ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 4
2015

Н. М. Меженная, В. Г. Михайлов (Москва, МГТУ, МИАН)**. О распределении частот знаков в неравновероятной мультициклической случайной последовательности по модулю 4.**

Пусть $n_1, \ldots, n_r \geqslant 2$ — взаимно простые натуральные числа. Мультициклическая случайная последовательность $\{Z_t\}_{t \geqslant 0}$ со значениями в $\{0, \ldots, M-1\}$ образуется по правилу

$$Z_t = X^{(1)}_{t(n_1)} + \ldots + X^{(r)}_{t(n_r)} \bmod M, \quad t = 0, 1, \ldots,$$

где $(X^{(j)}_0, \ldots, X^{(j)}_{n_j-1})$, $j = 1, \ldots, r$, — наборы независимых в совокупности случайных величин, распределенных на множестве неотрицательных вычетов по модулю M, а $t(n_j) = t - [t/n_j]n_j$. Отрезок $Z = (Z_0, Z_1, \ldots, Z_{n_1 \ldots n_r - 1})$ будем называть *циклом* мультициклической последовательности $\{Z_t\}$.

Двоичная мультициклическая случайная последовательность была изучена в работах [1], [2]. Нас интересует случай $M = 4$. Целью исследования является изучение асимптотического поведения при $n_1, \ldots, n_r \to \infty$ совместного распределения случайных величин $\varkappa_{a_2 a_1}(r)$ — количеств чисел в последовательности Z, имеющих двоичную запись $a_2 a_1$, $a_1, a_2 \in \{0, 1\}$.

Нетрудно показать (см. [3]), что формула

$$\varkappa_{a_2 a_1} = \frac{1}{4}\left(n_1 \cdots n_r + (-1)^{a_1}\beta(r) + 2(-1)^{a_2}\beta_{a_1}(r)\right), \quad a_1, a_2 \in \{0, 1\},$$

однозначно определяет вектор $\nabla(r) = (\beta(r), \beta_0(r), \beta_1(r))$ (понимаемый как вектор-столбец). Этим задача исследования совместного распределения величин $\varkappa_{a_2 a_1}$ сводится к изучению распределения вектора $\nabla(r)$.

В работе [3] был рассмотрен случай, когда распределение знаков $X^{(j)}_k$ является равномерным Здесь мы рассмотрим ситуацию, когда распределение знаков $X^{(j)}_k$ отличается от равномерного.

Сформулируем полученный нами результат. Введем обозначения

$$p^{(j)}_{a_2 a_1} = \mathbf{P}\{X^{(j)}_k = 2a_2 + a_1\}, \quad a_1, a_2 \in \{0, 1\},$$

$$\Sigma^{(j)} = \begin{pmatrix} p^{(j)}_0 q^{(j)}_0 & p^{(j)}_{00} q^{(j)}_{00} - p^{(j)}_{10} q^{(j)}_{10} & p^{(j)}_0 \big(p^{(j)}_{11} - p^{(j)}_{01}\big) \\ p^{(j)}_{00} q^{(j)}_{00} - p^{(j)}_{10} q^{(j)}_{10} & p^{(j)}_0 - \big(p^{(j)}_{00} - p^{(j)}_{10}\big)^2 & -\big(p^{(j)}_{00} - p^{(j)}_{10}\big)\big(p^{(j)}_{01} - p^{(j)}_{11}\big) \\ p^{(j)}_0 \big(p^{(j)}_{11} - p^{(j)}_{01}\big) & -\big(p^{(j)}_{00} - p^{(j)}_{10}\big)\big(p^{(j)}_{01} - p^{(j)}_{11}\big) & p^{(j)}_1 - \big(p^{(j)}_{01} - p^{(j)}_{11}\big)^2 \end{pmatrix},$$

где

$$q^{(j)}_0 = 1 - p^{(j)}_0, \quad q^{(j)}_{00} = 1 - p^{(j)}_{00}, \quad q^{(j)}_{10} = 1 - p^{(j)}_{10}.$$

Пусть

$$b^{(j)} = (p^{(j)}_{00} + p^{(j)}_{10}) - (p^{(j)}_{01} + p^{(j)}_{11}), \quad b^{(j)}_a = p^{(j)}_{0a} - p^{(j)}_{1a}, \quad a \in \{0, 1\},$$

$$e^{(j)} = \begin{pmatrix} b^{(j)} \\ b^{(j)}_0 \\ b^{(j)}_1 \end{pmatrix}, \quad B^{(j)} = \begin{pmatrix} b^{(j)} & 0 & 0 \\ 0 & b^{(j)}_0 & -b^{(j)}_1 \\ 0 & b^{(j)}_1 & b^{(j)}_0 \end{pmatrix}, \quad C_j = B^{(1)} \cdots B^{(j)}.$$

Будем использовать обозначение A^T для матрицы, полученной транспонированием матрицы A.

Теорема. *Пусть число $r \geqslant 2$ постоянно, каждая матрица $B^{(1)}, \ldots, B^{(r)}$ содержит хотя бы один ненулевой элемент, а числа $n_1 < \cdots < n_r$ стремятся к бесконечности. Тогда функция распределения вектора*

$$n_1^{1/2}\left((n_1, \ldots, n_r)^{-1} \nabla(r) - C_{r-1} e^{(r)}\right)$$

сходится к функции трехмерного нормального распределения с нулевым вектором средних и матрицей ковариаций Σ_r, которая вычисляется по рекуррентным формулам

$$\Sigma_1 = \Sigma^{(1)}, \qquad \Sigma_j = B^{(j)} \Sigma_{j-1} (B^{(j)})^T + C_{j-1} \Sigma^{(j)} C_{j-1}^T, \quad j = 2, \ldots, r.$$

З а м е ч а н и е 1. Условие теоремы о свойствах матриц $B^{(1)}, \ldots, B^{(r)}$ эквивалентно аналогичным условиям для матриц $\Sigma^{(1)}, \ldots, \Sigma^{(r)}$ или для векторов $e^{(1)}, \ldots, e^{(r)}$.

З а м е ч а н и е 2. В работе [4] доказано аналогичное одномерное утверждение для случая $M = 2$.

Работа Н. М. Меженной поддержана грантом РФФИ номер 14-01-00318а.

СПИСОК ЛИТЕРАТУРЫ

1. *Меженная Н. М., Михайлов В. Г.* О распределении числа единиц в выходной последовательности генератора Пола над полем $GF(2)$. — Матем. вопросы криптографии, 2013, №4, в. 4, с. 95–107.
2. *Mezhennaya N. M.* Convergence rate estimators for the number of ones in outcome sequence of MCV generator with M-dependent registers items. — Siberian Electron. Math. Rep., 2014, v. 11, p. 18–25.
3. *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.
4. *Меженная Н. М.* О распределении числа единиц в двоичной мультициклической последовательности. — Прикл. дискретн. математика, 2015, №1(27), с. 69–77.