Оценка количества n-квазигрупп на выходе алгоритма изотопного преобразования, гарантирующего криптографические свойства

С. С. Чаплыгина*

В работе рассматриваются n-квазигруппы в контексте свойств, важных для криптографических приложений. Для параметризованного семейства изотопных преобразований приводится оценка числа различных n-квазигрупп, получаемых из данной n-квазигруппы применением различных преобразований семейства.

Ключевые слова: n-квазигруппа, изотопия, полиномиальная полнота, простота, неаффинность, подквазигруппа.

1. Введение

Квазигруппы и их многомерные обобщения (n-квазигруппы) являются перспективным направлением в современной криптографии. Обзор алгоритмов на основе квазигрупп приведен, например, в работе [1]. Структуры большей арности, то есть n-квазигруппы, также востребованы исследователями, в качестве примера можно привести работу [2].

Для исследователей зачастую интересны квазигруппы и n-квазигруппы, обладающие определенным набором свойств, помогающим обеспечить стойкость для криптографических алгоритмов. Одним из важнейших свойств является полиномиальная полнота квазигрупп, предложенная В.А. Артамоновым и соавторами в работе [3]. Данное понятие переносится и на случай n-квазигрупп. Как было показано в работе [4], полиномиальная полнота эквивалентна одновременной простоте и неаффинности n-квазигруппы порядка $k \geq 5$. Еще одним примечательным свойством является отсутствие собственных подквазигрупп у n-квазигруппы. Данное свойство также рассматривалось В.А. Артамоновым и соавторами [5].

* *Чаплыгина Светлана Сергеевна* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: svetlana.chaplygina@math.msu.ru, ORCID: 0009-0002-4355-6706.

Chaplygina Svetlana Sergeevna — Postgraduate Student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

Для практических применений необходимо уметь получать n-квазигруппы, обладающие описанными выше свойствами. Одним из способов является преобразование данной n-квазигруппы в n-квазигруппу, обладающую особыми свойствами. В работе [6] было анонсировано семейство алгоритмов изотопного преобразования данной n-квазигруппы в полиномиально полную, простую и неаффинную n-квазигруппу без собственных подквазигрупп. Выбор конкретного алгоритма из семейства осуществлялся за счет параметризации.

В данной работе приводится оценка числа попарно различных n-квазигрупп на выходе семейства изотопных преобразований при варьировании параметров алгоритма.

2. Основные определения и результаты

Определение 1. Назовем конечной n-квазигруппой порядка $k \in \mathbb{N}$ такое множество $Q = \{q_1, \ldots, q_k\}$ с n-арной операцией $f\colon Q^n \to Q$, что для любых элементов $x_1, \ldots, x_n, y \in Q$ для любого i уравнение

$$f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n) = y$$

однозначно разрешимо. Другими словами, операция f обратима по каждому аргументу.

В дальнейшем речь в работе пойдёт об исследовании случая конечных n-квазигрупп, поэтому здесь и далее под термином "n-квазигруппа" будет подразумеваться "конечная n-квазигруппа", если не сказано иное.

Определение 2. Будем называть n-квазигруппы (Q, f) и (Q, g) порядка k изотопными, если существуют перестановки $\sigma, \sigma_1, \ldots, \sigma_n$ на Q, для которых выполнено тождество

$$f(x_1, \ldots, x_n) = \sigma(g(\sigma_1(x_1), \ldots, \sigma_n(x_n))).$$

В терминах таблиц умножения изотопия означает перестановку $(n-1)$-мерных слоёв и переименование элементов.

Без ограничения общности можно считать, что $Q = E_k$. Рассмотрим n-квазигрупповую операцию f как функцию k-значной логики. Обозначим через P_k множество всех функций k-значной логики, а через P_k^0 множество всех констант. Обозначим через $[A]$ для множества функций $A \subseteq P_k$ множество всех функций из P_k, которые можно получить из множества A с помощью операций суперпозиции.

Определение 3. Назовем n-квазигруппу (E_k, f) полиномиально полной, если выполнено равенство $\left[\{f\} \cup P_k^0\right] = P_k$.

