Общероссийский математический портал

В. О. Дрелихов, И. А. Круглов, Локальные характеристики выравнивающих свойств эпиморфизмов конечных абелевых групп, *Матем. вopr. криптогр.*, 2015, том 6, выпуск 3, 33–45

DOI: <https://doi.org/10.4213/mvk159>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.127.20

26 апреля 2023 г., 18:24:34

УДК: 512.541.5+519.212.2+519.254.1

Локальные характеристики выравнивающих свойств эпиморфизмов конечных абелевых групп

В. О. Дрелихов¹, И. А. Круглов²

¹ООО «Центр сертификационных исследований», Москва

²Академия криптографии Российской Федерации, Москва

Получено 30.V.2015

В работе исследуются локальные характеристики близости к равномерному распределению на множестве G^m для распределения случайного элемента вида $H(\vec{\xi})$, где $H : G^n \rightarrow G^m$ — отображение декартовых степеней некоторой конечной абелевой группы G , $\vec{\xi} = (\xi_1, \xi_2, \dots, \xi_n)$ — случайный элемент множества G^n . Основные результаты относятся к случаю, когда случайные элементы $\xi_1, \xi_2, \dots, \xi_n$ независимы и одинаково распределены, а отображение H является эпиморфизмом группы G^n на группу G^m .

Ключевые слова: выравнивание вероятностных распределений, эпиморфизм, коэффициенты Фурье

Local characteristics of smoothing properties of endomorphisms of finite Abelian groups

V. O. Drelikhov¹, I. A. Kruglov²

¹LLC «Sertification Research Center», Moscow

²Academy of Cryptography of the Russian Federation, Moscow

Abstract. Let G be a finite Abelian group, G^n be its n -fold Cartesian product, and $\vec{\xi} = (\xi_1, \xi_2, \dots, \xi_n)$ be a random element of G^n . We investigate the local characteristics of closeness of distribution of random element $H(\vec{\xi})$, where $H : G^n \rightarrow G^m$, to the uniform distribution on G^m . Main results are connected with the case of independent identically distributed elements $\xi_1, \xi_2, \dots, \xi_n$ and endomorphism H of group G^n onto the group G^m .

Key words: smoothing of distributions, endomorphism, Fourier coefficients

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 3, pp. 33–45 (Russian).

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. С математической точки зрения функционирование схемы выравнивания заключается в применении некоторого отображения, определенного на множестве последовательностей некоторой длины и принимающего значения в множестве последовательностей меньшей длины.

Процедура выравнивания вероятностных характеристик случайных последовательностей является составной частью комплекса мер, гарантирующего заданные значения характеристик в условиях, когда оперативный статистический контроль проводится на ограниченных участках последовательностей.

Одним из общих подходов к синтезу схем выравнивания является использование коммутативных групповых операций. Это обусловлено тем, что, с одной стороны, различные групповые операции могут быть эффективно реализованы на современной элементной базе микропроцессоров, с другой стороны, при обосновании выравнивающих свойств таких операций можно использовать математический аппарат дискретного преобразования Фурье.

В настоящей работе исследуется следующая вероятностная модель схем выравнивания. Пусть $(G, +)$ — некоторая конечная коммутативная группа, $|G| = q$, $q \geq 2$, n, m — натуральные числа, $n > m \geq 2$, $G^n = G \times G \times \dots \times G$ — n -я декартова степень множества G . Элементы множества G^n будем записывать в виде векторов-строк длины n , компоненты которых принимают значения в множестве G . Операция «+» индуцирует коммутативные групповые операции покоординатного сложения элементов декартовых степеней G^n и G^m , которые также будем обозначать символом «+».

Предположим, что имеется последовательность

$$\vec{\xi} = (\xi_1, \xi_2, \dots, \xi_n)$$

случайных элементов $\xi_1, \xi_2, \dots, \xi_n$, принимающих значения в группе G , и

$$p_{\vec{\xi}}(\vec{g}) = P(\vec{\xi} = \vec{g}), \quad \vec{g} \in G^n, \quad (1)$$

— распределение случайного элемента $\vec{\xi}$. Пусть

$$H : G^n \rightarrow G^m$$

— некоторое отображение соответствующих декартовых степеней. Определим последовательность

$$\vec{\eta} = H(\vec{\xi}), \quad \vec{\eta} = (\eta_1, \eta_2, \dots, \eta_m),$$

случайных элементов $\eta_1, \eta_2, \dots, \eta_m$, принимающих значения в группе G .

