Math-Net.Ru

Общероссийский математический портал

Б. А. Погорелов, М. А. Пудовкина, Характеризация отображений через свойство неизометричности, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 4, 77–116

DOI: <https://doi.org/10.4213/mvk309>

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: 35.173.219.12

26 апреля 2023 г., 06:48:05

Характеризация отображений через свойство неизометричности

Б. А. Погорелов¹, М. А. Пудовкина²

¹*Академия криптографии Российской Федерации, Москва*

²*Московский государственный технический университет
имени Н. Э. Баумана, Москва*

Получено 18.IV.2018

Аннотация. Для целочисленной метрики μ на векторном пространстве над полем $GF(2)$ вводится новая мера несогласованности преобразования g и метрики μ , названная показателем μ -неизометричности преобразования. В работе для целочисленных метрик, инвариантных относительно группы сдвигов, и разных классов преобразований, включая инволютивные APN, найдены показатели μ -неизометричности или их экстремальные оценки.

Ключевые слова: целочисленная метрика, инволюции, APN-преобразование, метрика Хемминга, аффинные преобразования

Characterization of mappings by the nonisometricity property

B. A. Pogorelov, M. A. Pudovkina

¹*Academy of Cryptography of the Russian Federation, Moscow*

²*Bauman Moscow State Technical University, Moscow*

Abstract. For an integer-valued metric μ on a vector space over $GF(2)$ we introduce a new measure which characterize the non-coordination between μ and transformation g of the space. It is called a nonisometric index of transformation g . In this paper we deal with metrics which are invariant under a translation group of the vector space over $GF(2)$. For different classes of transformations (including involutions and APN permutations) we find the values of nonisometric indices or their extremal estimates.

Keywords: integral metric, involution, APN permutation, Hamming metric, affine transformations

1. Введение

Многие свойства алгоритмов блочного шифрования, а также методы их криптоанализа связаны с существованием структур (разбиения t -грамм ($t \geq 1$), в той или иной мере инвариантных при действии групп подстановок, порожденных различными составляющими раундовых преобразований. Например, это импримитивность в методе гомоморфизмов, неравновероятность перехода гиперплоскостей в линейном методе, а также неравновероятность перехода разностей в разностном методе и др. Группы подстановок естественным образом разбиваются на классы интранзитивных, импримитивных, унипримитивных (т. е. примитивных, но не 2-транзитивных) и 2-транзитивных групп. Описание различных структур, инвариантных или частично инвариантных относительно действия групп, и их связь со свойствами алгоритмов шифрования – важная задача.

Как следует из классификационной теоремы О'Нэна–Скотта и ее обобщений, к числу важнейших структур относятся натурально-значные метрики, являющиеся естественными метриками графов орбиталов группы подстановок. Примером такой метрики является метрика Хемминга. Она соответствует экспоненцированию групп (см., например, [1]). Группа Джевонса – частный случай таких групп. Подметрики метрики Хемминга и их группы изометрий возникают в ряде классификационных задач [2, 3] и при описании ряда структур в алгоритмах блочного шифрования [4].

С точки зрения криптографических приложений интерес представляют метрики, а также иные структуры, связанные с группами $G_{XL} = \langle V_n^+, h \rangle$, $G_{XS} = \langle V_n^+, s \rangle$ и $G_{SL} = \langle s, h \rangle$, порожденными компонентами раундовой функции XSL-алгоритма блочного шифрования, где V_n^+ – регулярное подстановочное представление аддитивной группы сдвигов n -мерного векторного пространства V_n над полем $GF(2)$, h – линейное преобразование над V_n линейного слоя, s – преобразование пространства V_n слоя S -боксов. Связь, например, может выражаться тем, что некоторые из групп G_{XL} , G_{XS} , G_{SL} могут являться подгруппами группы изометрий метрики или иметь с ней непустое пересечение.

По аналогии со структурами, связанными с методами гомоморфизмов, линейном, разностном и др., возникают вопросы о степени рассеивания (несохранения) преобразованиями различных метрик и об их связи в этом смысле с другими структурами. Как и в случае нелинейности преобразований, меру рассеивания преобразованием структуры можно определять различными способами. В частности, линейная и

разностная характеристики дают представление о мере рассеивания соответствующих структур S -блоками. В [5] в качестве меры неимпримитивности рассматривался порядок $\mathbf{W}$ -примитивности $\chi_{\mathbf{W}}(g)$ подстановки $g \in S(V_n)$, заданный условием

$$\chi_{\mathbf{W}}(g) = \min \{ \chi(g, h) \mid h \in \text{IG}_{\mathbf{W}} \},$$

где $\chi(g, h) = |\{ \alpha \in V_n \mid \alpha^g \neq \alpha^h \}|$ для $h \in S(V_n)$, $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – нетривиальное разбиение пространства V_n с равномошными блоками, $\text{IG}_{\mathbf{W}}$ – наибольшая группа подстановок из симметрической группы $S(V_n)$, сохраняющая разбиение $\mathbf{W}$ (сплетение $S(W_0) \wr S_r$ групп подстановок $S(W_0)$, S_r). Порядок $\mathbf{W}$ -примитивности характеризует меру несогласованности подстановки g и группы $\text{IG}_{\mathbf{W}}$ относительно метрики Хемминга χ . В [5] показана его связь с параметрами, используемыми для оценки трудоемкости методов гомоморфизмов, вероятностных гомоморфизмов, а также разностного метода.

В настоящей работе рассматриваются метрики, для которых существует такое натуральное число d , что множество значений метрики есть $\{0, 1, \dots, d\}$. Такие метрики называются $(d + 1)$ -значными натуральными метриками (или «просто» натуральными метриками, см. [6]). Естественным примером натуральной метрики является метрика сильно связного графа, определяемая кратчайшими путями между парами его вершин.

Для произвольной натуральной метрики μ на V_n вводится новая мера $ni_g(\mu)$ несогласованности метрики и преобразования $g : V_n \rightarrow V_n$, названная показателем μ -неизометричности преобразования. Она характеризует степень несохранения преобразованием g метрики μ и является пропорциональной числу неупорядоченных пар элементов $\{\alpha, \alpha'\} \subset V_n$, $\alpha \neq \alpha'$, удовлетворяющих условию $\mu(\alpha, \alpha') \neq \mu(\alpha^g, \alpha'^g)$. Значение показателя μ -неизометричности удовлетворяет оценкам $0 \leq ni_g(\mu) \leq 1$. При этом $ni_g(\mu) = 0$ тогда и только тогда, когда $g \in \text{Isom}(\mu)$, где $\text{Isom}(\mu)$ – группа изометрий метрики μ . Для синтеза шифрсистем предпочтительными являются подстановки с большим значением показателя μ -неизометричности для каждой метрики μ на V_n . В некотором смысле получаем ситуацию, схожую с понятием «нелинейность», где важное место занимают максимально нелинейные в разных смыслах функции. Для анализа представляют интерес метрики и подстановки с малым значением показателя μ -неизометричности, равным нулю в «идеальном» случае. В этом случае возможно применение, например, метода гомоморфизмов или метода вероятностных гомоморфизмов, а

также метрического метода, основанного на существовании метрики, сохраняемой шифрсистемой (см., например, [7]). Хотя метод гомоморфизмов и метрический метод задаются разбиениями, в общем случае они независимы.

В работе в основном рассматриваются натуральные метрики μ на V_n с условием $V_n^+ \leq \text{Isom}(\mu)$. Множество всех таких метрик обозначается через M_n^+ . Метрика Хемминга принадлежит этому множеству. Согласно [10] для фиксированного числа d каждая $(d+1)$ -значная метрика из M_n^+ однозначно задается разбиением $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$ посредством условия

$$\mu_{\bar{B}} : (\alpha, \alpha') \mapsto j, \text{ если } \alpha \oplus \alpha' \in B_j \text{ для } j \in \{1, \dots, d\},$$

где $X^\times = X \setminus \{\vec{0}_n\}$ для $X \subseteq V_n$, $\vec{0}_n$ — n -мерный нулевой вектор, $\oplus$ — операция сложения в векторном пространстве V_n . Заметим, что блоки разбиения $B_1, \dots, B_d$ можно интерпретировать как модификацию усеченных разностей (см. [8]) в одном из обобщений разностного метода. Они также возникают в $\oplus_{\bar{B}}$ -марковских алгоритмах блочного шифрования (см. [9]).

В разделе 3 для показателя μ -неизометричности получена верхняя оценка в терминах расстояния от преобразования до группы изометрий метрики. Доказано, что для метрик из M_n^+ и преобразования $g \in S(V_n)$ показатель μ -неизометричности выражается через элементы матрицы переходов блоков упорядоченного разбиения $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$, задающего метрику. В частности, такой показатель найден для аффинных преобразований.

В [2] для исследования различных метрических свойств преобразований введена иерархия на множестве натуральных метрик посредством понятия подметрики ρ метрики μ , задаваемой условием $\rho(\alpha, \alpha') \leq \mu(\alpha, \alpha')$ для всех $\alpha, \alpha' \in V_n$. В настоящей работе для метрики μ и ее подметрики ρ указана связь показателей μ -неизометричности и ρ -неизометричности. Кроме того, получена связь показателей μ -неизометричности линейно-эквивалентных преобразований.

В [10] описан класс метрик из множества M_n^+ с наибольшей значностью, равной 2^n . Любая метрика из M_n^+ является подметрикой такой 2^n -значной метрики μ . Некоторые алгоритмы блочного шифрования являются инволютивными с равными функциями зашифрования и расшифрования. У таких алгоритмов функция зашифрования представима как композиция инволюций. В разделе 4

для 2^n -значной метрики $\mu \in M_n^+$ описываются свойства показателя μ -неизометричности инволюции $g \in S(V_n)$. Получена оценка сверху показателя μ -неизометричности произвольной инволюции. Показано, что оценка сверху достижима, если инволюция является APN-подстановкой.

В разделе 5 рассматриваются метрики $\mu \in M_n^+$, задаваемые разбиением $\mathbf{W}$ пространства V_n , у которых показатель μ -неизометричности полностью определяется элементами матрицы $\mathbf{c}^{(\mathbf{W})}(g)$, характеризующей рассеивание разбиения подстановкой $g \in S(V_n)$ и введенной в [5]. Для таких метрик получены достижимые верхние оценки. Кроме того, если $W_0 < V_n$ ($d = \dim W_0$), $\mathbf{W}$ – множество всех смежных классов группы $(V_n, \oplus)$ относительно подгруппы $(W_0, \oplus)$, то показатель μ -неизометричности выражен через элементы матрицы $\mathbf{c}^{(\mathbf{W})}(g)$ для каждой подстановки $g \in S(V_n)$. В случае $d \in \{1, n-1\}$ для метрик из [3] получена связь между подстановками с максимальным порядком $\mathbf{W}$ -примитивности и подстановками, для которых показатель $\mu_{\bar{W}}$ -неизометричности принимает наибольшее значение, где $\bar{W} = (W_0^\times, V_n/W_0)$. Показано, что для некоторых классов метрик верхняя оценка показателя μ -неизометричности может быть существенно меньше 1. Кроме того, для произвольной 3-значной метрики $\mu_{\bar{W}}$ ($\vec{0}_n \in W_0 \subset V_n$) найдены показатель $\mu_{\bar{W}}$ -неизометричности, а также его достижимая верхняя оценка. Приведен пример метрики μ , у которой из максимальной порядком $\mathbf{W}$ -примитивности вытекает максимальность значения показателя μ -неизометричности. Однако из максимальной порядком $\mathbf{W}$ -примитивности не следует максимальность порядком $\mathbf{W}$ -примитивности. Кроме того, указана метрика μ' , у которой максимальность порядком $\mathbf{W}$ -примитивности равносильна максимальной порядком μ' -неизометричности.

2. Основные обозначения, понятия и базовые свойства

Пусть $\mathbb{N}$ – множество всех натуральных чисел, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $\mathbb{Z}$ – кольцо целых чисел; $\mathbb{Z}_m$ – кольцо вычетов по модулю m ; $S(X)$ – симметрическая группа на множестве X , $S(X) = S_m$ при $|X| = m$; V_n – пространство n -мерных векторов над полем $GF(2)$; $\oplus$ – аддитивная операция векторного пространства V_n ; $\vec{0}_n$ – n -мерный нулевой вектор; $\|\alpha\|$ – вес Хемминга вектора $\alpha \in V_n$; $I(A)$ – индикатор выполнения условия A ; $\mathbb{R}$ – множество вещественных чисел;

$\mathbb{R}^+ = \{y \in \mathbb{R} | y \geq 0\}$; $\text{Isom}(\mu)$ – группа изометрий метрики μ ; χ_n – метрика Хемминга на V_n ; $\chi(g, h) = |\{\alpha \in V_n | \alpha^g \neq \alpha^h\}|$; $\text{IG}_{\mathbf{W}}$ – группа всех подстановок из $S(V_n)$, сохраняющих разбиение (систему импримитивности) $\mathbf{W}$; $\text{Im}(\varphi)$ – образ гомоморфизма φ , $\text{Ker}(\varphi)$ – ядро гомоморфизма φ .

Для разбиения с равномошными блоками $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ пространства V_n положим

$$\chi_{\mathbf{W}}(g) = \min \{\chi(g, h) | h \in \text{IG}_{\mathbf{W}}\}.$$

Для разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ пространства V_n и подстановки $g \in S(V_n)$ обозначим через $\mathbf{c}^{(\mathbf{W})}(g) = \left[\left[c_{i,j}^{(\mathbf{W})}(g) \right] \right] - (r \times r)$ -матрицу, где

$$c_{i,j}^{(\mathbf{W})}(g) = |W_i^g \cap W_j|, i, j = 0, 1, \dots, r-1.$$

Каждому вектору $\alpha = (\alpha_{n-1}, \dots, \alpha_1, \alpha_0) \in V_n$ сопоставим элемент $\tilde{\alpha} = 2^{n-1}\alpha_{n-1} + \dots + 2\alpha_1 + \alpha_0$ кольца $\mathbb{Z}_{2^n}$. Тогда на векторах из V_n можно определить действие подстановок из группы $S(\mathbb{Z}_{2^n})$, операции сложения и умножения по модулю 2^n , а на элементах кольца $\mathbb{Z}_{2^n}$ – операцию $\oplus$ покоординатного сложения векторов. Эти операции будем обозначать теми же знаками, что и соответствующие операции над числами или векторами. Из контекста всегда будет ясно, об операциях с элементами каких алгебраических структур идет речь. Все группы подстановок, если не оговорено противное, действуют на множестве V_n .

Введем для произвольной натуральной метрики μ меру $ni_g(\mu)$ несогласованности метрической структуры и подстановки g , пропорциональную числу неупорядоченных пар элементов $\{\alpha, \alpha'\} \subset V_n$, $\alpha \neq \alpha'$, удовлетворяющих условию $\mu(\alpha, \alpha') \neq \mu(\alpha^g, \alpha'^g)$.

