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.

Произвольный набор формул $(w_1, \ldots, w_m)$, в котором каждая формула w_j, $j \in \in \{1, \ldots, m\}$, либо имеет вид $v_{i_1} * v_{i_2}$, $i_1, i_2 \in \{1, \ldots, n\}$, либо является некоторой формулой v_i, $i \in \{1, \ldots, n\}$, будем называть *преобразованием* набора формул $(v_1, \ldots, v_n)$. Один из естественных способов построения произвольного набора формул $(w_1, \ldots, w_m)$ заключается в последовательном преобразовании набора переменных $(x_1, \ldots, x_n)$. Данный процесс допускает наглядную интерпретацию при использовании введённой терминологии сетей.

Пусть $(v_1, \ldots, v_n)$ — произвольный набор формул и Σ — однослойная сеть с множеством вершин $\{x_1^0, \ldots, x_n^{(0)}\} \cup \{x_1^{(1)}, \ldots, x_m^{(1)}\}$. Тогда определим набор формул $(w_1, \ldots, w_m)$ по следующим правилам:

— если вершине $x_j^{(1)}$ инцидентно ребро $(x_i^{(0)}, x_j^{(1)})$ с меткой 0, то полагаем $w_j = v_i$;

— если вершине $x_j^{(1)}$ инцидентны рёбра $(x_{i_1}^{(0)}, x_j^{(1)})$ и $(x_{i_2}^{(0)}, x_j^{(1)})$ с метками 1 и 2 соответственно, то полагаем $w_j = v_{i_1} * v_{i_2}$.

При этом будем говорить, что сеть Σ описывает *преобразование* набора формул $(v_1, \ldots, v_n)$ в набор формул $(w_1, \ldots, w_m)$.

Произвольная сеть Σ является произведением однослойных сетей, являющихся её слоями, и естественным образом описывает преобразование произвольного набора формул, являющееся произведением преобразований, соответствующих слоям.

Пусть $F \in \mathcal{Q}(\Omega)$ — произвольная квазигруппа и сеть Σ описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$. Тогда отображение $(w_1^F, \ldots, w_m^F)\colon \Omega^n \to \Omega^m$ будем обозначать через Σ^F. Будем говорить, что две сети Σ' и Σ'' *эквивалентны*, если при выборе любой квазигруппы F отображения Σ'^F и Σ''^F совпадают. Нетрудно понять, что если сети Σ' и Σ'' описывают преобразование набора переменных $(x_1, \ldots, x_n)$ в наборы формул $(w_1', \ldots, w_m')$ и $(w_1'', \ldots, w_m'')$ соответственно, то совпадение указанных наборов формул является достаточным условием для эквивалентности сетей Σ' и Σ''. В частности, если $\Sigma = \Sigma_1 \cdot \Sigma_2$, то при выборе любой квазигруппы F справедливо равенство $\Sigma^F = \Sigma_1^F \cdot \Sigma_2^F$.

2. Условия биективности и транзитивности сетей

Сеть Σ будем называть *биективной для множества* Ω, если при выборе любой квазигруппы $F \in \mathcal{Q}(\Omega)$ отображение Σ^F является биективным. Очевидно, что для биективности сети Σ с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$ необходимо, чтобы выполнялось равенство $|X_0| = |X_t|$. Сеть Σ с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$ будем называть *сетью постоянной ширины*, если $|X_0| = |X_1| = \ldots = |X_t|$.

Вершину $x_i^{(0)} \in X_0$ однослойной сети Σ постоянной ширины с множеством вершин $X_0 \cup X_1$ будем называть *неподвижной*, если сеть Σ содержит ребро $(x_i^{(0)}, x_i^{(1)})$. Однослойную сеть постоянной ширины будем называть *элементарной*, если все её вершины неподвижны и ровно одна вершина имеет степень захода 2. Нетрудно понять, что произвольная элементарная сеть является биективной для любого множества.

