О двоичных разрядных последовательностях над кольцами Галуа, допускающих эффект сокращения периода

С. А. КУЗЬМИН
e-mail: kzmn_sr@mail.ru

УДК 512.624.5

Ключевые слова: линейные рекуррентные последовательности, периоды последовательностей, примарные кольца, разрядные последовательности.

Аннотация

Найден класс двоичных разрядных последовательностей линейной рекурренты максимального периода над кольцом Галуа нечётной характеристики, допускающих эффект сокращения периода в два раза. Указано условие, при котором двоичные разрядные последовательности некоторой фиксированной линейной рекурренты максимального периода над кольцом Галуа, допускающие эффект сокращения периода, исчерпываются выделенным классом.

Abstract

S. A. Kuzmin, On binary digit-position sequences over Galois rings, admitting an effect of reduction of period, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 1, pp. 223—230.

A class of binary digit-position sequences, obtained from the linear recurring sequence of maximal period over Galois rings of odd characteristics and admitting an effect of twofold reduction of period, has been found. A condition was found when sequences of some fixed linear recurring sequence of maximal period over Galois fields with such property are exhausted only by that class.

1. Введение

Пусть задано некоторое кольцо Галуа $R = GR(p^{nm}, p^n)$, порождённое многочленом Галуа $F(x)$, $\deg F(x) = m$ (см., например, [5]), т. е. $R = \mathbb{Z}_{p^n}[x]/\big(F(x)\big)$, $u(i) = \big(u(i)\big)_{i=0}^{\infty}$ — линейная рекуррентная последовательность максимального периода над этим кольцом. Пусть $S = GR(p^{nml}, p^n)$ — расширение Галуа кольца R, $\mathrm{Aut}(S/R)$ — группа всех автоморфизмов кольца S, оставляющих на месте все элементы кольца R.

Определим функцию след $\mathrm{Tr}_R^S\colon S \to R$ равенством

$$\mathrm{Tr}_R^S(x) = \sum_{\tau \in \mathrm{Aut}(S \setminus R)} \tau(x).$$

Фундаментальная и прикладная математика, 2015, том 20, № 1, с. 223—230.

Обозначим через α корень многочлена $f(x)$, $\deg f(x) = l$, в кольце S. Из теоремы 8 из [5] следует существование единственного элемента $b \in S$, такого что $u(i) = \mathrm{Tr}_R^S(b\alpha^i)$, $i \geqslant 0$.

Всякий элемент

$$c = \sum_{j=0}^{m-1} c_j x^j \in GR(p^{nm}, p^n)$$

однозначно представи́м в виде вектора коэффициентов $(c_0, c_1, \ldots, c_{m-1})$, где $c_i \in \mathbb{Z}_{p^n}$, $i \in \overline{0, m-1}$. В свою очередь коэффициент c_i однозначно представи́м в виде

$$c_i = \sum_{s=0}^{d} c_{i,s} 2^s, \quad c_{i,s} \in \{0, 1\}, \quad d = [\log_2 p^n].$$

Тогда любой знак $u(i)$ некоторой линейной рекуррентной последовательности максимального периода u над кольцом Галуа представляется в виде

$$u(i) = \Big(\sum_{s=0}^{k} u_{0,s}(i) 2^s, \sum_{s=0}^{k} u_{1,s}(i) 2^s, \ldots, \sum_{s=0}^{k} u_{m-1,s}(i) 2^s \Big), \tag{1}$$

где $k = [\log_2 p^n]$.

Таким образом, последовательность вида

$$u(i)_{\bullet,s} = \big(u_{0,s}(i), u_{1,s}(i), \ldots, u_{m-1,s}(i)\big)$$

по аналогии с [3] будет являться s-й разрядной последовательностью линейной рекуррентной последовательности максимального периода $u(i)$ над кольцом Галуа.

