ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/2/1

УДК 621.391.1:004.7

РАССТОЯНИЕ ЕДИНСТВЕННОСТИ СЕМЕЙСТВА КООРДИНАТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПОЛУЧЕННЫХ УСЛОЖНЕНИЕМ ЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦОМ ГАЛУА[1]

Д.Н. Былков

Московский государственный институт радиотехники, электроники и автоматики

E-mail: Bilkov@gmail.com

В настоящей работе обсуждается наличие эквивалентных последовательностей при усложнении координатных ЛРП над кольцом Галуа, а также рассмотрен вопрос о минимальной длине, на которой выходные последовательности будут различимы.

***Ключевые слова*:** *координатные ЛРП, кольцо Галуа, эквивалентные состояния, расстояние единственности.*

Пусть $R = GR(q^n, p^n)$ – кольцо Галуа характеристики p^n, состоящее из q^n элементов [1], $n > 1$, $q = p^r$, e – единица. Для кольца Галуа R поле $\overline{R} = R/pR$ будем называть полем вычетов. Естественный эпиморфизм $R \to \overline{R}$ индуцирует эпиморфизм колец многочленов $R[x] \to \overline{R}[x]$. Образ многочлена $A(x) = \sum a_i x^i \in R[x]$ будем обозначать $\bar{A}(x)$: $\bar{A}(x) = \sum \bar{a}_i x^i \in \overline{R}[x]$.

Подмножество $B = \{b_0, \dots, b_{q-1}\}$ называется координатным множеством кольца R, если его элементы образуют полную систему вычетов по модулю идеала pR. В [1] показано, что каждый элемент $a \in R$ однозначно представляется в виде $a = a_0 + pa_1 + \dots + p^{n-1}a_{n-1}$, $a_s \in B$, $0 \le s \le n-1$, называемом разложением элемента a в координатном множестве B.

Пусть $l, t \in \mathbb{N}$ и t удовлетворяет условиям $1 \le t \le l$. Произвольную функцию $h: R^l \to B$ от переменных $x_1, \dots, x_l$ можно рассматривать как функцию от переменных x_{ij}, $0 \le i \le n-1$, $1 \le j \le l$, отображающую B^{nl} в B, где величины $x_{0j}, \dots, x_{n-1\,j}$ суть коэффициенты из разложения переменной x_j в координатном множестве B. Скажем, что отображение h биективно по переменной $x_{n-1\,t}$, если при произвольной фиксации $nl-1$ переменных

$$(x_{0\,1}, \dots, x_{n-1\,1}, \dots, x_{0\,t}, \dots, x_{n-2\,t}, x_{0\,t+1}, \dots, x_{n-1\,t+1}, \dots, x_{0\,l}, \dots, x_{n-1\,l}) \in B^{nl-1}$$

функция $\hat{h} = h(x_{0\,1}, \dots, x_{n-2\,t}, x, x_{0\,t+1}, \dots, x_{n-1\,l})$ – биекция.

Всюду далее $F(x)$ – унитарный многочлен над R, через $L_R(F)$ будем обозначать множество всех линейных рекуррентных последовательностей над R с характеристическим многочленом $F(x)$. Каждой последовательности u из $L_R(F)$ сопоставим последовательности $u_0, \dots, u_{n-1}$, получающиеся из разложения знаков последовательности u в координатном множестве B: $u(i) = u_0(i) + pu_1(i) + \dots + p^{n-1}u_{n-1}(i)$, $u_s(i) \in B$, $0 \le s \le n-1$, $i \ge 0$.

Зафиксируем параметры $l \in \mathbb{N}$, $1 \le t \le l$, и $s_1, \dots, s_l \in \mathbb{N}$. Рассмотрим алгоритм A, сопоставляющий каждой из последовательностей $u \in L_R(F)$ выходную последовательность $\tilde{u} = A(u)$ по правилу: $\tilde{u} = h(u(i+s_1), \dots, u(i+s_l))$, $i \ge 0$, где отображение h биективно по переменной $x_{n-1\,t}$.

Будем говорить, что алгоритм A не допускает эквивалентных состояний, если существует натуральное L со свойством

$$\forall\ u, v \in L_R(F) \quad (u \ne v) \Rightarrow ((\tilde{u}(0), \dots, \tilde{u}(L-1)) \ne (\tilde{v}(0), \dots, \tilde{v}(L-1))). \qquad (1)$$

В этом случае минимум $\mathrm{Ud}(F, A)$ значений L со свойством (1) назовем расстоянием единственности алгоритма A. В противном случае будем считать $\mathrm{Ud}(F, A) = \infty$.

