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].

В работе [2] Ф. М. Малышевым рассматривается несколько более общая ситуация, из которой может быть выведена теорема 1. Операция $[x_1, \ldots, x_n]$ называется *i-слабо обратимой справа*, $i = 1, \ldots, n-2$, если для всех $\bar{a} \in X^i$, $\bar{b}_1, \bar{b}_2 \in X^{n-i}$ из равенства $[\bar{a}, \bar{b_1}] = [\bar{a}, \bar{b_2}]$ следуют равенства $[\bar{b}_1, \bar{x}] = [\bar{b}_2, \bar{x}]$ для всех $\bar{x} \in X^i$. Аналогично определяется *i-слабая обратимость слева*.

Теорема 2 [2]. Пусть $n \geqslant 3$. Если n-квазигруппа является 1-слабо обратимой слева (справа), то при некоторой подстановке σ, групповой операции «$*$» на множестве X и автоморфизме θ группы «$*$» справедливо тождество

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

Первоначально в [2] эта теорема доказана для конечных множеств X, а затем в [3] отмечено, что она справедлива и для бесконечных множеств X.

Целью настоящей работы является установление аналогов теорем 1 и 2 для класса сильно зависимых функций.

Напомним, что *сильно зависимой* называется такая функция от n переменных (n-арная операция), у которой для каждой переменной x_i, $1 \leqslant i \leqslant n$, найдётся хотя бы один набор элементов $a_1, \ldots, a_{i-1}, a_{i+1} \ldots, a_n \in X$, при котором функция $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1} \ldots, a_n)$ становится подстановкой по переменной x_i Для конечных множеств X сильно зависимые операции обладают тем свойством, что бесповторная суперпозиция функций является сильно зависимой в том и только в том случае, когда каждая из функций, участвующих в суперпозиции, также является сильно зависимой.

Далее пусть X — конечное множество мощности $k \geqslant 2$. Введём понятие частичной обратимости справа (слева) применительно к классу сильно зависимых функций.

Определение 1. Сильно зависимая функция $f(x_1, \ldots, x_n)$ называется *i-частично обратимой справа*, $i = 1, \ldots, n-2$, если найдётся такой набор $\bar{a} \in X^i$, что при всех $\bar{b_1}, \bar{b_2} \in X^{n-i}$ из условия $f(\bar{a}, \bar{b_1}) = f(\bar{a}, \bar{b_2})$ следуют равенства $f(\bar{b_1}, \bar{x}) = f(\bar{b_2}, \bar{x})$ для всех $\bar{x} \in X^i$. Аналогично определяется *i-частичная обратимость слева* сильно зависимых функций слева.

Лемма 1. Для сильно зависимой функции f следующие условия равносильны:

а) f является i-частично обратимой справа и слева;

б) f допускает представление в виде бесповторных суперпозиций

$$f(x_1, \ldots, x_n) = g_1(\bar{x}, h(\bar{y}, \bar{z})) = g_2(h(\bar{x}, \bar{y}), \bar{z})$$

при всех $(x_1, \ldots, x_n) = (\bar{x}, \bar{y}, \bar{z}) \in X^i \times X^{n-2i} \times X^i$ и некоторых сильно зависимых операциях g_1, g_2, h.

Замечание 1. В случае квазигрупп свойства i-слабой обратимости справа и слева равносильны. Для сильно зависимых функций для выполнения условия п. б приходится требовать одновременно выполнимость обоих свойств.

Напомним, *моноидом* называется ассоциативная бинарная операция с единицей. Основным результатом является следующее обобщение теоремы Ф. Н. Малышева.

Теорема 3. Пусть $n \geqslant 3$, X — конечное множество. Если сильно зависимая функция f является 1-частично обратимой справа и слева, то при некоторой подстановке σ, моноиде «$*$» на множестве X и автоморфизме θ моноида «$*$» справедливо тождество

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

Доказательство основано на теореме Ф. Н. Сохацкого [4] о решении обобщённого уравнения общей ассоциативности для сильно зависимых операций.

Как следствие из предыдущей теоремы, получается следующее обобщение теоремы Глускина — Хоссу на случай сильно зависимых функций.

Теорема 4. Если сильно зависимая n-арная операция $[x_1, \ldots, x_n]$ на конечном множестве X удовлетворяет тожеству ассоциативности

$$[[x_1, \ldots, x_n], x_{n+1}, \ldots, x_{2n-1}] = [x_1, [x_2, \ldots, x_{n+1}], x_{n+2}, \ldots, x_{2n-1}],$$

то для некоторого моноида «$*$» на множестве X, автоморфизма θ моноида «$*$», такого, что $\theta^{n-1}(x) = a{*}x{*}a^{-1}$, $a \in X$ — обратимый элемент моноида «$*$», $\theta(a) = a$, справедливо тождество

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

В заключение приведём обобщение обратной теоремы Глускина — Хоссу.

Теорема 5. Если для сильно зависимой n-арной операции $[x_1, \ldots, x_n]$ справедливо представление

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

где «$*$» — моноид на множестве X; θ — автоморфизм моноида «$*$», такой, что $\theta^{n-1}(x) = a^{-1} * x * a$, $a \in X$ — обратимый элемент моноида «$*$», $\theta(a) = a$, то она является n-полугруппой.

ЛИТЕРАТУРА

1. *Гальмак А. М., Воробьев Г. Н.* О теореме Поста — Глускина — Хоссу // Проблемы физики, математики и техники. 2013. Вып. 1(14). С. 55–59.
2. *Малышев Ф. М.* О теореме Поста — Глускина — Хоссу для конечных квазигрупп и самоинвариантные семейства подстановок // Математический сборник. 2016. Т. 207. Вып. 2. С. 81–92.
3. *Малышев Ф. М.* Теорема Поста — Глускина — Хоссу для n-квазигрупп // Исследования по алгебре, теории чисел, функциональному анализу и смежным вопросам: межвуз. сб. науч. тр. Саратов: Изд-во Сарат. ун-та, 2016. Т. 8. С. 59–62.
4. *Сохацкий Ф. Н.* Обобщение двух теорем Белоусова для сильно зависимых функций k-значной логики // Исследования по теории бинарных и n-арных квазигрупп. Математические исследования. Кишинев: Штиинца, 1985. № 85. С. 105–115.

UDC 512.772.7 DOI 10.17223/2226308X/11/8

NFS FACTORIZATION: NEW HOPES

P. Kirchner

We describe new Number Field Sieve techniques. While *none* is proved (even under heuristics) to work for a concrete family of number fields, we hope such a family exist. If this is the case, we can factor a special integer n in time $L_n(1/3, (16/9)^{1/3})$, which doubles the length of n with respect to SNFS for the same time. This algorithm works by finding a strongly-ambiguous ideal in order to factor the relative discriminant of a prime degree Galois extension. In case this method can be adapted for factoring general numbers, it may reach a complexity $L_n(1/3, (32/9)^{1/3})$. A variant of the same