Основной задачей данной статьи является изучение периодов двоичных разрядных последовательностей, полученных из линейных рекуррентных последовательностей максимального периода над кольцами Галуа. Известно, что в этом случае период линейной рекуррентной последовательности максимального периода u над кольцом S с характеристическим многочленом Галуа $f(x)$ равен $T(u) = p^{n-1}(p^{ml} - 1)$ [1, с. 178].

Ранее двоичные разрядные последовательности рассматривались А. С. Кузьминым [3]. Им найдены все двоичные разрядные последовательности линейной рекуррентной последовательности максимального периода над конечным простым полем нечётной характеристики, в которых наблюдается эффект сокращения периода.

В настоящее время особый интерес представляет изучение p-ичных разрядных последовательностей над кольцами вычетов по модулю p^n. Это связано с тем, что данные последовательности обладают высокой линейной сложностью и могут быть использованы в датчиках псевдослучайных последовательностей. Библиографию по данной тематике можно найти, например, в [6].

Данная работа является некоторым обобщением работы [3] на случай $n \geqslant 1$, а также на случай непростого поля.

2. Основные результаты

При доказательстве результатов данной работы используется следующее предложение.

Предложение 1 [6, с. 43]. *Пусть $S = GR(p^{nml}, p^n)$ — расширение степени l кольца R, $u(i) = \mathrm{Tr}_R^S(b\alpha^i)$, $i \geqslant 0$, — линейная рекуррентная последовательность максимального периода над кольцом S. Тогда справедливо равенство*

$$u(i) + u\left(i + \frac{T(u)}{2}\right) = \mathrm{Tr}_R^S(b\alpha^i) + \mathrm{Tr}_R^S(b\alpha^{i+T(u)/2}) = 0 \pmod{p^n}. \qquad (2)$$

Перед доказательством основного результата работы сформулируем несколько вспомогательных утверждений.

Утверждение 2. *Для любого простого $p \geqslant 3$ в примарных кольцах вида $\mathbb{Z}_{p^{2k}}$, $k \in \mathbb{N}$, для периода двоичной разрядной последовательности u_1, полученной из линейной рекуррентной последовательности максимального периода u по правилу* (1) *при $m = 1$, справедливо соотношение $T(u_1) \mid T(u)/2$.*

Доказательство.

1. Если $u(i) = u(i + T(u)/2) = 0$, то очевидным образом выполняются равенства $u_1(i) = u_1(i + T(u)/2) = 0$.

2. Пусть $0 < u(i) < p^{2k}$ и $0 < u(i + T(u)/2) < p^{2k}$. Тогда, сложив эти неравенства, получим

$$0 \leqslant u(i) + u\left(i + \frac{T(u)}{2}\right) < 2p^{2k}.$$

Учитывая

$$u(i) + u\left(i + \frac{T(u)}{2}\right) \equiv 0 \pmod{p^{2k}},$$

получаем равенство

$$u(i) + u\left(i + \frac{T(u)}{2}\right) = p^{2k}.$$

В этом случае при представлении линейной рекуррентной последовательности максимального периода u в виде суммы разрядных последовательностей будут справедливы равенства

$$u(i) + u\left(i + \frac{T(u)}{2}\right) = u_0(i) + 2u_1(i) + 4b(i) + \\ + u_0\left(i + \frac{T(u)}{2}\right) + 2u_1\left(i + \frac{T(u)}{2}\right) + 4c(i) = p^{2k}, \quad b(i), c(i) \in \mathbb{N}.$$

Приведём полученное равенство по модулю 4. Получим

$$u_0(i) + 2u_1(i) + u_0\left(i + \frac{T(u)}{2}\right) + 2u_1\left(i + \frac{T(u)}{2}\right) \equiv 1 \pmod 4. \tag{3}$$