Ещё одним важным примером биективных сетей являются сети постоянной ширины, у которых степень захода каждой вершины равна 1. Такие сети будем называть *перестановочными*. Произвольная перестановочная сеть определяет отображение $\Omega^n \to \Omega^n$, не зависящее от выбора квазигруппы F и действующее на множестве Ω^n как перестановка координат вектора. Отсюда следует, что любая перестановочная сеть эквивалентна однослойной перестановочной сети. Также можно отметить, что произвольная перестановочная сеть эквивалентна произведению перестановочных сетей, у каждой из которых ровно две вершины не являются неподвижными — это следует из

известного результата о представлении произвольной перестановки в виде произведения транспозиций.

Элементарные и перестановочные сети являются примерами простейших биективных сетей и, как показывает следующая теорема, этих примитивов достаточно для реализации произвольной биективной сети постоянной ширины.

Теорема 1. Сеть Σ постоянной ширины является биективной для некоторого множества Ω, $|\Omega| \geqslant 2$, в том и только в том случае, когда она эквивалентна произведению

$$\Pi_L \cdot \Sigma_{L,1} \cdot \ldots \cdot \Sigma_{L,t} \text{ (или } \Sigma_{R,1} \cdot \ldots \cdot \Sigma_{R,t} \cdot \Pi_R),$$

где Π_L (Π_R) — перестановочная сеть; $\Sigma_{L,1}, \ldots, \Sigma_{L,t}$ ($\Sigma_{R,1}, \ldots, \Sigma_{R,t}$) — элементарные сети. При этом длина произведения равна количеству вершин сети Σ со степенью захода 2 и соответственно не зависит от выбора представления.

Следствие 1. Если сеть Σ постоянной ширины является биективной для некоторого множества Ω, $|\Omega| \geqslant 2$, то сеть Σ является биективной для всех множеств.

Указанные в теореме 1 представления биективной сети Σ в виде произведения элементарных сетей будем называть *каноническими представлениями* сети Σ. Количество вершин сети Σ со степенью захода 2 будем называть *весом* сети Σ и обозначать $\|\Sigma\|$.

Биективную сеть Σ будем называть *транзитивной для множества* Ω, если множество отображений $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$ является транзитивным. Основным результатом работы можно считать разработанный автором аппарат разметки сетей, который позволяет проверить транзитивность произвольной биективной сети, а при отрицательном ответе определить особенности строения сети, противоречащие транзитивности. С помощью этого аппарата, например, доказывается следующая теорема.

Теорема 2. Если биективная сеть Σ постоянной ширины является транзитивной для некоторого множества Ω, $|\Omega| \geqslant \|\Sigma\|$, то сеть Σ является транзитивной для любого множества, мощность которого строго больше чем $\|\Sigma\|$.

Стоит отметить, что аппарат разметки позволяет сформулировать и обосновать алгоритм модификации канонического представления произвольной биективной сети Σ постоянной ширины n. В результате применения алгоритма получается биективная сеть $\widehat{\Sigma}$ веса $\|\widehat{\Sigma}\| \leqslant \|\Sigma\| + 4n$, которая является транзитивной для большей части множеств.

Теорема 3. Модификация $\widehat{\Sigma}$ произвольной сети Σ является транзитивной для любого множества, мощность которого строго больше чем $\|\widehat{\Sigma}\|$.

Автор благодарит профессора А. В. Черемушкину за постановку задачи и внимание к проводимым исследованиям.

UDC 512.772.7 DOI 10.17223/2226308X/10/11

HYPERELLIPTIC CURVES, CARTIER — MANIN MATRICES AND LEGENDRE POLYNOMIALS

S. A. Novoselov

We investigate the hyperelliptic curves of the form $C_1 : y^2 = x^{2g+1} + ax^{g+1} + bx$ and $C_2 : y^2 = x^{2g+2} + ax^{g+1} + b$ over the finite field $\mathbb{F}_q$, $q = p^n$, $p > 2$. We transform these curves to the form $C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x$ and $C_{2,\rho} : y^2 = x^{2g+2} - 2\rho x^{g+1} + 1$ and