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

$$P(\eta_j = g_j, j \in \{1, \dots, m\} \setminus \{k\}) > 0, \quad (2)$$

рассмотрим условное распределение

$$P(\eta_k = g \mid \eta_j = g_j, j \in \{1, \dots, m\} \setminus \{k\}), \quad g \in G, \quad (3)$$

и нормированную величину его среднеквадратического отклонения от равномерного распределения на группе G :

$$\varepsilon_{g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m}^{(k)} = \sqrt{q \sum_{g \in G} \left(P(\eta_k = g \mid \eta_j = g_j, j \in \{1, \dots, m\} \setminus \{k\}) - \frac{1}{q} \right)^2}. \quad (4)$$

В работе установлены оценки сверху для величин (4), зависящие от характеристик распределения (1) компонент вектора $\vec{\xi}$ и от свойств отображения H .

Исследованию различных схем выравнивания посвящены работы отечественных специалистов Б. А. Егорова, Ю. И. Максимова, В. М. Капитонова и некоторых других, см., в частности, [1, 2, 3]. Среди многочисленных зарубежных работ по данной тематике можно выделить работы Р. Грэхема,

П. Диакониса и их последователей, см., например, [4, 5]. В перечисленных работах основное внимание уделено оценке того или иного расстояния (метрики) между распределением случайного элемента $\vec{\eta}$ и равномерным распределением на множестве G^m . Подобные величины уместно назвать глобальными характеристиками степени равновероятности распределения вектора $\vec{\eta}$, а величины вида (4) — локальными характеристиками. На наш взгляд, локальные характеристики более полно отражают полезные свойства исследуемых схем выравнивания. Отметим также, что применение результатов исследования глобальных характеристик при изучении величин вида (4) часто приводит к завышенным оценкам. Это связано с тем, что условные вероятности (3) выражаются в виде дробей с малыми значениями знаменателей (2).

Обозначим через $(\hat{G}, \cdot)$ группу всех попарно различных неприводимых комплексных характеров конечной абелевой группы $(G, +)$. Значение характера $\chi \in \hat{G}$ на элементе $g \in G$ будем обозначать через (g, χ) , при этом для любых $\phi, \psi \in \hat{G}$, $g \in G$

$$(g, \phi \cdot \psi) = (g, \phi) \cdot (g, \psi).$$

Пусть $\chi^{(0)}$ — единичный характер, для которого при любом $g \in G$

$$(g, \chi^{(0)}) = 1.$$

Обозначим через $\hat{G}^n$ множество всех векторов-столбцов длины n с элементами из множества $\hat{G}$:

$$\hat{G}^n = \{\phi^\perp = (\phi_1, \phi_2, \dots, \phi_n)^\top \mid \phi_1, \phi_2, \dots, \phi_n \in \hat{G}\},$$

$^\top$ — знак транспонирования. Каждому элементу $\phi^\perp = (\phi_1, \phi_2, \dots, \phi_n)^\top$ взаимно-однозначно соответствует комплексный неприводимый характер конечной абелевой группы G^n , который обозначим тем же символом $\phi^\perp$ и который определяется равенством

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

Поэтому можно считать, что множество $\hat{G}^n$ (множество $\hat{G}^m$) с операцией покомпонентного умножения элементов совпадает с группой неприводимых комплексных характеров группы G^n (группы G^m).

Пусть E — знак математического ожидания случайных величин с комплексными значениями. Рассмотрим коэффициенты преобразования Фурье вероятностной меры (1), см. [6]:

$$\hat{p}_{\vec{\xi}}(\phi^\perp) = E(\vec{\xi}, \phi^\perp) = \sum_{\vec{g} \in G^n} p_{\vec{\xi}}(\vec{g}) \cdot (\vec{g}, \phi^\perp), \quad \phi^\perp \in \hat{G}^n, \quad (5)$$

