ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 5
2015

Н. М. Меженная (Москва, МГТУ). **О числе появлений знаков в мультициклической случайной последовательности по модулю 4 с m-зависимыми знаками.**

Пусть $n_1, \dots, n_r \geqslant 2$ — взаимно простые натуральные числа, $X^{(j)} = (X_0^{(j)}, \dots, X_{n_j-1}^{(j)})$, $j = 1, \dots, r$, — наборы случайных величин, распределенных равномерно на множестве вычетов по модулю M. Мультициклическая случайная последовательность образуется по правилу

$$Z_t = \sum_{j=1}^{r} X_{t(n_j)} \bmod M, \tag{1}$$

где $t(n_j) = t \bmod n_j$. Последовательность вида (1) является математической моделью выходной последовательности генератора Пола (см. [1]), в которой наборы $X^{(1)}, \dots, X^{(r)}$ представляют собой заполнения регистров. В работах [2], [3] было проведено исследование свойств мультициклической последовательности по модулю 2. Свойства мультициклической последовательности при $M = 4$ и независимых равновероятных знаках в регистрах были исследованы в работе [4]. В частности, было получено совместное предельное распределение чисел появлений знаков в мультициклической последовательности, когда длины регистров стремятся к бесконечности. Настоящая работа посвящена изучению свойств мультициклической последовательности по модулю $M = 4$ вида (1) длины $T = n_1 \dots n_r$, когда случайные величины $X_0^{(j)}, \dots, X_{n_j-1}^{(j)}$, образующий j-й вектор $X^{(j)}$, зависимы.

Сформулируем два условия:

1. Пусть $X^{(j)} = (X_0^{(j)}, \dots, X_{n_j-1}^{(j)})$, $j = 1, \dots, r$, независимые в совокупности случайные векторы, и

$$\mathbf{P}\{X_k^{(j)} = 2a_2 + a_1\} = \frac{1}{4}, \quad a_1, a_2 \in \{0, 1\}, \quad k = 0, \dots, n_j - 1, \quad j = 1, \dots, r.$$

2. Пусть при каждом j случайные величины $X_0^{(j)}, \dots, X_{n_j-1}^{(j)}$ m-зависимы по кругу, т. е. в последовательности $X_0^{(j)}, \dots, X_{n_j-1}^{(j)}, X_0^{(j)}, \dots, X_{n_j-1}^{(j)}, \dots, X_0^{(j)}, \dots, X_{n_j-1}^{(j)}, \dots$ наборы $X_k, \dots, X_{k+l-1}$ и $X_{k+l+m}, \dots, X_{k+l+m+s}$ независимы при $k, l, s \geqslant 0$, $l + m + s < n_j$, а совместное распределение случайных величин $X_{i_1}^{(j)}, \dots, X_{i_k}^{(j)}$ инвариантно относительно циклического сдвига, то есть закон распределения набора случайных величин $X_{i_1}^{(j)}, \dots, X_{i_k}^{(j)}$ при $0 \leqslant i_1 < i_2 < \dots < i_k \leqslant n_j - 1$ совпадает с распределением набора $X_{(i_1+h)(n_j)}^{(j)}, \dots, X_{(i_k+h)(n_j)}^{(j)}$, где $h \in \mathbb{Z}$.

Определим величины $\delta^{(j)}, \delta_0^{(j)}, \delta_1^{(j)}$, $j = 1, \dots, r$, равенствами

$$\nu_{a_2a_1}^{(j)} = \frac{1}{4}\left(n_j + (-1)^{a_1}\delta^{(j)} + 2(-1)^{a_2}\delta_{a_1}^{(j)}\right),$$

где $\nu_{a_2a_1}^{(j)}$ — число знаков в $X^{(j)}$, двоичная запись которых равна a_2a_1, $a_1, a_2 \in \{0, 1\}$. Обозначим $\nu_{a_2a_1}^{(1,\dots,r)}$ число знаков в $Z_0 \dots, Z_{T-1}$, имеющих двоичную запись

a_2a_1, $a_1, a_2 \in \{0,1\}$. В работе [4] показано, что

$$\nu_{a_2a_1}^{(1,\dots,r)} = \frac{1}{4}\left(n_1\dots n_r + (-1)^{a_1}\delta^{(1,\dots,r)} + 2(-1)^{a_2}\delta_{a_1}^{(1,\dots,r)}\right),$$

где $\delta^{(1,\dots,r)} = \delta^{(1)}\dots\delta^{(r)}$, $\delta_0^{(1,\dots,r)} + \mathrm{i}\delta_1^{(1,\dots,r)} = \prod_{j=1}^{r}\left(\delta_0^{(j)} + \mathrm{i}\delta_1^{(j)}\right)$.

Нас интересует предельный при $n_1,\dots,n_r \to \infty$ закон распределения случайного вектора $\vec{\nu}^{(1,\dots,r)} = \left(\nu_{00}^{(1,\dots,r)},\dots,\nu_{11}^{(1,\dots,r)}\right)^T$. Ясно, что эта задача эквивалентна задаче о предельном законе распределения случайного вектора $\nabla^{(1,\dots,r)} = \left(\delta^{(1,\dots,r)}, \delta_0^{(1,\dots,r)}, \delta_1^{(1,\dots,r)}\right)^T$.