Определим норму элемента $a \in R$ и норму последовательности $y \in R^{<1>}$ следующим образом:

$$\|a\| = \max\{0 \le t \le n \mid a \in p^t R\},\ \|y\| = \max\{0 \le t \le n \mid y \in p^t R^{<1>}\}.$$

[1] Работа выполнена при финансовой поддержке Совета поддержки научных школ при Президенте РФ (номер проекта НШ – 8564.2006.10).

Положим $L_R(F)^* = \{u \in L_R(F) : \|u\| = 0\}$. Будем говорить, что многочлен $F(x) \in R[x]$ реверсивный, если $F(0) \in R^*$. Назовем многочлен $F(x) \in R[x]$ многочленом Галуа, если его образ $\overline{F}(x) \in \overline{R}[x]$ неприводим над $\overline{R}$. При условии $T(F) = p^{n-1}(q^m - 1)$, $m = \deg F(x)$, скажем, что $F(x)$ – многочлен максимального периода (ММП) над R.

Теорема 1. Пусть существует натуральное L, такое, что для любой последовательности $u \in L_R(F)^*$ для каждого $0 \le k \le n-1$ найдется $0 \le i_0 \le L-1$ со свойством

$$u(i_0 + s_j) = 0, \text{ для всех } j \in \{1, \ldots, l\} \setminus \{t\},$$
$$\|u(i_0 + s_t)\| = k.$$

Тогда верно неравенство $\mathrm{Ud}(F, A) \le L$.

Условия теоремы 1 выполняются, например, если $l = 1$ и $F(x)$ – многочлен максимального периода. В [1] показано, что на цикле линейной рекурренты максимального периода появятся все элементы кольца R, то есть справедливо неравенство $L \le T(F)$. В случае кольца $\mathbb{Z}_4$ можно указать более точные оценки величины L.

Теорема 2. Пусть $F(x) = x^m - x - 1 \in \mathbb{Z}_4[x]$, где $m > 2$. Тогда для любой последовательности $u \in L_{\mathbb{Z}_4}(F)^*$, для всех $z \in \{1, 3\}$ существует $i_0 \le 4m - 2$, такое, что $u(i_0) = z$. Причем указанная оценка достижима.

Теорема 3. Пусть $F(x) = x^m - x^k - 1$ – многочлен Галуа над кольцом $\mathbb{Z}_4$, где $1 < k < m$. Тогда для любой последовательности $u \in L_{\mathbb{Z}_4}(F)^*$, для всех $z \in \{1, 3\}$ существует $i_0 \le 3mk + 2m - 2k - 1$, такое, что $u(i_0) = z$.

Следующие результаты дают достаточные условия конечности величины $\mathrm{Ud}(F, A)$.

Теорема 4. Пусть $F(x)$ – многочлен Галуа степени m над кольцом R, удовлетворяющий условию

$$T(F) \ge p^{2(n-1)}(q^{nl} - 1)q^{m/2}.$$

Пусть также α – корень многочлена $F(x)$ в расширении $S = GR(q^{mn}, p^n)$ кольца R. Тогда при условии, что система $\alpha^{s_1}, \ldots, \alpha^{s_l}$ линейно независима над R, верно неравенство $\mathrm{Ud}(F, A) < \infty$.

Нетрудно заметить, что результат теоремы 4 нетривиален при выполнении неравенства $m \ge 2nl(1 + o(1))$.

Теорема 5. Пусть $l = t = 1$ и $F(x) = F_1(x)\,F_2(x)$, где $F_1(x)$, $F_2(x)$ – унитарные и реверсивные многочлены над R, такие, что $(T(F_1), T(F_2)) = 1$. Пусть также для произвольной последовательности $u \in L_R(F_s)^*$, $s = 1, 2$, для каждого $0 \le k \le n$ найдется $i_0 < T(F)$ со свойством $\|u(i_0)\| = k$. Тогда верно неравенство $\mathrm{Ud}(F, A) < \infty$.