а также коэффициенты преобразования Фурье условных распределений вида (3):

$$\begin{aligned} \Delta_{\chi}^{(k)}(g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m) = \\ = \sum_{g \in G} \mathbf{P}(\eta_k = g \mid \eta_j = g_j, j \in \{1, \dots, m\} \setminus \{k\}) \cdot (g, \chi), \end{aligned} \quad (6)$$

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

Для комплексного числа z обозначим через $\bar{z}$ комплексное число, сопряженное с z . Рассмотрим H как отображение конечных абелевых групп G^n и G^m и определим его коэффициенты Фурье (см. [7]):

$$\lambda_H(\psi^\perp, \phi^\perp) = \frac{1}{q^n} \sum_{\vec{g} \in G^n} \left(H(\vec{g}), \psi^\perp \right) \cdot \overline{(\vec{g}, \phi^\perp)}, \quad \psi^\perp \in \widehat{G}^m, \quad \phi^\perp \in \widehat{G}^n. \quad (7)$$

Справедливо следующее общее утверждение.

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

$$\varepsilon_{g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m}^{(k)} = \left(\sum_{\chi \neq \chi^{(0)}} |\Delta_{\chi}^{(k)}(g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m)|^2 \right)^{\frac{1}{2}}, \quad (8)$$

а также соотношения

$$\begin{aligned} \Delta_{\chi}^{(k)}(g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m) = \\ = \frac{\sum_{\psi^\perp: \psi_k = \chi} \sum_{\phi^\perp} \left[\lambda_H(\psi^\perp, \phi^\perp) \cdot \left(\prod_{i \neq k} \overline{(g_i, \psi_i)} \right) \cdot \widehat{p}_{\bar{\xi}}(\phi^\perp) \right]}{\sum_{\psi^\perp: \psi_k = \chi^{(0)}} \sum_{\phi^\perp} \left[\lambda_H(\psi^\perp, \phi^\perp) \cdot \left(\prod_{i \neq k} \overline{(g_i, \psi_i)} \right) \cdot \widehat{p}_{\bar{\xi}}(\phi^\perp) \right]}, \quad \chi \in \widehat{G}, \end{aligned} \quad (9)$$

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

Доказательство. Равенство (8) есть следствие равенства Парсеваля для коэффициентов преобразования Фурье (6). Для доказательства соотношений (9) заметим, что из определения условных вероятностей и формулы (6) следует, что для любых допустимых $k = 1, 2, \dots, m$, $g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m \in G$, $\chi \in \widehat{G}$:

$$\begin{aligned} \Delta_r^{(k)}(g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m) = \\ = \frac{\sum_{g \in G} \mathbf{P}(\eta_k = g, \eta_j = g_j, j \in \{1, \dots, m\} \setminus \{k\}) \cdot (g, \chi)}{\sum_{g \in G} \mathbf{P}(\eta_k = g, \eta_j = g_j, j \in \{1, \dots, m\} \setminus \{k\}) \cdot (g, \chi^{(0)})}. \end{aligned} \quad (10)$$

Для любых $\vec{x} \in G^n$ и $\vec{g} \in G^m$ определим значение индикатора

$$I(H(\vec{x}) = \vec{g}) = \begin{cases} 1, & H(\vec{x}) = \vec{g}, \\ 0, & H(\vec{x}) \neq \vec{g}. \end{cases}$$

Используя равенства (7) и соотношения ортогональности для неприводимых характеров групп G^n и G^m , можно вывести следующую формулу:

$$I(H(\vec{x}) = \vec{g}) = \frac{1}{q^m} \cdot \sum_{\psi^\perp \in \widehat{G}^m} \sum_{\phi^\perp \in \widehat{G}^n} \lambda_H(\psi^\perp, \phi^\perp) \cdot \overline{(\vec{g}, \psi^\perp)} \cdot (\vec{x}, \phi^\perp),$$

$$\vec{x} \in G^n, \quad \vec{g} \in G^m.$$

Из этой формулы и соотношения (5) следует, что для любого элемента $\vec{g} \in G^m$

$$\begin{aligned} P(\vec{\eta} = \vec{g}) &= EI(H(\vec{\xi}) = \vec{g}) = \\ &= \frac{1}{q^m} \cdot \sum_{\psi^\perp \in \widehat{G}^m} \sum_{\phi^\perp \in \widehat{G}^n} \lambda_H(\psi^\perp, \phi^\perp) \cdot \prod_{i=1}^m \overline{(g_i, \psi_i)} \cdot E(\vec{\xi}, \phi^\perp) = \\ &= \frac{1}{q^m} \cdot \sum_{\psi^\perp \in \widehat{G}^m} \sum_{\phi^\perp \in \widehat{G}^n} \lambda_H(\psi^\perp, \phi^\perp) \cdot \prod_{i=1}^m \overline{(g_i, \psi_i)} \cdot \widehat{p}_{\vec{\xi}}(\phi^\perp). \end{aligned} \quad (11)$$