Переходим к изложению основного результата работы. Пусть

$$\Sigma^{(j)} = \begin{pmatrix} {\sigma_0^{(j)}}^2 & \rho_{01}^{(j)}\sigma_0^{(j)}\sigma_1^{(j)} & \rho_{02}^{(j)}\sigma_0^{(j)}\sigma_2^{(j)} & \rho_{03}^{(j)}\sigma_0^{(j)}\sigma_3^{(j)} \\ \rho_{01}^{(j)}\sigma_0^{(j)}\sigma_1^{(j)} & {\sigma_1^{(j)}}^2 & \rho_{12}^{(j)}\sigma_1^{(j)}\sigma_2^{(j)} & \rho_{13}^{(j)}\sigma_1^{(j)}\sigma_3^{(j)} \\ \rho_{02}^{(j)}\sigma_0^{(j)}\sigma_2^{(j)} & \rho_{12}^{(j)}\sigma_1^{(j)}\sigma_2^{(j)} & {\sigma_2^{(j)}}^2 & \rho_{23}^{(j)}\sigma_2^{(j)}\sigma_3^{(j)} \\ \rho_{03}^{(j)}\sigma_0^{(j)}\sigma_3^{(j)} & \rho_{13}^{(j)}\sigma_1^{(j)}\sigma_3^{(j)} & \rho_{23}^{(j)}\sigma_2^{(j)}\sigma_3^{(j)} & {\sigma_3^{(j)}}^2 \end{pmatrix},$$

$$\sigma_{2a_2+a_1}^{(j)2} = \frac{3}{16} - \frac{m}{8} + 2\sum_{0<k'\leqslant m} P\{X_0^{(j)} = 2a_2+a_1, X_{k'}^{(j)} = 2a_2+a_1\},$$

$$\rho_{2a_2+a_1,2b_2+b_1}^{(j)} = \frac{-1-2m+32\sum_{0<k'\leqslant m} P\{X_0^{(j)} = 2a_2+a_1, X_{k'}^{(j)} = 2b_2+b_1\}}{16\sigma_{2a_2+a_1}^{(j)}\sigma_{2b_2+b_1}^{(j)}},$$

где $a_1, a_2, b_1, b_2 \in \{0,1\}$, $(a_2,a_1) \neq (b_2,b_1)$.

Положим

$$\Sigma_{\widetilde{\nabla}^{(j)}} = C\Sigma^{(j)}C^T, \quad C = \begin{pmatrix} 2 & 0 & 2 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

Теорема. *Пусть выполнены условия* 1 *и* 2, *при всех* j *матрицы* $\Sigma_{\widetilde{\nabla}^{(j)}}$ *невырождены и все* $n_j \to \infty$. *Если параметры* m *и* r *остаются фиксированными,* $\sigma_k^{(j)} = O(1)$, *то случайный вектор* $\widetilde{\nabla}^{(1,\dots,r)} = (n_1\dots n_r)^{-1/2}(\delta^{(1,\dots,r)}, \delta_0^{(1,\dots,r)}, \delta_1^{(1,\dots,r)})^T$ *сходится по распределению к случайному вектору* $(\eta,\eta_0,\eta_1)^T$, *где* $\eta = \prod_{j=1}^{r}\eta^{(j)}, \eta_0 + \mathrm{i}\eta_1 = \prod_{j=1}^{r}\left(\eta_0^{(j)} + \mathrm{i}\eta_1^{(j)}\right)$, *случайные векторы* $(\eta^{(j)}, \eta_0^{(j)}, \eta_1^{(j)})$ *независимы между собой и распределены по нормальному закону с нулевым средним и ковариационными матрицами* $\Sigma_{\widetilde{\nabla}^{(j)}}$.

З а м е ч а н и е. Предельные распределения из теоремы и теоремы 2 работы [4] совпадают, если при всех $j = 1,\dots,r$ $\sigma_0^{(j)} = \sigma_2^{(j)}$, $\sigma_0^{(j)}(\rho_{01}^{(j)}\sigma_1^{(j)} - \rho_{03}^{(j)}\sigma_3^{(j)}) = \sigma_2^{(j)}(\rho_{23}^{(j)}\sigma_3^{(j)} - \rho_{12}^{(j)}\sigma_1^{(j)})$.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ (тема 1.2640.2014).

СПИСОК ЛИТЕРАТУРЫ

1. *Pohl P.* Description of MCV, A pseudo-random number generator. — Scand. Actuarial J., 1976, v. 1, p. 1–14.
2. *Меженная Н. М., Михайлов В. Г.* О распределении числа единиц в выходной последовательности генератора Пола над полем GF(2). — Математические вопросы криптографии, 2013, т. 4, в. 4, с. 95–107.
3. *Mezhennaya N. M.* Convergence rate estimators for the number of ones in outcome sequence of MCV generator with m-dependent registers items. — Siberian Electronic Mathematical Reports, 2014, v. 11, p. 18–25.

4. *Меженная Н. М.*, *Михайлов В. Г.* О числе появлений знаков в мультициклической случайной последовательности по модулю 4. — Дискретн. матем., 2014, т. 26, в. 4, с. 51–58.