ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 18 МАТЕМАТИКИ Выпуск 4
2011

КОЗЛИТИН О. А.[*]

ПЕРИОДИЧЕСКИЕ СВОЙСТВА 2-ЛИНЕЙНОГО РЕГИСТРА СДВИГА НАД КОЛЬЦОМ ГАЛУА

Исследуется цикловая структура самоуправляемого 2-линейного регистра сдвига над кольцом Галуа четной характеристики. Показано, что при надлежащем выборе функции самоуправления и функции выхода почти все начальные заполнения индуцируют выходную последовательность максимально возможного периода.

Работа выполнена при поддержке гранта Президента РФ МК-24.2009.10.

Содержание

§1. Введение

Полилинейный регистр сдвига является естественным многомерным обобщением стандартного (одномерного) линейного регистра сдвига. Первоначально двумерный линейный (2-линейный) регистр сдвига был предложен японскими математиками Nomura и Fukuda в качестве декодера так называемого *двумерного циклического кода* [5]. Позже отечественные специалисты указали на возможность использования полилинейного регистра для выработки *псевдослучайных последовательностей* (ПСП) [3]. На основе 2-линейного регистра сдвига (2-ЛРС) над кольцом вычетов $\mathbf{Z}_{2^n}$ был построен генератор ПСП. В работе [1] исследованы его периодические свойства, а в работе [2] показано, что выходная последовательность обладает большим рангом и хорошими частотными характеристиками. Целью данной работы является изучение периодических свойств 2-ЛРС над произвольным кольцом Галуа четной характеристики.

---

[*] Лауреат II Общероссийского открытого конкурса «Отмеченная работа молодого исследователя в области прикладной и промышленной математики» (ОРМИ-ОПиПМ'2011). Данная конкурсная работа отмечена приглашенным пленарным докладом на осенней открытой сессии XII Всероссийского симпозиума по прикладной и промышленной математике, а также дипломом II степени с вручением серебряной медали.

Пусть $r, n \in \mathbf{N}$, $q = 2^r$, а $R = \mathbf{GR}(q^n, 2^n)$ есть кольцо Галуа мощности q^n и характеристики 2^n. Пусть $F(x)$ — многочлен максимального периода степени $m \geqslant 2$, $F(x) \in R[x]$. Обозначим $e_{i,j}$ матричную единицу, т. е. $(m \times m)$-матрицу, в которой на пересечении i-й строки и j-го столбца стоит 1, а на остальных позициях — 0 (счет строк и столбцов будет вестись с нуля). Рассмотрим $\mathbf{e}^{\downarrow}$ — записанный столбцом базис R-бимодуля $R_{m,m}$, состоящий из матричных единиц:

$$e_{0,0}, \ldots, e_{0,m-1}, e_{1,0}, \ldots, e_{1,m-1}, \ldots,$$

а также автоморфизмы φ_0 и φ_1 бимодуля $R_{m,m}$, определенные соотношением

$$\forall\, s \in \{0,1\}: \quad \varphi_s(x) = \vec{x}\,(S(F)^{1-s} \otimes S(F)^s)\,\mathbf{e}^{\downarrow},$$

где $\vec{x}$ — строка координат x в базисе $\mathbf{e}^{\downarrow}$, $\otimes$ — операция тензорного произведения матриц. Пусть $\tau = q^m - 1$, автоморфизм σ бимодуля $R_{m,m}$ таков, что

$$\sigma = \varphi_0^{2^{n-2}(\tau-1)}\,\varphi_1^{2^{n-2}(\tau+1)}, \tag{1}$$

и θ есть корень многочлена $F(x)$ в кольце $S = \mathbf{GR}(q^{mn}, 2^n)$. Элементу $\alpha = \theta^{2^{n-2}(\tau-1)}$ сопоставим его образ $\overline{\alpha}$ при естественном эпиморфизме $S \to S/2S$, а каждому значению $j \in \{1, 2, \ldots, m-1\}$ — минимальный многочлен $\mu_j(x)$ элемента $\overline{\alpha}^{q^j-1}$ над полем $\overline{R} = R/2R$. В следующем параграфе будет доказано следующее утверждение.

Утверждение 1. *Характеристический многочлен автоморфизма σ имеет следующее каноническое разложение*:

$$\chi_\sigma(x) = G_0(x)G_1(x)\cdots G_{m-1}(x), \tag{2}$$

где $G_0(x) = (x-1)^m$ и $\overline{G}_j(x) = \mu_j(x)$, $j = 1, 2, \ldots, m-1$.

