О. А. К о з л и т и н (Москва, ТВП)**. О выходной последовательности двоичного 2-линейного регистра сдвига.**

В литературе неоднократно высказывалась мысль о возможности использования самоуправляемых полилинейных регистров сдвига в качестве генераторов псевдослучайных последовательностей (см., например, [2] и [3]). В работе, представленной данным сообщением, впервые проведен расчет ряда специальных параметров двоичного самоуправляемого 2-линейного регистра сдвига (2-ЛРС).

Пусть $R = \mathbf{Z}_2$, $F(x) \in R[x]$ — многочлен максимального периода степени $m \geqslant 2$, ψ: $R_{m,m} \to R$. Опишем функционирование неавтономного 2-ЛРС $\mathfrak{A}$ с начальным заполнением $w(0) \in R_{m,m}$.

Рассмотрим такое отображение μ: $\mathbf{N}_0^2 \to R$, что $\mu[\overline{0, m-1} \times \overline{0, m-1}] = \omega(0)$, и в таблице каждая строка и каждый столбец суть линейные рекуррентные последовательности (ЛРП) с характеристическим многочленом $F(x)$. Такая таблица называется 2-*линейной рекуррентной последовательностью* [1]. По таблице под действием двоичной управляющей последовательности δ движется прямоугольное окно размерами $m \times m$: 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.

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

Если задать функцию обратной связи β: $R_{m,m} \to R$, то неавтономный 2-ЛРС $\mathfrak{A}$ можно превратить в автономный (самоуправляемый) 2-ЛРС $\mathfrak{A}^\beta$: $\delta(i) = \beta(w(i))$ для любых $i \geqslant 0$.

Мы будем рассматривать самоуправляемый 2-ЛРС $\mathfrak{A}^\beta$, функция выхода ψ которого возвращает элемент, стоящий в левом верхнем углу текущего заполнения. Опишем функцию обратной связи β.

Пусть φ_0 и φ_1 — частичные функции перехода 2-ЛРС $\mathfrak{A}$, а θ — корень многочлена $F(x)$ в его поле разложения.

Утверждение. *Характеристический многочлен линейного оператора* $\sigma = \varphi_0\,\varphi_1^{-1}$ *представляется в виде*

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

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* (1) *попарно различны и имеют степень* m.

Если для любых $j \in \{0, 1, \dots, m-1\}$

$$\widetilde{G}_j(x) = G_0(x)\cdots G_{j-1}(x)G_{j+1}(x)\cdots G_{m-1}(x),$$

то существуют такие многочлены $U_0(x), U_1(x), \dots, U_{m-1}(x) \in R[x]$, что

$$\widetilde{G}_0(x)U_0(x) + \widetilde{G}_1(x)U_1(x) + \cdots + \widetilde{G}_{m-1}(x)U_{m-1}(x) = 1.$$

Зададим функцию обратной связи β следующим образом: $\beta(a) = \psi[\widetilde{G}_0(\sigma)U_0(\sigma)(a)]$ для любых $a \in R_{m,m}$. Легко видеть, что функция β линейна.

Равенство (1) индуцирует следующее разложение пространства $R_{m,m}$ в прямую сумму собственных подпространств:

$$R_{m,m} = \operatorname{Ker} G_0(\sigma) \dot{+} \operatorname{Ker} G_1(\sigma) \dot{+} \cdots \dot{+} \operatorname{Ker} G_{m-1}(\sigma).$$

Это означает, что начальное заполнение $w(0)$ самоуправляемого 2-ЛРС $\mathfrak{A}^\beta$ однозначно представляется в виде

$$w(0) = a_0 + a_1 + \cdots + a_{m-1}, \tag{2}$$

где $a_j \in \operatorname{Ker} G_j(\sigma)$, $j = 0, 1, \ldots, m-1$. Всюду далее будем рассматривать начальные заполнения $w(0)$, в разложении (2) которых $a_0 \neq 0$.

Пусть вектор $\operatorname{typ} w(0) = (\delta_1, \delta_2, \ldots, \delta_{m-1}) \in R^{m-1}$ таков, что δ_j есть индикатор неравенства $a_j \neq 0$, $j = 1, 2, \ldots, m-1$. Положим $\tau = 2^m - 1$, $\tau_j = \tau/(2^{(m,j)} - 1)$, $j = 1, 2, \ldots, m-1$.

Теорема 1. *Во введенных обозначениях период $T(\gamma)$ выходной последовательности γ удовлетворяет равенству $T(\gamma) = [\tau_1^{\delta_1}, \tau_2^{\delta_2}, \ldots, \tau_{m-1}^{\delta_{m-1}}]\,\tau$. При этом равенство $T(\gamma) = \tau^2$ выполняется тогда и только тогда, когда $(\delta_1, 2\delta_2, 3\delta_3, \ldots, (m-1)\delta_{m-1}, m) = 1$. Ранг $\operatorname{rang}\gamma$ выходной последовательности γ удовлетворяет двойному неравенству*

$$m\Bigl(1 + \sum_{j=1}^{m-1} \delta_j \tau\Bigr) \geqslant \operatorname{rang}\gamma \geqslant m\Bigl(1 + \sum_{j=1}^{m-1} \delta_j \tau_j\Bigr).$$

Если δ_j есть индикатор равенства $(m, j) = 1$, $j = 1, 2, \ldots, m-1$, то $\operatorname{rang}\gamma = m + m\varphi(m)(2^m - 1)$, где φ — функция Эйлера.

Для всякого $z \in \{0, 1\}$ обозначим p_z относительную частоту появления знака z на цикле последовательности γ.

Теорема 2. *Если $\operatorname{typ} w(0) = (0, \ldots, 0, 1, 0, \ldots, 0)$, где 1 стоит на j-м месте, $1 \leqslant j \leqslant m-1$, то для любых $z \in \{0, 1\}$*

$$\left| p_z - \frac{\tau^2 + (-1)^z}{2\tau^2} \right| \leqslant \frac{1}{2}\left(\frac{1}{\tau_j} - \frac{1}{\tau}\right) 2^{m/2}.$$

В частности, если $(m, j) = 1$, то на цикле γ имеется $(\tau^2 + 1)/2$ нулей и $(\tau^2 - 1)/2$ единиц.

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

Работа выполнена при поддержке грантов Президента РФ МК-24.2009.10 и НШ-4.2008.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Псевдослучайные и полилинейные последовательности. — Труды по дискретной математике, 1997, т. 1, с. 139–202.
2. *Михайлов Д. А.* Унитарные полилинейные регистры сдвига и их периоды. — Дискретная математика, 2002, т. 14, в. 1, с. 30–59.
3. *Нечаев А. А.* Многомерные регистры сдвига и сложность мультипоследовательностей. — Труды по дискретной математике, 2003, т. 6, с. 150–165.