О полиномиально полных квазигруппах простого порядка

А. В. Галатенко, А. Е. Панкратьев, С. Б. Родин
(МГУ им. М. В. Ломоносова, Москва)

В работе формулируется критерий полиномиальной полноты квазигруппы простого порядка, а также показывается, что проверка полиномиальной полноты может быть проведена за время, полиномиальное от порядка.

Ключевые слова: квазигруппа, полиномиальная полнота, алгоритмическая сложность.

1. Введение

В настоящее время при разработке систем защиты информации активно исследуется возможность использования различных алгебраических структур, в том числе некоммутативных и неассоциативных. Отдельное направление исследований связано с применением квазигрупп. Табличное задание квазигруппы представляет собой латинский квадрат, шифрование по которому (так называемое табличное гаммирование) обладает свойством «совершенной секретности», отмеченным еще К. Шенноном [1]. Квазигруппы находят применение при решении различных задач криптографии [2], в том числе при разработке систем поточного шифрования [3, 4, 5].

Особый интерес при разработке поточных шифров представляют полиномиально (функционально) полные квазигруппы, что обусловлено NP-полнотой задачи распознавания разрешимости системы уравнений в функционально полной алгебре [6]. В этом направлении значительные результаты были получены В. А. Артамоновым с соавторами [7, 8].

В настоящей работе формулируется критерий полиномиальной полноты для квазигруппы простого порядка. Также приводится процедура проверки полиномиальной полноты, время выполнения которой полиномиально зависит от порядка квазигруппы.

2. Основные определения

Определение 1. Квазигруппой называется множество Q, на котором определена бинарная операция умножения (в дальнейшем обозначаемая символом f_Q или просто f, если из контекста ясно, о какой квазигруппе идет речь) такая, что для любых элементов $a, b \in Q$ уравнения $ax = b$ и $ya = b$ однозначно разрешимы в Q. Соответствующие решения обозначаются $x = a\backslash b$ и $y = b/a$ и называются, соответственно, левым и правым частным от деления b на a.

Квазигрупповая операция часто задается табличным способом: для множества элементов $\{q_1, \ldots, q_m\}$, составляющих квазигруппу Q, выписывается квадратная таблица размера $m \times m$ с окаймляющими строкой и столбцом.

	q_1	$\ldots$	q_m
q_1	a_{11}	$\ldots$	a_{1m}
$\vdots$	$\ldots$	$\ldots$	$\ldots$
q_m	a_{m1}	$\ldots$	a_{mm}

Здесь элемент $a_{ij} \in Q$ — результат применения квазигрупповой операции f к элементам q_i и q_j.

Для фиксированного (конечного) множества A обозначим через $\mathcal{O}_n(A)$ совокупность всех n-арных операций на A ($n \geqslant 0$) и пусть $\mathcal{O}(A) = \bigcup\limits_n \mathcal{O}_n(A)$. В данной работе под множеством A везде понимается множество элементов квазигруппы, поэтому мы будем использовать упрощенную запись $\mathcal{O}_n$ и $\mathcal{O}$.

На произвольном подмножестве $F \subseteq \mathcal{O}(A)$ естественным образом вводятся операции суперпозиции и замыкания (см., например, [9]). Обозначим замыкание множества F через $[F]$.

Определение 2. Квазигруппа Q называется полиномиально (или функционально) полной, если $[\{f_Q\} \cup \mathcal{O}_0] = \mathcal{O}$.

Заметим, что в случае квазигрупп порядка 2 и 3 задача проверки полиномиальной полноты тривиальна, поэтому в дальнейшем мы будем предполагать, что порядок квазигруппы больше или равен 5.

Для фиксированного простого числа p рассмотрим множество $\mathbb{Z}_p$ с естественным образом определенными операциями сложения и умножения. Известно (см., например, [10, Часть II, Теорема 1.4.3]), что любая функция из $\mathcal{O}(\mathbb{Z}_p)$ задается многочленом, причем одинственным обра-

зом с точностью до перестановки слагаемых и сомножителей. В случае, когда степень соответствующего многочлена не превышает 1, функция называется линейной.

