Полиномиальная полнота конечных квазигрупп

Галатенко А.В., Панкратьев А.Е., Родин С.Б.

Приводится обзор результатов, связанных с проверкой полиномиальной полноты конечных квазигрупп. Работа подготовлена по материалам доклада на семинаре “Теория автоматов”.

Ключевые слова: квазигруппа, латинский квадрат, полиномиальная полнота, простота, аффинность

Памяти Михаила Михайловича Глухова

1. Введение

В последние годы наблюдается интерес к построению перспективных криптосистем, основанных на различных алгебраических структурах, в том числе неассоциативных. Одной из первых работ, в которых раскрываются возможности применения квазигрупп в криптографии, является статья М.М. Глухова [1]. Впоследствии был предложен ряд криптосистем на основе конечных квазигрупп, или, что то же самое, латинских квадратов (см., например, [2, 3, 4]).

Желательным с точки зрения стойкости свойством при этом является полиномиальная полнота, в некотором смысле гарантирующая вычислительную невозможность атаки методом решения системы уравнений на биты ключа [5]. Критерий полиномиальной полноты для квазигрупп порядка 4 получен в работе [6]; для квазигрупп простого порядка критерий и полиномиальный от порядка алгоритм проверки приведены в [7]; обобщение на случай произвольного порядка сделано в [8].

2. Основные определения

Конечной квазигруппой порядка $k \in \mathbb{N}$ называется множество $Q = \{q_1, \ldots, q_k\}$ с бинарной операцией $f : Q \times Q \to Q$, такой что для любых $a, b \in Q$ уравнения $f(x, a) = b$ и $f(a, y) = b$ однозначно разрешимы.

Таблица умножения квазигруппы, то есть матрица $k \times k$ с окаймляющей строкой и окаймляющим столбцом, является латинским квадратом — в силу разрешимости уравнений каждая строка и каждый столбец матрицы является записью некоторой перестановки на множестве Q.

Квазигруппы (Q, f_1) и (Q, f_2) называются изотопными, если найдутся перестановки α, β, γ на множестве Q, такие что выполнено тождество

$$f_1(x, y) = \gamma^{-1}\left(f_2(\alpha(x), \beta(y)\right).$$

В терминах латинских квадратов это означает, что один квадрат может быть преобразован в другой перестановкой строк и столбцов, а также переименованием элементов.

Заметим, что функция f может естественным образом рассматриваться как элемент k-значной логики P_k. Благодаря этому в нашем распоряжении оказывается операция суперпозиции, а также знания о предполных классах. Используемые в дальнейшем понятия и факты из k-значной логики описаны, например, в [9].

Квазигруппа называется полиномиально полной, если система из функции f и всех констант полна: $\left[\{f\} \cup P_k^0\right] = P_k$. Квазигруппа называется простой, если операция f не сохраняет никакое нетривиальное отношение эквивалентности. Несложно заметить, что квазигрупповая операция может сохранять только равномерное разбиение (то есть порождающее равномощные классы эквивалентности), поэтому все квазигруппы простого порядка являются простыми.

Квазигруппа аффинна, если на множестве Q можно задать структуру абелевой группы $(Q, +)$, относительно которой найдутся автоморфизмы α и β и константа $c \in Q$, такие что $f(x, y) = \alpha(x) + \beta(y) + c$. В работе [10] по сути показано, что простая квазигруппа аффинна тогда и только тогда, когда f является квазилинейной функцией.

Известно ([11, 12]), что полиномиальная полнота эквивалентна одновременной простоте и неаффинности (невложенности f ни в один из классов $\mathfrak{U}$, $\mathfrak{L}$ в обозначениях [9]). Несложно увидеть, что при $k = 2$ или 3 все квазигрупповые операции линейны, поэтому полиномиально полных квазигрупп нет. Примеры полиномиально полных квазигрупп порядка 4 приведены в работе [6].

3. Случай квазигрупп простого порядка

В случае квазигрупп простого порядка отсутствие полиномиальной полноты эквивалентно одновременной линеаризуемости всех одноместных

функций вида $f(x,a)$ и $f(a,y)$ при $a \in Q$. Более формально, верен следующий факт.

