Math-Net.Ru

Общероссийский математический портал

В. Н. Цыпышев, Нижние оценки рангов координатных последовательностей линейных рекуррент максимального периода над собственным кольцом Галуа, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 3, 137–143

DOI: <https://doi.org/10.4213/mvk200>

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: 3.89.197.203

26 апреля 2023 г., 14:02:31

**Нижние оценки рангов
координатных последовательностей
линейных рекуррент максимального периода
над собственным кольцом Галуа**

В. Н. Цыпышев

Московский технологический университет МИРЭА, Москва

Получено 10.11.2015

Статья посвящается памяти А. С. Кузьмина

Аннотация. Кольцо Галуа называется собственным, если оно отлично от поля и от кольца вычетов. Для линейной рекуррентной последовательности максимального периода над собственным кольцом Галуа $R = GR(q^n, p^n)$, $p \geq 5$, получены нижние оценки рангов координатных последовательностей с такими номерами s , что $s = kr + 2$, $r = \lg_p q$, $k \in \mathbb{N}_0$.

Ключевые слова: кольцо Галуа, линейная рекуррентная последовательность, координатная последовательность, ранг последовательности

Lower estimates of ranks of coordinate sequences of maximal period linear recurrent sequences over the non-trivial Galois ring

V. N. Tsypyshev

Moscow Technological University MIREA, Moscow

Abstract. The Galois ring is called non-trivial if it is not a field and a residue ring. For the maximal period linear recurrent sequence over the non-trivial Galois ring $R = GR(q^n, p^n)$, $p \geq 5$, new lower estimates of ranks of coordinate sequences with numbers s such that $s = kr + 2$, $r = \lg_p q$, $k \in \mathbb{N}_0$ are obtained.

Key words: Galois ring, linear recurrent sequence, coordinate sequence, rank of sequence

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 3, pp. 137–143 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

Пусть $R = GR(q^n, p^n)$ — кольцо Галуа [11, 12], $q = p^r$, p — простое число, u — линейная рекуррента полного периода над кольцом R с характеристическим многочленом Галуа $F(x)$ степени m максимального периода $T(F) = T(u) = (q^m - 1)p^{n-1}$ [4]. Всюду далее кольцо R считается собственным, т. е. $r, n > 1$.

Подмножество $\Gamma(R) = \{\beta \in R: \beta^q = \beta\}$ (система представителей Тейхмюллера [3]) кольца Галуа $R = GR(q^n, p^n)$ называется p -адическим координатным множеством кольца R . Каждый элемент $a \in R$ однозначно представляется в виде

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

называемом разложением элемента a в координатном множестве $\Gamma(R)$. Функции

$$\gamma_s: R \rightarrow \Gamma(R), \quad \gamma_s(a) = a_s, \quad s \in \overline{0, n-1},$$

называются p -адическими координатными функциями.

Если u — последовательность над R , то последовательности u_s над множеством $\Gamma(R)$, определенные равенствами $u_s(i) = \gamma_s(u(i))$, $i \in \mathbb{N}_0$, называются координатными последовательностями в p -адическом координатном множестве $\Gamma(R)$.

Относительно операций

$$a \oplus b = \gamma_0(a + b) = (a + b)^{q^{n-1}}, \quad a \otimes b = \gamma_0(ab), \quad a, b \in \Gamma(R),$$

множество $\Gamma(R)$ образует поле $GF(q)$. Операцию умножения в поле $\Gamma(R)$ будем обозначать тем же символом, что и операцию умножения в кольце R .

Через $m_s(x)$ обозначается минимальный многочлен координатной последовательности u_s , $s \in \overline{0, n-1}$ над полем $\Gamma(R)$. Рангом последовательности u_s называется степень ее минимального многочлена: $\text{rank } u_s = \deg m_s(x)$.

Всюду далее, если нет дополнительных оговорок, предполагается, что $R = GR(q^n, p^n)$, $q = p^r$, и $R < S = GR(q^{mn}, p^n)$. Пусть θ — корень в кольце S многочлена Галуа $F(x) \in R[x]$ степени m . Известно [3], что для произвольной линейной рекурренты $u \in L_R(F)$ имеется единственная константа $\xi \in S$ со свойством

$$(\forall i \in \mathbb{N}_0) \quad u(i) = \text{Tr}_R^S(\xi \theta^i), \quad (1)$$

где Tr_R^S — функция “след” из расширения Галуа $S = GR(q^{mn}, p^n) = R[x]/(F(x))$ кольца R в кольцо R .

