УДК 519.7 DOI 10.17223/2226308X/10/9

О ПОКАЗАТЕЛЕ НЕИЗОМЕТРИЧНОСТИ ПРЕОБРАЗОВАНИЙ

Б. А. Погорелов, М. А. Пудовкина

В связи с исследованием линейных и гомоморфных моделей имеется значительное число работ, посвящённых расстояниям преобразований до аффинных и импримитивных групп. Качественные криптографические преобразования должны такие структуры рассеивать. Аналогичные вопросы для групп изометрий метрических пространств практически не рассматривались.

В работе вводится мера, характеризующая степень рассеивания преобразованием разбиения множества биграмм метрического пространства $(\mu, V_n(2))$ и названная показателем неизометричности преобразования. Получены верхние оценки показателя неизометричности для некоторых классов преобразований. Показано, что этот показатель выражается через элементы матрицы разностей переходов. Указаны связи: 1) показателей неизометричности в классах аффинно-смежных преобразований; 2) показателей неизометричности преобразований относительно метрики и её подметрик; 3) в терминах метрики Хемминга между подстановками, максимально далёкими от импримитивных групп $S_{2^{n-1}} \wr S_2$, $S_2 \wr S_{2^{n-1}}$, и с подстановками с максимальным показателем неизометричности.

Ключевые слова: *метрика Хемминга, группа изометрий, матрица разностей переходов, импримитивная группа.*

Многие методы криптоанализа основаны на существовании структур, сохраняемых или слабо рассеиваемых криптографическими преобразованиями. Такие структуры часто связаны с их группами автоморфизмов, например линейные структуры (векторные пространства) и аффинная группа, системы импримитивности и сплетения групп, метрические пространства и группы изометрий. Первые две используются в линейном и разностном методах, а также в методе гомоморфизмов. Для криптоанализа могут представлять интерес и другие структуры. Степень несохранения структуры при действии преобразования можно определять различными способами. В [1] в качестве такой меры для разбиения (структуры) $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ с равномощными блоками n-мерного векторного пространства V_n над полем $GF(2)$ выступает порядок $\mathbf{W}$-примитивности, который относительно метрики Хемминга χ на симметрической группе $S(V_n)$ характеризует меру удалённости подстановки $g \in S(V_n)$ от импримитивной группы $\mathrm{IG}_{\mathbf{W}}$, описываемой операцией сплетения $S(W_0) \wr S_r$ (элементами $\mathrm{IG}_{\mathbf{W}}$ являются все подстановки из $S(V_n)$, сохраняющие разбиение $\mathbf{W}$).

Для подстановки $g \in S(V_n)$ положим:

1) $\alpha^g = g(\alpha)$ для $\alpha \in V_n$;
2) $W^g = \{\beta^g : \beta \in W\}$ для $W \subseteq V_n$.

В [1] показано, что порядок $\mathbf{W}$-примитивности подстановки g выражается через элементы матрицы $\mathbf{c}^{(\mathbf{W})}(g) = \left(c_{i,j}^{(\mathbf{W})}(g)\right)$, где $c_{i,j}^{(\mathbf{W})}(g) = |W_i^g \cap W_j|$ для $i, j = 0, 1, \ldots, r-1$, а также описаны подстановки с максимальным порядком $\mathbf{W}$-примитивности. Порядок $\mathbf{W}$-примитивности может возникать в методе гомоморфизмов или вероятностных гомоморфизмов, а также в разностном методе. Вместе с тем из классификации примитивных групп подстановок видно, что ряд классов характеризуется как группы изометрий метрик. Но в криптографии соответствующие подходы пока не нашли должного развития, хотя метрики могут естественным образом появляться в случае криптосистем, построенных на базе регистров сдвига [2].

В работе вводится мера, характеризующая степень рассеивания преобразованием метрической структуры, названная *показателем неизометричности* подстановки $g \in S(V_n)$. Мера задаётся для произвольной метрики μ на V_n условием

$$\rho_\mu(g) = (2^n(2^n-1))^{-1} \left|\left\{(\alpha,\alpha') \in V_n^2 : \mu(\alpha,\alpha') \neq \mu(\alpha^g,\alpha'^g)\right\}\right|,$$

$0 \leqslant \rho_\mu(g) \leqslant 1$, причём $\rho_\mu(g) = 1$ тогда и только тогда, когда $g \in \mathrm{Isom}(\mu)$.