Определение 1. Для натуральной метрики μ на пространстве V_n и подстановки $g \in S(V_n)$ показателем μ -неизометричности назовем величину

$$\begin{aligned} ni_g(\mu) &= (2^{2n} - 2^n)^{-1} |\{(\alpha, \alpha') \in V_n^2 | \mu(\alpha, \alpha') \neq \mu(\alpha^g, \alpha'^g)\}| \\ &= (2^{2n-1} - 2^{n-1})^{-1} |\{ \{\alpha, \alpha'\} \subset V_n | \alpha \neq \alpha' \wedge \mu(\alpha, \alpha') \neq \mu(\alpha^g, \alpha'^g) \}|. \end{aligned}$$

Очевидно, что $ni_g(\mu) = 0$ тогда и только тогда, когда $g \in \text{Isom}(\mu)$. Для произвольной натуральной метрики μ нахождение верхней достижимой оценки показателя μ -неизометричности может оказаться трудной проблемой. Еще более сложной является проблема описания подстановок из $S(V_n)$, для которых достигается данная оценка. В разделах 4 и 5 она будет решена для некоторых классов метрик.

Опишем сначала базовые свойства показателя μ -неизометричности преобразования.

Для натуральной метрики μ на V_n рассмотрим разложение симметрической группы $S(V_n)$ на левые и правые смежные классы по подгруппе $\text{Isom}(\mu)$. Легко видеть, что показатель $ni_g(\mu)$ одинаков для всех подстановок g , принадлежащих одному смежному классу по подгруппе $\text{Isom}(\mu)$.

Лемма 1. Пусть μ – натуральная метрика на V_n , $h \in S(V_n)$, а $h(\text{Isom}(\mu))$, $(\text{Isom}(\mu))h$ – левые и правые смежные классы при разложении симметрической группы $S(V_n)$ по подгруппе $\text{Isom}(\mu)$. Тогда для каждой подстановки

$$g \in h(\text{Isom}(\mu)) \cup (\text{Isom}(\mu))h$$

справедливо равенство $ni_g(\mu) = ni_h(\mu)$.

Доказательство очевидно.

Для натуральной метрики μ на V_n и подстановки $g \in S(V_n)$ определим расстояние до группы изометрий равенством

$$\tilde{\chi}_\mu(g) = \min \{ \chi(g, h) | h \in \text{Isom}(\mu) \}.$$

Отметим, что обе величины $ni_g(\mu)$, $\tilde{\chi}_\mu(g)$ задаются метрикой μ . Кроме того, $ni_g(\mu)$ явно зависит от метрики μ , но не зависит от группы изометрий $\text{Isom}(\mu)$.

У разных натуральных метрик группы изометрий могут совпадать. Получение достижимых верхних оценок величины $\tilde{\chi}_\mu(g)$ для произвольной метрики, а также описание удовлетворяющих им подстановок из $S(V_n)$ являются открытыми вопросами и в данной работе не рассматриваются. В некоторых частных случаях такие оценки известны. Так, $\tilde{\chi}_\mu(g)$ является аналогом порядка **W**-примитивности, который характеризует меру несогласованности подстановки g и соответствующей импримитивной группы [5]. При этом, если метрика μ задается разбиением $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$, например посредством условия

$$\mu : (\alpha, \alpha') \mapsto j, \text{ если } \alpha \oplus \alpha' \in W_{j-1} \text{ для } j \in \{1, \dots, r\},$$

то $\chi_{\mathbf{W}}(g) \leq \tilde{\chi}_\mu(g)$ и $\text{Isom}(\mu) \leq \text{IG}_{\mathbf{W}}$ (см. утверждение 4).

Лемма 2. Для любой натуральной метрики μ на V_n и любой подстановки $g \in S(V_n)$ выполняется неравенство

$$ni_g(\mu) \leq 1 - \frac{(\tilde{\chi}_\mu(g))^2}{2^{2n} - 2^n} + \frac{\tilde{\chi}_\mu(g)}{2^{2n} - 2^n}. \quad (1)$$

Доказательство. Пусть подстановка $h \in \text{Isom}(\mu)$ такова, что $\tilde{\chi}_\mu(g) = \chi(g, h)$. Положим

$$U_{g,h} = \{\alpha \in V_n \mid \alpha^g = \alpha^h\}.$$

Ясно, что

$$|U_{g,h}| = 2^n - \chi(g, h) = 2^n - \tilde{\chi}_\mu(g).$$

Пусть

$$U = U_{g,h} \times (V_n \setminus U_{g,h}) \cup (V_n \setminus U_{g,h}) \times U_{g,h}.$$

Тогда

$$\begin{aligned} ni_g(\mu) &= (2^{2n} - 2^n)^{-1} \sum_{(\alpha, \alpha') \in U} \mathbf{I}(\mu(\alpha, \alpha') \neq \mu(\alpha^g, \alpha'^g)) \\ &\quad + (2^{2n} - 2^n)^{-1} \sum_{(\alpha, \alpha') \in (V_n \setminus U_{g,h})^2, \alpha \neq \alpha'} \mathbf{I}(\mu(\alpha, \alpha') \neq \mu(\alpha^g, \alpha'^g)) \\ &\leq (2^{2n} - 2^n)^{-1} (2 \cdot |U_{g,h} \times (V_n \setminus U_{g,h})| + |(V_n \setminus U_{g,h})|^2 - |V_n \setminus U_{g,h}|) \\ &= (2^{2n} - 2^n)^{-1} ((2^n - \tilde{\chi}_\mu(g))^2 - (2^n - \tilde{\chi}_\mu(g)) + 2\tilde{\chi}_\mu(g)(2^n - \tilde{\chi}_\mu(g))) \\ &= (2^{2n} - 2^n)^{-1} (2^n - \tilde{\chi}_\mu(g))(2^n + \tilde{\chi}_\mu(g) - 1) \\ &= 1 - \frac{(\tilde{\chi}_\mu(g))^2}{2^{2n} - 2^n} + \frac{\tilde{\chi}_\mu(g)}{2^{2n} - 2^n}. \end{aligned}$$

Заметим, что в неравенстве (1) верхняя оценка показателя μ -неизометричности, зависящая от величины $\tilde{\chi}_\mu(g)$, довольно «грубая». Очевидно, что она убывает при росте $\tilde{\chi}_\mu(g)$ и является наименьшей для $\tilde{\chi}_\mu(g) = \tilde{\chi}_\mu^{(\max)}$, где

$$\tilde{\chi}_\mu^{(\max)} = \max \{\tilde{\chi}_\mu(b) \mid b \in S(V_n)\}.$$

Такое поведение, скорее всего, связано с тем, что при возрастании $\tilde{\chi}_\mu(g)$ верхняя оценка становится менее «грубой».

3. Свойства показателя μ -неизометричности преобразований относительно V_n^+ -инвариантной метрики μ

Далее в разделах 3 и 4 рассматриваются метрики μ из множества M_n^+ , элементами которого являются все натуральные метрики на V_n , инвариантные, как и метрика Хемминга, относительно группы сдвигов V_n^+ , т. е. $V_n^+ \leq \text{Isom}(\mu)$.

Пусть $\mu_{\bar{B}} : V_n \times V_n \rightarrow \{0, \dots, d\}$ – натуральная метрика, инвариантная относительно группы V_n^+ и задаваемая упорядоченным разбиением $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$ посредством условия

$$\mu_{\bar{B}}(\alpha, \alpha') = j, \text{ если } \alpha \oplus \alpha' \in B_j \text{ для } j \in \{1, \dots, r\}. \quad (2)$$

Согласно определению множества M_n^+ в разделе 6 [10] для каждой метрики $\mu \in M_n^+$ существует такое упорядоченное разбиение $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$, что $\mu = \mu_{\bar{B}}$.

Для $\delta \in V_n$, $U, W \subseteq V_n$, $b \in S(V_n)$ положим

$$\hat{p}_{\delta, W}(b) = \sum_{\varepsilon \in W} \hat{p}_{\delta, \varepsilon}(b),$$

$$\hat{p}_{U, W}(b) = \sum_{(\delta, \varepsilon) \in U \times W} \hat{p}_{\delta, \varepsilon}(b) = \sum_{\delta \in U} \hat{p}_{\delta, W}(b),$$

где

$$\hat{p}_{\theta, \varepsilon}(b) = 2^{-n} \left| \left\{ \alpha \in V_n \mid (\theta \oplus \alpha)^b = \varepsilon \oplus \alpha^b \right\} \right|, \theta, \varepsilon \in V_n,$$

а $[\hat{p}_{\theta, \varepsilon}(b)]$ – матрица вероятностей переходов разностей подстановки b .

Утверждение 1. Для каждой подстановки $g \in S(V_n)$ и $(d+1)$ -значной метрики $\mu_{\bar{B}} \in M_n^+$, задаваемой упорядоченным разбиением $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$, справедливо равенство

$$ni_g(\mu_{\bar{B}}) = 1 - (2^n - 1)^{-1} \sum_{i=1}^d \hat{p}_{B_i, B_i}(g). \quad (3)$$

Доказательство следует из равенств

$$\begin{aligned} ni_g(\mu_{\bar{B}}) &= (2^n(2^n - 1))^{-1} |\{(\alpha, \alpha') \in V_n^2 \mid \mu_{\bar{B}}(\alpha, \alpha') \neq \mu_{\bar{B}}(\alpha^g, \alpha'^g)\}| \\ &= (2^n(2^n - 1))^{-1} \sum_{i=1}^d \sum_{\delta \in B_i} |\{\alpha \in V_n \mid (\alpha \oplus \delta)^g \oplus \alpha^g \notin B_i\}| \\ &= (2^n - 1)^{-1} \sum_{i=1}^d \sum_{\delta \in B_i} (1 - \hat{p}_{\delta, B_i}(g)) = (2^n - 1)^{-1} \sum_{i=1}^d |B_i| \end{aligned}$$

$$-(2^n - 1)^{-1} \sum_{i=1}^d \hat{p}_{B_i, B_i}(g) = 1 - (2^n - 1)^{-1} \sum_{i=1}^d \hat{p}_{B_i, B_i}(g).$$

Из утверждения 1 вытекает, что $ni_g(\mu_{\bar{B}}) = 1$ (т.е. показатель $\mu_{\bar{B}}$ -неизометричности достигает максимума) тогда и только тогда, когда $\hat{p}_{B_i, B_i}(g) = 0$ для каждого $j \in \{1, \dots, d\}$.

Для линейных преобразований равенство (3) упрощается.

Лемма 3. Для каждого линейного преобразования $g \in GL_n$ и $(d+1)$ -значной метрики $\mu_{\bar{B}} \in M_n^+$, задаваемой упорядоченным разбиением $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$, справедливо равенство

$$ni_g(\mu_{\bar{B}}) = 1 - (2^{2n} - 2^n)^{-1} \sum_{i=1}^d \left| B_i \cap B_i^{g^{-1}} \right|. \quad (4)$$

Доказательство. Так как

$$(\alpha \oplus \varepsilon)^g \oplus \alpha^g = \varepsilon^g$$

для всех $\alpha, \varepsilon \in V_n$, то для каждого $i \in \{1, \dots, d\}$ справедливо равенство

$$\hat{p}_{B_i, B_i}(g) = \sum_{\delta \in B_i \cap B_i^{g^{-1}}} \hat{p}_{\delta, \delta^g}(g) = 2^{-n} \left| B_i \cap B_i^{g^{-1}} \right|.$$

Заметим, что произвольному преобразованию $g \in S(V_n)$ и упорядоченному разбиению $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$ (или пространства V_n) естественным образом ставится в соответствие $(d \times d)$ -матрица $\tilde{\mathbf{c}}^{(\bar{B})}(g) = \left[\left[\tilde{c}_{i,j}^{(\bar{B})}(g) \right] \right]$, где $\tilde{c}_{i,j}^{(\bar{B})}(g) = |B_i^g \cap B_j|$, $i, j = 1, \dots, d$. В терминах элементов матрицы $\tilde{\mathbf{c}}^{(\bar{B})}(g)$ равенство (4) принимает вид

$$ni_g(\mu_{\bar{B}}) = 1 - (2^{2n} - 2^n)^{-1} \sum_{i=1}^d \tilde{c}_{i,i}^{(\bar{B})}(g^{-1}).$$

Кроме того, если $B'_1 = B_1 \cup \{0\}$, $B'_i = B_i$ для $i = 2, \dots, d$, $\mathbf{B} = \{B'_1, \dots, B'_d\}$, $|B'_1| = |B'_2| = \dots = |B'_d|$, то $\tilde{c}_{i,i}^{(\bar{B})}(g) = c_{i,i}^{(\mathbf{B})}(g)$ для $i = 2, \dots, d$, а $\tilde{c}_{1,1}^{(\bar{B})}(g) = c_{1,1}^{(\mathbf{B})}(g) - 1$. Таким образом, для натуральных метрик, задаваемых разбиением $\mathbf{B}$ с равномошными блоками, показатель μ -неизометричности «явно» выражается через элементы матрицы $\mathbf{c}^{(\mathbf{B})}(g^{-1})$ для линейных преобразований. Такие метрики будут встречаться также в разделе 5.

Укажем связь между показателями μ -неизометричности линейно-эквивалентных преобразований.

Для упорядоченного разбиения $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$ и подстановки $a \in S(V_n)$ положим $\bar{B}^a = (B_1^a, \dots, B_d^a)$. Согласно [10], если $\mu_{\bar{B}} \in M_n^+$ и $a \in GL_n$, то $\mu_{\bar{B}^a} \in M_n^+$.

Лемма 4. Пусть:

- 1) $\mu_{\bar{B}} - (d+1)$ -значная метрика из M_n^+ , задаваемая упорядоченным разбиением $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$.
- 2) $a, a' -$ произвольные преобразования из GL_n .
- 3) $g -$ произвольная подстановка из $S(V_n)$, а подстановка $g_{a,a'} \in S(V_n)$ задана условием $g_{a,a'} : x \mapsto x^{aga'}$.