Теорема 6. Пусть $l = t = 1$ и $F(x) = F_1(x)\,F_2(x)$, где $F_1(x)$, $F_2(x)$ – взаимно простые, унитарные, реверсивные многочлены Галуа над R, степеней m и k соответственно, такие, что

$$d_0 \ge p^{2(n-1)}q^{m/2},\ d_1 \ge p^{2(n-1)}q^{k/2},$$

где $t_i = T(F_i)$, $d_i = t_i / (t_1, t_2)$, $i = 1, 2$. Пусть также выполнено равенство $(T(\overline{F}_1), T(\overline{F}_2)) = 1$. Тогда верно неравенство $\mathrm{Ud}(F, A) < \infty$.

В некоторых случаях удается получить более точные оценки величины $\mathrm{Ud}(F, A)$. Всюду далее $R = \mathbb{Z}_4$, $l = t = 1$, $h(x) = x_{11}$ и вместо $\mathrm{Ud}(F, A)$ будем писать $\mathrm{Ud}(F)$. В [2] показано, что если $F(x)$ – многочлен максимального периода степени m, то для любой u из $L_R(F)^*$ выполнено равенство $\mathrm{rank}(u_1) = m(m+3)/2$. И поэтому $\mathrm{Ud}(F) \le m(m+3)/2$. Ниже приводятся оценки расстояния единственности для трехчленов вида $F(x) = x^m + ax^k + b$, $(a, b) \ne (1, 1)$.

Вид $F(x)$	Дополнительные условия	Теоретически полученная верхняя оценка $\mathrm{Ud}(F)$	Точные значения $\mathrm{Ud}(F)$ для $m \le 18$
$x^m - x^k - 1$	$\overline{F}(x)$ примитивный, $k < (m^2 - m)/(2m - 3)$	$m(3 + k) - 2k + 1$	$\mathrm{Ud}(F) \le 3m$
	$\overline{F}(x)$ примитивный, $k \ge (m^2 - m)/(2m - 3)$	$m(3 + m - k) - m + k + 1$	
	k делит m	$4m - 2k + 1$	
	$m - k$ делит m	$3m + k + 1$	
$x^m - 3x^k - 1$	$\overline{F}(x)$ примитивный, $k < (m^2 - 2m)/(2m - 3)$	$m(3 + k) - k + 1$	$\mathrm{Ud}(F) \le 3m$
	$\overline{F}(x)$ примитивный, $k \ge (m^2 - 2m)/(2m - 3)$	$m(3 + m - k) - 2m + 2k + 1$	
	k делит m	$4m - k + 1$	
	$m - k$ делит m	$2m + 2k + 1$	
$x^m - x^k - 3$	$\overline{F}(x)$ примитивный, $k < (m - 1)/2$	$m(3 + k) - k + 1$	$\mathrm{Ud}(F) \le 4m$
	$\overline{F}(x)$ примитивный, $k \ge (m - 1)/2$	$m(3 + m - k) - m + k + 1$	
	k делит m	$4m - k + 1$	
	$m - k$ делит m	$3m + k + 1$	

Оказывается, для большого числа трехчленов максимального периода теоретическая оценка расстояния единственности существенно меньше $m(m + 3) / 2$. Имеющиеся результаты точного вычисления на ПК расстояния единственности для указанных многочленов позволяют выдвинуть гипотезу о том, что для таких многочленов $\mathrm{Ud}(F) \le 4m$.

Показано, что если $F(x) \in \{x^{2+2i} + x^i + 1, x^{2+3i} + x + 1, x^{4+3i} + x^2 + 1\}$, $i \ge 0$, то $\mathrm{Ud}(F) = \infty$.

В отдельных случаях можно указать точное значение величины $\mathrm{Ud}(F)$.

Теорема 7. Пусть $R = \mathbb{Z}_4$, $l = t = 1$, $h(x) = x_{11}$ и $F(x) = x^m - x - 1$. Тогда справедливо равенство $\mathrm{Ud}(F) = 3m$.

Автор выражает глубокую благодарность А.А. Нечаеву за помощь в проведении исследования и ценные советы по оформлению данной работы.

ЛИТЕРАТУРА

1. *Кузьмин А.С.*, *Куракин В.Л.*, *Нечаев А.А.* Кольца Галуа в приложениях к кодам и рекуррентам // Труды Академии криптографии РФ. Тема 26. М., 1998.
2. *Нечаев А.А.* Код Кердока в циклической форме // Дискретная математика. 1989. Т. 4. № 1. С. 123 – 139.