Эффективность проверки существования n-подквазигрупп

А. В. Галатенко[1], А. Е. Панкратьев[2], В. М. Староверов[3]

В работе описан алгоритм проверки наличия n-подквазигрупп, приведена оценка временной и пространственной сложности и исследована практическая эффективность этого алгоритма.

Ключевые слова: n-квазигруппы, n-подквазигруппы

1. Введение

В последние годы возник интерес к использованию некоммутативных и неассоциативных алгебраических структур для построения криптоалгоритмов [1]. Одним из ярких примеров некоммутативных и неассоциативных структур являются конечные квазигруппы, на основе которых построено значительное количество шифров, хэш-функций, алгоритмов электронной подписи и других криптографических примитивов (см., например, обзоры [2, 3]). Привлекают интерес и структуры более высокой арности — n-квазигруппы при $n \geq 3$. Публикуются работы о криптографически важных свойствах n-квазигрупп [4, 5, 6], предлагаются реализации алгоритмов (см., например, [7]).

Одним из криптографически важных свойств n-квазигрупп является "бедная" структура n-подквазигрупп (подмножеств, сохраняемых n-квазигрупповой операцией). В целом наличие нетривиальных n-подквазигрупп нежелательно, так как может привести к вырождению операции со всего универсума на универсум n-подквазигруппы; в ряде случаев n-подквазигруппы порядка 1, т.е. "неподвижные точки", считаются допустимыми. Таким образом, приобретают актуальность задачи эффективной проверки наличия произвольных собственных n-подквазигрупп и собственных n-квазигрупп порядка не ниже 2. В работе [6] были предложены алгоритмы для решения этих задач и приведена

[1] *Галатенко Алексей Владимирович* — старший научный сотрудник каф. МаТИС мех.-мат. ф-та МГУ, e-mail: agalat@msu.ru.

Galatenko Alexei Vladimirovich — senior researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, MaTIS chair

[2] *Панкратьев Антон Евгеньевич* — доцент каф. МаТИС мех.-мат. ф-та МГУ, e-mail: apankrat@intsys.msu.ru.

Pankratiev Anton Evgenievich — associate professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, MaTIS chair

[3] *Староверов Владимир Михайлович* — доцент каф. выч. мат. мех.-мат. ф-та МГУ, e-mail: staroverovvl@imscs.msu.ru.

Staroverov Vladimir Mikhailovich — associate professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Computational Mathematics

оценка временной сложности. Мы уточняем результаты [6], добавив к ним оценки пространственной сложности и практической эффективности.

Дальнейшее изложение имеет следующую структуру. В разделе 2 даются необходимые определения и формулируется основной результат. В разделе 3 описывается программная реализация алгоритма и приводятся результаты тестирования. Раздел 4 является заключением.

2. Основные понятия и результаты

Определение 1. *Конечной n-квазигруппой называется пара (Q, f), где $Q = \{q_1, \ldots, q_k\}$ — конечное множество, а $f\colon Q^n \to Q$ такова, что при произвольной фиксации любых $n-1$ переменных результат является биекцией, то есть перестановкой на множестве Q. При этом операция f называется n-квазигрупповой.*

В дальнейшем все структуры будут конечными, поэтому для краткости слово "конечный" будет опускаться.

Определение 2. *Пусть $Q' \subset Q$, $1 \leq |Q'| < |Q|$. Если $f(Q') = Q'$, то говорим, что n-квазигруппа (Q, f) содержит собственную n-подквазигруппу (Q', f'), где f' — ограничение операции f на $(Q')^n$. Если дополнительно выполнено условие $|Q'| > 1$, то подквазигруппа называется нетривиальной.*

В дальнейшем для краткости мы будем отождествлять n-подквазигруппу (Q', f') с множеством Q'.

Определение 3. *Пусть M, $|M| < \infty$ — некоторое множество, $t \in \mathbb{N}$, $M_1, \ldots, M_t$ — подмножества M. Множество $M_0 \subseteq M$ называется системой представителей для $M_1, \ldots, M_t$, если для всех i от 1 до t найдется элемент $m_i \in M_0$, такой что $m_i \in M_i$.*

Элемент $m_i \in M_0$, такой что $m_i \in M_i$, называется представителем множества M_i. Заметим, что представители для различных i могут совпадать.

Пусть n-квазигруппы заданы таблично. В этом случае вычисление значения f на заданном наборе является элементарной операцией. Случай функционального задания n-квазигрупп является предметом будущих исследований.

Авторами предлагается алгоритм проверки наличия n-подквазигрупп порядка $\geq d$ на основе использования систем представителей частичных замыканий всех d-элементных подмножеств Q.

