ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 24 МАТЕМАТИКИ Выпуск 3
2017

Н. М. Меженная, **В. Г. Михайлов** (Москва, МГТУ им. Н. Э. Баумана, МИ РАН)**. Предельная теорема для частот знаков в мультициклической последовательности над прямой суммой групп вычетов по модулю 2.**

Пусть G — прямая сумма m групп $\mathbb{Z}_2$, $m \geqslant 2$, а $n_1, \ldots, n_r \geqslant 2$ — взаимно простые натуральные числа. Мультициклический генератор псевдослучайных элементов группы G содержит r циклических регистров длин $n_1, \ldots, n_r$, ячейки которых заполнены элементами $X_0^{(j)}, \ldots, X_{n_j-1}^{(j)} \in G$, $j = 1, \ldots, r$, соответственно. Он вырабатывает последовательность $\{Z_t\}_{t\geqslant 0}$ (называемую *мультициклической последовательностью*) по правилу

$$Z_t = X_{t(n_1)}^{(1)} + \cdots + X_{t(n_r)}^{(r)} \quad t = 0, 1, \ldots,$$

где $t(n_j) = t - [t/n_j]n_j$. Здесь и далее через $[x]$ обозначена целая часть числа x.

Отрезок $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_{n_1 \ldots n_r - 1})$ принято называть *циклом* мультициклической последовательности $\{Z_t\}$.

Обозначим $\widehat{h} = (h_1, \ldots, h_m), h_i \in \mathbb{Z}_2, i = 1, \ldots, m$ элемент группы G, $\widehat{0} = (0, \ldots, 0)$ — нулевой элемент группы G.

Пусть

$$\varkappa(\widehat{h}) = \sum_{i=0}^{n_1 \ldots n_r - 1} I\{Z_i = \widehat{h}\}, \quad \widehat{h} \in G.$$

— случайные величины, называемые *частотами* элементов $h \in G$ в мультициклической последовательности $\mathbf{Z}$.

Введем обозначения $X^{(j)} = (X_0^{(j)}, \ldots, X_{n_j-1}^{(j)})$, $j = 1, \ldots, r$,

$$X_{k_j}^{(j)} = (X_{k_j}^{1,(j)}, \ldots, X_{k_j}^{m,(j)}), \quad k_j = 0, \ldots, n_j - 1, \ j = 1, \ldots, r, \tag{1}$$

где $X_{k_j}^{u,(j)} \in \mathbb{Z}_2$.

Нас интересует случай, когда наборы $X^{(j)} = (X_0^{(j)}, \ldots, X_{n_j-1}^{(j)})$, $j = 1, \ldots, r$, образованы независимыми в совокупности случайными величинами, распределенными *равномерно* на множестве элементов группы G. Тогда случайные величины $X_{k_j}^{u,(j)}$ в (**??**) независимы в совокупности и равномерно распределены на $\mathbb{Z}_2$. В этом случае набор $Z_t = \left(Z_t{}^1, \ldots, Z_t{}^m\right)$ состоит из независимых в совокупности случайных элементов группы $\mathbb{Z}_2$ (нулей и единиц).

Пусть при $\widehat{h} = (h_1, \ldots, h_m) \in G$

$$\widetilde{\varkappa}(\widehat{h}) = \frac{2^m \varkappa(\widehat{h}) - n_1 \ldots n_r}{\sqrt{n_1 \ldots n_r}}.$$

Через Φ_r обозначим распределение произведения r независимых стандартных гауссовских случайных величин.

Теорема. *Пусть случайные величины $X_t^{(j)}$ независимы в совокупности и распределены равномерно на G. Тогда при $n_1 \to \infty, \ldots, n_r \to \infty$ распределение вектора*

$(\widetilde{\varkappa}(\widehat{h}), \widehat{h} \in G)$ сходится к распределению вектора $(\alpha(\widehat{h}), \widehat{h} \in G)$, где

$$\alpha(\widehat{h}) = \sum_{(g_1,\ldots,g_m)\in G\setminus\{\widehat{0}\}} (-1)^{g_1h_1+\ldots+g_mh_m}\xi_{g_1,\ldots,g_m},$$

а случайные величины $\xi_{g_1,\ldots,g_m}, (g_1,\ldots,g_m) \in G\setminus\{\widehat{0}\}$, независимы в совокупности и имеют распределение Φ_r.

Следствие. *Пусть выполнены условия теоремы* 2. *Тогда для каждого $\widehat{h} \in G$ при $n_1 \to \infty, \ldots, n_r \to \infty$ распределение случайной величины $\widetilde{\varkappa}(\widehat{h})$ сходится к (2^m-1)-кратной свертке распределения Φ_r.*

З а м е ч а н и е. При $m = 1$ аналогичная предельная теорема была доказана в работе [1]. Там же была получена оценка скорости сходимости в этой предельной теореме.

СПИСОК ЛИТЕРАТУРЫ

1. *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, № 4, с. 95–107.