О. А. Козлитин (Москва, ТВП)**. Описание двоичных 2-линейных регистров сдвига максимального периода.**

В 2002 г. в работе [1] была высказана мысль о возможности использования самоуправляемых 2-линейных регистров сдвига (2-ЛРС) для выработки псевдослучайных последовательностей (ПСП) и поставлена задача исследования периодических свойств таких ПСП. В работе, представленной данным сообщением, найден критерий максимальности периода выходной последовательности двоичного самоуправляемого 2-ЛРС.

Пусть $\mathbf{R} = \mathbb{Z}_2$, $F_0(x), F_1(x) \in R[x]$ — многочлены степеней $m_0 \geqslant 2$ и $m_1 \geqslant 2$ соответственно, $\psi\colon R_{m_0,m_1} \to \mathbf{R}$ — функция, возвращающая элемент, находящийся в первой строке и первом столбце ее аргумента. Опишем функционирование неавтономного 2-ЛРС $\mathfrak{A}$ с начальным заполнением $w(0) \in R_{m_0,m_1}$.

Рассмотрим такое отображение $\mu\colon \mathbb{N}_0^2 \to \mathbf{R}$, что $\mu[\{0,1,\dots,m_0-1\}\times\{0,1,\dots,m_1-1\}] = w(0)$, и в таблице

$\mu(0,0)$	$\mu(0,1)$	$\mu(0,2)$	$\dots$	$\mu(0,j)$	$\dots$
$\mu(1,0)$	$\mu(1,1)$	$\mu(1,2)$	$\dots$	$\mu(1,j)$	$\dots$
$\mu(2,0)$	$\mu(2,1)$	$\mu(2,2)$	$\dots$	$\mu(2,j)$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\mu(i,0)$	$\mu(i,1)$	$\mu(i,2)$	$\dots$	$\mu(i,j)$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

каждый столбец есть линейная рекуррентная последовательность (ЛРП) с характеристическим многочленом $F_0(x)$, а каждая строка — ЛРП с характеристическим многочленом $F_1(x)$. По таблице под действием двоичной управляющей последовательности δ движется прямоугольное окно размерами $m_0 \times m_1$: если очередной знак δ равен 0, то окно сдвигается на один шаг вниз, а если 1, то на один шаг вправо (в начальный момент времени окно располагается в левом верхнем углу таблицы). Текущее заполнение окна $w(i)$ считается текущим заполнением регистра $\mathfrak{A}$, а значение $\psi(w(i))$ — очередным знаком выходной последовательности γ.

Если задать функцию обратной связи $\beta\colon R_{m_0,m_1} \to \mathbf{R}$, то неавтономный 2-ЛРС $\mathfrak{A}$ можно превратить в автономный (самоуправляемый) 2-ЛРС $\mathfrak{A}^\beta$: $\delta(i) = \beta(w(i))\ \forall\, i \geqslant 0$. Из результатов работы [2] следует, что период $T(\gamma)$ выходной последовательности γ удовлетворяет неравенству

$$T(\gamma) \leqslant (2^{m_0} - 1)(2^{m_1} - 1). \tag{1}$$

Ниже будет сформулирован критерий обращения неравенства (1) в равенство.

Пусть φ_0 и φ_1 — частичные функции перехода 2-ЛРС $\mathfrak{A}$.

Утверждение. *Если $F_0(x) = F_1(x) = F(x)$ — многочлен максимального периода степени m, а θ — корень многочлена $F(x)$ в его поле разложения, то характеристический многочлен линейного оператора $\sigma = \varphi_0^{-1}\,\varphi_1$ представляется в виде*

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

где $G_0(x) = (x \oplus 1)^m$, и $G_j(x) \in R[x]$ — минимальный многочлен элемента θ^{2^j-1}, $j = 1, 2, \dots, m-1$. Все сомножители в разложении (2) *попарно различны и имеют степень m.*

В условиях утверждения начальное заполнение $w(0) \in R_{m,m}$ самоуправляемого 2-ЛРС $\mathfrak{A}^\beta$ однозначно представляется в виде

$$w(0) = a_0 + a_1 + \cdots + a_{m-1}, \tag{3}$$

где $a_j \in \operatorname{Ker} G_j(\sigma)$, $j = 0, 1, \ldots, m-1$. В работе [3] показано, что матрица a_0 из разложения (3) имеет вид

$$a_0 = \begin{pmatrix} u(0) & u(1) & \ldots & u(m-1) \\ u(1) & u(2) & \ldots & u(m) \\ \vdots & \vdots & \ddots & \vdots \\ u(m-1) & u(m) & \ldots & u(2m-2) \end{pmatrix},$$

где $u \in L_R(F)$. Будем говорить, что ЛРП u *ассоциирована* с матрицей a_0.

Теорема. *Неравенство* (1) *обращается в равенство тогда и только тогда, когда*

1) $F_0(x) = F_1(x) = F(x)$, *причем* $T(F) = 2^m - 1$, *где* $m = m_0 = m_1$;

2) *существует такая булева функция* f *от* m *переменных, что*

a) $f(0, 0, \ldots, 0) = 0$;

b) *для всякого* $i \geqslant 0$ *верно равенство* $\beta(w(i)) = f(u(i), u(i+1), \ldots, u(i+m-1))$, *где* $u \in L_R(F)$ — ЛРП, *ассоциированная с* a_0;

c) $(\|f\|, 2^m - 1) = 1$, *где* $\|f\|$ — *вес булевой функции* f;

3) $\varepsilon_0 = 1$ *и* $(\varepsilon_1, 2\varepsilon_2, \ldots, (m-1)\varepsilon_{m-1}) = 1$, *где* ε_j — *индикатор того, что* $a_j \neq 0$, $j = 0, 1, \ldots, m-1$.

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

Работа выполнена при поддержке гранта Президента РФ НШ-4.2010.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Нечаев А. А.* Многомерные регистры сдвига и сложность мультипоследовательностей. — В кн.: Труды по дискретной математике. Т. 6. М.: Физматлит, 2002, с. 150–165.
2. *Михайлов Д. А.* Унитарные полилинейные регистры сдвига и их периоды. — Дискретн. матем., 2002, т. 14, в. 1, с. 30–59.
3. *Козлитин О. А.* Периодические свойства простейшего 2-линейного регистра сдвига. — Дискретн. матем., 2007, т. 19, в. 3, с. 51–78.