Для выработки псевдослучайных последовательностей на основе линейной рекурренты над кольцом Галуа может применяться способ, состоящий в выборе одного или нескольких p -адических разрядов каждого из знаков этой последовательности с последующим усложнением. В этой связи представляет интерес нахождение минимальных многочленов и либо точных значений рангов последовательностей u_l , $l = \overline{0, n-1}$, либо их нетривиальных оценок.

В [10] были получены нижние оценки рангов координатных последовательностей линейных рекуррент максимального периода над собственным кольцом Галуа, а также минимальные многочлены последовательностей u_l , $l = 0, 1$, над собственным кольцом Галуа.

В [2] найдены минимальный многочлен и ранг первой координатной последовательности линейной рекурренты u над собственным кольцом Галуа в произвольном координатном множестве.

В [13, 14, 7] описаны делители и кратные минимального многочлена второй p -адической координатной последовательности ЛРП МП над собственным кольцом Галуа нечетной характеристики в зависимости от начального вектора этой ЛРП. Как следствие, получены нетривиальные верхняя и нижняя оценки ранга второй координатной последовательности ЛРП МП над собственным кольцом Галуа нечетной характеристики.

Другие результаты в этой области автору неизвестны.

Пусть $M, w \in \mathbb{N}$. Обозначим через $\mathcal{I}(M, w)$ множество таких векторов $\vec{j} = (j_1, \dots, j_M)$, $0 \leq j_l \leq p-1$, $l = \overline{1, M}$, что $j_1 + j_2 + \dots + j_M = w$, и через $\left\{ \begin{smallmatrix} M \\ w \end{smallmatrix} \right\}$ обозначим мощность множества $\mathcal{I}(M, w)$. Отметим, что $\left\{ \begin{smallmatrix} M \\ w \end{smallmatrix} \right\}$ есть число заполнений M различных ячеек w неразличимыми предметами при условии, что в каждую ячейку попадает не более $p-1$ предметов.

Справедливы равенства [6, с. 215]:

$$\left\{ \begin{smallmatrix} M \\ w \end{smallmatrix} \right\} = \begin{cases} \sum_{s=0}^{\min\{w, (M-w)/p\}} (-1)^s \binom{w}{s} \binom{M+w-ps-1}{M-1}, & \text{если } 0 \leq w \leq M(p-1), \\ 0 & \text{в противном случае.} \end{cases}$$

Всюду далее будем считать, что векторы $\vec{j}$, составляющие множество $\mathcal{I}(M, w)$, упорядочены в лексикографическом порядке по возрастанию.

Положим $\mathcal{F}(x) = \gamma_0(F(x))$. Известно [10], что $\mathcal{F}(x)^{p^{s-1}+1} \mid m_s(x)$ при $s = \overline{1, n-1}$, откуда следует оценка Нечаева–Кузьмина

$$m(p^{s-1} + 1) \leq \text{rank } u_s, \quad s \geq 0. \quad (2)$$

Пусть $\theta_s = \gamma_s(\theta)$, $\xi_s = \gamma_s(\xi)$, $s = \overline{0, n-1}$. Если $F(x)$ — многочлен максимального периода, то θ_0 — примитивный элемент поля $\Gamma(S)$ и $\theta_1 \neq 0$.

Пусть

$$H(x) = \prod_{\substack{\vec{\lambda} \in \mathcal{I}(m,p), \\ \vec{\zeta} \in \mathcal{I}(m,p-1)}} \left(x \ominus \theta_0^{\sum_{l=0}^{m-1} p^{rm+rl-2} (\lambda_l + p\zeta_l)} \right),$$

где $\vec{\lambda} = (\lambda_0, \dots, \lambda_{m-1})$, $\vec{\zeta} = (\zeta_0, \dots, \zeta_{m-1})$.

Известно [14, Theorem 2.1], [7, теорема 3.1], что если u — линейная рекуррента максимального периода над собственным кольцом Галуа, то $H(x)^p \mid m_2(x)$ при $p \geq 5$.