Воспользовавшись выражением (11) для преобразования числителя и знаменателя дроби в правой части соотношения (10) и соотношениями ортогональности для неприводимых характеров группы G , получим формулу (9).

Лемма доказана. $\square$

Далее рассматривается частный случай, в котором соотношение (9) упрощается: предполагается, что случайные элементы последовательности $\xi_1, \xi_2, \dots, \xi_n$ независимы и имеют одно и то же распределение

$$p_\xi(g) = P(\xi_i = g), \quad g \in G, \quad i = 1, 2, \dots, n. \quad (12)$$

Введем коэффициенты преобразования Фурье вероятностной меры (12):

$$\widehat{p}_\xi(\chi) = E(\xi, \chi) = \sum_{g \in G} p_\xi(g) \cdot (g, \chi), \quad \chi \in \widehat{G}.$$

Тогда формула (9) принимает следующий вид.

Следствие. Для любых $k = 1, 2, \dots, m$ и $g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m \in G$, удовлетворяющих неравенству (2), справедливо равенство

$$\begin{aligned} & \Delta_{\chi}^{(k)}(g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m) = \\ &= \frac{\sum_{\psi^\downarrow, \psi_k = \chi} \sum_{\phi^\downarrow} \left[\lambda_H(\psi^\downarrow, \phi^\downarrow) \cdot \left(\prod_{i \neq k} \overline{g_i, \psi_i} \right) \cdot \left(\prod_{j=1}^n \widehat{p}_\xi(\phi_j) \right) \right]}{\sum_{\psi^\downarrow, \psi_k = \chi^{(0)}} \sum_{\phi^\downarrow} \left[\lambda_H(\psi^\downarrow, \phi^\downarrow) \cdot \left(\prod_{i \neq k} \overline{g_i, \psi_i} \right) \cdot \left(\prod_{j=1}^n \widehat{p}_\xi(\phi_j) \right) \right]}, \quad \chi \in \widehat{G}. \end{aligned} \quad (13)$$

Доказательство. Из равенства

$$(\vec{\xi}, \phi^\downarrow) = \prod_{j=1}^n (\xi_j, \phi_j)$$

и условия независимости случайных элементов $\xi_1, \xi_2, \dots, \xi_n$ следует, что

$$\widehat{p}_{\vec{\xi}}(\phi^\downarrow) = \prod_{j=1}^n \widehat{p}_\xi(\phi_j), \quad \phi^\downarrow = (\phi_1, \phi_2, \dots, \phi_n)^\top \in \widehat{G}^n. \quad (14)$$

Равенство (13) является следствием соотношений (14) и (9).

Следствие доказано. $\square$

Возможности применения соотношений (8) и (13) для оценки величин (4) во многом зависят от количества ненулевых элементов в наборе (7) коэффициентов Фурье отображения H . Минимальное число данных коэффициентов достигается, если отображение H является гомоморфизмом группы G^n в группу G^m , то есть для любых элементов $\vec{g}, \vec{h} \in G^n$ выполнено равенство

$$H(\vec{g} + \vec{h}) = H(\vec{g}) + H(\vec{h}).$$

Если гомоморфизм H не является сюръективным, то число элементов в образе $H(G^n)$ не превосходит половины числа элементов множества G^m . Следовательно, для обеспечения близости величин (4) к нулю необходимо, чтобы гомоморфизм H был сюръективным.

