Построение 1,2-простых квазигрупп, изотопных заданным

С. С. Чаплыгина[1]

В работе приводится алгоритм получения изотопными преобразованиями простой квазигруппы из некоторой заданной квазигруппы. Также доказывается, что алгоритм имеет квадратичную сложность и что полученная в результате квазигруппа не содержит собственных подквазигрупп. Приведен пример реализации алгоритма на языке Python.

Ключевые слова: квазигруппа, простота квазигруппы, подквазигруппа, изотопность квазигрупп, латинский квадрат.

1. Введение

Конечные квазигруппы (или латинские квадраты, если их рассматривать в терминах таблиц Кэли) вызывают интерес у различных исследователей в области криптографии и кодирования (см., например, [1]). Для исследователей зачастую важны квазигруппы, которые обладают некоторыми особыми свойствами. Одним из желательных свойств является полиномиальная полнота [2], обеспечивающая NP-полноту задачи проверки разрешимости уравнений [3]. Известно, что полиномиальная полнота эквивалента одновременной простоте и неаффинности [4]. Еще одним важным свойством является отсутствие собственных подквазигрупп или собственных подквазигрупп порядка не меньшего 2, что отражено в работе [5]. В работе Т. Кепки [6] доказано, что любую конечную квазигруппу порядка > 2 с помощью изотопий можно перевести в квазигруппу, не имеющую собственных подквазигрупп, или в квазигруппу, не имеющую собственных подквазигрупп порядка ≥ 2 и одновременно простую.

В данный работе излагается квадратичный алгоритм преобразования произвольной квазигруппы порядка > 2 в изотопную квазигруппу, не имеющую собственных подквазигрупп, созданный на основе работы Т. Кепки [6]. Кроме того, показывается, что результирующая квазигруппа является простой.

Автор выражает искреннюю благодарность к.ф.-м.н., с.н.с. Галатенко Алексею Владимировичу за постановку задачи и поддержку в работе.

[1] *Чаплыгина Светлана Сергеевна* — студент 3 курса каф. МаТИС мех.-мат. ф-та МГУ, e-mail: Svetlana.Chaplygina@student.msu.ru.

Chaplygina Svetlana Sergeevna — 3rd year student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of MaTIS.

2. Основные понятия и результаты

В дальнейшем все структуры будут полагаться конечными, поэтому для краткости слово “конечный” будет опускаться.

Определение 1. *Квазигруппой порядка $k \in \mathbb{N}$ называется такое множество $Q = \{q_1, \ldots, q_k\}$ с бинарной операцией $\cdot\colon Q \times Q \to Q$, что для любых $a, b \in Q$ уравнения $x \cdot a = b$ и $a \cdot y = b$ однозначно разрешимы.*

Таблицы Кэли квазигрупп являются латинскими квадратами, и наоборот, любой латинский квадрат является таблицей Кэли квазигруппы.

Определение 2. *Собственной подквазигруппой квазигруппы $(Q, \cdot)$ называется пара $(Q', \cdot')$, где Q' — собственное подмножество Q, замкнутое относительно $\cdot$, а операция $\cdot'$ является сужением $\cdot$ на $Q' \times Q'$.*

В дальнейшем для краткости будем отождествлять собственные подквазигруппы с множеством Q'.

Без ограничения общности можно считать, что $Q = \{0, \ldots, k-1\}$, а операция $\cdot$ есть функция k-значной логики от двух переменных.

Определение 3. *Квазигруппа $(Q, \cdot)$ называется полиномиально полной, если $\left[\{\cdot\} \cup P_k^0\right] = P_k$, где P_k^0 — множество всех констант.*

Определение 4. *Квазигруппа $(Q, \cdot)$ называется простой (или в терминах работы [6], 1-простой), если операция $\cdot$ не сохраняет ни одного нетривиального отношения эквивалентности.*

Определение 5. *Квазигруппа $(Q, \cdot)$ называется аффинной, если существует абелева группа $(Q, +)$, автоморфизмы α и β этой группы и константа $c \in Q$, для которых выполнено тождество $x \cdot y \equiv \alpha(x) + \beta(y) + c$.*

В работе [6] использовались следующие понятия.

Определение 6. *Квазигруппа $(Q, \circ)$ называется 2-простой, если она не содержит собственных подквазигрупп, и 3-простой, если она не содержит собственных подквазигрупп порядка ≥ 2.*

Определение 7. *Квазигруппа $(Q, \circ)$ называется левой (правой) лупой, если существует такой элемент $j \in Q$, что для любого $x \in Q$ выполнено равенство $j \cdot x = x$, ($x \cdot j = x$, соответственно). Если существует $j \in Q$, такой что $j \cdot x = x \cdot j = x$ для любого $x \in Q$, то квазигруппа называется лупой.*

Определение 8. *Квазигруппы $Q(\cdot)$ и $Q(\circ)$ будем называть изотопными, если существуют перестановки $\sigma_1, \sigma_2, \sigma_3$ на Q, для которых выполнено $\forall x, y \in Q\colon \quad x \cdot y = \sigma_3^{-1}(\sigma_1(x) \circ \sigma_2(y))$.*

В терминах таблиц Кэли это означает возможность преобразования одной таблицы в другую перестановкой строк, столбцов, а также переименованием элементов.