Кроме того [14, Theorem 2.1], [7, теорема 3.1], если $\xi_1 \neq 0$, $p \geq 5$ и, дополнительно, для любого $\vec{\zeta} \in \mathcal{I}(m,p)$ выполнены условия

$$\sum_{\substack{\varkappa=\overline{0,m-1}: \zeta_\varkappa > 0}} \oplus \left(\frac{\xi_1}{\xi_0} \right)^{p^{rm+r\varkappa-1}} \neq 0,$$

$$\sum_{\substack{l=\overline{0,m-1}: \zeta_l > 0}} \oplus \gamma_0 \left(\frac{\zeta_l}{\zeta_0! \zeta_1! \dots \zeta_{m-1}!} \right) \left(\frac{\theta_1}{\theta_0} \right)^{\sum_{\varkappa=0}^{m-1} \zeta_\varkappa p^{rm+r\varkappa-1} - p^{rm+rl-1}} \neq 0,$$

то для многочлена $Z(x) = \prod_{\vec{\zeta} \in \mathcal{I}(m,p)} (x \ominus \theta_0^{\sum_{l=0}^{m-1} p^{rm+rl-1} \zeta_l})$ имеет место делимость $Z(x)^p \mid m_2(x)$.

Пусть u — ЛРП МП над кольцом $R = GR(q^n, p^n)$ с минимальным многочленом $F(x)$.

В [10, теорема 1.3] доказано, что для произвольного кольца Галуа $R = GR(q^n, p^n)$, $q = p^r$, и произвольного $s \in \overline{1, n-1}$

$$m_s(x) = \mathcal{F}(x)^{p^{s-1}+1} \cdot f_{s,1}(x)^{p^{s-1}} \dots f_{s,k}(x)^{p^{s-1}-k+1} \dots f_{s,p^{s-1}}(x), \quad (3)$$

где $f_{s,k}(x)$ — сепарабельный многочлен, $k = \overline{1, p^{s-1}}$, и

$$\mathcal{F}(x) \cdot f_{s,1}(x) \dots f_{s,p^{s-1}}(x) \mid x^{\tau_0} \ominus e,$$

где $\tau_s = (q^m - 1)p^s$, $m = \deg F(x)$, $s = \overline{0, n-1}$.

Поскольку $F(x)$ — многочлен максимального периода, при $s = \overline{0, n-1}$ имеет место равенство $x^{\tau_s} - e \equiv p^{s+1} \Phi_{s+1}(x) \pmod{F(x)}$, причем $\deg \Phi_{s+1}(x) < m$, $\bar{\Phi}_{s+1}(x) \neq 0$.

Следуя [2], положим $u^{(s)} = \Phi_s(x) \cdot u$ и $u_t^{(s)} = \gamma_t(u^{(s)})$, $s, t = \overline{0, n-1}$.

При $p \geq 3$ для произвольного кольца Галуа R в [10, лемма 2.1] доказано, что $u_0^{(s)} = u_0^{(1)}$, $s \geq 1$, и $u_1^{(s)} = u_1^{(2)}$, $s \geq 2$.

Пусть $\{u_{s,t}\}$ обозначает последовательность с общим членом вида $u_{s,t} = (x^{\tau_0} \ominus e)^{p^{s-1}-p^t} \cdot u_s, s \geq t+2, t \geq 0, s, t \in \overline{0, n-1}$.

Утверждение 1 (Дорофеев Н.В., личное сообщение, 1993 г.) . Для собственного кольца Галуа $R = GR(q^n, p^n), q = p^r, r \geq 2, p \geq 3$, выполнены следующие соотношения: $u_{s,s-2}^p = (u_0^{(1)})^{(p-1)p^r} \cdot u_{s-1} \ominus \frac{(u_0^{(1)})^p}{2} \oplus \xi(p, s, t)$, а при $t < s-2$

$$u_{s,t}^{p^{s-t-1}} = (u_0^{(1)})^{(p-1)\sum_{i=0}^{s-t-2} p^{r+i}} \cdot u_{t+1} \ominus \frac{(u_0^{(1)})^{p+(p-1)\sum_{i=1}^{s-t-2} p^{r+i}}}{2} \oplus \xi(p, s, t), \quad (4)$$

