многочленом

$$G_{k_1, \dots, k_s}(x) = \prod_{\xi_K} (x - \xi_K),$$

где произведение берется по всем различным элементам ξ_K (определенным в (27), (28)), когда наборы

$$K = (k_{10}, \dots, k_{1, m_1 - 1}, \dots, k_{s0}, \dots, k_{s, m_s - 1})$$

удовлетворяют условиям

$$k_{t0} + \dots + k_{t, m_t - 1} = k_t, \quad k_{tr} \geq 0, \quad t = 1, \dots, s, \quad r = 0, 1, \dots, m_t - 1.$$

Мы считаем, что набору $K = (0, 0, \dots, 0)$ соответствует элемент $\xi_K = e$ и, следовательно, $G_{0, \dots, 0}(x) = x - e$.

Докажем, что элементы $\bar{\xi}_K$ различны при различных наборах K . Предположим, что $\bar{\xi}_K = \bar{\xi}_{K'}$, где K, K' — два набора, удовлетворяющих указанным условиям. Введем обозначения

$$\begin{aligned} b_t &= k_{t0} + pk_{t1} + \dots + p^{m_t-1}k_{t,m_t-1}, \\ b'_t &= k'_{t0} + pk'_{t1} + \dots + p^{m_t-1}k'_{t,m_t-1}, \quad t = 1, \dots, s. \end{aligned}$$

Так как $k_{t0} + \dots + k_{t,m_t-1} = k_t$ и $k_t < M_t \leq p$, то b_t — число из отрезка $\{0, 1, \dots, p^{m_t} - 1\}$ веса $w(b_t) = k_t$. Аналогично

$$b'_t \in \{0, 1, \dots, p^{m_t} - 1, \quad w(b'_t) = k'_t.$$

Согласно определениям (27), (28)

$$\bar{\xi}_K = \bar{\xi}_{10}^{b_1} \dots \bar{\xi}_{s0}^{b_s}, \quad \bar{\xi}_{K'} = \bar{\xi}_{10}^{b'_1} \dots \bar{\xi}_{s0}^{b'_s}.$$

Так как числа $m_1, \dots, m_s$ попарно взаимно просты, из равенства $\bar{\xi}_K = \bar{\xi}_{K'}$ следует, что

$$\bar{\xi}_{t0}^{b_t - b'_t} \in GF(p), \quad t = 1, \dots, s.$$

Так как $w(b_t) = k_t < M_t$ и $w(b'_t) = k'_t < M_t$, применима лемма 1, в силу которой

$$b_t = b'_t, \quad t = 1, \dots, s.$$

Из равенства $b_t = b'_t$ и условий

$$k_{t0} + \dots + k_{t,m_t-1} = k_t < p, \quad k'_{t0} + \dots + k'_{t,m_t-1} = k'_t < p$$

следует, что

$$k_{t0} = k'_{t0}, \dots, k_{t,m_t-1} = k'_{t,m_t-1}, \quad t = 1, \dots, s.$$

Таким образом, наборы K и K' совпадают. Тем самым мы доказали, что при различных наборах K элементы $\bar{\xi}_K$ различны.

Для многочлена $G_{k_1, \dots, k_s}(x)$ тогда справедливо равенство

$$G_{k_1, \dots, k_s}(x) = \prod_K (x - \xi_K), \quad (33)$$

где произведение берется по всем наборам

$$K = (k_{10}, \dots, k_{1,m_1-1}, \dots, k_{s0}, \dots, k_{s,m_s-1}),$$

удовлетворяющим условиям

$$k_{t0} + \dots + k_{t,m_t-1} = k_t, \quad k_{tr} \geq 0, \quad t = 1, \dots, s, \quad r = 0, 1, \dots, m_t - 1.$$

Степень многочлена $G_{k_1, \dots, k_s}(x)$ равна числу таких наборов и равна

$$\deg G_{k_1, \dots, k_s}(x) = \binom{m_1 + k_1 - 1}{k_1} \dots \binom{m_s + k_s - 1}{k_s}.$$