Из (3) следует, что

$$u_0(i) + u_0\left(i + \frac{T(u)}{2}\right) \equiv 1 \pmod 2.$$

Поскольку $u_r(i)$ и $u_r(i + T(u)/2)$ принадлежат множеству $\{0, 1\}$, где $r \in \{0, 1\}$, то справедливо равенство $u_0(i) + u_0(i + T(u)/2) = 1$, и следовательно, $u_1(i) = u_1(i + T(u)/2)$ для любого $i \in \mathbb{N}$. □

Утверждение 3. *Для любого простого $p \geqslant 3$, такого что $p - 1 \equiv 0 \pmod 4$, в примарных кольцах вида $\mathbb{Z}_{p^{2k+1}}$, $k \in \mathbb{N}_0$, для периода двоичной разрядной последовательности u_1, полученной из линейной рекуррентной последовательности максимального периода u по правилу* (1) *при $m = 1$, справедливо соотношение $T(u_1) \mid T(u)/2$.*

Доказательство. В случае $u(i) = u(i + T(u)/2) = 0$ утверждение очевидно, так как очевидным образом выполняются равенства $u_1(i) = u_1(i + T(u)/2) = 0$. Заметим, что так как $p - 1 \equiv 0 \pmod 4$, то

$$p^{2k+1} - 1 = (p - 1)\sum_{t=0}^{2k} p^t \equiv 0 \pmod 4.$$

В этом случае, так же как и в утверждении 2, когда $u(i)$ и $u(i + T(u)/2)$ одновременно не равны нулю, будет справедливо равенство (3).

Таким образом, проводя рассуждения, аналогичные утверждению 2, получаем, что $u_1(i) = u_1(i + T(u)/2)$ для любого $i \in \mathbb{N}$. □

Утверждение 4. *Для любого простого $p \geqslant 3$, такого что*

$$p = a(s)2^s + 2^s - 1, \quad a(s) \geqslant 0, \quad s \geqslant 2,$$

в примарных кольцах вида $\mathbb{Z}_{p^{2k+1}}$, $k \in \mathbb{N}_0$, для периода двоичной разрядной последовательности u_s, полученной из линейной рекуррентной последовательности максимального периода u по правилу (1) *при $m = 1$, справедливо соотношение $T(u_s) \mid T(u)/2$.*

Доказательство. Если $u(i) = u(i + T(u)/2) = 0$, то, очевидно, верно равенство

$$u_s(i) = u_s\left(i + \frac{T(u)}{2}\right).$$

Если $0 < u(i) < p^{2k}$ и $0 < u(i + T(u)/2) < p^{2k}$, то, проводя рассуждения, аналогичные доказательству второго пункта утверждения 2, получим равенство $u(i + T(u)/2) = p^{2k+1} - u(i)$.

Справедливы равенства

$$p^{2k+1} = (a(s)2^s + 2^s - 1)^{2k+1} = (2^s - 1)^{2k+1} + 2^{s+1}a'(s) = \\ = 2^{s+1}a''(s) + (2k+1)2^s - 1 = a'''(s)2^{s+1} + 2^s - 1,$$

где $a'(s), a''(s), a'''(s) \in \mathbb{N}$. Представим обе части полученного выражения в двоичном виде, получаем

$$\sum_{j=0}^{s-1} u_j \left(i + \frac{T(u)}{2}\right) 2^j + u_s \left(i + \frac{T(u)}{2}\right) 2^s + u'_{s+1} \left(i + \frac{T(u)}{2}\right) 2^{s+1} = \\ = 2^s - 1 + a'''(s)2^{s+1} - \sum_{j=0}^{s-1} u_j(i)2^j + u_s(i)2^s + u'_{s+1}(i)2^{s+1}, \quad (4)$$