Доказано, что показатель неизометричности одинаков для всех подстановок из $S(V_n)$, принадлежащих одному смежному классу по подгруппе $\mathrm{Isom}(\mu)$.

Пусть $X^\times = X \setminus \{\mathbf{0}_n\}$ для подмножества $X \subseteq V_n$; $\oplus$ — операция сложения в V_n; $\mathbf{0}_n$ — нулевой вектор пространства V_n. Рассмотрим множество $M_{n,d}^+$ всех $(d+1)$-значных метрик на V_n, инвариантных относительно группы сдвигов пространства V_n и принимающих каждое значение из множества $\{0,1,\ldots,d\}$, $M_n^+ = \bigcup\limits_{d=1}^{\infty} M_{n,d}^+$. Каждая метрика $\mu \in M_{n,d}^+$ [3] однозначно задаваема упорядоченным разбиением $\bar{B} = (B_1,\ldots,B_d)$ множества $V_n^\times$ условием

$$\mu : (\alpha,\alpha') \mapsto j, \text{ если } \alpha \oplus \alpha' \in B_j \text{ для } j = 1,\ldots,d$$

и обозначается через $\mu_{\bar{B}}$. Для каждого $g \in S(V_n)$ доказано равенство

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

где

$$\hat{p}_{\delta,\varepsilon}(g) = 2^{-n} \left|\{\alpha \in V_n : (\alpha \oplus \delta)^g = \alpha^g \oplus \varepsilon\}\right|, \ \delta,\varepsilon \in V_n,$$
$$\hat{p}_{\Lambda,\Delta}(g) = \sum_{(\delta,\varepsilon)\in\Lambda\times\Delta} \hat{p}_{\delta,\varepsilon}(g), \quad \Delta,\Lambda \subseteq V_n,$$

т. е. $\hat{p}_{\delta,\varepsilon}(g)$ — элемент матрицы разностей переходов преобразования g.

Доказано, что для любых подстановок $g \in S(V_n)$, метрик $\mu \in M_n^+$ и подметрик $\mu' \in M_n^+$ метрики μ [4] справедливо неравенство $\rho_\mu(g) \geqslant \rho_{\mu'}(g)$.

Указаны классы метрик из M_n^+, задаваемых разбиением $\mathbf{W}$ пространства V_n, у которых показатель изометричности полностью характеризуется элементами матрицы $\mathbf{c}^{(\mathbf{W})}(g)$ для каждой подстановки $g \in S(V_n)$. Для метрик из этих классов получены достижимые верхние оценки. В частности, найден показатель неизометричности для произвольной 3-значной метрики $\mu_{\left(W_0^\times, V_n^\times/W_0\right)}$ ($\mathbf{0}_n \in W_0 \subset V_n$), а также получена его достижимая верхняя оценка. Кроме того, в случае $W_0 < V_n$ ($d = \dim W_0$) показатель неизометричности выражен через элементы матрицы $c^{(\mathbf{W})}(g)$ для каждой подстановки $g \in S(V_n)$ и доказано равенство $\mathrm{Isom}\mu_{\left(W_0^\times, V_n^\times/W_0\right)} = S_{2^d} \wr S_{2^{n-d}}$. В случае $d \in \{1, n-1\}$ для метрик из [5] получена связь между подстановками с максимальным порядком $\mathbf{W}$-примитивности и подстановками, для которых показатель неизометричности для метрики $\mu_{\left(W_0^\times, V_n^\times/W_0\right)}$ принимает наибольшее значение.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности // Дискретная математика. 2013. Т. 25. № 3. С. 78–95.
2. *Погорелов Б. А.* Основы теории групп подстановок. Ч. 1. Общие вопросы. М.: В/ч 33965, 1986. 316 с.

3. *Погорелов Б. А., Пудовкина М. А.* Натуральные метрики и их свойства. Ч. 2. Метрики типа Хемминга // Математические вопросы криптографии. 2012. Т. 3. № 1. С. 71–95.
4. *Погорелов Б. А.* Подметрики метрики Хемминга и теорема А. А. Маркова // Труды по дискретной математике. 2006. Т. 9. С. 190–219.
5. *Погорелов Б. А., Пудовкина М. А.* Подметрики метрики Хемминга и преобразования, распространяющие искажения в заданное число раз // Труды по дискретной математике. 2007. Т. 10. С. 202–238.