Тогда

$$ni_{g_{a,a'}}(\mu_{\bar{B}}) = 1 - (2^n - 1)^{-1} \sum_{i=1}^d \hat{p}_{B_i^a, B_i^{(a')^{-1}}}(g). \quad (5)$$

Кроме того, если $B_i^{aa'} = B_i$ для каждого $i \in \{1, \dots, d\}$, то

$$ni_{g_{a,a'}}(\mu_{\bar{B}}) = ni_{g_{a,a'}}(\mu_{\bar{B}^a}).$$

Доказательство. Так как для любых $\alpha, \varepsilon \in V_n$ справедливо равенство

$$(\alpha \oplus \varepsilon^{a^{-1}})^{g_{a,a'}} \oplus \alpha^{g_{a,a'}} = (\alpha^a \oplus \varepsilon)^{ga'} \oplus \alpha^{aga'},$$

то $\hat{p}_{\varepsilon^{a^{-1}}, \delta a'}(g_{a,a'}) = \hat{p}_{\varepsilon, \delta}(g)$. Поэтому для каждого $i \in \{1, \dots, d\}$ справедливо равенство

$$\begin{aligned} \hat{p}_{B_i, B_i}(g_{a,a'}) &= \sum_{\delta \in B_i} \sum_{\delta' \in B_i} \hat{p}_{\delta, \delta'}(g_{a,a'}) = \sum_{\delta \in B_i} \sum_{\delta' \in B_i} \hat{p}_{\delta a, \delta' (a')^{-1}}(g) \\ &= \sum_{\delta \in B_i^a} \sum_{\delta' \in B_i^{(a')^{-1}}} \hat{p}_{\delta, \delta'}(g). \end{aligned}$$

Отсюда следует, что

$$\begin{aligned} ni_{g_{a,a'}}(\mu_{\bar{B}}) &= 1 - (2^n - 1)^{-1} \sum_{i=1}^d \hat{p}_{B_i, B_i}(g_{a,a'}) \\ &= 1 - (2^n - 1)^{-1} \sum_{i=1}^d \hat{p}_{B_i^a, B_i^{(a')^{-1}}}(g). \end{aligned}$$

Очевидно, что для произвольного $j \in \{1, \dots, d\}$ равенства $B_j^a = B_j^{(a')^{-1}}$, $B_j^{aa'} = B_j$ равносильны. Кроме того, если $B_j^a = B_j^{(a')^{-1}}$ для каждого $j \in \{1, \dots, d\}$, то

$$ni_{g_{a,a'}}(\mu_{\bar{B}}) = 1 - (2^n - 1)^{-1} \sum_{i=1}^d \hat{p}_{B_i^a, B_i^a}(g) = ni_{g_{a,a'}}(\mu_{\bar{B}^a}).$$

Для метрики μ и ее подметрики μ' укажем связь между показателями μ -неизометричности и μ' -неизометричности.

Лемма 5. Пусть $\bar{B} = (B_1, \dots, B_d)$, $\bar{U} = (U_1, \dots, U_t)$ – такие упорядоченные разбиения множества $V_n^\times$, что $\mu_{\bar{B}}, \mu_{\bar{U}} \in M_n^+$ и $\mu_{\bar{U}}$ – подметрика метрики $\mu_{\bar{B}}$. Тогда $ni_g(\mu_{\bar{B}}) \geq ni_g(\mu_{\bar{U}})$ для каждой подстановки $g \in S(V_n)$. Кроме того, равенство

$$ni_g(\mu_{\bar{B}}) = ni_g(\mu_{\bar{U}})$$

выполняется тогда и только тогда, когда

$$\hat{p}_{\delta, \varepsilon}(g) = 0 \text{ для всех } (\delta, \varepsilon) \in (V_n^\times \times V_n^\times) \setminus \left(\bigcup_{j=1}^d (B_j \times B_j) \right). \quad (6)$$

Доказательство. Пусть $J = (J_1, \dots, J_t)$ – такое разбиение множества $\{1, \dots, d\}$, что $U_i = \bigcup_{t \in J_i} B_t$ для $i = 1, \dots, t$. Очевидно, что для каждого $i \in \{1, \dots, t\}$ выполняется неравенство

$$\sum_{j \in J_i} \hat{p}_{B_j, B_j}(g) \leq \sum_{j \in J_i} \sum_{c \in J_i} \hat{p}_{B_j, B_c}(g) \leq \hat{p}_{U_i, U_i}(g),$$

из которого вытекает неравенство $\sum_{i=1}^d \hat{p}_{B_i, B_i}(g) \leq \sum_{i=1}^t \hat{p}_{U_i, U_i}(g)$. Таким образом, $ni_g(\mu_{\bar{B}}) \geq ni_g(\mu_{\bar{U}})$.

Приведем условия на элементы $\hat{p}_{\delta, \varepsilon}(g)$ матрицы вероятностей переходов разностей подстановки g , при которых справедливо равенство

$$ni_g(\mu_{\bar{B}}) = ni_g(\mu_{\bar{U}}). \quad (7)$$

Подставляя равенство (3) в (7), получаем

$$\sum_{i=1}^d \hat{p}_{B_i, B_i}(g) = \sum_{i=1}^t \sum_{j \in J_i} \sum_{c \in J_i} \hat{p}_{B_j, B_c}(g),$$

т. е. $\hat{p}_{\delta,\varepsilon}(g) = 0$ для всех $(\delta, \varepsilon) \in (V_n^\times \times V_n^\times) \setminus \left(\bigcup_{j=1}^d (B_j \times B_j) \right)$.

Очевидно, что из равенства (6) вытекает справедливость равенства (7) для каждой подстановки $g \in S(V_n)$ только при условии $\mu_{\bar{B}} = \mu_{\bar{U}}$.

4. Показатель μ -неизометричности инволюций

В алгоритмах шифрования часто используются инволютивные преобразования. Рассмотрим показатели μ -неизометричности, а также его верхние и нижние оценки для классов инволюций. Большая часть результатов получена для метрик из множества M_n^+ с наибольшей значностью, равной 2^n . Согласно [10] любая метрика $\rho \in M_n^+$ является подметрикой некоторой 2^n -значной метрики $\mu \in M_n^+$. Поэтому из леммы 5 следует, что из верхней оценки показателя μ -неизометричности вытекает верхняя оценка показателя ρ -неизометричности. Заметим, что описание некоторых свойств показателя μ -неизометричности может проще осуществляться для 2^n -значной метрики $\mu \in M_n^+$, а не для ее подметрик.

Пусть $\mu_{\bar{B}}$ – произвольная 2^n -значная метрика, $\bar{B} = (B_1, \dots, B_{2^n-1})$. Из теоремы 6.2 [10] (в работе описаны все 2^n -значные метрики) следует равенство $|B_i| = 1$ для $i = 1, \dots, 2^n - 1$. Из утверждения 1 вытекает, что

$$ni_g(\mu_{\bar{B}}) = 1 - (2^n - 1)^{-1} \sum_{\varepsilon \in V_n^\times} \hat{p}_{\varepsilon,\varepsilon}(g). \quad (8)$$

Из равенства (8) следует, что для фиксированного $j \in \{0, 1\}$ тогда и только тогда справедливо равенство $ni_g(\mu_{\bar{B}}) = j$ (т. е. достижимы экстремальные значения показателя μ -неизометричности), когда $\hat{p}_{\varepsilon,\varepsilon}(g) = j$ для каждого $\varepsilon \in V_n^\times$.

Для подстановки $g \in S(V_n)$ положим $Q^{(g)} = \{\lambda \in V_n \mid \lambda^g = \lambda\}$, $\bar{Q}^{(g)} = V_n \setminus Q^{(g)}$. Очевидно, что $Q^{(g)}$ – множество всех неподвижных точек подстановки g , а $\bar{Q}^{(g)}$ – множество мобильных точек.

Пусть также

$$\Theta(g) = \{\alpha \oplus \beta \mid \{\alpha, \beta\} \subseteq \bar{Q}^{(g)}, \alpha \oplus \beta = \alpha^g \oplus \beta^g, \alpha \neq \beta\},$$

$$\Delta(g) = \{\beta \oplus \beta' \mid \{\beta, \beta'\} \subseteq Q^{(g)}, \beta \neq \beta'\},$$

$T(g)$ – множество всех независимых транспозиций подстановки g , т. е.

$$g = \prod_{(\beta, \beta') \in T(g)} (\beta, \beta').$$

Утверждение 2. Пусть $n \geq 2$, g – произвольная инволюция из $S(V_n)$. Тогда:

1) для всех $\alpha, \beta \in V_n$ справедливо неравенство

$$\hat{p}_{\alpha \oplus \beta, \alpha^g \oplus \beta^g}(g) \geq 2^{1-n}, \quad (9)$$

2) для всех $\delta, \theta \in V_n^\times$ справедливо равенство

$$\hat{p}_{\delta, \theta}(g) = \hat{p}_{\theta, \delta}(g), \quad (10)$$

3) справедливы соотношения

$$\hat{p}_{\theta, \theta}(g) \geq 2^{1-n} \text{ для каждого } \theta \in \Theta(g) \cup \Delta(g), \quad (11)$$

$$\hat{p}_{\theta, \theta}(g) = 0 \text{ для каждого } \theta \notin \Theta(g) \cup \Delta(g). \quad (12)$$

Доказательство. 1) Зафиксируем произвольные $\alpha, \beta \in V_n$. Положим

$$\varepsilon = \alpha \oplus \beta, \lambda = \alpha^g \oplus \beta^g.$$

Тогда

$$(\alpha \oplus \varepsilon)^g = \beta^g = \alpha^g \oplus \lambda,$$

$$(\beta \oplus \varepsilon)^g = \alpha^g = \beta^g \oplus \lambda.$$

Значит, $\hat{p}_{\alpha \oplus \beta, \alpha^g \oplus \beta^g}(g) \geq 2^{1-n}$.

2) Зафиксируем произвольные векторы $\delta, \theta \in V_n^\times$. Если выполняется равенство $(\lambda \oplus \delta)^g = \lambda^g \oplus \theta$ для некоторого $\lambda \in V_n$, то

$$(\lambda^g \oplus \theta)^g = (\lambda^g)^g \oplus \delta = \lambda \oplus \delta.$$

Отсюда следует, что $\hat{p}_{\delta, \theta}(g) = \hat{p}_{\theta, \delta}(g)$.

3) Пусть $\hat{p}_{\theta, \theta}(g) > 0$ для произвольного $\theta \in V_n^\times$. Очевидно, что

$$\hat{p}_{\theta, \theta}(g) = 2^{-n} |\{\alpha \in V_n | \alpha^g \oplus (\alpha \oplus \theta)^g = \theta\}|.$$

Положим

$$A(\theta) = \{\alpha \in V_n | \alpha^g \oplus (\alpha \oplus \theta)^g = \theta\}.$$

Очевидно, что если $\alpha \in A(\theta)$, то $\alpha \oplus \theta \in A(\theta)$. Тогда

$$(\alpha \oplus \theta, \alpha^g \oplus \theta) \in T(g) \text{ для каждого } \alpha \in A(\theta). \quad (13)$$

Возможны два случая: $\alpha \in Q^{(g)} \cap A(\theta)$ или $\alpha \in \bar{Q}^{(g)} \cap A(\theta)$. Пусть $\alpha \in Q^{(g)} \cap A(\theta)$. Тогда из включения (13) вытекает, что

$$\alpha \oplus \theta \in Q^{(g)} \cap A(\theta),$$

т. е.

$$\theta \in \alpha \oplus (Q^{(g)} \cap A(\theta)).$$

Значит,

$$\theta \in (Q^{(g)} \cap A(\theta)) \oplus (Q^{(g)} \cap A(\theta)) \setminus \{\vec{0}_n\} \subseteq \Delta(g).$$

Очевидно, что для каждого $\delta \in \Delta(g)$ существуют такие $\beta, \beta' \in Q^{(g)}$, что $\delta = \beta \oplus \beta'$. Так как $\beta^g \oplus (\beta')^g = \beta \oplus \beta' = \delta$, то из неравенства (9) вытекает условие $\hat{p}_{\delta, \delta}(g) \geq 2^{1-n}$ для каждого $\delta \in \Delta(g)$.

Пусть $\alpha \in \bar{Q}^{(g)} \cap A(\theta)$. Тогда справедливы включения

$$\alpha \oplus \theta \in \bar{Q}^{(g)}, \alpha^g \oplus \theta \in \bar{Q}^{(g)},$$

т. е.

$$\theta \in \bar{Q}^{(g)} \oplus \bar{Q}^{(g)} \setminus \{\vec{0}_n\}. \quad (14)$$

Так как $(\alpha \oplus \theta, \alpha^g \oplus \theta), (\alpha, \alpha^g) \in T(g)$, то

$$\alpha \oplus \theta \oplus \alpha = \theta, (\alpha \oplus \theta)^g \oplus \alpha^g = \theta.$$

Значит, $\theta \in \Theta(g)$.

Для каждого $\delta \in \Theta(g)$ существуют такие $\lambda, \lambda' \in \bar{Q}^{(g)}$, что

$$\delta = \lambda \oplus \lambda' = \lambda^g \oplus (\lambda')^g.$$

Тогда из неравенства (9) вытекает условие $\hat{p}_{\delta, \delta}(g) \geq 2^{1-n}$ для каждого $\delta \in \Theta(g)$. Таким образом, $\hat{p}_{\theta, \theta}(g) \geq 2^{1-n}$, если $\theta \in \Theta(g) \cup \Delta(g)$. Кроме того, $\hat{p}_{\theta, \theta}(g) = 0$, если $\theta \notin \Theta(g) \cup \Delta(g)$. Применяя утверждение 2, получим верхнюю оценку показателя $\mu_{\bar{B}}$ -неизометричности.

Следствие 1. Пусть g – произвольная инволюция из $S(V_n)$ и $\mu_{\bar{B}}$ – 2^n -значная метрика из M_n^+ . Тогда

$$ni_g(\mu_{\bar{B}}) \leq 1 - 2^{1-n} |\Theta(g) \cup \Delta(g)| (2^n - 1)^{-1}. \quad (15)$$

Доказательство следует из равенств (8), (12) и неравенства (11).

Так как

$$|\Delta(g)| \leq C_q^2, |\Theta(g)| \leq C_{2^n - q + 1}^2,$$

то из оценки (15) следует, что для инволюций из $S(V_n)$ верхняя оценка показателя μ -неизометричности преобразования зависит от числа его неподвижных точек, а также от строения множеств $\Theta(g)$, $\Delta(g)$. Далее для некоторых классов инволюций найдем показатель $\mu_{\bar{B}}$ -неизометричности.

Определение 2. Преобразование $g : V_n \rightarrow V_n$ называется APN (almost perfect nonlinear) (см. [11]), если

$$\max \{ \hat{p}_{\varepsilon, \theta}(g) | \varepsilon, \theta \in V_n^\times \} = 2^{1-n}.$$

APN-инволюцией будем называть инволюцию на пространстве V_n , являющуюся APN-подстановкой. Множество APN-инволюций не пусто. Так, при нечетном $n \geq 3$ подстановка $s_n \in S(GF(2^n))$, заданная условием

$$s_n : x \mapsto \begin{cases} x^{-1}, & \text{если } x \neq 0, \\ 0, & \text{если } x = 0, \end{cases}$$

является APN-инволюцией. Известно [12], что APN-инволюций не существует для четного $n \in \{2, 4\}$, а при $n \geq 6$ их описание остается открытым вопросом.

Получим показатель $\mu_{\bar{B}}$ -неизометричности APN-инволюций.