Для всякого $j \in \{0, 1, \ldots, m-1\}$ положим $H_j(x) = \chi_\sigma(x)/G_j(x)$. В силу утверждения 1 существуют такие многочлены $U_0(x), U_1(x), \ldots, U_{m-1}(x)$, что $U_0(x)H_0(x) + U_1(x)H_1(x) + \cdots + U_{m-1}(x)H_{m-1}(x) = 1$. Пусть отображение ψ: $R_{m,m} \to R$ возвращает элемент, стоящий в первой строке и первом столбце своего аргумента, а tr — функция «след» из $\overline{R}$ в $\mathbf{Z}_2$. Рассмотрим *функцию самоуправления* β: $R_{m,m} \to \mathbf{Z}_2$, определенную равенством $\beta(x) = \mathrm{tr}\{\overline{\psi(U_0(\sigma)H_0(\sigma)(x))}\}$ для любого $x \in R_{m,m}$.

Пусть функция перехода h_β автономного автомата

$$\mathfrak{A}^\beta = (R_{m,m}, R, h_\beta, \psi) \tag{3}$$

задана соотношением $h_\beta(x) = \varphi_{\beta(x)}(x)$ для каждого $x \in R_{m,m}$.

Следуя [3], будем называть автомат (3) *самоуправляемым* 2-*линейным регистром сдвига* (самоуправляемым 2-ЛРС).

Всюду далее фраза «свойство выполняется почти для всех состояний» означает, что доля состояний, для которых свойство не выполняется, есть $o(1)$ при $m \to \infty$. Перечислим основные результаты этой работы.

1. Разложение (2) индуцирует следующее однозначное представление последовательности состояний w автомата $\mathfrak{A}^{\beta}$:

$$w = \cdots$$

Если $\cdots$ и

$$\cdots,$$

то период $T(\gamma)$ выходной последовательности γ вычисляется по формуле

$$T(\gamma) = \cdots \tag{4}$$

2. Неравенство (4) обращается в равенство тогда и только тогда, когда

$$\cdots$$

Почти для всех начальных заполнений $w(0)$ справедливо соотношение

$$T(\gamma) = \cdots.$$

3. Число $N(\mathfrak{A}^{\beta})$ начальных состояний $w(0)$, для которых неравенство (4) обращается в равенство, выражается формулой

$$N(\mathfrak{A}^{\beta}) = \cdots$$

где μ — функция Мебиуса. Таким образом, почти все состояния 2-ЛРС $\mathfrak{A}^{\beta}\ldots$

§2. Эффект сокращения периода

Изучим периодические свойства выходной последовательности γ. Поскольку

$$\forall\, i \geqslant 0: \quad \gamma(i) = \psi(w(i)),$$

очевидно, $T(\gamma) \mid T(w)$. В этом параграфе будет показано, при каких условиях отсутствует эффект сокращения периода, т. е. выполняется равенство

$$T(\gamma) = T(w). \tag{5}$$

Напомним, что $S = \mathbf{GR}\,(q^{mn}, 2^n)$. Имеет место следующее 2-*адическое разложение* всякого элемента $x \in S$:

$$x = x_0 + 2x_1 + 2^2 x_2 + \cdots + 2^{n-1} x_{n-1},$$

где $x_i^{q^m} = x_i$, $i = 0, 1, \ldots, n-1$. Рассмотрим автоморфизм φ кольца S, определенный равенством

$$\forall\, a \in S: \quad \varphi(x) = \sum_{i=0}^{n-1} 2^i x_i^q.$$

Из следствия 2 вытекает, что $N(\mathfrak{A}^\beta) =$
при $m \to \infty$, т. е.

$$T(\gamma) = \ldots \qquad m \to \infty,$$

для почти всех начальных заполнений $w(0)$ 2-ЛРС $\mathfrak{A}^\beta$.

§4. Заключение

Подведем итоги. В данной работе впервые вычислена цикловая структура самоуправляемого 2-линейного регистра сдвига над кольцом Галуа четной характеристики. Показано, что почти все состояния этого автомата и почти для всех начальных заполнений регистра .

Автор выражает глубокую признательность профессору А. А. Нечаеву за постановку задачи и постоянное внимание к этой работе.

СПИСОК ЛИТЕРАТУРЫ

1. *Козлитин О. А.* Периодические свойства простейшего 2-линейного регистра сдвига. — Дискретн. матем., 2007, т. 19, в. 3, с. 51–78.
2. *Козлитин О. А.* Свойства выходной последовательности простейшего самоуправляемого 2-линейного регистра сдвига. — Дискретн. матем., 2007, т. 19, в. 4, с. 70–96.
3. *Нечаев А. А.* Многомерные регистры сдвига и сложность мультипоследовательностей. — В сб.: Труды по дискретной математике. Т. 6. М.: Физматлит, 2002, с. 150–164.
4. *Нечаев А. А.* Цикловые типы линейных подстановок над конечными коммутативными кольцами. — Матем. сб., 1993, т. 184, в. 3, с. 21–56.
5. *Nomura T.*, *Fukuda A.* Linear recurring planes and two-dimensional cyclic codes. — Electron. Comm. Japan, 1971, v. 54, № 3, p. 23–30.

Поступила в редакцию
12.III.2010