УДК 519.714.5 DOI 10.17223/2226308X/10/10

ОБ ОДНОМ ПОДХОДЕ К ПОСТРОЕНИЮ ТРАНЗИТИВНОГО МНОЖЕСТВА БЛОЧНЫХ ПРЕОБРАЗОВАНИЙ

И. В. Чередник

Пусть Ω — произвольное конечное множество и $\mathcal{Q}(\Omega)$ — семейство всех бинарных квазигрупп, определённых на множестве Ω. Отображение $\Omega^n \to \Omega^n$, $n \in \mathbb{N}$, реализуемое сетью Σ с одной бинарной операцией F, будем обозначать Σ^F. Доказывается критерий биективности всех преобразований из множества $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$, а также определяются условия для транзитивности этого множества.

Ключевые слова: *сети, квазигруппы.*

1. Понятие сети

Пусть $\{x_1, x_2, \ldots, x_n\}$ — множество переменных и $*$ — символ бинарной операции. Множество всех формул в алфавите $\{x_1, \ldots, x_n, *\}$ будем обозначать $\mathcal{W}$. При сопоставлении символу $*$ конкретной бинарной квазигруппы $F \in \mathcal{Q}(\Omega)$ формула $w(x_1, \ldots, x_n)$ реализует отображение $w^F \colon \Omega^n \to \Omega$.

Для исследования свойств отображений $(w_1^F, \ldots, w_m^F) \colon \Omega^n \to \Omega^m$, $F \in \mathcal{Q}(\Omega)$, соответствующих определённому набору формул $(w_1, \ldots, w_m) \in \mathcal{W}^m$, введём дополнительное представление отображений в виде сети.

Пусть $t, n_0, n_1, \ldots, n_t \in \mathbb{N}$ и

$$X_0 = \{x_1^{(0)}, x_2^{(0)}, \ldots, x_{n_0}^{(0)}\},\ X_1 = \{x_1^{(1)}, x_2^{(1)}, \ldots, x_{n_1}^{(1)}\},\ \ldots,\ X_t = \{x_1^{(t)}, x_2^{(t)}, \ldots, x_{n_t}^{(t)}\}$$

— семейство попарно непересекающихся конечных непустых множеств. Тогда *квазигрупповой сетью* (далее просто сетью) длины t будем называть простой ориентированный граф Σ с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$, содержащий только рёбра вида $(x_i^{(s-1)}, x_j^{(s)})$, $s \in \{1, \ldots, t\}$, с тем ограничением, что степень захода каждой вершины $x_j^{(s)}$, $s \in \{1, \ldots, t\}$, равна 1 или 2. При этом если степень захода вершины $x_j^{(s)}$ равна 1, то ребро $(x_i^{(s-1)}, x_j^{(s)})$ имеет метку 0, а если степень захода вершины $x_j^{(s)}$ равна 2, то рёбра $(x_{i_1}^{(s-1)}, x_j^{(s)})$ и $(x_{i_2}^{(s-1)}, x_j^{(s)})$ имеют различные метки из множества $\{1, 2\}$. Число n_0 будем называть *размерностью* сети Σ, а число $\max\{n_0, \ldots, n_t\}$ — *шириной* сети Σ. Подграф Σ_s сети Σ, основанный на множестве вершин $X_{s-1} \cup X_s$, будем называть *s-м слоем* сети Σ. Сеть Σ будем называть *однослойной*, если она имеет длину 1.

Пусть Σ' и Σ'' — сети с множествами вершин $X' = X'_0 \cup X'_1 \cup \ldots \cup X'_s$ и $X'' = X''_0 \cup X''_1 \cup \ldots \cup X''_t$ соответственно и при этом $X' \cap X'' = X'_s = X''_0$. Тогда естественным образом можно определить сеть длины $s+t$ с множеством вершин $X'_0 \cup X'_1 \cup \ldots \cup X'_s \cup X''_1 \cup \ldots \cup X''_t$, которую будем называть *произведением* сетей Σ' и Σ'' и обозначать $\Sigma' \cdot \Sigma''$. Нетрудно понять, что всякая сеть является произведением своих слоёв.