О Б О З Р Е Н И Е
П Р И К Л А Д Н О Й И П Р О М Ы Ш Л Е Н Н О Й
Том 22 М А Т Е М А Т И К И Выпуск 4
2015

В. О. Д р е л и х о в, **И. А. К р у г л о в** (Москва, «Центр сертификационных исследований», АКРФ)**. Локальные характеристики выравнивающих свойств отображений конечных абелевых групп.**

Многие современные криптографические алгоритмы используют последовательности случайных элементов конечных множеств. При этом для обеспечения стойкости данных алгоритмов большое значение имеет достаточная близость вероятностных характеристик используемых случайных последовательностей к соответствующим характеристикам последовательностей с независимыми равновероятными элементами. Для выработки случайных последовательностей целесообразно использование датчиков шума, построенных на основе различных физических явлений. Довольно часто оказывается, что характеристики выходных последовательностей физических датчиков шума существенно отличаются от характеристик случайных равновероятных последовательностей. В этом случае применяются различные схемы выравнивания (сглаживания) вероятностных характеристик выходных последовательностей физических датчиков. Исследованию различных схем выравнивания посвящены, в частности, работы [1], [2], [3], [4], [5].

В настоящей работе мы рассмотрим следующую вероятностную модель схем выравнивания. Пусть $(G,+)$ — некоторая конечная коммутативная группа, $|G|=q, q\geqslant 2$, n,m — натуральные числа, $n>m\geqslant 2$, $G^n=G\times G\times\ldots\times G$ — n-я декартова степень множества G. Декартовы степени G^n и G^m являются коммутативными группами относительно операций покоординатного сложения элементов.

Предположим, что имеется исходная последовательность $\overrightarrow{\xi}=(\xi_1,\xi_2,\ldots,\xi_n)$ случайных элементов $\xi_1,\xi_2,\ldots,\xi_n$, принимающих значения в группе G,

$$p_{\overrightarrow{\xi}}(\overrightarrow{g})=\mathbf{P}\left\{\overrightarrow{\xi}=\overrightarrow{g}\right\}\quad\left(\overrightarrow{g}\in G^n\right)\tag{1}$$

— распределение случайного элемента $\overrightarrow{\xi}$. Для выравнивания вероятностных характеристик распределения (1) используется некоторое отображение $H: G^n\to G^m$, результатом действия которого является последовательность $\overrightarrow{\eta}=H(\overrightarrow{\xi})$, $\overrightarrow{\eta}=(\eta_1,\eta_2,\ldots,\eta_m)$, случайных элементов $\eta_1,\eta_2,\ldots,\eta_m$, принимающих значения в группе G.

В приложениях представляет интерес случай, когда величина q принимает небольшие значения по сравнению с величинами n и m. В связи с этим, для любого $k=1,2,\ldots,m$ и любых элементов $g_1,\ldots,g_{k-1},g_{k+1},\ldots,g_m\in G$, удовлетворяющих неравенству

$$\mathbf{P}\left\{\eta_1=g_1,\ldots,\eta_{k-1}=g_{k-1},\eta_{k+1}=g_{k+1},\ldots,\eta_m=g_m\right\}>0,\tag{2}$$

рассмотрим условное распределение

$$\mathbf{P}\left\{\eta_k=g\right\}$$

$$\overline{q}\Big)^2\Big]^{1/2}.$$

Величины вида (4) мы будем называть локальными характеристиками схем выравнивания. На наш взгляд, введенные локальные характеристики наиболее полно отражают полезные свойства исследуемых схем.

Обозначим через $\widehat{G}$ группу всех попарно различных неприводимых комплексных характеров конечной коммутативной группы G. Значение характера $\chi \in \widehat{G}$ на элементе $g \in G$ будем обозначать через (g, χ). Пусть $\chi^{(0)}$ — единичный характер, для которого $(g, \chi^{(0)}) = 1.$ при любом $g \in G$.

Элементы $\overrightarrow{\phi} = (\phi_1, \phi_2, \ldots, \phi_n) \in \widehat{G}^n$ можно рассматривать как комплексные неприводимые характеры конечной коммутативной группы G^n, для которых

$$(\overrightarrow{g}, \overrightarrow{\phi}) = (g_1, \phi_1) \cdot (g_2, \phi_2) \cdot \ldots \cdot (g_n, \phi_n), \quad \overrightarrow{g} = (g_1, g_2, \ldots g_n) \in G^n.$$

Рассмотрим коэффициенты преобразования Фурье вероятностной меры (1), см. [6]:

$$\widehat{p}_{\overrightarrow{\xi}}(\overrightarrow{\phi}) = \sum_{\overrightarrow{g} \in G^{(n)}} p_{\overrightarrow{\xi}}(\overrightarrow{g}) \cdot (\overrightarrow{g}, \overrightarrow{\phi}), \quad \overrightarrow{\phi} \in \widehat{G}^n,$$