где

$$\xi(p, s, t) = \begin{cases} (\bar{\Phi}_1(x)^2 \cdot u_0)^p, & p = 3, t = 0, s = 2, \\ (\bar{\Phi}_1(x)^2 \cdot u_0)^p \cdot (u_0^{(1)})^{(p-1)\sum_{i=1}^{s-2} p^{r+i}}, & p = 3, t = 0, s > 2, \\ 0 & \text{в остальных случаях.} \end{cases} \quad (5)$$

1. Основной результат

Теорема 1. Пусть $R = GR(q^n, p^n)$ — собственное кольцо Галуа, $q = p^r, p \geq 5, r \geq 2, F(x)$ — многочлен максимального периода степени m над кольцом R , u — ненулевая по модулю pR последовательность с характеристическим многочленом $F(x), S = GR(q^{mn}, p^n)$ — расширение Галуа кольца R, θ — корень $F(x)$ в $S, \xi \in S$ удовлетворяет условию (1). Пусть $\theta_s = \gamma_s(\theta), \xi_s = \gamma_s(\xi), s = \overline{0, n-1}$.

Тогда для каждого такого натурального $s > 2$, что $s \equiv 2 \pmod{r}$, выполнено неравенство

$$m(p^{s-1} + 1) + p^{s-1} \left\{ \begin{matrix} m \\ p \end{matrix} \right\} \left\{ \begin{matrix} m \\ p-1 \end{matrix} \right\} \leq \text{rank } u_s. \quad (6)$$

Кроме того, если $\xi_1 \neq 0$ и для всех $\vec{\zeta} \in \mathcal{I}(m, p)$

$$\sum_{\kappa=\overline{0, m-1}: \zeta_\kappa > 0} \oplus \left(\frac{\xi_1}{\xi_0} \right)^{p^{rm+r\kappa-1}} \neq 0, \quad (7)$$

$$\sum_{l=\overline{0, m-1}: \zeta_l > 0} \oplus \gamma_0 \left(\frac{\zeta_l}{\zeta_0! \zeta_1! \dots \zeta_{m-1}!} \right) \left(\frac{\theta_1}{\theta_0} \right)^{\sum_{\kappa=0}^{m-1} \zeta_\kappa p^{rm+r\kappa-1} - p^{rm+r\kappa-1}} \neq 0, \quad (8)$$

то для тех же s имеет место неравенство

$$m(p^{s-1}+1) + p^{s-1} \begin{Bmatrix} m \\ p \end{Bmatrix} \begin{Bmatrix} m \\ p-1 \end{Bmatrix} + p^{s-1} \begin{Bmatrix} m \\ p \end{Bmatrix} \leq \text{rank } u_s. \quad (9)$$

Доказательство. Пусть $s \geq 3$. Тогда, согласно (4), (5),

$$\begin{cases} u_{s,0}^{p^{s-1}} = (u_0^{(1)})^{p^{s-1}-1} u_1 \ominus \frac{(u_0^{(1)})^{p^{s-1}}}{2}, \\ u_{2,0}^p = (u_0^{(1)})^{p-1} u_1 \ominus \frac{(u_0^{(1)})^p}{2}. \end{cases} \quad (10)$$

Заметим, что для тех $i \in \mathbb{N}_0$, для которых $u_0^{(1)}(i) = 0$, также и $u_{2,0}(i) = u_{s,0}(i) = 0$. Поэтому далее мы рассматриваем только такие $i \in \mathbb{N}_0$, что $u_0^{(1)}(i) \neq 0$.