В связи с этим всюду далее предполагается, что отображение H является эпиморфизмом (то есть сюръективным гомоморфизмом) группы G^n на группу G^m . В этом случае определен инъективный гомоморфизм $\widehat{H} : \widehat{G}^n \rightarrow \widehat{G}^m$ соответствующих групп неприводимых характеров, для которого

$$\widehat{H}(\psi^\downarrow) = \psi^\downarrow \circ H, \quad \psi^\downarrow \in \widehat{G}^m,$$

« $\circ$ » — композиция отображений. Для любых $\vec{g} \in G^n, \psi^\perp \in \widehat{G}^m$ выполнено равенство

$$\left(H(\vec{g}), \psi^\perp \right) = \left(\vec{g}, \widehat{H}(\psi^\perp) \right). \quad (15)$$

Множество $\widehat{H}(\widehat{G}^m)$ есть аннулятор (в группе $\widehat{G}^n$) ядра эпиморфизма H .

Из равенств (7), (15) и соотношений ортогональности для неприводимых характеров группы G^n вытекает следующее равенство для любых $\psi^\perp \in \widehat{G}^m, \phi^\perp \in \widehat{G}^n$:

$$\lambda_H(\psi^\perp, \phi^\perp) = \begin{cases} 1, & \phi^\perp = \widehat{H}(\psi^\perp), \\ 0, & \phi^\perp \neq \widehat{H}(\psi^\perp). \end{cases} \quad (16)$$

Чтобы использовать соотношения (16), введем дополнительные обозначения. Для любого элемента $\phi^\perp = (\phi_1, \phi_2, \dots, \phi_n)^\top \in \widehat{G}^n$ положим

$$\|\phi^\perp\| = |\{j = 1, 2, \dots, n \mid \phi_j \neq \chi^{(0)}\}|.$$

Для любых $k = 1, 2, \dots, m$ и $\chi \in \widehat{G}$ рассмотрим следующее подмножество $L_{k,\chi} \subset \widehat{G}^n$:

$$L_{k,\chi} = \{\widehat{H}(\psi^\perp) \mid \psi^\perp = (\psi_1, \psi_2, \dots, \psi_m)^\top \in \widehat{G}^m \setminus (\chi^{(0)}, \dots, \chi^{(0)})^\top, \psi_k = \chi\}, \quad (17)$$

а также целые неотрицательные числа

$$N_{k,\chi}(t) = |\{\phi^\perp \in L_{k,\chi} \mid \|\phi^\perp\| = t\}|, \quad t = 1, 2, \dots, n. \quad (18)$$

Положим также

$$\widehat{\delta}_{\max} = \max \left\{ |\widehat{p}_\xi(\chi)|, \quad \chi \in \widehat{G} \setminus \chi^{(0)} \right\}.$$

Основным результатом данной работы является следующее утверждение.

Теорема. Пусть отображение H является эпиморфизмом группы G^n на группу G^m , а случайные элементы последовательности $\xi_1, \xi_2, \dots, \xi_n$ независимы и одинаково распределены. Тогда при любом $k = 1, 2, \dots, m$ и любых элементах $g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m \in G$ из условия

$$1 - \sum_{t=1}^n N_{k,\chi^{(0)}}(t) \cdot (\widehat{\delta}_{\max})^t > 0 \quad (19)$$

следует неравенство

$$\varepsilon_{g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m}^{(k)} \leq \frac{1}{1 - \sum_{t=1}^n N_{k, \chi^{(0)}}(t) \cdot (\widehat{\delta}_{\max})^t} \cdot \sqrt{\sum_{\chi \in \widehat{G} \setminus \chi^{(0)}} \left[\sum_{t=1}^n N_{k, \chi}(t) \cdot (\widehat{\delta}_{\max})^t \right]^2}. \quad (20)$$

Доказательство. Согласно соотношениям (11) и (16) при любом $\vec{g} \in G^n$

$$\mathbf{P}(\vec{\eta} = \vec{g}) = \frac{1}{q^m} \cdot \sum_{\psi^\perp \in \widehat{G}^m} \prod_{i=1}^m \overline{(g_i, \psi_i)} \cdot \prod_{j=1}^n \widehat{p}_\xi(\phi_j). \quad (21)$$

В слагаемых правой части равенства (21) элементы $\phi_1, \phi_2, \dots, \phi_n \in \widehat{G}$ определяются из соотношений $(\phi_1, \phi_2, \dots, \phi_n)^\top = \phi^\perp, \phi^\perp = \widehat{H}(\psi^\perp)$.