Теорема 1. *Предложенный алгоритм корректно определяет наличие n-подквазигрупп порядка $\geq d$. В случае $d = 1$ временная сложность составляет $O\left(k^{\frac{n^2+n+1}{n+1}} \log^{\frac{n}{n+1}} k\right)$, а пространственная сложность есть $O(k^n)$ при фиксированном n и $k \to \infty$. В случае $d = 2$ временная сложность составляет $O\left(k^{\frac{n^2+2n+4}{n+2}} \log^{\frac{n}{n+2}} k\right)$, а пространственная сложность есть $O(k^n)$ при фиксированном $n \geq 3$ и $O\left(k^{5/2} \log^{1/3} k\right)$ при $n = 2$ и $k \to \infty$.*

Заметим, что таблица Кэли n-квазигрупповой операции состоит из k^n элементов.

3. Оценка практической эффективности

Алгоритм был программно реализован и протестирован для случая $n = 3$ на рабочей станции с 8-ядерным процессором i7–3770 CPU @3.40GHz и 32 гигабайтами памяти. Оказалось, что в случае $d = 1$ алгоритм практически мгновенно обрабатывает 3-квазигруппу любого порядка, помещающуюся в оперативную память. В случае $d = 2$ время увеличивается, но все еще не превосходит минуты. Максимальные времена обработки в секундах приведены в следующей таблице.

d	$\lvert Q\rvert = 256$	$\lvert Q\rvert = 512$	$\lvert Q\rvert = 1024$	$\lvert Q\rvert = 2048$
1	0	0	3	5
2	1	1	6	42

4. Заключение

В работе описан алгоритм проверки наличия n-подквазигрупп, приведена оценка временной и пространственной сложности и исследована практическая эффективность этого алгоритма. В дальнейшем планируется исследовать случай функционального задания операции.

Список литературы

[1] Markov V. T., Mikhalev A. V., Nechaev A. A., “Nonassociative algebraic structures in cryptography and coding”, *Journal of Mathematical Sciences*, **245**:2 (2020), 178–196.

[2] Глухов М. М., “О применениях квазигрупп в криптографии”, *Прикладная дискретная математика*, 2008, № 2, 28–32.

[3] Shcherbacov V. A., “Quasigroups in cryptology”, *Computer Science Journal of Moldova*, **17**:2(50) (2009), 193–228.

[4] Dimitrova V., Mihajloska H., "Classification of ternary quasigroups of order 4 applicable in cryptography", Proceedings of the 7th International Conference for Informatics and Information Technology (CIIT 2010), 2010, 145–148.

[5] Галатенко А. В., Панкратьев А. Е., Староверов В. М., "Проверка полиномиальной полноты n-квазигрупп", Материалы XVIII Международной конференции «Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории», 2020, 146–150.

[6] Галатенко А. В., Панкратьев А. Е., Староверов В. М., "Об одном алгоритме проверки существования нетривиальных n-подквазигрупп", Материалы XIX Международной конференции «Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории», 2021, 100–103.

[7] Dömösi P., Horváth G., "A novel cryptosystem based on abstract automata and Latin cubes", *Studia Scientiarum Mathematicarum Hungarica*, **52**:2 (2015), 221–232.

Efficiency of deciding existence of n-subqusdigroups

Galatenko A.V., Pankratiev A.E., Staroverov V.M.

We describe an algorithm that decides the presence of n-subquasigroups, estimate temporal and spatial complexity of this algorithm and investigate practical efficiency.

Keywords: n-quasigroup, n-subquasigroup

References

[1] Markov V. T., Mikhalev A. V., Nechaev A. A., "Nonassociative algebraic structures in cryptography and coding", *Journal of Mathematical Sciences*, **245**:2 (2020), 178–196.

[2] Glukhov M. M., "Applications of quasigroups in cryptography", *Applied Discrete Mathematics*, 2008, № 2, 28–32 (In Russian).

[3] Shcherbacov V. A., "Quasigroups in cryptology", *Computer Science Journal of Moldova*, **17**:2(50) (2009), 193–228.

[4] Dimitrova V., Mihajloska H., "Classification of ternary quasigroups of order 4 applicable in cryptography", Proceedings of the 7th International Conference for Informatics and Information Technology (CIIT 2010), 2010, 145–148.

[5] Galatenko A. V., Pankratiev A. E., Staroverov V. M., "Deciding polynomial completeness of n-quasigroups", Proc. 18th Int. Conf. "Algebra, number theory and discrete geometry: modern problems, applications and problems of history", 2020, 146–150 (In Russian).

[6] Galatenko A. V., Pankratiev A. E., Staroverov V. M., "An algorithm for deciding existence of nontrivial n-subquasigroups", Proc. 19th Int. Conf. "Algebra, number theory and discrete geometry: modern problems, applications and problems of history", 2021, 100–103 (In Russian).

[7] Dömösi P., Horváth G., "A novel cryptosystem based on abstract automata and Latin cubes", *Studia Scientiarum Mathematicarum Hungarica*, **52**:2 (2015), 221–232.