а также коэффициенты преобразования Фурье условных распределений (3):

$$\Delta_\chi^{(k)}(g_1, \ldots, g_{k-1}, g_{k+1}, \ldots, g_m) =$$

$$\sum_{g \in G} \mathbf{P}\{\eta_k = g/\eta_1 = g_1, \ldots, \eta_{k-1} = g_{k-1}, \eta_{k+1} = g_{k+1}, \ldots, \eta_m = g_m\} \cdot (g, \chi),$$

$$\chi \in \widehat{G}, \quad k = 1, 2, \ldots, m, \quad g_1, \ldots, g_{k-1}, g_{k+1}, \ldots, g_m \in G.$$

Для комплексного числа z обозначим через $\overline{z}$ комплексное число, сопряженное к z. Определим коэффициенты Фурье отображения H конечных коммутативных групп G^n и G^m (см. [7]):

$$\lambda_H(\overrightarrow{\psi}, \overrightarrow{\phi}) = \frac{1}{q^n} \sum_{\overrightarrow{g} \in G^n} \Big(H(\overrightarrow{g}), \overrightarrow{\psi}\Big) \cdot \overline{\Big(\overrightarrow{g}, \overrightarrow{\phi}\Big)}, \quad \overrightarrow{\psi} \in \widehat{G}^m, \quad \overrightarrow{\phi} \in \widehat{G}^n.$$

Справедливо следующее общее утверждение.

Теорема. *Для любых* $k = 1, 2, \ldots, m$ *и* $g_1, \ldots, g_{k-1}, g_{k+1}, \ldots, g_m \in G$ *удовлетворяющих неравенству* (2), *имеет место равенство*

$$\varepsilon^{(k)}_{g_1, \ldots, g_{k-1}, g_{k+1}, \ldots, g_m} = \left(\sum_{\chi \neq \chi^{(0)}} |\Delta_\chi^{(k)}(g_1, \ldots, g_{k-1}, g_{k+1}, \ldots, g_m)|^2 \right)^{1/2}, \tag{5}$$

а также соотношения

$$\Delta_\chi^{(k)}(g_1, \ldots, g_{k-1}, g_{k+1}, \ldots, g_m)$$

$$= \frac{\sum_{\overrightarrow{\psi}, \psi_k = \chi} \sum_{\overrightarrow{\phi}} \Big[\lambda_H(\overrightarrow{\psi}, \overrightarrow{\phi}) \cdot \Big(\prod_{i \neq k} \overline{(g_i, \psi_i)}\Big) \cdot \widehat{p}_{\overrightarrow{\xi}}(\overrightarrow{\phi})\Big]}{\sum_{\overrightarrow{\psi}, \psi_k = \chi^{(0)}} \sum_{\phi\downarrow} \Big[\lambda_H(\overrightarrow{\psi}, \overrightarrow{\phi}) \cdot \Big(\prod_{i \neq k} \overline{(g_i, \psi_i)}\Big) \cdot \widehat{p}_{\overrightarrow{\xi}}(\overrightarrow{\phi})\Big]}, \quad \chi \in \widehat{G}, \tag{6}$$

суммирование в которых проводится по $\overrightarrow{\psi} = (\psi_1, \psi_2, \ldots, \psi_m) \in \widehat{G}^m$, $\overrightarrow{\phi} = (\phi_1, \phi_2, \ldots, \phi_n) \in \widehat{G}^n$.

СПИСОК ЛИТЕРАТУРЫ

1. *Егоров Б. А.*, *Максимов Ю. И.* Об одной последовательности случайных величин, принимающих значения из компактной коммутативной группы. — Теория вероятн. и ее примен., 1968, т. 13, в. 4, с. 621–630.
2. *Капитонов В. М.* О скорости сходимости последовательности распределений, определяемых схемой авторегрессии на компактной группе. — Теория вероятн. и ее примен., 1973, т. 18, в. 3, с. 608–615.
3. *Максимов Ю. И.* О цепях Маркова, связанных с двоичными регистрами сдвига со случайными элементами. Труды по дискретной математике. Т. 1. 1997, с. 203–220.
4. *Chung F.*, *Diaconis P.*, *Gracham R. L.* A random walk problem arising in random number generation. — The Annals of Probability, 1987, v. 15, p. 1148–1165.
5. *Hildebrand M.* Random processes of the form $X_{n+1} = a_n \cdot X_n + b_n (\mathrm{mod} p)$. — The Annals of Probability, 1993, v. 21, p. 710–720.
6. *Гренандер У.* Вероятности на алгебраических структурах. М.: Мир, 1965.
7. *Солодовников Вик. И.* Бент-функции из конечной абелевой группы в конечную абелеву группу. — Дискретн. матем., 2004, т. 14, в. 1, с. 99–113.