ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 25 МАТЕМАТИКИ Выпуск 3
2018

Н. М. Меженная, В. Г. Михайлов (Москва, МГТУ им. Н. Э. Баумана, МИ РАН)**. Центральная предельная теорема для числа единиц в неравновероятной мультициклической последовательности.**

Обобщенный мультициклический генератор, определяемый булевой функцией $f(y_1,\dots,y_r)$, состоит из r регистров длин $m_1,\dots,m_r$, заполненных знаками $(x_0^{(j)},\dots,x_{m_j-1}^{(j)})$, $j=1,\dots,r$. Он определяет мультициклическую последовательность по правилу

$$z_t = f\big(x_{t(m_1)}^{(1)},\dots,x_{t(m_r)}^{(r)}\big), \tag{1}$$

где $t(m_j) = t \bmod m_j$. При $f(y_1,\dots,y_r) = y_1 \oplus \dots \oplus y_r$ обобщенный мультициклический генератор совпадает с обычным генератором Пола [1]. Далее будем считать, что функция f существенно зависит от всех r аргументов.

Последовательность вида (1) является чисто периодической с периодом длины $L = m_1 \dots m_r$. Нас интересует предельный при $m_1,\dots,m_r \to \infty$ закон распределения случайной величины ξ, равной числу единиц в цикле последовательности (1) длины L.

Будем использовать обозначения $\mathrm{wt}(f)$ для веса функции f ([2, с. 75]) и $W_f(z)$ — для коэффициента Уолша–Адамара функции f в точке $z \in \{0,1\}^r$ ([2, с. 77]):

$$W_f(z) = \sum_{u\in\{0,1\}^r} (-1)^{f(u)+z_1u_1+\dots+z_ru_r}.$$

Пусть также $\mathbf{1}_{(j_1,\dots,j_k)}$ — двоичный вектор, множество единиц которого равно $\{j_1,\dots,j_k\}$.

Теорема. *Пусть обобщенный мультициклический генератор с r регистрами длин $m_1,\dots,m_r$ задается булевой функцией f, заполнения $x_k^{(j)}$ ячеек регистров случайны, независимы в совокупности и $\mathbf{P}\{x_k^{(j)}=1\} = 1-\mathbf{P}\{x_k^{(j)}=0\} = p_j \in (0,1)$, $k=0,\dots,m_j-1$, $j=1,\dots,r$, причем все $p_j \neq 1/2$. Если число $r \geqslant 2$ фиксировано, а $m_1,\dots,m_r \to \infty$, то закон распределения случайной величины $B^{-1}\left(\frac{2^r\xi}{m_1\dots m_r} - A\right)$ сходится к стандартному нормальному закону, где*

$$A = \mathrm{wt}(f) - \frac{1}{2}\sum_{k=1}^{r}\sum_{1\leqslant j_1<\dots<j_k\leqslant r} W_f(\mathbf{1}_{(j_1,\dots,j_k)})\prod_{l=1}^{k}(1-2p_{j_l}), \quad B^2 = \sum_{j=1}^{r} b_j^2 > 0,$$

$$b_j = \frac{\sqrt{p_j(1-p_j)}}{\sqrt{m_j}}\Big(W_f(\mathbf{1}_{(j)}) + \sum_{k=1}^{r-1}\sum_{1\leqslant j_1<\dots<j<\dots<j_k\leqslant r} W_f(\mathbf{1}_{(j_1,\dots,j,\dots,j_k)})\prod_{l=1}^{k}(1-2p_{j_l})\Big).$$

Замечание 1. Условие $p_j \neq 1/2$, $j=1,\dots,r$, теоремы объясняется тем, что иначе трудно гарантировать, что $B^2 > 0$ для функции f общего вида.

Замечание 2. Случай, когда все $p_j = 1/2$, $j=1,\dots,r$, описан в [3].

Замечание 3. Частный случай, когда $f(y_1,\dots,y_r) = y_1 \oplus \dots \oplus y_r$ (генератор Пола) и вероятности знаков p_j могут отличаться от $1/2$, был рассмотрен в [4].

СПИСОК ЛИТЕРАТУРЫ

1. *Pohl P.* Description of MCV, a pseudo-random number generator. — Scand. Actuarial J., 1976, v. 1, p. 1–14.
2. *Логачев О. А.*, *Сальников А. А.*, *Смышляев С. В.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004, 470 с.
3. *Меженная Н. М.*, *Михайлов В. Г.* О числе единиц в выходной последовательности мультициклического генератора, определяемого булевой функцией. — Дискретные модели в теории управляющих систем: X Международная конференция, Москва и Подмосковье, Алексеев В. Б., Романов Д. С., Данилов Б. Р. (ред.) М.: Макс Пресс, 2018, 296 с, с. 195–198.
4. *Меженная Н. М.* О распределении числа единиц в двоичной мультициклической последовательности. — Прикладная дискретная математика, 2015, т. 1, с. 69–77.