Теорема 1. Пусть $n \geq 3$ и $g \in S(V_n)$ является APN-инволюцией, $q = |Q^{(g)}|$,

$$\Lambda(g) = \{ \alpha \oplus \alpha^g | \{ \alpha, \alpha^g \} \subseteq \bar{Q}^{(g)} \}.$$

Тогда

$$\hat{p}_{\theta, \theta}(g) = \begin{cases} 2^{1-n}, & \text{если } \theta \in \Lambda(g) \cup \Delta(g), \\ 0, & \text{если } \theta \in V_n^\times \setminus (\Lambda(g) \cup \Delta(g)), \end{cases}$$

и справедливо равенство

$$ni_g(\mu_{\bar{B}}) = 1 - (2^n - 1)^{-1} (q(q - 2)/2^n + 1). \quad (16)$$

Доказательство. Покажем, что

$$\Lambda(g) \cap \Delta(g) = \emptyset. \quad (17)$$

Предположим, что $\Lambda(g) \cap \Delta(g) \neq \emptyset$. Значит, существует такой $\varepsilon \in \Lambda(g) \cap \Delta(g)$, что

$$\varepsilon = \beta \oplus \beta' = \alpha \oplus \alpha^g$$

для некоторых $\beta, \beta' \in Q^{(g)}$ и $\alpha \in \bar{Q}^{(g)}$. Тогда для каждого $\lambda \in \{ \beta, \beta', \alpha, \alpha^g \}$ справедливо равенство

$$\lambda^g \oplus (\lambda \oplus \varepsilon)^g = \varepsilon.$$

Поэтому $\hat{p}_{\varepsilon, \varepsilon}(g) \geq 2^{2-n}$, но g – APN-подстановка. Следовательно, $\Lambda(g) \cap \Delta(g) = \emptyset$.

Найдем показатель $\mu_{\bar{B}}$ -неизометричности. Для этого покажем, что $\hat{p}_{\theta,\theta}(g) = 0$ для каждого $\theta \in V_n^\times \setminus (\Lambda(g) \cup \Delta(g))$.

Пусть существует такой вектор $\delta \in V_n^\times \setminus (\Lambda(g) \cup \Delta(g))$, что $\hat{p}_{\delta,\delta}(g) > 0$. Так как g – APN-подстановка, то $\hat{p}_{\delta,\delta}(g) = 2^{1-n}$. Значит,

$$\beta' \oplus \beta = \delta, (\beta')^g \oplus \beta^g = \delta$$

для некоторых $\beta, \beta' \in V_n$, т. е.

$$(\beta \oplus \delta)^g = \beta^g \oplus \delta. \quad (18)$$

Возможны два случая: $\beta \in Q^{(g)}$ или $\beta \in \bar{Q}^{(g)}$.

Если $\beta \in Q^{(g)}$, то равенство (18) принимает вид

$$(\beta \oplus \delta)^g = \beta \oplus \delta.$$

Значит, $\beta \oplus \delta \in Q^{(g)}$, а поэтому $\delta \in \Delta(g)$, но по предположению $\delta \notin \Delta(g)$.

Если $\beta \in \bar{Q}^{(g)}$, то $(\beta, \beta^g) \in T(g)$, $(\beta \oplus \delta, \beta^g \oplus \delta) \in T(g)$. Возможны два случая:

$$(\beta, \beta^g) = (\beta \oplus \delta, \beta^g \oplus \delta) \text{ или } (\beta, \beta^g) \neq (\beta \oplus \delta, \beta^g \oplus \delta).$$

Если $(\beta, \beta^g) = (\beta \oplus \delta, \beta^g \oplus \delta)$, то $\beta^g = \beta \oplus \delta$. Значит, $\delta = \beta^g \oplus \beta$ и $\delta \in \Lambda(g)$, но по предположению $\delta \notin \Lambda(g)$.

Если же $(\beta, \beta^g) \neq (\beta \oplus \delta, \beta^g \oplus \delta)$, то при $\varepsilon = \beta \oplus \beta^g$ равенство

$$(\vartheta \oplus \varepsilon)^g = \vartheta^g \oplus \varepsilon$$

справедливо для каждого $\vartheta \in \{\beta, \beta^g, \beta \oplus \delta, \beta^g \oplus \delta\}$. Поэтому $\hat{p}_{\beta \oplus \beta^g, \beta \oplus \beta^g}(g) \geq 2^{2-n}$, что для APN-подстановки g невозможно. Таким образом, $\hat{p}_{\theta,\theta}(g) = 0$ для каждого $\theta \in V_n^\times \setminus (\Lambda(g) \cup \Delta(g))$.

Отсюда следует, что

$$\begin{aligned} ni_g(\mu_{\bar{B}}) &= 1 - (2^n - 1)^{-1} \sum_{\varepsilon \in V_n^\times} \hat{p}_{\varepsilon,\varepsilon}(g) \\ &= 1 - (2^n - 1)^{-1} 2^{1-n} \cdot (|\Lambda(g)| + |\Delta(g)|) \\ &= 1 - (2^n - 1)^{-1} 2^{1-n} \cdot (q(q-2)/2 + 2^{n-1}). \end{aligned}$$

Из равенства (12) и неравенства (11) следует, что $\Theta(g) = \Lambda(g)$ для APN-инволюции. Отсюда и из равенства (17) имеем

$$|\Theta(g) \cup \Delta(g)| = |\Lambda(g)| + |\Delta(g)| = q(q-2)/2 + 2^{n-1}.$$

Таким образом, для APN-инволюций достижима верхняя граница в неравенстве (15).

Получим верхнюю оценку числа неподвижных точек APN-инволюций. Из нее будут следовать экстремальные оценки показателя $\mu_{\overline{B}}$ -неизометричности APN-инволюций.

Следствие 2. Пусть $n \geq 3$ и $g \in S(V_n)$ является APN-инволюцией. Тогда

$$|Q^{(g)}| \leq 1 + (2^{n-1} - 1)^{1/2} \quad (19)$$

и справедливы неравенства

$$1 - 2^{-n} - (2^n - 1)^{-1} \leq ni_g(\mu_{\overline{B}}) \leq 1 - (2^n - 1)^{-1}.$$

Доказательство. Получим оценку числа $|Q^{(g)}|$ неподвижных точек. Положим $q = |Q^{(g)}|$. Так как g – инволюция, то q четно. Из равенства (17) и включения $\Lambda(g) \cup \Delta(g) \subseteq V_n^\times$ вытекает

$$|\Lambda(g)| + |\Delta(g)| \leq 2^n - 1. \quad (20)$$

Так как g – APN-инволюция, то

$$|\Delta(g)| = C_q^2, \quad |\Lambda(g)| = 2^{n-1} - q/2$$

и неравенство (20) имеет вид

$$q(q-1)/2 + 2^{n-1} - q/2 \leq 2^n - 1.$$

Значит, $q(q-2)/2 \leq 2^{n-1} - 1$, т. е. $q \leq 1 + (2^{n-1} - 1)^{1/2}$.

Из равенства (16) и неравенства (17) следует, что

$$\begin{aligned} & 1 - (2^n - 1)^{-1} 2^{1-n} \cdot (2^{n-1} - 1 + 2^{n-1}) \\ & \leq 1 - 2^{1-n} - (2^n - 1)^{-1} \leq ni_g(\mu_{\overline{B}}). \end{aligned}$$

Кроме того, из равенства (16) и условия $q(q-2) \geq 0$ следует оценка

$$ni_g(\mu_{\overline{B}}) \leq 1 - (2^n - 1)^{-1}.$$

Из доказательства следствия 2 вытекает, что наибольшее значение показателя $\mu_{\overline{B}}$ -неизометричности APN-инволюции, равное $1 - (2^n - 1)^{-1}$, достигается при $|Q^{(g)}| \in \{0, 2\}$.

Для произвольных метрики $\mu \in M_n^+$ и множества $W \subset V_n$ найдем показатель μ -неизометричности инволюций вида

$$g_{W,\lambda} = \prod_{\alpha \in W} (\alpha, \alpha \oplus \lambda),$$

где $\lambda \in V_n^\times$. Если W – подпространство размерности $n - 1$ и $\lambda \notin W$, то получаем подстановку-сдвиг $g_{W,\lambda} = h_\lambda \in S(V_n)$, задаваемую условием $h_\lambda : \alpha \mapsto \alpha \oplus \lambda$.

Заметим, что нахождение показателя χ_n -неизометричности произвольного преобразования из $S(V_n)$ в общем случае является нетривиальной задачей. Показатель χ_n -неизометричности в работе удалось найти только для некоторых классов преобразований. Одним из таких классов является множество транспозиций. Далее понадобится следующий вспомогательный результат.

Лемма 6. Пусть $\lambda \in V_n^\times$, $\vec{0}_n \in W \subset V_n$,

$$W \cap \{W \oplus \lambda\} = \emptyset, g_{W,\lambda} = \prod_{\alpha \in W} (\alpha, \alpha \oplus \lambda)$$

и

$$U_W(\lambda) = \left\{ \theta \in V_n^\times \mid (W \oplus \langle \lambda \rangle)^{h_\theta} = W \oplus \langle \lambda \rangle \right\},$$

$$c_\delta(W, \lambda) = |W \oplus \langle \lambda, \delta \rangle| - |(W \oplus \langle \lambda \rangle) \cap (W \oplus \delta \oplus \langle \lambda \rangle)|.$$

Тогда для всех $\delta, \delta' \in V_n^\times$ справедливо равенство

$$\hat{p}_{\delta, \delta'}(g_{W, \lambda}) = \begin{cases} 1, & \text{если } \delta' = \delta, \delta \in U_W(\lambda), \\ 1 - 2^{-n} c_\delta(W, \lambda), & \text{если } \delta' = \delta, \delta \notin U_W(\lambda), \\ 2^{-n} c_\delta(W, \lambda), & \text{если } \delta' = \delta \oplus \lambda, \delta \notin U_W(\lambda), \\ 0, & \text{если } \delta' \notin \{\delta, \delta \oplus \lambda\}. \end{cases} \quad (21)$$

Доказательство. Ясно, что

$$\bar{Q}^{(g_{W, \lambda})} = V_n \setminus Q^{(g_{W, \lambda})} = \bigcup_{\alpha \in W} \{\alpha, \alpha \oplus \lambda\} = W \oplus \langle \lambda \rangle,$$

$$Q^{(g_{W, \lambda})} = V_n \setminus (W \oplus \langle \lambda \rangle).$$

Приведем условия на элементы $\beta \in V_n$, $\delta, \delta' \in V_n^\times$, при которых $(\beta \oplus \delta)^{g_{W, \lambda}} = \beta^{g_{W, \lambda}} \oplus \delta'$. Для этого рассмотрим следующие случаи.

1) Если $\{\beta, \beta \oplus \delta\} \subseteq Q^{(g_{W, \lambda})}$, то $(\beta \oplus \delta)^{g_{W, \lambda}} = \beta \oplus \delta$, а поэтому $\delta' = \delta$.

2) Если $\beta \in Q^{(g_{W,\lambda})}$, $\beta \oplus \delta \in \bar{Q}^{(g_{W,\lambda})}$, то

$$\delta \neq \lambda, (\beta \oplus \delta)^{g_{W,\lambda}} = \beta \oplus \delta' = \beta \oplus \delta \oplus \lambda,$$

а поэтому

$$\delta' = \delta \oplus \lambda.$$

3) Если $\beta \in \bar{Q}^{(g_{W,\lambda})}$, $\beta \oplus \delta \in Q^{(g_{W,\lambda})}$, то $\delta \neq \lambda$, $\beta \oplus \delta = \beta^{g_{W,\lambda}} \oplus \delta'$, а поэтому

$$\delta' = \beta \oplus \delta \oplus \beta^{g_{W,\lambda}} = \delta \oplus \lambda.$$

4) Если $\{\beta, \beta \oplus \delta\} \subseteq \bar{Q}^{(g_{W,\lambda})}$, то

$$(\beta \oplus \delta)^{g_{W,\lambda}} = \beta \oplus \delta \oplus \lambda, \beta^{g_{W,\lambda}} \oplus \delta' = \beta \oplus \lambda \oplus \delta',$$

а поэтому $\beta \oplus \delta \oplus \lambda = \beta \oplus \lambda \oplus \delta'$, причем

$$\delta' = \delta, \delta \in (W \oplus W \oplus \langle \lambda \rangle) \setminus \{\vec{0}_n\}.$$

Очевидно, что если $\delta \in U_W(\lambda)$, то для каждого $\beta \in V_n$ справедливо включение

$$\{\beta, \beta \oplus \delta\} \subseteq Q^{(g_{W,\lambda})} \text{ или } \{\beta, \beta \oplus \delta\} \subseteq \bar{Q}^{(g_{W,\lambda})}. \quad (22)$$

Заметим, что включение $\{\beta, \beta \oplus \delta\} \subseteq Q^{(g_{W,\lambda})}$ (п. 1) равносильно условию $\beta \notin \bar{Q}^{(g_{W,\lambda})} \cup (\bar{Q}^{(g_{W,\lambda})} \oplus \delta)$, причем

$$\bar{Q}^{(g_{W,\lambda})} \cup (\bar{Q}^{(g_{W,\lambda})} \oplus \delta) = W \oplus \langle \lambda, \delta \rangle. \quad (23)$$

Кроме того, включения $\{\beta, \beta \oplus \delta\} \subseteq \bar{Q}^{(g_{W,\lambda})}$ (п. 4) и

$$\beta \in (W \oplus \langle \lambda \rangle) \cap (W \oplus \langle \lambda \rangle \oplus \delta)$$

равносильны. Отсюда следует, что для каждого $\delta \in V_n^\times$ справедливо равенство

$$\hat{p}_{\delta,\delta}(g_{W,\lambda}) = 1 - 2^{-n} (|W \oplus \langle \lambda, \delta \rangle| - |(W \oplus \langle \lambda \rangle) \cap (W \oplus \langle \lambda \rangle \oplus \delta)|). \quad (24)$$

Из пп. 1–4 и равенств (22)–(24) следует, что для всех $\delta, \delta' \in V_n^\times$ выполняется равенство (21).