Определение 4. Собственной подквазигруппой n-квазигруппы (E_k, f) называется пара (Q', f'), где Q' — собственное подмножество E_k, замкнутое относительно квазигрупповой операции f, а операция f' является сужением f на множество $Q' \times \ldots \times Q'$.

Определение 5. Назовём n-квазигруппу простой, если она не сохраняет ни одного нетривиального отношения эквивалентности.

Определение 6. Квазигруппа называется аффинной, если найдётся абелева группа $(E_k, +)$, автоморфизмы $\alpha_1, \ldots, \alpha_n$ этой группы и константа $c \in E_k$, для которых выполнено тождество $f(x_1, \ldots, x_n) \equiv \alpha_1(x_1) + \ldots + \alpha_n(x_n) + c$.

В работе [6] было анонсировано семейство изотопных преобразований, гарантирующее выполнение приведенных выше свойств для выходной n-квазигруппы порядка $k \geq 5$ для $n \geq 3$. Данный алгоритм можно представить как последовательное применение трех шагов, каждый из которых является изотопией. Первые два шага определяют перестановки из множества $\{\sigma_1, \ldots, \sigma_n\}$ перестановок из определения изотопии. Третий шаг определяет перестановку-переименование σ.

Было показано, что для фиксированной n-квазигруппы и для произвольной фиксированной параметризации первых двух шагов при варьировании перестановки σ в рамках алгоритма n-квазигруппы на выходе преобразования будут попарно различны. Была получена следующая оценка числа n-квазигрупп после применения алгоритма:

Утверждение 1. *Пусть (E_k, f) n-квазигруппа порядка $k \geq 5$ для $n \geq 3$. Количество попарно различных n-квазигрупп после применения алгоритма изотопного преобразования к n-квазигруппе (E_k, f) при различном выборе параметров алгоритма не меньше $\left(\frac{k-1}{6}\right)^{\frac{k-1}{2}}$.*

Список литературы

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

[2] Y. Cheng, Y. Xu, “Stream cipher based on Latin cubes”, *Proceedings of the First International Conference on Information Science and Electronic Technology*, 2015, 137–140. DOI: 10.2991/iset-15.2015.35.

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

[4] S. S. Chaplygina, A. V. Galatenko, “Polynomial completeness and completeness of finite n-quasigroups”, *Quasigroups and Related Systems*, **32**:2 (2024), 207–223.

[5] В. А. Артамонов, С. Чакрабарти, Ш. К. Тивари, В. Т. Марков, "Алгебраические свойства подквазигрупп и построение конечных квазигрупп", *Алгебра и логика*, **61**:4 (2022), 375–400.

[6] С. С. Чаплыгина, "Изотопные преобразования n-квазигрупп, улучшающие криптографические свойства", принято к публикации, *Международная конференция Мальцевские чтения. Тезисы докладов*, 2026.

Статья поступила 6 ноября 2026 г.

An estimate for the number of n-quasigroups at the output of the isotopic transformation algorithm, which guarantees cryptographic properties

S. S. Chaplygina

The paper considers n-quasigroups in the context of properties relevant to cryptographic applications. For a parameterized family of isotopic transformations, an estimate is given for the number of distinct n-quasigroups obtained from a given n-quasigroup by applying different transformations of the family.

Keywords: n-quasigroup, isotopy, polynomial completeness, simplicity, non-affineness, subquasigroup.

References

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

[2] Y. Cheng, Y. Xu, "Stream cipher based on Latin cubes", *Proceedings of the First International Conference on Information Science and Electronic Technology*, 2015, 137–140. DOI: 10.2991/iset-15.2015.35.

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

[4] S. S. Chaplygina, A. V. Galatenko, "Polynomial completeness and completeness of finite n-quasigroups", *Quasigroups and Related Systems*, **32**:2 (2024), 207–223.

[5] V. A. Artamonov, S. Chakrabarti, S. K. Tiwari, V. T. Markov, "Algebraic Properties of Subquasigroups and Construction of Finite Quasigroups", *Algebra and Logic*, **61**:4 (2022), 251–270. DOI: 10.1007/s10469-023-09695-1.

[6] S. S. Chaplygina, "Isotopic transformations of n-quasigroups improving cryptographic properties", accepted for publication, *International Conference "Mal'tsev Readings". Book of Abstracts*, 2026 (In Russian).

Received on November 6, 2026