УДК 519.7

ВТОРАЯ КООРДИНАТНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ ЛИНЕЙНОЙ РЕКУРРЕНТЫ МАКСИМАЛЬНОГО ПЕРИОДА НАД КОЛЬЦОМ $\mathbb{Z}_8$[1]

Д. Н. Былков

Описывается аналитическое строение второй координатной последовательности линейной рекурренты над кольцом $\mathbb{Z}_8$. Уточняется нижняя оценка ранга (линейной сложности), строятся классы многочленов и рекуррент максимального периода, у которых достигается максимально возможный ранг.

Ключевые слова: *линейная рекуррентная последовательность над кольцом, координатная последовательность, ранг, аналитическое строение.*

Пусть $R = \mathbb{Z}_8$, $F(x) \in R[x]$ — *многочлен максимального периода* (*МП-многочлен*) степени m, т. е. унитарный (со старшим коэффициентом e) многочлен степени m с максимально возможным при данном m периодом $T(F) = 2^2(2^m - 1)$ [1]. Обозначим через $L_R(F)$ множество всех линейных рекуррент над R с характеристическим многочленом $F(x)$, а через $L_R(F)^*$ — подмножество линейных рекуррент $u \in L_R(F)$ периода $T(u) = T(F)$, т. е. *линейных рекуррентных последовательностей максимального периода* (*МП ЛРП*).

Подмножество $K = \{k_0, k_1\} \subset R$ назовем *координатным множеством* кольца R (см., например, [1]), если справедливы соотношения $k_0 \in 2R$, $k_1 \in R^*$. Примером координатного множества кольца R является *двоичное координатное множество* $K = \{0, 1\}$. Пусть $a \in R$, хорошо известно разложение $a = a_0 + 2a_1 + 2^2a_2$, $a_i = \gamma_i^K(a) \in K$, $i = 0, 1, 2$, называемое разложением элемента a в координатном множестве K. Элемент a_2 будем называть *старшей координатой* элемента a в координатном множестве K. На множестве K можно задать структуру поля: $a \circledast b = \gamma_0^K(a * b)$, $* \in \{+, \cdot\}$.

Пусть $F(x) \in R[x]$ — *унитарный многочлен Галуа* (т. е. неприводимый по модулю 2) степени $m \geqslant 5$. Рассмотрим последовательность $u_2 = \gamma_2^K(u)$, полученную разложением знаков ЛРП u в координатном множестве K: $u_2(i) = \gamma_2^K(u(i))$, $i \in \mathbb{N}_0$.

Для случая, когда многочлен $F(x)$ является отмеченным ($T(F) = 2^m - 1$), в работе [2] найдено разложение второй двоичной координатной последовательности u_2 в сумму биномиальных последовательностей.

В настоящей работе найдено биномиальное разложение второй координатной последовательности $\gamma_2^K(u)$ при произвольном выборе координатного множества K. Пусть θ — корень многочлена $F(x)$ в расширении S кольца R, $\Gamma(S) = \{a^{2^{3m}} = a : a \in S\}$ — координатное множество Тейхмюллера. Тогда знак ЛРП u представляется в виде $u(i) = \mathrm{Tr}_R^S(\xi\theta^i)$, $\xi \in \Gamma(S)$. Пусть также $\xi = \xi_0 + 2\xi_1 + 4\xi_2$, $\theta = \theta_0 + 2\theta_1 + 4\theta_2$ — разложения элементов ξ и θ в координатном множестве $\Gamma(S)$. Тогда справедлива

Теорема 1. Для знака последовательности u_2 справедливо равенство

$$u_2(i) = \binom{i}{2} \mathrm{tr}(\xi_0(\nu+\nu^2)w^i) \oplus i s_2(i) \oplus s_1(i) \oplus g^K(i\,\mathrm{tr}(\xi_0\nu w^i) + \mathrm{tr}(\xi_1 w^i) + \sigma_2(\xi_0 w^i), \mathrm{tr}(\xi_0\nu w^i)),$$

[1]Работа выполнена при поддержке гранта президента РФ № НШ-6260.2012.10.