Заметим, что в обозначениях леммы 6

$$c_\delta(W, \lambda) = 0 \text{ тогда и только тогда, когда } \delta \in U_W(\lambda). \quad (25)$$

Утверждение 3. Пусть подстановка $g_{W,\lambda} = \prod_{\alpha \in W} (\alpha, \alpha \oplus \lambda)$ удовлетворяет условиям леммы 6, а метрика $\mu_{\bar{B}} \in M_n^+$ задана упорядоченным разбиением $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$. Тогда

$$ni_{g_{W,\lambda}}(\mu_{\bar{B}}) = (2^{2n} - 2^n)^{-1} \sum_{i=1}^d \sum_{\delta \in B_i \setminus (U_W(\lambda) \cup (B_i \oplus \lambda))} c_\delta(W, \lambda). \quad (26)$$

Кроме того, если $B_i \cap (B_i \oplus \lambda) = \emptyset$ для $i = 1, \dots, d$, то

$$ni_{g_{W,\lambda}}(\mu_{\bar{B}}) = (2^{2n} - 2^n)^{-1} \sum_{\delta \in V_n^\times} c_\delta(W, \lambda).$$

Доказательство. Из равенства (21) следует, что

$$\sum_{\delta' \in \{\delta, \delta \oplus \lambda\}} \hat{p}_{\delta, \delta'}(g_{W,\lambda}) = 1 \text{ для каждого } \delta \in V_n^\times.$$

Для произвольного множества $B \in \{B_1, \dots, B_d\}$ положим

$$B(\lambda) = \{\alpha \in V_n \mid \{\alpha, \alpha \oplus \lambda\} \subseteq B\}.$$

Очевидно, что $B(\lambda) = B \cap (B \oplus \lambda)$. Заметим также, что $(B^{(1)}, B^{(2)}, B^{(3)})$ – разбиение множества B , где

$$B^{(1)} = U_W(\lambda) \cap B, B^{(2)} = B(\lambda) \setminus U_W(\lambda),$$

$$B^{(3)} = B \setminus ((B \oplus \lambda) \cup U_W(\lambda)).$$

Из равенства (21) имеем

$$\begin{aligned} \hat{p}_{B,B}(g_{W,\lambda}) &= \sum_{(\delta, \varepsilon) \in B \times B} \hat{p}_{\delta, \varepsilon}(g_{W,\lambda}) = \sum_{\delta \in U_W(\lambda) \cap B} \hat{p}_{\delta, \delta}(g_{W,\lambda}) \\ &+ \sum_{\delta \in B(\lambda) \setminus U_W(\lambda)} (\hat{p}_{\delta, \delta}(g_{W,\lambda}) + \hat{p}_{\delta, \delta \oplus \lambda}(g_{W,\lambda})) + \sum_{\delta \in B \setminus (B(\lambda) \cup U_W(\lambda))} \hat{p}_{\delta, \delta}(g_{W,\lambda}) \\ &= |U_W(\lambda) \cap B| + |B(\lambda) \setminus U_W(\lambda)| + \sum_{\delta \in B \setminus (B(\lambda) \cup U_W(\lambda))} (1 - 2^{-n} c_\delta(W, \lambda)) \\ &= |B| - |B \setminus ((B \oplus \lambda) \cup U_W(\lambda))| + \sum_{\delta \in B \setminus (B(\lambda) \cup U_W(\lambda))} (1 - 2^{-n} c_\delta(W, \lambda)) \\ &= |B| - \sum_{\delta \in B \setminus ((B \oplus \lambda) \cup U_W(\lambda))} 2^{-n} c_\delta(W, \lambda). \end{aligned} \quad (27)$$

Из равенств (3), (27) вытекает, что

$$\begin{aligned}
 ni_{g_{W,\lambda}}(\mu_{\overline{B}}) &= 1 - (2^n - 1)^{-1} \sum_{i=1}^d \hat{p}_{B_i, B_i}(g_{W,\lambda}) \\
 &= 1 - (2^n - 1)^{-1} \cdot \sum_{i=1}^d \left(|B_i| - \sum_{\delta \in B_i \setminus ((B_i \oplus \lambda) \cup U_W(\lambda))} 2^{-n} c_\delta(W, \lambda) \right) \\
 &= (2^{2n} - 2^n)^{-1} \sum_{i=1}^d \sum_{\delta \in B_i \setminus ((B_i \oplus \lambda) \cup U_W(\lambda))} c_\delta(W, \lambda).
 \end{aligned}$$

Если $B_i \cap (B_i \oplus \lambda) = \emptyset$ для $i = 1, \dots, d$, то в силу равенства (27)

$$\begin{aligned}
 ni_{g_{W,\lambda}}(\mu_{\overline{B}}) &= (2^{2n} - 2^n)^{-1} \sum_{i=1}^d \sum_{\delta \in B_i \setminus U_W(\lambda)} c_\delta(W, \lambda) \\
 &= (2^{2n} - 2^n)^{-1} \left(\sum_{\delta \in V_n^\times} c_\delta(W, \lambda) - \sum_{\delta \in U_W(\lambda)} c_\delta(W, \lambda) \right). \tag{28}
 \end{aligned}$$

Из (25) и (28) получаем искомое равенство

$$ni_{g_{W,\lambda}}(\mu_{\overline{B}}) = (2^{2n} - 2^n)^{-1} \sum_{\delta \in V_n^\times} c_\delta(W, \lambda).$$

В качестве примера применения утверждения 3 найдем показатель χ_n -неизометричности инволюции

$$g_{W,\lambda} = \prod_{\alpha \in W} (\alpha, \alpha \oplus \lambda)$$

для произвольного подпространства $W < V_n$, $q = \dim W$, и вектора $\lambda \in V_n^\times \setminus W$ нечетного веса Хемминга. Очевидно, что

$$W \cap \{W \oplus \lambda\} = \emptyset,$$

$$U_W(\lambda) = \{\theta \in V_n^\times \mid W \oplus \langle \lambda \rangle \oplus \theta = W \oplus \langle \lambda \rangle\} = (W \oplus \langle \lambda \rangle) \setminus \{\vec{0}_n\}.$$

Тогда

$$\begin{aligned}
 ni_{g_{W,\lambda}}(\chi_n) &= (2^{2n} - 2^n)^{-1} \sum_{i=1}^n \sum_{\delta \in B_i \setminus (U_W(\lambda) \cup (B_i \oplus \lambda))} c_\delta(W, \lambda) \\
 &= (2^{2n} - 2^n)^{-1} \sum_{i=1}^n \sum_{\delta \in B_i \setminus (W \oplus \langle \lambda \rangle)} c_\delta(W, \lambda) \\
 &= (2^{2n} - 2^n)^{-1} \sum_{\delta \in V_n^\times \setminus (W \oplus \langle \lambda \rangle)} c_\delta(W, \lambda) = (2^{2n} - 2^n)^{-1} 2^{q+2} (2^n - 2^{q+1}). \tag{29}
 \end{aligned}$$

Из равенства (28) вытекает, что если $\dim W = q = n - 1$, то $ni_{g_{W,\lambda}}(\chi_n) = 0$, а

$$g_{W,\lambda} = \prod_{\alpha \in W} (\alpha, \alpha \oplus \lambda) = h_\lambda,$$

т. е. $g_{W,\lambda}$ – преобразование-сдвиг пространства V_n , $h_\lambda \in \text{Isom}(\chi_n)$.

Из равенства (29) также вытекает, что если $W_i < V_n$, $\dim W_i = n - i$ для $i = 1, \dots, n$, то

$$0 \leq ni_{g_{W_r,\lambda}}(\chi_n) < ni_{g_{W_j,\lambda}}(\chi_n) \leq 2^{2-n} - 2^{2-n}(2^n - 1)^{-1},$$

если $1 \leq r < j \leq n$. Причем для любой транспозиции $g_{W_n,\lambda}$, где $W_n = \{\vec{0}_n\}$, справедливо равенство

$$ni_{g_{W_n,\lambda}}(\chi_n) = 2^{2-n} - 2^{2-n}(2^n - 1)^{-1}.$$

Таким образом, в классе инволюций наименьшее значение показателя χ_n -неизометричности преобразования $g_{W,\lambda}$, равное 0, достигается на преобразовании-сдвиге пространства V_n при $\dim W = n - 1$, а наибольшее значение – на транспозиции при $\dim W = 0$.

В качестве следствия утверждения 3 найдем показатель $\mu_{\bar{B}}$ -неизометричности преобразования

$$g_{\{\gamma\},\lambda} = g_{W,\lambda} = (\gamma, \gamma \oplus \lambda).$$

Это позволит найти показатель χ_n -неизометричности транспозиций.

Лемма 7. Пусть метрика $\mu_{\bar{B}} \in M_n^+$ задана упорядоченным разбиением $\bar{B} = (B_1, \dots, B_d)$ множества $V_n^\times$, (λ, γ) – произвольный элемент множества $V_n^\times \times V_n$,

$$g_{\{\gamma\},\lambda} = (\gamma, \gamma \oplus \lambda).$$

Тогда

$$ni_{g_{\{\gamma\},\lambda}}(\mu_{\bar{B}}) = 2^{2-n}(2^n - 1)^{-1} \left(\sum_{i=1}^d |B_i \setminus (B_i \oplus \lambda)| - 1 \right). \quad (30)$$

В частности, всегда

$$ni_{g_{\{\gamma\},\lambda}}(\mu_{\bar{B}}) \leq 2^{2-n} - 2^{2-n}(2^n - 1)^{-1}, \quad (31)$$

а если $B_i \cap (B_i \oplus \lambda) = \emptyset$ для $i = 1, \dots, d$, то

$$ni_{g_{\{\gamma\},\lambda}}(\mu_{\bar{B}}) = 2^{2-n} - 2^{2-n}(2^n - 1)^{-1}. \quad (32)$$

Доказательство. Из утверждения 3 вытекает, что

$$U_{\{\gamma\}}(\lambda) = \{\theta \in V_n^\times \mid \gamma \oplus \langle \lambda \rangle \oplus \theta = \gamma \oplus \langle \lambda \rangle\} = \{\lambda\}. \quad (33)$$

Так как $0 \notin B_i$, то $\{0, \lambda\} \not\subseteq B_i$, а поэтому $\{0, \lambda\} \not\subseteq B_i \oplus \lambda$ для каждого $i \in \{1, \dots, d\}$. Следовательно, существует такое $j \in \{1, \dots, d\}$, что $\lambda \in B_j \setminus (B_j \oplus \lambda)$. Из равенств (25), (32) получаем

$$\begin{aligned} ni_{g_{\{\gamma\}, \lambda}}(\mu_{\bar{B}}) &= (2^{2n} - 2^n)^{-1} \sum_{i=1}^d \sum_{\delta \in B_i \setminus (\{\lambda\} \cup (B_i \oplus \lambda))} c_\delta(\{\gamma\}, \lambda) \\ &= 4(2^{2n} - 2^n)^{-1} \sum_{i=1}^d |B_i \setminus (\{\lambda\} \cup (B_i \oplus \lambda))| \\ &= 2^{2-n}(2^n - 1)^{-1} \left(\sum_{i=1}^d |B_i \setminus (B_i \oplus \lambda)| - 1 \right). \end{aligned}$$

Для показателя $\mu_{\bar{B}}$ -неизометричности транспозиции приведем пример достижимости верхней оценки неравенства (31). Рассмотрим произвольный вектор $\lambda \in V_n^\times$ нечетного веса Хемминга и метрику Хемминга χ_n ($\mu_{\bar{B}} = \chi_n$), у которой

$$B_i = \{\alpha \in V_n \mid \|\alpha\| = i\} \text{ для } i = 1, \dots, n.$$

Легко видеть, что $B_i \cap (B_i \oplus \lambda) = \emptyset$ для $i = 1, \dots, n$. Поэтому для произвольной транспозиции $g_{\{\gamma\}, \lambda} = (\gamma, \gamma \oplus \lambda)$ справедливо равенство

$$ni_{g_{\{\gamma\}, \lambda}}(\chi_n) = 2^{2-n} - 2^{2-n}(2^n - 1)^{-1}.$$

Показатель χ_n -неизометричности таких транспозиций $g_{\{\gamma\}, \lambda}$ достигает наибольшего значения среди множества всех показателей χ_n -неизометричности транспозиций из $S(V_n)$.

5. Связь μ -неизометричности и $\mathbf{W}$ -примитивности

Укажем класс метрик из M_n^+ , задаваемых разбиением $\mathbf{W} = \{W_0, \dots, W_{2^n-d-1}\}$ пространства V_n , у которых показатель μ -неизометричности выражается через элементы матрицы $\mathbf{c}^{(\mathbf{W})}(g)$ для подстановки $g \in S(V_n)$. Напомним, что такие метрики уже упоминались в разделе 3. В данном разделе рассматриваются блоки разбиения $\mathbf{W}$, связанные между собой посредством алгебраических соотношений, в частности W_i — i -й смежный класс группы $(V_n, \oplus)$ по подгруппе

W_0 ($i = 0, \dots, 2^{n-d} - 1$). Такие метрики могут быть использованы при атаках на основе инвариантных подпространств (см., например, [13, 14]) или при атаках на основе усеченных разностей (см., например, [8]). Заметим, что при $d = 0$ возникают метрики из M_n^+ с наибольшей значностью (равной 2^n), рассмотренные в разделе 4, а при $d = n - 1$ – 3-значные метрики, некоторые из них рассматривались в [2, 3].

Утверждение 4. Пусть $\delta_0, \dots, \delta_{n-1}$ – базис пространства V_n , разбиение $\mathbf{W} = \{W_0, \dots, W_{2^{n-d}-1}\}$ пространства V_n таково, что:

- 1) $W_0 = \langle \delta_0, \dots, \delta_{d-1} \rangle$, $\dim W_0 = d$, $W_0 < V_n$,
- 2) W_i – i -й смежный класс группы $(V_n, \oplus)$ по подгруппе $(W_0, \oplus)$, причем

$$W_i = i_0 \delta_d \oplus i_1 \delta_{d+1} \oplus \dots \oplus i_{n-d-1} \delta_{n-1} \oplus W_0,$$

если $i = i_0 + 2i_1 + \dots + 2^{n-d-1}i_{n-d-1}$, где $i_0, i_1, \dots, i_{n-d-1} \in \{0, 1\}$ и $i \in \{1, \dots, 2^{n-d} - 1\}$.

Тогда функция $\mu : V_n^2 \rightarrow \{0, 1, \dots, 2^{n-d}\}$, заданная условием

$$\mu : (\alpha, \alpha') \mapsto j + 1, \text{ если } \alpha \oplus \alpha' \in W_j^\times, j \in \{0, 1, \dots, 2^{n-d} - 1\}, \quad (34)$$

является $(2^{n-d} + 1)$ -значной метрикой из M_n^+ и

$$\text{Isom}(\mu) = S_{2^d} \wr V_{n-d}^+.$$

Доказательство. Так как $\mu(\beta, \lambda) = \mu(\vec{0}_n, \beta \oplus \lambda)$ для всех $\beta, \lambda \in V_n$, то достаточно показать, что

$$\mu(\vec{0}_n, \lambda) \leq \mu(\vec{0}_n, \theta) + \mu(\vec{0}_n, \theta \oplus \lambda) \text{ для всех } \theta, \lambda \in V_n.$$

Пусть $\lambda \in W_i$, $\theta \in W_j$ для некоторых $i, j \in \{0, \dots, 2^{n-d} - 1\}$. Тогда

$$\mu(\vec{0}_n, \lambda) = i + 1, \mu(\vec{0}_n, \theta) = j + 1,$$

где

$$\lambda = i_0 \delta_d \oplus i_1 \delta_{d+1} \oplus \dots \oplus i_{n-d-1} \delta_{n-1} \oplus \lambda_0,$$

$$\theta = j_0 \delta_d \oplus j_1 \delta_{d+1} \oplus \dots \oplus j_{n-d-1} \delta_{n-1} \oplus \theta_0$$

для некоторых $i_t, j_t \in \{0, 1\}$ при $t = 0, \dots, n - d - 1$ и $\lambda_0, \theta_0 \in W_0$.