Используя (21) и соотношения ортогональности для неприводимых характеров группы G , получим оценку для числителя дроби в правой части (10):

$$\begin{aligned} & \left| \sum_{g \in G} \mathbf{P}(\eta_k = g, \eta_j = g_j, j \in \{1, \dots, m\} \setminus \{k\}) \cdot (g, \chi) \right| \leq \\ & \leq \frac{1}{q^{m-1}} \cdot \sum_{\phi^\perp \in L_{k, \chi}} (\widehat{\delta}_{\max})^{\|\phi^\perp\|} \leq \frac{1}{q^{m-1}} \cdot \sum_{t=1}^n N_{k, \chi}(t) \cdot (\widehat{\delta}_{\max})^t, \end{aligned} \quad (22)$$

а также следующую оценку для величины в знаменателе этой дроби:

$$\begin{aligned} & \left| \mathbf{P}(\eta_j = g_j, j \in \{1, \dots, m\} \setminus \{k\}) - \frac{1}{q^{m-1}} \right| \leq \\ & \leq \frac{1}{q^{m-1}} \cdot \sum_{\phi^\perp \in L_{k, \chi^{(0)}} \setminus (\chi^{(0)}, \dots, \chi^{(0)})^\top} (\widehat{\delta}_{\max})^{\|\phi^\perp\|} \leq \frac{1}{q^{m-1}} \cdot \sum_{t=1}^n N_{k, \chi^{(0)}}(t) \cdot (\widehat{\delta}_{\max})^t. \end{aligned} \quad (23)$$

Из соотношений (23) и (19) получим неравенства

$$0 < \frac{1}{q^{m-1}} \cdot \left(1 - \sum_{t=1}^n N_{k, \chi^{(0)}}(t) \cdot (\widehat{\delta}_{\max})^t \right) \leq \mathbf{P}(\eta_j = g_j, j \in \{1, \dots, m\} \setminus \{k\}). \quad (24)$$

В частности, выполнено условие (2). Оценка (20) следует из соотношений (8), (10), (22), (24).

Теорема доказана. $\square$

Введем обозначение

$$\rho = \sqrt{q \cdot \sum_{g \in G} \left(p_{\xi}(g) - \frac{1}{q} \right)^2}$$

для нормированной величины среднеквадратического отклонения распределения элементов исходной последовательности $\vec{\xi}$ от равномерного распределения на множестве G . Ввиду равенства Парсеваля имеет место неравенство

$$\hat{\delta}_{\max} \leq \rho.$$

Непосредственно из теоремы получим следующее утверждение.

Следствие. При выполнении условий теоремы при любом $k = 1, 2, \dots, t$ и любых элементах $g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m \in G$ из условия

$$1 - \sum_{t=1}^n N_{k, \chi^{(0)}}(t) \cdot \rho^t > 0 \quad (25)$$

следует неравенство

$$\varepsilon_{g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_m}^{(k)} \leq \frac{1}{1 - \sum_{t=1}^n N_{k, \chi^{(0)}}(t) \cdot \rho^t} \cdot \sqrt{\sum_{\chi \in \hat{G} \setminus \chi^{(0)}} \left[\sum_{t=1}^n N_{k, \chi}(t) \cdot \rho^t \right]^2}. \quad (26)$$

Заметим, что в случае $q = 2$ выполнено равенство $\rho = \hat{\delta}_{\max}$. Можно привести примеры того, что это равенство выполняется и при $q > 2$.

Рассмотрим подробнее случай, когда группа $(G, +)$ является циклической группой порядка q с нейтральным элементом $g^{(0)}$. Пусть $Z_q = \{0, 1, \dots, q-1\}$ — кольцо наименьших неотрицательных вычетов по модулю q ; обозначим через

$$\vartheta = \exp\left(\frac{2\pi i}{q}\right)$$

комплексный примитивный корень из единицы степени q . В данном случае существуют порождающие элементы $\tilde{g} \in G$, $\tilde{\chi} \in \hat{G}$ соответствующих групп, для которых выполняются равенства

$$G = \{g^{(0)}, \tilde{g}, \dots, (q-1) \cdot \tilde{g}\}, \quad \hat{G} = \{\chi^{(0)}, \tilde{\chi}, \dots, \tilde{\chi}^{q-1}\},$$

$$(\nu \cdot \tilde{g}, \tilde{\chi}^\mu) = \vartheta^{\nu \cdot \mu}, \quad \nu, \mu \in \{0, 1, \dots, q-1\}.$$