где

$$u'_{s+1}(i) = \sum_{j=s+1}^{d} u_j(i)2^{j-s+1}, \quad d = [\log_2 p^{2k+1}],$$

для любого $i \in \mathbb{N}$. Следовательно, справедливы равенства

$$\sum_{j=0}^{s-1} u_j \left(i + \frac{T(u)}{2}\right) 2^j = \sum_{j=0}^{s-1} \left(1 - u_j(i)\right) 2^j,$$

$$2^{s+1}u'_{s+1} \left(i + \frac{T(u)}{2}\right) + u_s \left(i + \frac{T(u)}{2}\right) 2^s = 2^{s+1} \left(a(s) - u'_{s+1}(i)\right) - u_s(i)2^s.$$

При приведении последнего равенства по модулю 2^{s+1} получаем $u_s(i) = u_s(i + T(u)/2)$. □

Замечание. Соотношение $u_r(i) = u_r(i + T(u)/2) \oplus 1$, $r < s$, является своего рода аналогом соотношений из [4, с. 43].

Утверждение 5. *Пусть двоичные разрядные последовательности u_r, $r \in \overline{0,k}$, образованы по правилу* (1) *при $m = 1$ из линейной рекуррентной последовательности максимального периода u, на цикле которой присутствуют хотя бы по одному разу все элементы из $\mathbb{Z}_{p^n} \setminus \{0\}$. Тогда если r отличается от номеров разрядных последовательностей, указанных в утверждениях* 2—4, *то $T(u_r)$ не делит $T(u)/2$.*

Доказательство. Не ограничивая общности, положим $z = \{1, s\}$. Из доказательства утверждений 2—4 непосредственно вытекает, что $T(u_r)$ не делит $T(u)/2$ в случаях, когда $r < 1$ для утверждений 2 и 3 и $r < s$ для соответствующего s из утверждения 4, так как для $r < z$ выполняется равенство $u_z(i) = u_z(i + T(u)/2) \oplus 1$.

Докажем, что при $r > z$ $T(u_r)$ не делит $T(u)/2$. Заметим, что по утверждениям 2—4 для последовательности u_z имеет место соотношение $T(u_z) \mid T(u)/2$ и $u_z(i) = u_z(i + T/2)$. Предположим, что $T(u_r)$ делит $T(u)/2$. Тогда для любого $i \in \mathbb{N}$ будет верно соотношение $u_r(i) = u_r(i + T/2)$. Следовательно, z-й

и r-й разряды в парах чисел j и $p^n - j$ для $j \in \overline{0, p^n - 1}$ должны изменяться одинаковым образом для каждой пары.

Рассмотрим последовательность пар чисел

$$\{(0, p^n), (1, p^n - 1), \ldots, (j-1, p^n - j + 1), (j, p^n - j), \ldots\},$$

представляющую пары элементов кольца $\mathbb{Z}_{p^n}$, лежащие на полупериоде линейной рекуррентной последовательности максимального периода. Положим j равным 2^z. В этом случае в указанной выше последовательности впервые произойдёт смена z-го разряда в паре $(j, p^n - j)$. Заметим, что z-й и более младшие разряды в числе $p^n - j$ изменились за счёт заимствования из разряда, лежащего в диапазоне (z, r). Заимствование из разрядов, больших или равных r, невозможно, иначе получим противоречие с предположением о том, что $u_r(i) = u_r(i + T(u)/2)$ для любого $i \in \mathbb{N}$, так как $u_r(i) = 0$ для чисел $j < 2^r$.

Максимальное теоретически возможное количество заимствований из диапазона (z, r), при котором не затрагивается r-й разряд числа, равно $2^{r-z} - 1$, столько же раз должны измениться разряды числа j в диапазоне (z, r), для того чтобы в представленной последовательности первый раз мог измениться r-й разряд. Однако, когда j стало равным 2^z, разряды в диапазоне (z, r) числа j не изменялись, а в числе $p^n - j$ произошло заимствование, далее с каждой сменой разряда z происходило одно заимствование. Следовательно, для числа $j' = 2^r$ равенство (2) не выполняется, а значит, предположение неверно. □

Теперь можно доказать следующую теорему.

