УДК 519.714.5 DOI 10.17223/2226308X/11/6

k-ТРАНЗИТИВНОСТЬ ОДНОГО КЛАССА БЛОЧНЫХ ПРЕОБРАЗОВАНИЙ

И. В. Чередник

Пусть Ω — произвольное конечное множество, $\mathcal{Q}(\Omega)$ — семейство всех бинарных квазигрупп, определенных на множестве Ω, и $\Sigma^F\colon \Omega^n \to \Omega^n$ — отображение, реализуемое сетью Σ ширины $n \in \mathbb{N}$ с одной бинарной операцией $F \in \mathcal{Q}(\Omega)$. В работе определяются условия k-транзитивности множества преобразований $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$, предлагается эффективный способ проверки k-транзитивности этого множества и приводятся параметры результата работы алгоритма построения таких сетей Σ, у которых множество преобразований $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$ является k-транзитивным.

Ключевые слова: *сети, квазигруппы, k-транзитивность.*

В работе [1] определяется понятие отображения $\Sigma^F\colon \Omega^n \to \Omega^n$, реализуемого сетью Σ ширины $n \in \mathbb{N}$ с одной бинарной операцией $F \in \mathcal{Q}(\Omega)$, и проводится первичное исследование криптографических свойств семейства отображений $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$. Кратко перечислим основные результаты, полученные в [1].

Сеть Σ будем называть *биективной для множества* Ω, если при выборе любой квазигруппы $F \in \mathcal{Q}(\Omega)$ отображение Σ^F является биективным.

Теорема 1 [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

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

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

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 называется *весом* сети Σ и обозначается $\|\Sigma\|$.

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

Биективную сеть Σ будем называть *транзитивной для множества* Ω, если множество отображений $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$ является транзитивным. Основным результатом работы [1] можно считать разработанный автором аппарат разметки сетей, который позволяет проверить транзитивность произвольной биективной сети, а при отрицательном ответе определить особенности строения сети, противоречащие транзитивности. Например, с его помощью доказываются следующие утверждения.

Теорема 2 [1]. Пусть Σ — биективная сеть ширины n и Ω — множество мощности строго больше чем $\|\Sigma\|$. Тогда следующие утверждения эквивалентны:

1) сеть Σ является транзитивной для множества Ω;
2) сеть Σ допускает нетривиальную правильную непротиворечивую разметку элементами множества Ω при любых ограничениях.

Следствие 2 [1]. Для биективной сети Σ следующие утверждения эквивалентны:

1) сеть Σ является транзитивной для некоторого множества, мощность которого строго больше чем $\|\Sigma\| + n$;
2) сеть Σ является транзитивной для произвольного множества, мощность которого строго больше чем $\|\Sigma\| + n$.

Теорема 3 [1]. Сеть Σ допускает нетривиальные правильные непротиворечивые разметки при всех возможных ограничениях из $\mathbb{N}$ в том и только в том случае, когда сеть Σ допускает нетривиальные правильные непротиворечивые разметки при всех возможных ограничениях из Ω_2.

Кроме того, аппарат разметки позволил сформулировать и обосновать в [1] алгоритм модификации канонического представления произвольной биективной сети Σ, в результате применения которого строится биективная сеть $\widehat{\Sigma}$, транзитивная для всех множеств достаточно большой мощности.

Теорема 4 [1]. Пусть Σ — произвольная биективная сеть ширины n. Тогда её модификация $\widehat{\Sigma}$ имеет вес $\|\widehat{\Sigma}\| = \|\Sigma\| + 3n - 3$ и является транзитивной для любого множества Ω, мощность которого больше чем $\|\Sigma\| + 4n - 3$.

Следствие 3 [1]. Для любого $n \geqslant 2$ существует сеть $\widehat{\Sigma}$ ширины n и веса $3n - 3$, которая транзитивна для всех множеств, мощность которых больше чем $4n - 3$.

Естественным продолжением исследования криптографических свойств семейства отображений, реализуемых сетью Σ с одной бинарной операцией $F \in \mathcal{Q}(\Omega)$, представляется изучение вопроса о кратной транзитивности множества $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$. Биективную сеть Σ будем называть *k-транзитивной для множества* Ω, если множество отображений $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$ является k-транзитивным. Оказалось, что введённый в [1] аппарат разметки сетей допускает вполне естественное обобщение, которое позволяет исследовать сложное свойство k-транзитивности при $k \geqslant 2$.

Теорема 5. Пусть Σ — биективная сеть ширины n и Ω — множество мощности строго больше чем $k\|\Sigma\|$. Тогда следующие утверждения эквивалентны:

1) сеть Σ является k-транзитивной для множества Ω;
2) сеть Σ допускает нетривиальную правильную непротиворечивую k-разметку элементами множества Ω при любых ограничениях.