Зафиксируем произвольную пару таких элементов $\tilde{g}, \tilde{\chi}$. Между множеством всех гомоморфизмов $H : G^n \rightarrow G^m$ и множеством $(Z_q)_{n,m}$ матриц над кольцом Z_q размеров $n \times m$ можно установить взаимно-однозначное соответствие, при котором гомоморфизму H соответствует матрица $A_H = [a_H(j, i)]_{n \times m} \in (Z_q)_{n,m}$, определяемая равенствами

$$H(\vec{e}_j) = (a_H(j, 1) \cdot \tilde{g}, \dots, a_H(j, m) \cdot \tilde{g}), \quad j = 1, 2, \dots, n,$$

где $\vec{e}_j = (g^{(0)}, \dots, g^{(0)}, \tilde{g}, g^{(0)}, \dots, g^{(0)}) \in G^n$ — вектор с единственным элементом $\tilde{g}$ на j -м месте.

Гомоморфизм H сюръективен тогда и только тогда, когда взаимно прост с числом q наибольший общий делитель всех миноров порядка m (т. е. m -й инвариантный делитель) матрицы A_H , рассматриваемой как целочисленная матрица.

Из равенства (15) следует, что при любых $r_1, r_2, \dots, r_m \in Z_q$

$$\begin{aligned} \hat{H} \left(((\tilde{\chi})^{r_1}, (\tilde{\chi})^{r_2}, \dots, (\tilde{\chi})^{r_m})^\top \right) = \\ = \left((\tilde{\chi})^{\sum_i a_H(1,i)r_i}, (\tilde{\chi})^{\sum_i a_H(2,i)r_i}, \dots, (\tilde{\chi})^{\sum_i a_H(n,i)r_i} \right)^\top. \end{aligned} \quad (27)$$

Рассмотрим (правый) модуль Z_q^n векторов-столбцов длины n над кольцом Z_q . Для любого элемента $l^\downarrow = (l_1, l_2, \dots, l_n)^\top \in Z_q^n$ имеет место равенство

$$\| ((\tilde{\chi})^{l_1}, (\tilde{\chi})^{l_2}, \dots, (\tilde{\chi})^{l_n})^\top \| = \| l^\downarrow \|, \quad \| l^\downarrow \| = |\{j = 1, 2, \dots, n \mid l_j \neq 0\}|. \quad (28)$$

Обозначим через $A_{H,1}^\downarrow, A_{H,2}^\downarrow, \dots, A_{H,m}^\downarrow$ столбцы матрицы A_H и для каждого $k = 1, 2, \dots, m$ рассмотрим подмодуль

$$W_k = \langle A_{H,1}^\downarrow, \dots, A_{H,k-1}^\downarrow, A_{H,k+1}^\downarrow, \dots, A_{H,m}^\downarrow \rangle_{Z_q}$$

модуля Z_q^n , порожденный множеством $\{A_{H,1}^\downarrow, \dots, A_{H,k-1}^\downarrow, A_{H,k+1}^\downarrow, \dots, A_{H,m}^\downarrow\}$. Из соотношений (15), (17), (18), (27), (28) следует, что при любых $k = 1, 2, \dots, m, r \in Z_q, t = 1, 2, \dots, n$ выполняется равенство

$$N_{k,\tilde{\chi}^r}(t) = \left| \{l^\downarrow \in W_k + A_{H,k}^\downarrow \cdot r \mid \|l^\downarrow\| = t\} \right|. \quad (29)$$

Таким образом, в случае циклической группы $(G, +)$ применение оценок (20) сводится к определению весовой структуры смежных классов $W_k + A_{H,k}^\downarrow \cdot r$ по подмодулю модуля Z_q^n . Для решения последней задачи можно воспользоваться известными результатами исследования весовой структуры кодов над кольцами вычетов и, в частности, над простыми полями.