Теорема 6. *Пусть задано кольцо Галуа $R = GR(p^{nm}, p^n)$, $m \in \mathbb{N}$, $p = a(s)2^{s+1} + 2^s - 1$, $a(s) \geqslant 0$. Пусть также u — линейная рекуррентная последовательность максимального периода над этим кольцом с характеристическим многочленом $f(x)$, $\deg f(x) = l$, и*

$$z = \begin{cases} 1, & \text{если } n = 2k \text{ или если } n = 2k-1 \text{ и } p \equiv 1 \pmod 4, \\ s, & \text{если } n = 2k-1 \text{ и } p \equiv 3 \pmod 4, \end{cases}$$

для некоторого $k \in \mathbb{N}$. Тогда для периода $T(u_{\bullet,z})$ двоичной разрядной последовательности $u_{\bullet,z}$, образованной из линейной рекуррентной последовательности максимального периода u по правилу (1), верно соотношение $T(u_{\bullet,z}) \mid T(u)/2$.

В случае, когда хотя бы одна из компонент m-мерного вектора коэффициентов $(c_0, c_1, \ldots, c_{m-1})$, где $c_i \in \mathbb{Z}_{p^n}$, представляющего элементы $c \in R$, лежащие на цикле последовательности u, принимает все значения из $\mathbb{Z}_{p^n} \setminus \{0\}$, такая последовательность $u_{\bullet,z}$ будет единственной.

Доказательство. Нетрудно убедиться, что данная теорема является обобщением утверждений 2—5 на случай произвольного $m \in \mathbb{N}$. Зафиксируем m. Тогда знак $u(i)$ линейной рекуррентной последовательности максимального периода u над $GR(p^{nm}, p^n)$ представим в виде (1) и равенство (2) принимает вид

$$u(i)+u\left(i+\frac{T(u)}{2}\right)=\left(\sum_{s=0}^{k}u_{0,s}(i)2^s,\sum_{s=0}^{k}u_{1,s}(i)2^s,\dots,\sum_{s=0}^{k}u_{m-1,s}(i)2^s\right)+$$
$$+\left(\sum_{s=0}^{k}u_{0,s}\left(i+\frac{T(u)}{2}\right)2^s,\sum_{s=0}^{k}u_{1,s}\left(i+\frac{T(u)}{2}\right)2^s,\dots,\right.$$
$$\left.\sum_{s=0}^{k}u_{m-1,s}\left(i+\frac{T(u)}{2}\right)2^s\right)=0, \tag{5}$$

где $k=[\log_2 p^n]$. Здесь каждая координата m-мерного вектора представляет собой некоторый элемент кольца $\mathbb{Z}_{p^n}$ и равенство

$$\sum_{s=0}^{k}u_{v,s}(i)2^s+\sum_{s=0}^{k}u_{v,s}\left(i+\frac{T(u)}{2}\right)2^s\equiv 0\ (\mathrm{mod}\ p^n)$$

выполняется для любого $u_{v,s}(i)\in\{0,1\}$, $v\in\overline{0,m-1}$. Следовательно, аналогично утверждениям 2—4 проверяется выполнение соотношения $u_{v,z}(i)=$ $=u_{v,z}(i+T(u)/2)$ для любого $v\in\overline{0,m-1}$ и некоторого $z\in\{1,s\}$, зависящего от вида простого числа $p>2$ и чётности n. Из этого следует, что $T(u_{\bullet,z})\mid T(u)/2$.

Единственность будет следовать непосредственно из утверждения 5 и дополнительного условия теоремы, так как в этом случае хотя бы в одной координате m-мерных векторов из соотношения (5) равенство $u_{v,r}(i)=u_{v,r}(i+T(u)/2)$, $r\neq z$, выполняться не будет. □

В частном случае с учётом результатов [2] справедливо следующее утверждение.