Так как

$$\theta \oplus \lambda = (i_0 \oplus j_0) \delta_d \oplus (i_1 \oplus j_1) \delta_{d+1} \oplus \dots \oplus (i_{n-d-1} \oplus j_{n-d-1}) \delta_{n-1} \oplus \lambda_0 \oplus \theta_0,$$

то $\lambda_0 \oplus \delta_0 \in W_0$ и $\theta \oplus \lambda \in W_c$, где

$$c = (i_0 \oplus j_0) + (i_1 \oplus j_1)2 + \dots + (i_{n-d-1} \oplus j_{n-d-1})2^{n-d-1}.$$

Очевидно, что

$$2^t i_t \leq 2^t ((i_t \oplus j_t) + j_t) \text{ для } t = 0, \dots, n-d-1.$$

Отсюда следует неравенство $i \leq j + c$, т. е.

$$\mu(\vec{0}_n, \lambda) \leq \mu(\vec{0}_n, \theta) + \mu(\vec{0}_n, \theta \oplus \lambda).$$

Пусть $g \in \text{Isom}(\mu)$. Если $\alpha, \alpha' \in V_n$ таковы, что $\alpha \oplus \alpha' \in W_i$, то справедливо включение

$$\alpha^g \oplus (\alpha')^g \in W_i,$$

равносильное равенству

$$(\beta \oplus W_i)^g = \beta^g \oplus W_i \text{ для каждого } \beta \in V_n, \quad (35)$$

где $i = 0, \dots, 2^{n-d}-1$. Следовательно, $\text{Isom}(\mu)$ – импримитивная группа с системой импримитивности $\mathbf{W}$.

Пусть $\varphi_{\mathbf{W}} : \text{Isom}(\mu) \rightarrow S(\{0, \dots, 2^{n-d}-1\})$ – естественный гомоморфизм импримитивной группы с системой импримитивности $\mathbf{W}$. При $\beta = \vec{0}_n$ из равенства (35) следуют соотношения $W_i^g = \vec{0}_n^g \oplus W_i$ для $i = 0, \dots, 2^{n-d}-1$. Поэтому $\text{Im}(\varphi_{\mathbf{W}}) = V_{n-d}^+$.

Так как W_i – i -й смежный класс группы $(V_n, \oplus)$ по W_0 , то из равенства (35) и условия $W_0^g = W_0$ следуют равенства

$$W_i^g = W_i \text{ для каждого } i \in \{1, \dots, 2^{n-d}-1\}.$$

Поэтому $g \in \text{Ker}(\varphi_{\mathbf{W}})$ тогда и только тогда, когда $W_0^g = W_0$. Таким образом, $\text{Isom}(\mu) = S_{2^d} \wr V_{n-d}^+$.

Заметим, что $\text{IG}_{\mathbf{W}} = S_{2^d} \wr S_{2^{n-d}}$ для разбиения

$$\mathbf{W} = \{W_0, \dots, W_{2^{n-d}-1}\}, |W_0| = \dots = |W_{2^{n-d}-1}| = 2^d,$$

приведенного в условии утверждения 4, а $\text{Isom}(\mu) = S_{2^d} \wr V_{n-d}^+$.

Для метрики μ , заданной условием (34), выразим показатель μ -неизометричности через элементы матрицы $\mathbf{c}^{(\mathbf{W})}(g)$.

Утверждение 5. Пусть $d \in \{1, \dots, n-1\}$, разбиение $\mathbf{W} = \{W_0, \dots, W_{2^{n-d}-1}\}$ пространства V_n таково, что:

- 1) Выполнены условия 1, 2 утверждения 4.
- 2) Отображение $v : \{0, \dots, 2^{n-d} - 1\}^2 \rightarrow \{0, \dots, 2^{n-d} - 1\}$ задано условием $v : (i, j) \mapsto v(i, j)$, если $W_i \oplus W_j = W_{v(i,j)}$.
- 3) Функция $\mu : V_n^2 \rightarrow \{0, \dots, 2^{n-d}\}$ задана условием (34).

Тогда

$$\begin{aligned} ni_g(\mu) &= 1 + (2^n - 1)^{-1} \\ &\quad - (2^{2n} - 2^n)^{-1} \sum_{i=0}^{2^{n-d}-1} \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} c_{v(i,j),t}^{(\mathbf{W})}(g) c_{j,v(t,i)}^{(\mathbf{W})}(g). \end{aligned} \quad (36)$$

Доказательство. Очевидно, что для каждого $i \in \{0, \dots, 2^{n-d} - 1\}$ выполняется равенство

$$\begin{aligned} &|\{(\alpha, \varepsilon) \in V_n \times W_i^\times | (\alpha \oplus \varepsilon)^g \oplus \alpha^g \in W_i^\times\}| \\ &= \sum_{j=0}^{2^{n-d}-1} |\{(\alpha, \varepsilon) \in W_j \times W_i^\times | (\alpha \oplus \varepsilon)^g \oplus \alpha^g \in W_i^\times\}|. \end{aligned} \quad (37)$$

Для всех $i, j \in \{0, \dots, 2^{n-d} - 1\}$, $i \neq 0$, справедливо равенство

$$\begin{aligned} &|\{(\alpha, \varepsilon) \in W_j \times W_i | (\alpha \oplus \varepsilon)^g \in \alpha^g \oplus W_i\}| \\ &= \sum_{t=0}^{2^{n-d}-1} |W_{v(i,j)}^g \cap W_t| \cdot |\{\alpha \in W_j | W_t = \alpha^g \oplus W_i\}| \\ &= \sum_{t=0}^{2^{n-d}-1} |W_{v(i,j)}^g \cap W_t| \cdot |W_j^g \cap W_{v(t,i)}| \\ &= \sum_{t=0}^{2^{n-d}-1} c_{v(i,j),t}^{(\mathbf{W})}(g) c_{j,v(t,i)}^{(\mathbf{W})}(g). \end{aligned} \quad (38)$$

Если же $i = 0$, то для каждого $j \in \{0, \dots, 2^{n-d} - 1\}$ имеем

$$\begin{aligned} &|\{(\alpha, \varepsilon) \in W_j \times W_0^\times | (\alpha \oplus \varepsilon)^g \in \alpha^g \oplus W_0\}| \\ &= \sum_{t=0}^{2^{n-d}-1} |\{(\alpha, \varepsilon) \in (W_j \cap W_t^{g^{-1}}) \times W_0^\times | (\alpha \oplus \varepsilon)^g \in W_t\}| \\ &= \sum_{t=0}^{2^{n-d}-1} |W_j^g \cap W_t| \cdot (|W_j^g \cap W_t| - 1) = \sum_{t=0}^{2^{n-d}-1} c_{j,t}^{(\mathbf{W})}(g) (c_{j,t}^{(\mathbf{W})}(g) - 1) \\ &= \sum_{t=0}^{2^{n-d}-1} (c_{j,t}^{(\mathbf{W})}(g))^2 - \sum_{t=0}^{2^{n-d}-1} c_{j,t}^{(\mathbf{W})}(g) = \sum_{t=0}^{2^{n-d}-1} (c_{j,t}^{(\mathbf{W})}(g))^2 - 2^d. \end{aligned} \quad (39)$$

Заметим, что в равенстве (39) учтено следующее:

1) $v(0, j) = v(j, 0) = j$.

2) Если $\varepsilon = 0$, то из условия $\alpha \in W_j \cap W_t^{g^{-1}}$ следует включение $(\alpha \oplus \varepsilon)^g \in W_t$ для любых $t, j \in \{0, \dots, 2^{n-d} - 1\}$.

Из равенств (37), (38), (39) получаем, что

$$\hat{p}_{W_i^\times, W_i^\times}(g) = 2^{-n} \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} c_{v(i,j),t}^{(\mathbf{W})}(g) c_{j,v(t,i)}^{(\mathbf{W})}(g) - \mathbf{I}(i=0),$$

где $i = 0, \dots, 2^{n-d} - 1$.

Отсюда и из равенства (3) получаем равенство

$$\begin{aligned} ni_g(\mu) &= 1 - (2^n - 1)^{-1} \sum_{i=0}^{2^{n-d}-1} \hat{p}_{W_i^\times, W_i^\times}(g) \\ &= 1 + (2^n - 1)^{-1} - (2^{2n} - 2^n)^{-1} \sum_{i=0}^{2^{n-d}-1} \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} c_{v(i,j),t}^{(\mathbf{W})}(g) c_{j,v(t,i)}^{(\mathbf{W})}(g). \end{aligned}$$

В следующей лемме дается «более компактная» запись равенства (36).

Лемма 8. Пусть метрика $\mu \in M_n^+$ задана условием (34). Тогда для каждой подстановки $g \in S(V_n)$ справедливо равенство

$$ni_g(\mu) = 1 + (2^n - 1)^{-1} - (2^{2n} - 2^n)^{-1} \sum_{i=0}^{2^{n-d}-1} \left(q_i^{(\mathbf{W})}(g) \right)^2, \quad (40)$$

где

$$q_t^{(\mathbf{W})}(g) = \sum_{j=0}^{2^{n-d}-1} c_{j,j \oplus t}^{(\mathbf{W})}(g) \text{ для } t = 0, \dots, 2^{n-d} - 1.$$

Доказательство. Из утверждений 4, 5 следует, что для всех $i, j \in \{0, \dots, 2^{n-d} - 1\}$ справедливо равенство $W_i \oplus W_j = W_{i \oplus j}$. Поэтому функция $v : \{0, \dots, 2^{n-d} - 1\}^2 \rightarrow \{0, \dots, 2^{n-d} - 1\}$ задана условием

$v : (i, j) \mapsto i \oplus j$. Тогда

$$\begin{aligned}
 & \sum_{i=0}^{2^{n-d}-1} \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} c_{i \oplus j, t}^{(\mathbf{W})}(g) c_{j, t \oplus i}^{(\mathbf{W})}(g) \\
 &= \sum_{a=0}^{2^{n-d}-1} \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} c_{a, t}^{(\mathbf{W})}(g) c_{j, j \oplus t \oplus a}^{(\mathbf{W})}(g) \\
 &= \sum_{a=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} c_{a, t}^{(\mathbf{W})}(g) \sum_{j=0}^{2^{n-d}-1} c_{j, j \oplus t \oplus a}^{(\mathbf{W})}(g) \\
 &= \sum_{a=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} c_{a, t}^{(\mathbf{W})}(g) q_{a \oplus t}^{(\mathbf{W})}(g) \\
 &= \sum_{i=0}^{2^{n-d}-1} q_i^{(\mathbf{W})}(g) \sum_{a=0}^{2^{n-d}-1} c_{a, a \oplus i}^{(\mathbf{W})}(g) = \sum_{i=0}^{2^{n-d}-1} \left(q_i^{(\mathbf{W})}(g) \right)^2.
 \end{aligned}$$

Отсюда и из (36) получаем

$$ni_g(\mu) = 1 + (2^n - 1)^{-1} - (2^{2n} - 2^n)^{-1} \sum_{i=0}^{2^{n-d}-1} \left(q_i^{(\mathbf{W})}(g) \right)^2.$$

Для показателя μ -неизометричности метрики μ , заданной условием (34), получим оценку сверху.

Утверждение 6. Пусть $\mathbf{W} = \{W_0, \dots, W_{2^{n-d}-1}\}$ – разбиение пространства V_n , $|W_0| = \dots = |W_{2^{n-d}-1}| = 2^d$ и метрика $\mu : V_n^2 \rightarrow \{0, \dots, 2^{n-d}\}$ задана условием

$$\mu : (\alpha, \alpha') \mapsto i + 1, \text{ если } \alpha \oplus \alpha' \in W_i^\times, i \in \{0, \dots, 2^{n-d} - 1\}.$$

Тогда:

1) Для каждой подстановки $g \in S(V_n)$ справедливо неравенство

$$ni_g(\mu) \leq 1 - (2^d - 1)(2^n - 1)^{-1}.$$

2) Равенство

$$ni_g(\mu) = 1 - (2^d - 1)(2^n - 1)^{-1} \quad (41)$$

достигается тогда и только тогда, когда

$$\sum_{j=0}^{2^{n-d}-1} c_{j, j \oplus t}^{(\mathbf{W})}(g) = 2^d, t = 0, \dots, 2^{n-d} - 1.$$

3) Если при $d \geq n/2$ подстановка $g \in S(V_n)$ находится на максимальном расстоянии от группы $\text{IG}_{\mathbf{W}}$, равно $2^n - 2^{\max\{d, n-d\}}$, то справедливо равенство (40).

Доказательство. Из равенства (39) следует, что

$$ni_g(\mu) = 1 + (2^n - 1)^{-1} - (2^{2n} - 2^n)^{-1} \sum_{i=0}^{2^{n-d}-1} \left(q_i^{(\mathbf{W})}(g) \right)^2,$$

где

$$q_t^{(\mathbf{W})}(g) = \sum_{j=0}^{2^{n-d}-1} c_{j, j \oplus t}^{(\mathbf{W})}(g) \text{ для } t = 0, \dots, 2^{n-d} - 1.$$

Так как $(j, j \oplus t) \neq (j, j \oplus t')$ для всех $t, j, j' \in \{0, \dots, 2^{n-d} - 1\}$, $j \neq j'$, то

$$\sum_{t=0}^{2^{n-d}-1} q_t^{(\mathbf{W})}(g) = 2^n. \quad (42)$$

Очевидно, что если $y \in \mathbb{R}^+$ и $\sum_{i=0}^{m-1} x_i = y$, $0 \leq x_i \leq y$, то

$$\min \left\{ \sum_{i=0}^{m-1} x_i^2 \mid 0 \leq x_i \leq y, i = 0, \dots, m-1 \right\} = y^2/m,$$

при этом $\sum_{i=0}^{m-1} x_i^2 = y^2/m$ тогда и только тогда, когда

$$x_0 = \dots = x_{m-1} = y/m.$$

Отсюда и из равенства (42) следует, что

$$\sum_{i=0}^{2^{n-d}-1} \left(q_i^{(\mathbf{W})}(g) \right)^2 \geq 2^{n+d},$$

причем равенство $\sum_{i=0}^{2^{n-d}-1} \left(q_i^{(\mathbf{W})}(g) \right)^2 = 2^{n+d}$ выполняется тогда и только тогда, когда $q_t^{(\mathbf{W})}(g) = 2^d$ для $t = 0, \dots, 2^{n-d} - 1$.