Рассмотрим последовательность $\bar{u}_1^{k_1} \dots \bar{u}_s^{k_s}$ над полем $\bar{R}$. Ввиду (26)

$$\begin{aligned} & \bar{u}_1^{k_1}(i) \dots \bar{u}_s^{k_s}(i) \\ &= \sum_{\substack{k_{t0} + \dots + k_{t, m_t-1} = k_t \\ k_{tr} \geq 0, 1 \leq t \leq s}} \prod_{t=1}^s \frac{k_t!}{k_{t0}! \dots k_{t, m_t-1}!} (\bar{a}_{t0} \bar{\xi}_{t0}^i)^{k_{t0} + p k_{t1} + \dots + p^{m_t-1} k_{t, m_t-1}}. \end{aligned} \quad (34)$$

В правой части находится сумма биномиальных последовательностей с корнями $\bar{\xi}_K$. Так как $k_t < p$ и $\bar{u}_t \neq 0$, коэффициенты при биномиальных последовательностях, равные произведению полиномиальных коэффициентов и степеней элементов $\bar{a}_{t0}$, не равны нулю в поле $\bar{R}$. Как показано выше, корни $\bar{\xi}_K$ биномиальных последовательностей различны при различных наборах K . Следовательно, минимальный многочлен последовательности (34) над полем $\bar{R}$ равен

$$\prod_K (x - \bar{\xi}_K)$$

и совпадает с многочленом $\bar{G}_{k_1, \dots, k_s}(x)$. При этом последовательность $u_1^{k_1} \dots u_s^{k_s}$ над кольцом R аннулируется многочленом $G_{k_1, \dots, k_s}(x)$, поэтому $G_{k_1, \dots, k_s}(x)$ — минимальный многочлен ЛРП $u_1^{k_1} \dots u_s^{k_s}$ над кольцом R . Более того, из приведенных рассуждений следует, что $G_{k_1, \dots, k_s}(x)$ — минимальный многочлен ЛРП $cu_1^{k_1} \dots u_s^{k_s}$ для любой константы $c \in R \setminus \{0\}$.

Из того, что элементы $\bar{\xi}_K$ различны при различных наборах K следует, во-первых, что многочлены $\bar{G}_{k_1, \dots, k_s}(x)$ не имеют общих корней в поле разложения $\bar{S}$ и, следовательно, попарно взаимно просты над полем $\bar{R}$ при различных $(k_1, \dots, k_s)$ таких, что $0 \leq k_t < M_t$, $t = 1, \dots, s$, и, во-вторых, что многочлен $\bar{G}_{k_1, \dots, k_s}(x)$ не имеет кратных корней в поле разложения $\bar{S}$. Из (2.1) в [17] теперь следует, что многочлены $G_{k_1, \dots, k_s}(x)$, где $0 \leq k_t < M_t$, $t = 1, \dots, s$, попарно взаимно просты над кольцом R .

В результате получаем, что ЛРП v есть сумма последовательностей

$$c_{k_1, \dots, k_s} u_1^{k_1} \dots u_s^{k_s}, \quad c_{k_1, \dots, k_s} \neq 0,$$

минимальные многочлены $G_{k_1, \dots, k_s}(x)$ которых над кольцом R попарно взаимно просты. В силу утверждение 6(б) из [17] произведение

$$G(x) = \prod_{\substack{k_1, \dots, k_s \geq 0 \\ c_{k_1, \dots, k_s} \neq 0}} G_{k_1, \dots, k_s}(x) \quad (35)$$

минимальных многочленов этих последовательностей является минимальным многочленом ЛРП v над кольцом R . При этом

$$\begin{aligned} \text{rank}_R v = \deg G(x) &= \sum_{\substack{k_1, \dots, k_s \geq 0 \\ c_{k_1, \dots, k_s} \neq 0}} \deg G_{k_1, \dots, k_s}(x) \\ &= \sum_{\substack{k_1, \dots, k_s \geq 0 \\ c_{k_1, \dots, k_s} \neq 0}} \binom{m_1 + k_1 - 1}{k_1} \dots \binom{m_s + k_s - 1}{k_s} = \Phi^*(m_1, \dots, m_s), \end{aligned}$$

что и требовалось доказать.