3. Критерий полиномиальной полноты квазигруппы простого порядка

Теорема 1. *Пусть p — простое число, $p \geqslant 5$, Q — квазигруппа порядка p. Тогда следующие условия эквивалентны:*

1) *Q не является полиномиально полной;*
2) *существует биективное отображение множества $\{q_1, \ldots, q_p\}$ на множество $\mathbb{Z}_p$, при котором квазигрупповая операция становится линейной функцией;*
3) *существует биективное отображение множества $\{q_1, \ldots, q_p\}$ на множество $\mathbb{Z}_p$, при котором все строки и столбцы матрицы, задающей квазигрупповую операцию, становятся линейными функциями.*

Эквивалентность условий 2 и 3 доказывается непосредственной проверкой.

Доказательство эквивалентности условия 1 и условий 2 и 3 ведется от противного. При этом используется следующий факт [11, Гл. II, § 3]. Назовем подгруппу перестановок над множеством $\{q_1, \ldots, q_p\}$ базисной, если из элементов этой подгруппы и произвольной функции, существенно зависящей более чем от одной переменной и принимающей все p значений, могут быть получены все функции. В случае, когда p простое, базисность имеет место тогда и только тогда, когда выполнены следующие условия:

(a) подгруппа не сохраняет никакое нетривиальное подмножество множества $\{q_1, \ldots, q_p\}$;

(b) для любого отображения множества $\{q_1, \ldots, q_p\}$ на множество $\mathbb{Z}_p$ найдется элемент подгруппы, не являющийся линейным.

4. Процедура распознавания полноты квазигруппы простого порядка

В этом разделе мы покажем, что в случае квазигруппы простого порядка полиномиальная полнота может быть распознана с сложностью, полиномиальной от порядка квазигруппы. На вход поступает матрица операции, записанная в элементах $\{q_1, \ldots, q_p\}$. На выход выводится отображение множества $\{q_1, \ldots, q_p\}$ на множество $\mathbb{Z}_p$, линеаризующее операцию, или отказ, если такое отображение не существует.

Идея распознающей процедуры следующая. Достаточно проверить, что квазигрупповая операция не является линейной ни для какого отображения множества $\{q_1, \ldots, q_p\}$ на множество $\mathbb{Z}_p$. Предположим, что операция линейна, и попробуем восстановить соответствующее отображение. Получим перестановку $x + d$, переберем всевозможные способы выбрать значение 0 и d, выведем отображение $\{q_1, \ldots, q_p\}$ на множество $\mathbb{Z}_p$ и восстановим коэффициенты. Невозможность выполнения процедуры на одном из шагов будет означать полиномиальную полноту.

Теорема 2. *Задача проверки полиномиальной полноты квазигрупп простого порядка решается за время, полиномиальное от порядка квазигруппы.*

Работа поддержана грантом РФФИ–ДСТ 15–51–45031 «Развитие некоммутативных и неассоциативных алгебраических структур и их приложения к теории передачи и защиты информации».

Список литературы

[1] Shannon C. Communication theory of secrecy systems // Bell System Techn. J. — 1949. — 28, № 4. — P. 656–715. [Рус. перевод: Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. — М.: Иностранная литература, 1963. — С. 333–369].

[2] Глухов М. М. О применениях квазигрупп в криптографии // ПДМ. — 2008. — № 2. — С. 28–32.

[3] Markovski S., Gligoroski D., Bakeva V. Quasigroup String Processing: Part 1 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XX. — 1999. — 1–2. — P. 13–28.

[4] Markovski S., Kusacatov V. Quasigroup String Processing: Part 2 // Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci. XXI. — 2000. — 1–2. — P. 15–32.

[5] Shcherbacov V. Quasigroup based crypto-algorithms // arXiv: 1201.3016v1.

[6] Horváth G., Nehaniv Gh. L., Szabó Cs. An assertion concerning functionally complete algebras and NP-completeness // Acta Sci. Math. (Szeged). — 2010. — 76. — P. 35–48.

[7] Artamonov V. A., Chakrabarti S., Gangopadhyay S., Pal S. K. On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts // Quasigroups and Related Systems. — 2013. — Vol. 21, No. 2. — P. 117–130.

[8] Artamonov V. A., Chakrabarti S., Pal S. K. Characterization of Polynomially Complete Quasigroups based on Latin Squares for Cryptographic Transformations // Discrete Applied Mathematics. — 2016. — P. 5–17.

[9] Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2010.

[10] Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory. — Berlin: Springer, 2006.

[11] Кудрявцев В. Б. Функциональные системы.— М.: Изд-во МГУ, 1982.