Теорема 1 ([7]). *Пусть p — простое число, $p \geq 5$, (Q,f) — 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, то есть линейными перестановками набора $(0,1,\ldots,p-1)$.*

Используя это утверждение, несложно построить полиномиальный от порядка квазигруппы алгоритм, проверяющий полиномиальную полноту. Достаточно заметить, что после умножения всех перестановок-строк латинского квадрата на перестановку, обратную первой строке, в случае неполноты все строки примут вид $x+d_i$, $d_i \in Q$, и для восстановления линеаризующего отображения по сути достаточно перебрать всевозможные варианты для константы, соответствующей второй строке. Для каждого варианта потребуется найти коэффициенты линейного представления (с константной сложностью) и проверить истинность найденного представления (со сложностью, квадратичной от порядка). Таким образом, верно следующее утверждение.

Теорема 2 ([7]). *Задача проверки полиномиальной полноты квазигрупп простого порядка решается за время, кубическое от порядка квазигруппы.*

Заметим, что уже в случае порядка 4 описанная идеология перестает работать, так как полиномиально полные квазигруппы порядка 4 существуют, но все перестановки квазилинейны.

Из теоремы 1 вытекает ряд несложных следствий.

Следствие 1 ([7]). *Почти все квазигруппы простого порядка полиномиально полны и не изотопны полиномиально неполным квазигруппам.*

Следствие 2 ([7]). *Для любой квазигруппы простого порядка, не являющейся полиномиально полной, существует изотопная ей полиномиально полная квазигруппа.*

Из теоремы 1 также следует, что в случае отсутствия полиномиальной полноты строки и столбцы латинского квадрата, задающего операцию f, при некоторой кодировке соответствуют линейным функциям вида $ax + b \mod p$, где параметр a одинаков для всех строк (столбцов). Как известно, линейная перестановка либо является тождественной, либо представляет из себя циклический сдвиг (случай $a = 1$, $b \neq 0$), либо состоит из одной неподвижной точки и s циклов длины t, $st = p-1$. Для удобства в первых двух случаях будем считать, что $s = 1$. Изменение кодировки действует на перестановки как сопряжение, то есть сохраняет цикловую структуру.

Следствие 3 ([7]). *Если в латинском квадрате простого порядка есть строка (столбец) с нелинейной цикловой структурой, или же две строки (два столбца) с линейной цикловой структурой, но различными значениями параметра s, то соответствующая квазигруппа является полиномиально полной.*

Заметим, что условия следствия 3 могут быть проверены со сложностью, квадратичной от порядка квазигруппы, поэтому разумно добавить такую проверку в начало процедуры распознавания полиномиальной полноты, имеющей, как было указано выше, кубическую сложность.

4. Случай порядка, не представимого в виде степени простого числа

Из результатов работы [10] следует, что если порядок квазигруппы не представим в виде p^t ни для какого простого p и натурального t, то полиномиальная полнота эквивалентна простоте. Проверка простоты квзигруппы может быть проведена, например, так. Для каждой пары (q_1, q_i), где q_1 — выделенный элемент Q, а q_i — произвольный элемент Q, отличный от q_1, строится транзитивное замыкание отношения $q_1 \sim q_i$ относительно операции f. Такое замыкание несложно вычислить со сложностью, кубической от порядка квазигруппы; при умножении на число пар, которые требуется рассмотреть, получается итоговая сложность алгоритма $O\left(k^4\right)$.

Теорема 3 ([8]). *Существует процедура проверки простоты квазигруппы порядка k, имеющая сложность $O\left(k^4\right)$.*

Следствие 4. *Пусть $k \in \mathbb{N}$ не представимо в виде p^t ни для какого простого p и натурального t. Тогда существует процедура проверки полиномиальной полноты квазигрупп, имеющая сложность $O\left(k^4\right)$.*

5. Общий случай

Для построения алгоритма определения полиномиальной полноты в общем случае остается рассмотреть процедуру проверки аффинности. Несложно заметить, что для аффинных квазигрупп домножение всех строк-перестановок соответствующего латинского квадрата L на перестановку, обратную первой строке, с последующей перестановкой строк позволяет получить таблицу Кэли L' для абелевой группы $(Q, +)$ из определения аффинности; после этого искомое представление $f(x, y) = \alpha(x) + \beta(y) + c$ может быть легко восстановлено. Заметим, что самым трудоемким этапом здесь является проверка ассоциативности операции, задаваемой матрицей L', то есть процедура кубическая по сложности.