где $\nu = \theta_1/\theta_0$, $\mathrm{tr}(x) = \mathrm{tr}^{\Gamma(S)}_{\{0,1\}}(x)$, многочлен g^K определяется лишь выбором K,

$$s_2(i) = \mathrm{tr}(\xi_0\nu w^i)\sigma_2(\xi_0 w^i) \oplus \sigma_2(\xi_0\nu w^i) \oplus \mathrm{tr}(\xi_0\nu w^i)\,\mathrm{tr}(\xi_1 w^i) \oplus \mathrm{tr}(\xi_0\theta_2 w^{i-1}) \oplus \mathrm{tr}(\xi_1\nu w^i);$$
$$s_1(i) = \sigma_4(\xi_0 w^i) \oplus \sigma_2(\xi_1 w^i) \oplus \mathrm{tr}((\xi_0 \oplus \xi_1)w^i)\sigma_2(\xi_0 w^i) \oplus \mathrm{tr}(\xi_0 w^i)\sigma_3(\xi_0 w^i) \oplus \mathrm{tr}(\xi_2 w^i);$$
$$\sigma_2(x) = \sum_{0\leqslant i<j\leqslant m-1} x^{2^i+2^j}, \sigma_3(x) = \sum_{0\leqslant i<j<k\leqslant m-1} x^{2^i+2^j+2^k}, \sigma_4(x) = \sum_{0\leqslant i<j<k<s\leqslant m-1} x^{2^i+2^j+2^k+2^s}.$$

Доказательство теоремы 1 получено при помощи метода *исключения младших координат*, разработанного В. Л. Куракиным [3].

На основе результата теоремы 1 удалось уточнить известные оценки линейной сложности (ранга) второй двоичной координатной последовательности и получить оценки ранга в случае произвольного координатного множества.

В работе [1] получены нижние оценки ранга двоичной координатной последовательности $u_2 = \gamma_2^{\{0,1\}}(u)$ в случае, когда $F(x)$ — МП-многочлен. В частности, описаны ограничения на выбор МП-многочлена $F(x)$, при которых для произвольной ЛРП $u \in L_R(F)^*$ справедливы неравенства

$$3m + 2\binom{m}{3} + \binom{m}{4} \leqslant \mathrm{rk}\, u_2 \leqslant 3m + 2\binom{m}{3} + 2\binom{m}{2} + \binom{m}{4}, \tag{1}$$

причём верхняя оценка в неравенстве (1) справедлива для любого МП-многочлена.

Справедлива

Теорема 2.

а) Если гарантированный ранг системы элементов $\{\nu, \nu^2, \ldots, \nu^{2^{m-1}}\}$ не меньше 3 или $\mathrm{tr}(\nu) = e$, то для произвольной МП ЛРП $u \in L_R(F)^*$ справедливо неравенство

$$\mathrm{rk}(\gamma_2^K(u)) \geqslant 3m + 2\binom{m}{3} + \binom{m}{4}. \tag{2}$$

б) Если элемент ν образует нормальный самодвойственный базис $\Gamma(S)$ над $\{0,1\}$ и элемент $\xi \in S$ имеет вид $\xi = (3+4c)\theta^t$ для некоторых $c \in S$, $t \in \mathbb{N}$, то для ЛРП $u \in L_R(F)^*$ вида $u(i) = \mathrm{Tr}(\xi\theta^i)$ верхнее неравенство из (1) обращается в равенство.

Так как условию $\mathrm{tr}(\nu) = e$ удовлетворяет половина всех МП-многочленов, то нижняя оценка (2) справедлива не менее чем для половины МП-многочленов и произвольного координатного множества K.

ЛИТЕРАТУРА

1. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A.* Linear Recurring Sequences over Rings and Modules // J. Math. Sci. (New York). 1995. V. 76. No. 6. P. 2793–2915.
2. *Helleseth T. and Martinsen H. M.* Binary sequences of period $2^m - 1$ with large linear complexity // Information and Computation. 1999. V. 151. P. 73–91.
3. *Куракин В. Л.* Первая координатная последовательность линейной рекурренты максимального периода над кольцом Галуа // Дискретная математика. 1994. Т. 6. № 2. С. 88–100.