Следствие 7. *Пусть u — линейная рекуррентная последовательность максимального периода над кольцом Галуа $R=GR(p^{nm},p^n)$ с характеристическим многочленом Галуа $f(x)$, $\deg f(x)=l$. Тогда для существования единственной полученной из линейной рекуррентной последовательности максимального периода u двоичной разрядной последовательности, допускающей эффект сокращения периода в два раза, достаточно, чтобы среди элементов $u(0),u(1),\dots,u(l-1)$ был хотя бы один обратимый и выполнялось неравенство $l\geqslant 2(nm+n-1)/m$.*

Доказательство. Для доказательства следствия достаточно заметить, что при сформулированных условиях согласно [2, следствие 3.4] на цикле линейной рекуррентной последовательности максимального периода u встречаются все элементы кольца R. □

Если в условиях теоремы 6 положить $n=1$, то справедливо следующее утверждение.

Следствие 8. *Пусть $F=GF(p^m)$ — расширение простого поля $GF(p)$ степени m, $p=a(s)2^{s+1}+2^s-1$, $a(s)\geqslant 0$, u — линейная рекуррентная последовательность максимального периода над этим полем. Тогда для периода $T(u_{\bullet,s})$*

двоичной разрядной последовательности $u_{\bullet,s}$, образованной из последовательности u по правилу (1) *при $n = 1$, верно соотношение $T(u_{\bullet,s}) \mid T(u)/2$ и последовательность $u_{\bullet,s}$ единственная с этим свойством.*

Доказательство. Для доказательства следствия достаточно положить $n = 1$ в доказательстве теоремы 6. Единственность последовательности $u_{\bullet,s}$ будет следовать из того, что на цикле линейной рекуррентной последовательности максимального периода u над конечным полем F встречаются все возможные элементы этого поля (см., например, [2, с. 331]), а следовательно, в m-мерном векторе коэффициентов $(c_0, c_1, \ldots, c_{m-1})$, где $c_i \in \mathbb{Z}_p$, представляющем элементы $c \in F$, лежащие на цикле последовательности u, будет существовать как минимум одна компонента, пробегающая все значения из $\mathbb{Z}_p \setminus \{0\}$, и применимы рассуждения, аналогичные утверждению 5. □

Замечание. Заметим, что если p — число Мерсенна и $n = 1$, то рассуждения, аналогичные представленным выше, провести нельзя и соотношение $T(u_{\bullet,s}) \mid T(u)/2$ окажется невыполненным.

3. Заключение

В работе найден класс двоичных разрядных последовательностей, линейной рекурренты максимального периода над кольцом Галуа нечётной характеристики, допускающих эффект сокращения периода в два раза. Указано условие, при котором двоичные разрядные последовательности некоторой фиксированной линейной рекуррентной последовательности максимального периода над кольцом Галуа, допускающие эффект сокращения периода, исчерпываются только выделенным классом. Полученный результат является обобщением работы [3] на случай $n \geqslant 1$, а также на случай непростого поля.

Литература

[1] Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. Т. 2. — М.: Гелиос АРВ, 2003.

[2] Камловский О. В., Кузьмин А. С. Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа // Фундамент. и прикл. матем. — 2000. — Т. 6, № 4. — С. 1083—1094.

[3] Кузьмин А. С. О периодах разрядов в r-ичной системе счисления знаков линейных рекуррентных последовательностей над конечными простыми полями // Безопасн. информ. технол. — 1995. — Вып. 4. — С. 71—75.

[4] Кузьмин А. С., Маршалко Г. Б., Нечаев А. А. Восстановление линейной рекуррентной последовательности на примарным кольцом вычетов по её усложнению // Матем. вопр. криптогр. — 2010. — Т. 1, № 2. — С. 31—56.

[5] Нечаев А. А. Код Кердока в циклической форме. — Дискрет. матем. — Т. 1, № 4. — С. 123—139.

[6] Труды по дискретной математике. Т. 1 / Ред. В. Н. Сачков. — М.: ТВП, 1997.