Таким образом,

$$ni_g(\mu) = 1 + (2^n - 1)^{-1}$$

$$-(2^{2n} - 2^n)^{-1} \sum_{i=0}^{2^{n-d}-1} \left(q_i^{(\mathbf{W})}(g) \right)^2 \leq 1 - (2^d - 1)(2^n - 1)^{-1}.$$

Если $d \geq n/2$, то согласно утверждению 5 [5]

$$\chi_{\mathbf{W}}(g) \leq 2^n - 2^d$$

для каждой подстановки $g \in S(V_n)$, причем равенство $\chi_{\mathbf{W}}(g) = 2^n - 2^d$ имеет место тогда и только тогда, когда элементы матрицы $\mathbf{c}^{(\mathbf{W})}(g) = \left[\left[c_{i,j}^{(\mathbf{W})}(g) \right] \right]$ равны $c_{i,j}^{(\mathbf{W})}(g) = 2^{2d-n}$ для $i, j = 0, \dots, 2^{n-d} - 1$. Отсюда и из равенства (40) получаем

$$ni_g(\mu) = 1 + (2^n - 1)^{-1} - 2^{3(n-d)+4d-2n} (2^{2n} - 2^n)^{-1} = 1 - (2^d - 1)(2^n - 1)^{-1}.$$

Для $d < n/2$ приведем пример того, что для метрики μ на V_n , заданной условием (34), существует подстановка $b \in S(V_n)$, находящаяся на максимальном расстоянии от группы $\text{IG}_{\mathbf{W}}$, равно $2^n - 2^{\max\{d, n-d\}}$ (см утверждение 5 [5]), у которой показатель μ -неизометричности удовлетворяет неравенству

$$ni_b(\mu) < 1 - (2^d - 1)(2^n - 1)^{-1}.$$

Пусть $n \geq 4$, $d = 1$, $\mathbf{W} = \{W_0, \dots, W_{2^{n-1}-1}\}$ – разбиение пространства V_n , $|W_0| = \dots = |W_{2^{n-1}-1}| = 2$. Рассмотрим матрицу $\mathbf{c}^{(\mathbf{W})}(b) = \left[\left[c_{i,j}^{(\mathbf{W})}(b) \right] \right]$, элементы которой заданы условием

$$c_{i,j}^{(\mathbf{W})}(b) = \begin{cases} 1, & \text{если } j \in \{i+1, i+2\}, i \notin \{1, 2, 2^{n-1}-2, 2^{n-1}-1\}, \\ 1, & \text{если } i = 1, j \in \{0, 2\} \text{ или } i = 2, j \in \{0, 1\}, \\ 1, & \text{если } i = 2^{n-1}-2, j \in \{3, 2^{n-1}-1\}, \\ 1, & \text{если } i = 2^{n-1}-1, j \in \{3, 4\}, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Ясно, что $\sum_{j=0}^{2^{n-1}-1} c_{j,j}^{(\mathbf{W})}(b) = 0$. Поэтому согласно п. 2 утверждения 6

$$ni_b(\mu) < 1 - (2^n - 1)^{-1}, \quad (43)$$

т.е. в п. 1 утверждения 6 имеет место строгое неравенство.

Как отмечалось выше, частным случаем натуральных метрик, удовлетворяющих утверждению 4, являются 3-значные. Далее для 3-значной подметрики метрики, описанной в утверждении 6, найдем показатель μ -неизометричности.

Утверждение 7. Для каждой 3-значной метрики $\mu \in M_n^+$ существует такое подмножество $W_0 \subset V_n$, $\vec{0}_n \in W_0$, что метрика μ задана условием

$$\mu : (\alpha, \alpha') \mapsto \begin{cases} 1, & \text{если } \alpha \oplus \alpha' \in W_0^\times, \\ 2, & \text{если } \alpha \oplus \alpha' \in V_n/W_0. \end{cases} \quad (44)$$

Показатель μ -неизометричности равен

$$ni_g(\mu) = 1 - (2^n - 1)^{-1} \left(2^n - 2^{d+1} + 1 + 2\hat{p}_{W_0^\times, W_0^\times}(g) \right). \quad (45)$$

Кроме того, если $W_0 < V_n$, $d = \dim W_0$, W_i — i -й смежный класс группы $(V_n, \oplus)$ по $(W_0, \oplus)$ для $i = 0, \dots, 2^{n-d} - 1$, $\mathbf{W} = \{W_0, \dots, W_{2^{n-d}-1}\}$, то $\text{Isom}(\mu) = S_{2^d} \wr S_{2^{n-d}}$ и

$$ni_g(\mu) = (2^{2n-1} - 2^{n-1})^{-1} \left(2^{d+n} - \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} \left(c_{j,t}^{(\mathbf{W})}(g) \right)^2 \right). \quad (46)$$

Доказательство. Пусть $U = V_n^\times/W_0$. Из утверждения 1 следует, что

$$ni_g(\mu) = 1 - (2^n - 1)^{-1} \left(\hat{p}_{U, U}(g) + \hat{p}_{W_0^\times, W_0^\times}(g) \right).$$

Обозначим

$$a_1 = \left| \{(\alpha, \varepsilon) \in V_n \times (V_n^\times \setminus W_0) \mid (\alpha \oplus \varepsilon)^g \notin \alpha^g \oplus W_0\} \right|,$$

$$a_2 = \left| \{(\alpha, \varepsilon) \in V_n \times W_0^\times \mid (\alpha \oplus \varepsilon)^g \notin \alpha^g \oplus W_0\} \right|,$$

$$a_3 = \left| \{(\alpha, \varepsilon) \in V_n \times W_0^\times \mid (\alpha \oplus \varepsilon)^g \in \alpha^g \oplus W_0\} \right|.$$

Заметим, что

$$a_1 + a_2 = 2^{2n} - 2^{n+d}, a_3 + a_2 = 2^{n+d} - 2^n.$$

Отсюда следует, что

$$a_1 = 2^{2n} - 2^{n+d} - 2^{n+d} + 2^n + a_3.$$

Поэтому

$$\begin{aligned}\hat{p}_{U,U}(g) &= 2^{-n} a_1 = 2^{-n} (2^{2n} - 2^{n+d+1} + 2^n + a_3) \\ &= 2^n - 2^{d+1} + 1 + \hat{p}_{W_0^\times, W_0^\times}(g).\end{aligned}$$

Таким образом,

$$\begin{aligned}ni_g(\mu) &= 1 - (2^n - 1)^{-1} \left(\hat{p}_{U,U}(g) + \hat{p}_{W_0^\times, W_0^\times}(g) \right) \\ &= 1 - (2^n - 1)^{-1} \left(2^n - 2^{d+1} + 1 + 2\hat{p}_{W_0^\times, W_0^\times}(g) \right).\end{aligned}$$

Если $W_0 < V_n$, то из равенств (38), (39) имеем

$$\begin{aligned}ni_g(\mu) &= 1 \\ &- (2^{2n} - 2^n)^{-1} \left(2^{2n} - 2^n - 2^{d+1+n} + 2 \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} \left(c_{j,t}^{(\mathbf{W})}(g) \right)^2 \right) \\ &= (2^{2n-1} - 2^{n-1})^{-1} \left(2^{d+n} - \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} \left(c_{j,t}^{(\mathbf{W})}(g) \right)^2 \right).\end{aligned}$$

Покажем, что $\text{Isom}(\mu) = S_{2^d} \wr S_{2^{n-d}}$. Пусть $g \in \text{Isom}(\mu)$. Тогда для всех $\alpha, \alpha' \in V_n$, удовлетворяющих условию $\alpha \oplus \alpha' \in W_0$, справедливо включение $\alpha^g \oplus \alpha'^g \in W_0$, которое равносильно равенству $(\beta \oplus W_0)^g = \beta^g \oplus W_0$ для каждого $\beta \in V_n$. Отсюда вытекает равенство $\text{Isom}(\mu) = S_{2^d} \wr S_{2^{n-d}}$.

Очевидно, что для любых $g \in S(V_n)$, $W_0 \subset V_n$ справедливо равенство

$$ni_g \left(\mu_{(W_0^\times, V_n/W_0)} \right) = ni_g \left(\mu_{(V_n/W_0, W_0^\times)} \right).$$

Следствие 3. Пусть $W_0 < V_n$, $d = \dim W_0$, W_i – i -й смежный класс группы $(V_n, \oplus)$ по W_0 для $i = 0, \dots, 2^{n-d} - 1$, $\mathbf{W} = \{W_0, \dots, W_{2^{n-d}-1}\}$, а метрика $\mu \in M_n^+$ задана условием

$$\mu : (\alpha, \alpha') \mapsto \begin{cases} 1, & \text{если } \alpha \oplus \alpha' \in W_0^\times, \\ 2, & \text{если } \alpha \oplus \alpha' \in V_n/W_0. \end{cases}$$

Тогда

$$ni_g(\mu) \leq \begin{cases} (2^n - 1)^{-1} (2^{d+1} - 2), & \text{если } d < n/2, \\ (2^n - 1)^{-1} 2^{2d-n+1} (2^{n-d} - 1), & \text{если } d \geq n/2. \end{cases}$$

Кроме того,

1) если $d < n/2$, то

$$ni_g(\mu) = (2^n - 1)^{-1} (2^{d+1} - 2)$$

тогда и только тогда, когда в каждой строке матрицы $\mathbf{c}^{(\mathbf{W})}(g)$ ровно 2^d элементов равны 1, остальные – 0,

2) если $d \geq n/2$, то

$$ni_g(\mu) = (2^n - 1)^{-1} 2^{2d-n+1} (2^{n-d} - 1)$$

тогда и только тогда, когда $c_{i,j}^{(\mathbf{W})}(g) = 2^{2d-n}$ для всех $i, j \in \{0, \dots, 2^{n-d} - 1\}$.

Доказательство. Из утверждения 7 следует, что

$$ni_g(\mu) = (2^{2n-1} - 2^{n-1})^{-1} \left(2^{d+n} - \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} \left(c_{j,t}^{(\mathbf{W})}(g) \right)^2 \right).$$

Очевидно, что если $y \in \mathbb{R}^+$ и $\sum_{i=0}^{m-1} x_i = y$, $0 \leq x_i \leq y$, то

$$\min \left\{ \sum_{i=0}^{m-1} x_i^2 \mid 0 \leq x_i \leq y, i = 0, \dots, m-1 \right\} = y^2/m,$$

при этом $\sum_{i=0}^{m-1} x_i^2 = y^2/m$ тогда и только тогда, когда

$$x_0 = \dots = x_{m-1} = y/m.$$

Кроме того,

$$\sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} c_{j,t}^{(\mathbf{W})}(g) = 2^n.$$

Если $d < n/2$, то подстановка $g \in S(V_n)$ в метрике Хемминга находится на максимальном расстоянии $2^n - 2^{n-d}$ от группы $\text{IG}_{\mathbf{W}}$, если в каждой строке ровно 2^d элементов равны 1, остальные – 0. Поэтому

$$ni_g(\mu) = (2^{2n-1} - 2^{n-1})^{-1} (2^{d+n} - 2^d 2^{n-d}) = (2^n - 1)^{-1} (2^{d+1} - 2).$$

Если $d \geq n/2$, то подстановка $g \in S(V_n)$ в метрике Хемминга находится на максимальном расстоянии $2^n - 2^d$ от группы $\text{IG}_{\mathbf{W}}$, при этом $c_{i,j}^{(\mathbf{W})}(g) = 2^{2d-n}$ для $i, j = 0, \dots, 2^{n-d} - 1$. В этом случае

$$\begin{aligned} ni_g(\mu) &= (2^{2n-1} - 2^{n-1})^{-1} \left(2^{d+n} - \sum_{j=0}^{2^{n-d}-1} \sum_{t=0}^{2^{n-d}-1} 2^{4d-2n} \right) \\ &= (2^{2n-1} - 2^{n-1})^{-1} (2^{d+n} - 2^{4d-2n+2(n-d)}) \\ &= (2^{2n-1} - 2^{n-1})^{-1} 2^{2d} (2^{n-d} - 1) \\ &= (2^n - 1)^{-1} 2^{2d-n+1} (2^{n-d} - 1). \end{aligned}$$

Для $i = 0, 1$ положим $V_n^{(i)} = \{\alpha \in V_n \mid \|\alpha\| \equiv i \pmod{2}\}$.

Следствие 4. Пусть $\mathbf{W} = \left\{ \left(V_n^{(0)} \right)^\times, V_n^{(1)} \right\}$ и 3-значная метрика $\mu: V_n^2 \rightarrow \{0, 1, 2\}$ задана условием

$$\mu: (\alpha, \alpha') \mapsto \begin{cases} 1, & \text{если } \alpha \oplus \alpha' \in \left(V_n^{(0)} \right)^\times, \\ 2, & \text{если } \alpha \oplus \alpha' \in V_n^{(1)}. \end{cases}$$

Тогда $\text{Isom}(\mu) = S_{2^{n-1}} \wr S_2$ и для каждой подстановки $g \in S(V_n)$ справедливо равенство

$$ni_g(\mu) = (2^{2n-2} - 2^{n-2})^{-1} \left(2^{2n-2} - \left(c_{0,0}^{(\mathbf{W})}(g) \right)^2 - \left(c_{0,1}^{(\mathbf{W})}(g) \right)^2 \right).$$

Доказательство. В условиях утверждения 7 имеем $d = n - 1$, $W_0 = V_n^{(0)}$, $W_1 = V_n^{(1)}$. Заметим, что

$$c_{j,0}^{(\mathbf{W})}(g) + c_{j,1}^{(\mathbf{W})}(g) = c_{0,j}^{(\mathbf{W})}(g) + c_{1,j}^{(\mathbf{W})}(g) = 2^{n-1}$$

для $j = 0, 1$. Отсюда следует, что

$$c_{0,0}^{(\mathbf{W})}(g) = c_{1,1}^{(\mathbf{W})}(g), c_{0,1}^{(\mathbf{W})}(g) = c_{1,0}^{(\mathbf{W})}(g).$$

Так как $V_n^{(0)} < V_n$, то из равенства (46) получаем, что

$$\begin{aligned} ni_g(\mu) &= (2^{2n-1} - 2^{n-1})^{-1} \\ &\times \left(2^{2n-1} - \left(c_{0,0}^{(\mathbf{W})}(g) \right)^2 - \left(c_{0,1}^{(\mathbf{W})}(g) \right)^2 - \left(c_{1,0}^{(\mathbf{W})}(g) \right)^2 - \left(c_{1,1}^{(\mathbf{W})}(g) \right)^2 \right) \\ &= (2^{2n-1} - 2^{n-1})^{-1} \left(2^{2n-1} - 2 \left(c_{0,0}^{(\mathbf{W})}(g) \right)^2 - 2 \left(c_{0,1}^{(\mathbf{W})}(g) \right)^2 \right) \\ &= (2^{2n-2} - 2^{n-2})^{-1} \left(2^{2n-2} - \left(c_{0,0}^{(\mathbf{W})}(g) \right)^2 - \left(c_{0,1}^{(\mathbf{W})}(g) \right)^2 \right). \end{aligned}$$

Из утверждения 7 вытекает равенство $\text{Isom}(\mu) = S_{2^{n-1}} \wr S_2$.