Из (10) и приведенных выше равенств и условия следует, что если

$$s \equiv 2 \pmod{r}, \quad (11)$$

то указанная система примет вид

$$\begin{cases} u_{s,0}^p = (u_0^{(1)})^{p-1} u_1 \ominus \frac{(u_0^{(1)})^p}{2}, \\ u_{2,0}^p = (u_0^{(1)})^{p-1} u_1 \ominus \frac{(u_0^{(1)})^p}{2}. \end{cases}$$

В самом деле, если $s-2 = kr$, $k \in \mathbb{N}$, то $p^r - 1 \mid p^{kr} - 1 = p^{s-2} - 1$ и $p^{r-1} \mid p(p^{s-2}-1) = (p^{s-1}-1) - (p-1)$, значит, для произвольного $\alpha \in \Gamma(R) \setminus \{0\}$ имеем $\alpha^{(p^{s-1}-1)-(p-1)} = e$, т.е. $\alpha^{p^{s-1}-1} = \alpha^{p-1}$. Следовательно, при условии (11) имеет место равенство $u_{s,0} = u_{2,0}$, поэтому при этом условии $m_{u_{s,0}}(x) = m_{u_{2,0}}(x)$. Поскольку для произвольного кольца Галуа справедливо равенство

$$m_{u_{s,t}}(x) = \frac{m_{u_s}(x)}{\text{НОД}(m_{u_s}(x), (x^{\tau_0} \ominus e)^{p^{s-1}-p^t})} = \mathcal{F}(x)^{p^t+1} \cdot f_{s,1}^{p^t} \cdots f_{s,p^t}(x),$$

то $f_{s,1}(x) = f_{2,1}(x)$ при $p \geq 5$. Так как $H(x) \mid f_{2,1}(x)$, то отсюда, с учетом (3), следует неравенство (6). Поскольку, кроме того, $Z(x) \mid f_{2,1}(x)$ при условиях $\xi_1 \neq 0$, (7) и (8), то выполнено соотношение (9). $\square$

2. Выводы

Нетрудно видеть, что оценки (6), (9) в значительной мере улучшают известную ранее оценку Нечаева–Кузьмина (2) [10].

К сожалению, полученные здесь оценки не распространяются на все координатные последовательности u_s .

Список литературы

- [1] Былков Д. Н., “Вторая координатная последовательность линейной рекурренты максимального периода над кольцом $\mathbb{Z}_8$ ”, *Проблемы дискретн. матем. Приложение*, № 6 (2013), 9–10.
- [2] Куракин В. Л., “Первая координатная последовательность линейной рекурренты максимального периода над кольцом Галуа”, *Дискретная математика*, **6**:2 (1994), 88–100.
- [3] Нечаев А. А., “Код Кердока в циклической форме”, *Дискретная математика*, **1**:4 (1989), 123–139.
- [4] Нечаев А. А., “Линейные рекуррентные последовательности над коммутативными кольцами”, *Дискретная математика*, **3**:4 (1991), 107–121.
- [5] Нечаев А. А., “Цикловые типы линейных подстановок над конечными коммутативными кольцами”, *Матем. сборник*, **184**:4 (1993), 21–56.
- [6] Сачков В. Н., *Введение в комбинаторные методы дискретной математики*, М.: Наука, 1982, 384 с.
- [7] Цыпышев В. Н., “Вторая координатная последовательность линейной рекурренты максимального периода над собственным кольцом Галуа нечетной характеристики”, *Дискретная математика*, **28**:1 (2016), 123–149.
- [8] Helleseht T., Martinsen M., “Binary sequences of period $2^m - 1$ with large linear complexity”, *Inf. and Comput.*, **151** (1999), 73–91.
- [9] Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyshev V. N., “Linear and polylinear recurring sequences over Abelian groups and modules”, *J. Math. Sci.*, **102**:6 (2000), 4598–4626.
- [10] Kuzmin A. S., Nechaev A. A., “Linear recurrent sequences over Galois rings”, *Contemporary Math.*, **184** (1995), 237–254.
- [11] McDonald C., *Finite rings with identity*, New York: Marcel Dekker, 1974, 495 с.
- [12] Radghavendran R., “A class of finite rings”, *Compositio Math.*, **22**:1 (1970), 49–57.
- [13] Tsypyshev V. N., “Rank estimations of the second coordinate sequence of MP-LRS over nontrivial Galois ring of odd characteristic”. In: *Proc. II Int. Sci. Conf. on Problems of Security and Counter-Terrorism Activity*, Moscow: MCCME, 2007, 287–289. (In Russian.)
- [14] Tsypyshev, V. N., “Second coordinate sequence of the MP-LRS over nontrivial Galois ring of odd characteristic” (2015), <http://eprint.iacr.org/2015/1040>.