Следствие 6. В условиях теоремы 4 многочлен $G(x)$, определяемый соотношениями (35), (33), (28), (27), (24) и (23), является минимальным многочленом ЛРП v над кольцом R . Справедливо равенство

$$\text{Ann}(v) = (G(x), pH(x)),$$

где

$$H(x) = \prod_{\substack{k_1, \dots, k_s \geq 0 \\ \bar{c}_{k_1 \dots k_s} \neq 0}} G_{k_1, \dots, k_s}(x).$$

Доказательство. Из доказательства теоремы 4 следует, что $G(x)$ — минимальный многочлен ЛРП v над кольцом R и $\bar{H}(x)$ — минимальный многочлен ЛРП $\bar{v}$ над полем $\bar{R}$. Отсюда вытекают все утверждения следствия.

Заметим, что если многочлен $\Phi(x_1, \dots, x_s)$ свободен от квадратов, то есть степень d_t многочлена Φ по переменной x_t удовлетворяет условию $d_t \leq 1$, $t = 1, \dots, s$, то $d_t < M_t$ (при $m_t \geq 2$) и для такого многочлена выполняются условия теоремы 4. Следовательно, теорема 4 обобщает результат статьи [10] не только на последовательности над кольцом $\mathbf{Z}_{p^2}$, но и на более широкий класс многочленов Φ в случае последовательностей над полем $GF(p)$. В связи с этим сформулируем отдельно следствие теорем 3 и 4 для последовательностей над полем.

Следствие 7. Пусть u_t , $t = 1, \dots, s$, — ЛРП над полем $P = GF(p)$ с неприводимым характеристическим многочленом $F_t(x) \in P[x]$ степени $m_t \geq 1$, и

$$v(i) = \Phi(u_1(i), \dots, u_s(i)), \quad i \geq 0,$$

где $\Phi(x_1, \dots, x_s) \in P[x_1, \dots, x_s]$. Тогда

$$\text{rank}_P v \leq \Phi^*(m_1, \dots, m_s),$$

где $\Phi^*(x_1, \dots, x_s)$ — многочлен над полем рациональных чисел $\mathbf{Q}$, определяемый соотношениями (18), (19), (21). Пусть

- (1) u_t — ЛРП максимального периода над полем P , $t = 1, \dots, s$;
- (2) числа $m_1, \dots, m_s$ попарно взаимно просты;
- (3) степень многочлена $\Phi(x_1, \dots, x_s)$ по переменной x_t меньше, чем $\min\{p, m_t, (p-2)m_t/(p-1) + 1\}$, $t = 1, \dots, s$.

Тогда

$$\text{rank}_P v = \Phi^*(m_1, \dots, m_s). \quad (36)$$

Отметим, что в случае, когда многочлен $\Phi(x_1, \dots, x_s)$ свободен от квадратов, равенство (36) доказано в работах [4, 5, 6, 10] при значительно более общих условиях на последовательности $u_1, \dots, u_s$. Таким образом, по сравнению с указанными статьями, в следствии 7 рассматриваются многочлены Φ более общего вида, но на последовательности $u_1, \dots, u_s$ накладываются более сильные ограничения.

В условиях следствия 7 можно также описать характеристический многочлен ЛРП v над полем P . Пусть $\xi_t \in GF(p^{m_t})$ — корень многочлена $F_t(x)$, $t = 1, \dots, s$. Для $k_1, \dots, k_s \geq 0$ положим

$$G_{k_1, \dots, k_s}(x) = \prod_{\xi_1^{d_1} \dots \xi_s^{d_s}} (x - \xi_1^{d_1} \dots \xi_s^{d_s}),$$