Согласно [3] равенство $\text{Isom}(\mu) = S_{2^{n-1}} \wr S_2$ справедливо и для 3-значной метрики $\mu_{(V_n/W_0, W_0^\times)} \in M_n^+$, свойства которой описаны в [2] как подметрики метрики Хемминга. Очевидно, что $\mu_{(W_0^\times, V_n/W_0)} \in M_n^+$.

Укажем теперь для метрики $\mu \in \left\{ \mu_{(W_0^\times, V_n/W_0)}, \mu_{(V_n/W_0, W_0^\times)} \right\}$ оценку сверху показателя μ -неизометричности; она будет вытекать из следующего следствия.

Следствие 5. Пусть 3-значная метрика $\mu : V_n^2 \rightarrow \{0, 1, 2\}$ задана условием

$$\mu : (\alpha, \alpha') \mapsto \begin{cases} 1, & \text{если } \alpha \oplus \alpha' \in (V_n^{(0)})^\times, \\ 2, & \text{если } \alpha \oplus \alpha' \in V_n^{(1)}. \end{cases}$$

Тогда для каждой подстановки $g \in S(V_n)$ справедлива оценка

$$0 \leq ni_g(\mu) \leq 2^{n-1}(2^n - 1)^{-1}.$$

Кроме того, равенство $ni_g(\mu) = 2^{n-1}(2^n - 1)^{-1}$ достигается тогда и только тогда, когда

$$c_{0,0}^{(\mathbf{W})}(g) = c_{0,1}^{(\mathbf{W})}(g) = 2^{n-2}.$$

Доказательство вытекает из следствия 3 при $d = n - 1$.

Пусть $\mathbf{W} = \{V_n^{(1)}, V_n^{(0)}\}$. Согласно утверждению 5 [5] подстановка $g \in S(V_n)$ находится относительно метрики Хемминга на максимальном расстоянии от группы $\text{IG}_{\mathbf{W}}$, равном $\chi_{\mathbf{W}}(g) = 2^{n-1}$, если

$$c_{1,1}^{(\mathbf{W})}(g) = c_{2,2}^{(\mathbf{W})}(g) = c_{1,2}^{(\mathbf{W})}(g) = c_{2,1}^{(\mathbf{W})}(g) = 2^{n-2}.$$

Из следствия 5 вытекает, что если $\chi_{\mathbf{W}}(g) = 2^{n-1}$, то значение показателя $\mu_{(W_0^\times, V_n^\times/W_0)}$ -неизометричности для подстановки g максимально и равно $ni_g(\mu) = 2^{n-1}(2^n - 1)^{-1}$. Однако если $ni_g(\mu) = 2^{n-1}(2^n - 1)^{-1}$, то существуют такие подстановки $g \in S(V_n)$, что $\chi_{\mathbf{W}}(g) < 2^{n-1}$.

Для разбиения $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ множества V_n зададим отображение $\varphi^{(\mathbf{W})} : V_n \rightarrow \{0, \dots, r-1\}$ условием $\varphi^{(\mathbf{W})} : \beta \mapsto i$, если $\beta \in W_i$, где $i \in \{0, \dots, r-1\}$.

Следствие 6. Пусть 3-значная метрика $\mu : V_n^2 \rightarrow \{0, 1, 2\}$ задана условием

$$\mu : (\alpha, \alpha') \mapsto \begin{cases} 1, & \text{если } \alpha \oplus \alpha' = \vec{1}_n, \\ 2, & \text{если } \alpha \oplus \alpha' \notin \{\vec{0}_n, \vec{1}_n\}. \end{cases}$$

Тогда $\text{Isom}(\mu) = S_2 \wr S_{2^{n-1}}$ и для каждой подстановки $g \in S(V_n)$ справедливо равенство

$$ni_g(\mu) = 2(1 - \hat{p}_{\vec{1}_n, \vec{1}_n}(g))(2^n - 1)^{-1}. \quad (47)$$

Кроме того,

$$ni_g(\mu) = (2^{2n-2} - 2^{n-2})^{-1} \left(2^n - \sum_{\beta \in \{0\} \times V_{n-1}} c_{\beta, \varphi(\mathbf{W})(\beta g)}^{(\mathbf{W})}(g) \right),$$

где $W_\beta = \{\beta, \beta \oplus \vec{1}_n\}$ при $\beta \in \{0\} \times V_{n-1}$ и

$$\mathbf{W} = \{W_\beta | \beta \in \{0\} \times V_{n-1}\}.$$

Доказательство. При $d = 1$ из равенства (45) имеем

$$\begin{aligned} ni_g(\mu) &= 1 - (2^n - 1)^{-1} (2^n - 2^2 + 1 + 2\hat{p}_{\vec{1}_n, \vec{1}_n}(g)) \\ &= 2(1 - \hat{p}_{\vec{1}_n, \vec{1}_n}(g))(2^n - 1)^{-1}, \end{aligned}$$

а из утверждения 7 вытекает равенство $\text{Isom}(\mu) = S_2 \wr S_{2^{n-1}}$.

Заметим, что для каждого $\alpha \in V_n$ справедливо равенство

$$\begin{aligned} &\{\alpha, \alpha \oplus \vec{1}_n\}^g \cap \{\alpha^g, \alpha^g \oplus \vec{1}_n\} \\ &= \begin{cases} \{\alpha^g, \alpha^g \oplus \vec{1}_n\}, & \text{если } (\alpha \oplus \vec{1}_n)^g = \alpha^g \oplus \vec{1}_n, \\ \{\alpha^g\}, & \text{если } (\alpha \oplus \vec{1}_n)^g \neq \alpha^g \oplus \vec{1}_n. \end{cases} \end{aligned}$$

Поэтому для каждого блока $W_\beta \in \mathbf{W}$ имеем

$$c_{\beta, \varphi(\mathbf{W})(\beta g)}^{(\mathbf{W})}(g) = \begin{cases} 2, & \text{если } (\beta \oplus \vec{1}_n)^g = \beta^g \oplus \vec{1}_n, \\ 1, & \text{если } (\beta \oplus \vec{1}_n)^g \neq \beta^g \oplus \vec{1}_n. \end{cases}$$

Откуда следует равенство

$$\begin{aligned} & \left| \left\{ \alpha \in V_n \mid (\alpha \oplus \vec{1}_n)^g \oplus \alpha^g = \vec{1}_n \right\} \right| \\ &= 2 \sum_{\beta \in \{0\} \times V_{n-1}} (c_{\beta, \varphi(\mathbf{W})(\beta g)}^{(\mathbf{W})}(g) - 1) = 2 \sum_{\beta \in \{0\} \times V_{n-1}} c_{\beta, \varphi(\mathbf{W})(\beta g)}^{(\mathbf{W})}(g) - 2^n. \end{aligned}$$

Поэтому

$$\hat{p}_{\vec{1}_n, \vec{1}_n}(g) = 2^{1-n} \left(\sum_{\beta \in \{0\} \times V_{n-1}} c_{\beta, \varphi(\mathbf{w})_{(\beta g)}}^{(\mathbf{w})}(g) \right) - 1.$$

Отсюда и из равенства (47) имеем

$$\begin{aligned} ni_g(\mu) &= 2(1 - \hat{p}_{\vec{1}_n, \vec{1}_n}(g))(2^n - 1)^{-1} \\ &= 2 \left(2 - 2^{1-n} \left(\sum_{\beta \in \{0\} \times V_{n-1}} c_{\beta, \varphi(\mathbf{w})_{(\beta g)}}^{(\mathbf{w})}(g) \right) \right) (2^n - 1)^{-1} \\ &= (2^{2n-2} - 2^{n-2})^{-1} \left(2^n - \sum_{\beta \in \{0\} \times V_{n-1}} c_{\beta, \varphi(\mathbf{w})_{(\beta g)}}^{(\mathbf{w})}(g) \right). \end{aligned}$$

Очевидно, что справедливо равенство

$$ni_g(\mu_{(\{\vec{1}_n\}, V_n^\times \setminus \{\vec{1}_n\})}) = ni_g(\mu_{(V_n^\times \setminus \{\vec{1}_n\}, \{\vec{1}_n\})}).$$

Заметим, что свойства метрики $\mu_{(\{V_n^\times \setminus \{\vec{1}_n\}\}, \{\vec{1}_n\})}$, являющейся подметрикой метрики Хемминга, описаны в [2].

Для метрики $\mu \in \left\{ \mu_{(\{\vec{1}_n\}, V_n^\times \setminus \{\vec{1}_n\})}, \mu_{(V_n^\times \setminus \{\vec{1}_n\}, \{\vec{1}_n\})} \right\}$ приведем оценку сверху показателя μ -неизометричности.

Следствие 7. Пусть 3-значная метрика $\mu : V_n^2 \rightarrow \{0, 1, 2\}$ задана условием

$$\mu : (\alpha, \alpha') \mapsto \begin{cases} 1, & \text{если } \alpha \oplus \alpha' = \vec{1}_n, \\ 2, & \text{если } \alpha \oplus \alpha' \notin \{\vec{0}_n, \vec{1}_n\}. \end{cases}$$

Тогда для каждой подстановки $g \in S(V_n)$ справедлива оценка

$$0 \leq ni_g(\mu) \leq 2(2^n - 1)^{-1}.$$

Кроме того, равенство $ni_g(\mu) = 2(2^n - 1)^{-1}$ достигается тогда и только тогда, когда $\hat{p}_{\vec{1}_n, \vec{1}_n}(g) = 0$.

Доказательство непосредственно следует из равенства (47).

Для метрики $\mu_{(\{\vec{1}_n\}, V_n^\times \setminus \{\vec{1}_n\})}$ укажем связь между подстановками, находящимися относительно метрики Хемминга на максимальном расстоянии от группы $IG_{\mathbf{w}}$, и подстановками, для которых показатель $\mu_{(\{\vec{1}_n\}, V_n^\times \setminus \{\vec{1}_n\})}$ -неизометричности принимает наибольшее значение.

Следствие 8. Пусть $\mathbf{W} = \left\{ \left\{ \beta, \beta \oplus \vec{1}_n \right\} \mid \beta \in V_n \right\}$ и $g \in S(V_n)$.

- 1) Тогда и только тогда подстановка g находится относительно метрики Хемминга на максимальном расстоянии от группы $\text{IG}\mathbf{W}$, равном 2^{n-1} , когда $\hat{p}_{\vec{1}_n, \vec{1}_n}(g) = 0$.
- 2) Условия $\chi_{\mathbf{W}}(g) = 2^{n-1}$ и $ni_g(\mu) = 2(2^n - 1)^{-1}$ равносильны.

Доказательство. Согласно утверждению 6 [5] справедливо неравенство $\chi_{\mathbf{W}}(g) \leq 2^{n-1}$, причем $\chi_{\mathbf{W}}(g) = 2^{n-1}$ тогда и только тогда, когда элементы матрицы $\mathbf{c}^{(\mathbf{W})}(g) = \left(c_{\beta, \gamma}^{(\mathbf{W})}(g) \right)$ равны

$$c_{\beta, \gamma}^{(\mathbf{W})}(g) = \begin{cases} 1, & \text{если } \beta^g \in \left\{ \gamma, \gamma \oplus \vec{1}_n \right\}, \\ 0, & \text{если } \beta^g \notin \left\{ \gamma, \gamma \oplus \vec{1}_n \right\}, \end{cases}$$

где $\beta, \gamma \in \{0\} \times V_{n-1}$. Отсюда и из равенства (38) вытекает условие $\hat{p}_{\vec{1}_n, \vec{1}_n}(g) = 0$. Из равенства (47) имеем

$$ni_g(\mu) = 2(2^n - 1)^{-1} \text{ при } \hat{p}_{\vec{1}_n, \vec{1}_n}(g) = 0.$$

Таким образом, для метрики μ , приведенной в условии утверждения 5, максимальное значение показателя μ -неизометричности $ni_g(\mu)$ достигается для тех и только тех подстановок $g \in S(V_n)$, для которых максимально значение $\chi_{\mathbf{W}}$ (такие подстановки в [5] названы **W**-примитивными).

На основе 3-значных метрик в следствиях 5, 8 указаны различные связи между **W**-примитивными подстановками и подстановками с максимальным значением показателя μ -неизометричности $ni_g(\mu)$. Так, рассмотрены следующие случаи.

- 1) **W**-примитивность подстановки равносильна максимальности значения показателя μ -неизометричности (следствие 8).
- 2) Из максимальности значения показателя μ -неизометричности подстановки не следует ее **W**-примитивность (следствие 5).

Список литературы

- [1] Dixon J., Mortimer B., *Permutation groups*, Carleton Univ., 1996, 346 pp.
- [2] Погорелов Б. А., “Подметрики метрики Хемминга и теорема А.А. Маркова”, *Труды по дискретной математике*, **9**, М.: Гелиос АРВ, 2006, 190–219.
- [3] Погорелов Б. А., Пудовкина М.А., “Подметрики Хемминга и их группы изометрий”, *Труды по дискретной математике*, **11:2** (2008), 147–191.
- [4] Пудовкина М. А., *Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации*, Дис. д-ра физ.-матем. наук, Томск. гос. ун-т, 2016, 300 с.
- [5] Погорелов Б. А., Пудовкина М. А., “О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности”, *Дискретная математика*, **25:3** (2013), 78–95.
- [6] Погорелов Б.А., Пудовкина М.А., “Натуральные метрики и их свойства. Ч.1. Подметрики и надметрики”, *Математические вопросы криптографии*, **2:4** (2011), 49–74.
- [7] Погорелов Б.А., *Основы теории групп подстановок. Ч. 1. Общие вопросы*, М., 1986, 316 с.
- [8] Knudsen L.R., “Truncated and higher order differentials”, FSE 1995, Lect. Notes Comput. Sci., **1008**, 1995, 196–211.
- [9] Погорелов Б. А., Пудовкина М. А., “Разбиения на биграммах и марковость алгоритмов блочного шифрования”, *Математические вопросы криптографии*, **8:1** (2017), 5–40.
- [10] Погорелов Б. А., Пудовкина М. А., “Натуральные метрики и их свойства. Ч. 2. Метрики типа Хемминга”, *Математические вопросы криптографии*, **3:1** (2012), 71–95.
- [11] Nyberg K., Knudsen L.R., “Provable security against differential cryptanalysis”, CRYPTO 1992, Lect. Notes Comput. Sci., **740**, 1993, 566–574.
- [12] Brinkmann M., Leander G., “On the classification of APN functions up to dimension five”, *Des. Codes Cryptogr.*, **49** (2008), 273–288.
- [13] Leander G., Abdelraheem M. A., AlKhzaimi H., Zenner E., “A cryptanalysis of PRINT-cipher: the invariant subspace attack”, CRYPTO 2011, Lect. Notes Comput. Sci., **6841**, 2011, 206–221.
- [14] Leander G., Minaud B., Ronjom S., “A generic approach to invariant subspace attacks: cryptanalysis of Robin, iSCREAM and Zorro”, EUROCRYPT 2015, Part I, Lect. Notes Comput. Sci., **9056**, 2015, 254–283.