Следствие 4. Для биективной сети Σ следующие утверждения эквивалентны:

1) сеть Σ является k-транзитивной для некоторого множества, мощность которого строго больше чем $k\|\Sigma\| + kn$;
2) сеть Σ является k-транзитивной для произвольного множества, мощность которого строго больше чем $k\|\Sigma\| + kn$.

Следующий результат позволяет эффективно проверять k-транзитивность произвольной биективной сети для достаточно больших множеств.

Теорема 6. Сеть Σ допускает нетривиальные правильные непротиворечивые k-разметки при всех возможных ограничениях из $\mathbb{N}$ в том и только в том случае, когда сеть Σ допускает нетривиальные правильные непротиворечивые k-разметки при всех возможных ограничениях из Ω_{k+1}.

В заключение отметим, что аппарат k-разметки позволяет сформулировать и обосновать алгоритм модификации канонического представления произвольной биективной сети Σ, в результате применения которого строится биективная сеть $\widehat{\Sigma}$, k-транзитивная для всех множеств достаточно большой мощности.

Теорема 7. Пусть Σ — произвольная биективная сеть ширины n. Тогда её модификация $\widehat{\Sigma}$ имеет вес $\|\widehat{\Sigma}\| \leqslant \|\Sigma\| + 6n - 7$ и является k-транзитивной для любого множества Ω, мощность которого больше чем $k\|\Sigma\| + 7k(n-1)$.

Следствие 5. Для любого $n \geqslant 2$ существует сеть $\widehat{\Sigma}$ ширины n и веса $6n-7$, которая k-транзитивна для всех множеств, мощность которых больше чем $7k(n-1)$.

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

ЛИТЕРАТУРА

1. *Чередник И. В.* Один подход к построению транзитивного множества блочных преобразований // Прикладная дискретная математика. 2017. №38. С. 5–34.

УДК 519.719.1 DOI 10.17223/2226308X/11/7

ОБОБЩЕНИЕ ТЕОРЕМ ГЛУСКИНА — ХОССУ И МАЛЫШЕВА НА СЛУЧАЙ СИЛЬНО ЗАВИСИМЫХ n-АРНЫХ ОПЕРАЦИЙ

А. В. Черемушкин

Доказываются аналоги теорем Глускина — Хоссу о строении n-групп и Малышева о строении n-квазигрупп с условием слабой обратимости справа и слева применительно к случаю сильно зависимых операций над конечным множеством.

Ключевые слова: *n-арные группа, n-арная полугруппа, сильно зависимая операция, слабо обратимая операция.*

Пусть $n \geqslant 0$ и X — непустое множество. *n-Полугруппой* называется n-арная операция $f(x_1, \ldots, x_n) = [x_1, \ldots, x_n]$ на множестве X, удовлетворяющая тождествам ассоциативности

$$[x_1, \ldots, x_{i-1}, [x_i, \ldots, x_{i+n-1}], x_{i+n}, \ldots, x_{2n-1}] = \\ = [x_1, \ldots, x_{j-1}, [x_j, \ldots, x_{j+n-1}], x_{j+n}, \ldots, x_{2n-1}],$$

$1 \leqslant i < j \leqslant n$. Если при этом n-полугруппа является n-квазигруппой, т. е. для каждого $i = 1, \ldots, n$ унарная функция $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1} \ldots, a_n)$ является подстановкой по переменной x_i при всех $a_1, \ldots, a_{i-1}, a_{i+1} \ldots, a_n \in X$, то она называется *$n$-группой*.

Строение n-группы над произвольным, не обязательно конечным, множеством X описывается следующей теоремой Л. М. Глускина и М. Хоссу.

Теорема 1. Для любой n-группы $[x_1, \ldots, x_n]$ найдутся некоторая групповая операция «$*$» на множестве X, автоморфизм θ группы «$*$» и $a \in X$, такие, что $\theta^{n-1}(x) = a * x * a^{-1}$, $\theta(a) = a$ и справедливо тождество

$$[x_1, \ldots, x_n] = x_1 * \theta(x_2) * \theta^2(x_3) * \ldots * \theta^{n-2}(x_{n-1}) * a * x_n, \quad x_i \in X,\ i = 1, \ldots, n.$$

Заметим, что данную теорему обычно называют обратной теоремой Глускина — Хоссу, а прямая теорема утверждает, что всякая n-квазигруппа такого вида является n-группой. С историей и различными обобщениями этой теоремы можно познакомиться в обзоре [1].