Аккуратное описание алгоритма, кратко представленного выше, приведено в работе [8].

Теорема 4 ([8])**.** *Существует процедура проверки аффинности квазигруппы порядка k, имеющая сложность $O\left(k^3\right)$.*

Таким образом, верен следующий факт.

Теорема 5 ([8])**.** *Существует процедура проверки полиномиальной полноты квазигруппы порядка k, имеющая сложность $O\left(k^4\right)$.*

6. Обобщение на случай n-квазигрупп

Пусть $n, k \in \mathbb{N}$, $n > 2$; n-квазигруппой порядка k называется множество $Q = \{q_1, \ldots, q_k\}$ с n-арной операцией f, такой что для любых элементов $a_1, a_2, \ldots, a_n, b \in Q$ все уравнения

$$\begin{aligned} f(x, a_2, a_3, \ldots, a_n) &= b, \\ f(a_1, x, a_3, \ldots, a_n) &= b, \\ &\vdots \\ f(a_1, a_2, \ldots, a_{n-1}, x) &= b \end{aligned}$$

однозначно разрешимы в Q. Понятие полиномиальной полноты для n-квазигрупп вводится аналогично случаю квазигрупп. Критерии полиномиальной полноты и алгоритмы распознавания также естественным образом переносятся на n-квазигруппы. Отметим, что наиболее трудоемкие операции (вычисление транзитивного замыкания и проверка ассоциативности) не зависят от значения параметра n, так что сложностные характеристики не меняют порядок при переходе от квазигрупп к 3-квазигруппам. Итоговый результат примет следующий вид.

Теорема 6 ([8]). *Пусть $n \in \mathbb{N}$, $n > 2$ —фиксированный параметр. Тогда полиномиальная полнота n-квазигруппы порядка k может быть установлена со сложностью $O\left(k^{n+1}\right)$.*

Список литературы

[1] М.М. Глухов, "О применениях квазигрупп в криптографии", *ПДМ*, 2008, 2, 28–32.

[2] V. Shcherbacov, "Quasigroup based crypto-algorithms", arXiv:1201.3016v1.

[3] Y. Wu, Y. Zhou, J.P. Noonan, S. Agaian, C.L.P. Chen, "A Novel Latin Square Image Cipher", arXiv:1204.2310v1.

[4] A. Mileva, S. Markovski, "Quasigroup String Transformations and Hash Function Design", in: D. Davcev, J.M. Gómez (eds) *ICT Innovations*, Springer, 2009, 367–376.

[5] G. Horváth, C.L. Nehaniv, Cs. Szabó, "An assertion concerning functionally complete algebras and NP-completeness", *Theoret. Comput. Sci.*, **407** (2008), 591–595.

[6] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, "On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts", *Quasigroups and Related Systems*, **21**:2 (2013), 117–130.

[7] A.V. Galatenko, A.E. Pankratiev, S.B. Rodin, "Polynomially Complete Quasigroups of Prime Order", *Algebra and Logic*, **57**:5, (2018), 327–335.

[8] А.В. Галатенко, А.Е. Панкратьев, "О сложности проверки полиномиальной полноты конечных квазигрупп", *Дискрет. матем.*, **30**:4 (2018), 3–11.

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

[10] V.A. Artamonov, S. Chakrabarti, S.K. Pal, "Characterizations of highly non-associative quasigroups and associative triples", *Quasigroups and Related Systems*, **25** (2017), 1–19.

[11] J. Hagemann, C. Herrmann, "Arithmetical locally equational classes and representation of partial functions", *Universal Algebra, Esztergom (Hungary)*, **29** (1982), 345–360.

[12] В.Л. Югай, "Об одном критерии полиномиальной полноты квазигрупп", *Интеллектуальные системы. Теория и приложения*, **21**:3 (2017), 131–135.

Polynomial completeness of finite quasigroups
Galatenko A.V., Pankratiev A.E., Rodin S.B.

We give a survey of results connected to deciding polynomial completeness of finite quasigroups. The paper is based on a report presented at the seminar "Automata theory".

Keywords: quasigroup, Latin square, polynomial completeness, simplicity, affinity