В качестве примера рассмотрим следующую схему выравнивания на основе линейного регистра сдвига длины m над кольцом Z_q (эта схема исследовалась в работах [1, 2, 3]). Пусть

$$f(X) = X^m - f_{m-1}X^{m-1} - \dots - f_1X - f_0, \quad f_i \in Z_q,$$

— произвольный унитарный многочлен степени m над кольцом Z_q . Для любого элемента $\vec{x} = (x_1, x_2, \dots, x_n) \in Z_q^n$ определим рекурсивно последовательность векторов

$$\vec{y}^{(j)} \in Z_q^m, \quad j = 0, 1, \dots, n, \quad \vec{y}^{(j)} = (y_1^{(j)}, y_2^{(j)}, \dots, y_m^{(j)}),$$

зависящую от $\vec{x}$, в которой

$$\vec{y}_i^{(0)} = 0, \quad i = 1, 2, \dots, m,$$

и для любого $j = 1, 2, \dots, n$:

$$(y_1^{(j)}, y_2^{(j)}, \dots, y_m^{(j)}) = (y_2^{(j-1)}, \dots, y_m^{(j-1)}, y_1^{(j-1)} \cdot f_0 + \dots + y_m^{(j-1)} \cdot f_{m-1} + x_j).$$

Положим

$$H(\vec{x}) = \vec{y}^{(n)}.$$

Отображение $H : Z_q^n \rightarrow Z_q^m$ является эпиморфизмом модулей.

Рассмотрим линейную рекуррентную последовательность

$$\vec{u} = (u_1, u_2, \dots, u_m, \dots, u_n, u_{n+1}, \dots, u_{n+m-1})$$

над кольцом Z_q с характеристическим многочленом $f(X)$ и начальным вектором $(u_1, u_2, \dots, u_m) = (0, 0, \dots, 0, 1)$ ($\vec{u}$ — начальный отрезок генератора семейства всех линейных рекуррентных последовательностей с характеристическим многочленом $f(X)$). Для строк $\vec{A}_H^{(1)}, \vec{A}_H^{(2)}, \dots, \vec{A}_H^{(n)}$ матрицы A_H выполнены равенства:

$$\vec{A}_H^{(n-j+1)} = (u_j, u_{j+1}, \dots, u_{j+m-2}, u_{j+m-1}), \quad j = 1, 2, \dots, n.$$

Отсюда следуют равенства для столбцов матрицы A_H :

$$A_{H,i}^\downarrow = (u_{i+n-1}, u_{i+n-2}, \dots, u_{i+1}, u_i)^\top, \quad i = 1, 2, \dots, m.$$

Следовательно, в рассматриваемом случае столбцы матрицы A_H порождают (n, m) -код K , который эквивалентен рекурсивному коду K_f над кольцом Z_q с характеристическим многочленом $f(X)$: кодовые слова кода K получаются путем выписывания элементов кодовых слов кода K_f в обратном порядке. Согласно равенству (29) числа $N_{k, \tilde{\chi}'}(t)$ представляют собой элементы весовой структуры соответствующих смежных классов по реверсивному коду K_f .

Отметим, что в случае $q = 2$ близкие результаты для оценки величины $\sum_{\vec{y} \in Z_2^{(m)}} \left(P(\vec{\eta} = \vec{y}) - \frac{1}{2^m} \right)^2$ получены Ю. И. Максимовым в [3].

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.*, **13**:4 (1968), 621–630.
- [2] Капитонов В. М., “О скорости сходимости последовательности распределений, определяемых схемой авторегрессии на компактной группе”, *Теория вероятн. и ее примен.*, **18**:3 (1973), 608–615.
- [3] Максимов Ю. И., “О цепях Маркова, связанных с двоичными регистрами сдвига со случайными элементами”, *Труды по дискретной математике*, **1** (1997), 203–220.
- [4] Chung F., Diaconis P., Gracham R. L. A random walk problem arising in random number generation, *Ann. Probab.*, **15**:3 (1987), 1148–1165.
- [5] Hildebrand M., “Random processes of the form $X_{n+1} = a_n \cdot X_n + b_n \pmod{p}$ ”, *Ann. Probab.*, **21**:2 (1993), 710–720.
- [6] Гренандер У., *Вероятности на алгебраических структурах*, М.: Мир, 1965, 274 с.
- [7] Солодовников Вик. И., “Бент-функции из конечной абелевой группы в конечную абелеву группу”, *Дискретная математика*, **14**:1 (2004), 99–113.