где произведение берется по всем различным элементам $\xi_1^{d_1} \dots \xi_s^{d_s}$ поля $GF(p^{m_1 \dots m_t})$, когда $0 \leq d_t \leq p^{m_t} - 1$, $w(d_t) = k_t$, $t = 1, \dots, s$. Мы полагаем, что $G_{0, \dots, 0}(x) = x - e$. Тогда многочлен

$$G(x) = \prod_{\substack{k_1, \dots, k_s \geq 0 \\ c_{k_1 \dots k_s} \neq 0}} G_{k_1, \dots, k_s}(x)$$

является характеристическим многочленом последовательности v над полем P . Если числа $m_1, \dots, m_s$ попарно взаимно просты, u_t — ЛРП максимального периода над полем P и степень многочлена $\Phi(x_1, \dots, x_s)$ по переменной x_t меньше, чем $\min\{p, m_t, (p-2)m_t/(p-1)+1\}$, $t = 1, \dots, s$, то справедливо равенство

$$G_{k_1, \dots, k_s}(x) = \prod_{d_1, \dots, d_s} (x - \xi_1^{d_1} \dots \xi_s^{d_s}),$$

где произведение берется по всем $d_1, \dots, d_s$ таким, что $0 \leq d_t \leq p^{m_t} - 1$, $w(d_t) = k_t$, $t = 1, \dots, s$, и многочлен $G(x)$ является минимальным многочленом последовательности v над полем P .

Список литературы

1. Bernasconi J., Günter C. G. Analysis of a nonlinear feedforward logic for binary sequence generators. *Lect. Notes Comput. Sci.* (1986) **219**, 161–166.
2. Brynielsson L. On the linear complexity of combined shift register sequences. *Lect. Notes Comput. Sci.* (1986) **219**, 156–160.
3. Chan A. H., Goresky M., Klapper A. On the linear complexity of feedback registers. *IEEE Trans. Inform. Theory* (1990) **36**, №3, 640–644.
4. Golić S. D. On the linear complexity of functions of periodic $GF(q)$ sequences. *IEEE Trans. Inform. Theory* (1989) **35**, №1, 69–75.
5. Herlestam T. On the complexity of functions of linear shift register sequences. In: *Int. Symp. Inform. Theory*, Les Arc, France, 1982.
6. Herlestam T. On functions of linear shift register sequences. *Lect. Notes Comput. Sci.* (1986) **219**, 119–129.
7. Key E. L. An analysis of the structure and complexity of nonlinear binary sequence generators. *IEEE Trans. Inform. Theory*, (1976) **22**, №6, 732–736.
8. Klapper A. The vulnerability of geometric sequences based on fields of odd characteristic. *J. Cryptology*, (1994) **7**, 33–51.
9. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurrences over rings and modules. *J. Math. Sci.* (1995) **76**, № 6, 2793–2915.
10. Rueppel R. A., Staffelbach O. J. Products of linear recurring sequences with maximum complexity. *IEEE Trans. Inform. Theory* (1987) **33**, № 1, 126–131.

11. Selmer E. S. Linear recurrence relations over finite fields. In: *Dep. Math., Univ. Bergen*, Norway, 1966.
12. Vajda I., Nemetz T. Substitution of characters in q -ary m -sequences. *Lect. Notes Comput. Sci.* (1991) **508**, 96–105.
13. Zierler N., Mills W. H. Products of linear recurring sequences. *J. Algebra* (1973) **27**, №1, 147–157.
14. Глухов М. М., Елизаров В. П., Нечаев А. А. *Алгебра*, ч. II. Москва, 1991.
15. Лидл Р., Нидеррайтер Г. *Конечные поля*, т. 2. Мир, Москва, 1988.
16. Нечаев А. А. Код Кердока в циклической форме. *Дискретная математика* (1989) **1**, №4, 123–139.
17. Нечаев А. А. Линейные рекуррентные последовательности над коммутативными кольцами. *Дискретная математика* (1991) **3**, №4, 107–121.
18. Нечаев А. А., Куракин В. Л. *Линейные коды и полилинейные рекурренты*. Москва, 1997.
19. Сачков В. Н. *Введение в комбинаторные методы дискретной математики*. Наука, Москва, 1982.

Статья поступила 14.06.1998.