Рассмотрим следующий алгоритм для квазигруппы $Q(\cdot)$ порядка n.

Перестановкой строк и столбцов добьемся преобразования данной квазигруппы $Q(\cdot)$ в лупу $Q(\star)$. Затем сделаем циклический сдвиг строк $1, 2, \ldots, n-1 \to 2, 3, \ldots, n-1, 1$, первая строка (то есть строка 0) остается на месте. Наконец, переставим столбцы 0 и 1.

Данный алгоритм является алгоритмизацией (с сужением на конечный случай) доказательства утверждений из работы [6]. Элементарными операциями считаются чтение из памяти или запись в память элемента из множества $Q = E_k$, а также арифметические операции на $\mathbb{Z}_k$.

Основным результатом данной работы являются утверждения:

Теорема 1. *Выходом алгоритма является 2-простая квазигруппа, изотопная входной квазигруппе. Временная сложность алгоритма есть* $O(k^2)$ *при* $k \to \infty$.

Теорема 2. *Квазигруппа, полученная в результате алгоритма, является простой, то есть не сохраняет ни одного нетривиального отношения эквивалентности.*

Так как все квазигруппы порядка 3 аффинны, в случае $k = 3$ на выходе алгоритма могут возникать аффинные квазигруппы, то есть квазигруппы, не являющиеся полиномиально полными.

Алгоритм был реализован на языке программирования Python и протестирован на наборе квазигрупп различного порядка. Время работы программы квадратично зависело от порядка входных квазигрупп.

Код реализации можно найти на github под открытой MIT лицензией (https://github.com/Rinroli/simple-quasigroups). Там же находятся небольшая документация и примеры.

3. Заключение

В работе был построен квадратичный алгоритм получения с помощью изотопии одновременно простой и 2-простой квазигруппы из некоторой заданной. Этот алгоритм был программно реализован и протестирован на наборе квазигрупп различного порядка. Проведенные эксперименты показали, что время работы программы квадратично зависит от порядка квазигрупп.

В дальнейшем планируется обобщить результаты на структуры более высоких размерностей.

Список литературы

[1] Chauhan D., Gupta I., Verma R., "Quasigroups and their applications in cryptography", *Cryptologia*, **45**:3 (2021), 227-265.

[2] 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*, **21**:2 (2013), 117–130.

[3] G. Horváth, C.L. Nehaniv, Cs. Szabó, "An assertion concerning functionally complete algebras and NP-completeness", *Theoretical Computer Science*, **407** (2008), 591–595.

[4] Hagemann J. and Herrmann C., "Arithmetical locally equational classes and representation of partial functions", *Colloquia Math. Soc. Janos Bolyai*, **29** (1982), 345–360.

[5] Галатенко А.В., Панкратьев А.Е., Староверов В.М., "Об одном алгоритме проверки существования подквазигрупп", *Чебышевский сборник*, **22**:2 (2021), 76–89.

[6] Kepka T., "A note on simple quasigroups", *Acta Universitatis Carolinae. Mathematica et Physica.*, **19**:2 (1978), 59–60.

Construction of 1,2-simple quasigroups isotopic to the given ones

Chaplygina S.S.

The paper provides an algorithm for obtaining a simple quasigroup from a given one in isotopic way, proves that the algorithm has quadratic complexity and that the result doesn't contain proper subquasigroups. Python implementation of the algorithm is given.

Keywords: quasigroup, simplicity of quasigroup, subquasigroup, isotropy of quasigroups, Latin square.

References

[1] Chauhan D., Gupta I., Verma R., "Quasigroups and their applications in cryptography", *Cryptologia*, **45**:3 (2021), 227-265.

[2] 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*, **21**:2 (2013), 117–130.

[3] G. Horváth, C.L. Nehaniv, Cs. Szabó, "An assertion concerning functionally complete algebras and NP-completeness", *Theoretical Computer Science*, **407** (2008), 591–595.

[4] Hagemann J. and Herrmann C., "Arithmetical locally equational classes and representation of partial functions", *Colloquia Math. Soc. Janos Bolyai*, 1982, №29, 245–360.

[5] Galatenko A.V., Pankratiev A.E., Staroverov V.M., "An algorithm for checking the existence of subquasigroups", *Chebyshevskii sbornik*, **22**:2 (2021), 76–89 (In Russian).

[6] Kepka T., "A note on simple quasigroups", *Acta Universitatis Carolinae. Mathematica et Physica.*, **19**:2 (1978), 59–60.