Квадратичный алгоритм проверки бесформенности конечных квазигрупп

Р. А. Жигляев*

В работе приводится алгоритм проверки бесформенности конечных квазигрупп, имеющий квадратичную по порядку квазигруппы сложность по времени и по памяти. В частности, представлен квадратичный алгоритм проверки отсутствия собственных подквазигрупп как одного из свойств, входящего в понятие бесформенности.

Ключевые слова: квазигруппа, подквазигруппа, бесформенность .

1. Введение

Конечные квазигруппы применяются в криптографических алгоритмах Edon-R' [1] и NaSHA [2], построении A-кодов и однонаправленных функций [3]. Важные криптографические требования к ним – отсутствие собственных подквазигрупп и бесформенность: подквазигруппы могут упрощать атаки на криптосистему, а их отсутствие входит в более обширное понятие бесформенности. Для ускорения работы криптосистем необходимо проверять требуемые свойства с наибольшей эффективностью.

В работе предложены алгоритмы проверки бесформенности и существования собственной подквазигруппы с квадратичной по порядку квазигруппы сложностью по времени и памяти.

2. Основные определения

Определение 1. Конечное множество Q, на котором задана бинарная операция умножения $*$: $Q \times Q \to Q$, такая, что для любых элементов $a, b \in Q$ уравнения $a * x = b$ и $y * a = b$ однозначно разрешимы в Q, называется *конечной квазигруппой*. Операцию $*$ будем называть квазигрупповой.

Далее речь будет идти только о конечных квазигруппах, поэтому слово «конечная» будет опускаться, а множество Q будем считать непустым.

* *Жигляев Родион Алексеевич* — аспирант каф. МаТИС мех.-мат. факультета МГУ, e-mail: rzhiglyaev@mail.ru, ORCID: 0000-0002-2008-8674.

Zhigliaev Rodion Alekseevich — PhD student, Department of Mathematical Theory of Intelligent Systems, Faculty of Mechanics and Mathematics, Moscow State University.

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

Будем считать, что все квазигруппы заданы своими таблицами умножения, а вычисление умножения в квазигруппе будем считать элементарной операцией.

Определение 2. Пусть задана квазигруппа $(Q, *)$ и $Q' \subset Q$, $1 \leq |Q'| < |Q|$. Если для любых элементов $a, b \in Q'$ верно, что $a * b \in Q'$, то будем говорить, что квазигруппа $(Q, *)$ содержит собственную подквазигруппу $(Q', *')$, где $*'$ — ограничение операции $*$ на $Q' \times Q'$.

Определение 3. Квазигруппа $(Q, *)$ порядка N называется бесформенной, если:

- квазигруппа не идемпотентна, т.е. $\exists x \in Q$, т.ч. $x * x \neq x$;
- квазигруппа не коммутативна, т.е. $\exists x, y \in Q$, т.ч. $x * y \neq y * x$;
- квазигруппа не ассоциативна, т.е. $\exists x, y, z \in Q$, т.ч. $(x * y) * z \neq x * (y * z)$;
- квазигруппа не содержит ни левой, ни правой единицы, т.е. не существует $e_1 \in Q$, т.ч. $\forall x \in Q\ e_1 * x = x$, и не существует $e_2 \in Q$, т.ч. $\forall x \in Q\ x * e_2 = x$;
- квазигруппа не содержит собственных подквазигрупп;
- не существует целого k с $0 < k < 2N$, при котором выполняется хотя бы одно из тождеств

$$\underbrace{x * (x\ ... * (x}_{k} * y)) = y,\ y = ((y * \underbrace{x) * ...\ x) * x}_{k}\ \forall x, y \in Q.$$

3. Описание алгоритма

Проверка бесформенности заключается в поочередной проверке каждого из свойств, входящих в определение. Проверка идемпотентности, коммутативности и существования единиц, очевидно, осуществляется простым перебором с не более чем квадратичной сложностью по времени и памяти. Для проверки ассоциативности известен квадратичный алгоритм, представленный в работе [4]. Для проверки существования собственной подквазигруппы можно воспользоваться описанным далее алгоритмом.

Алгоритм 1 Проверка существования собственной подквазигруппы

выбрать $a \in Q$ и пометить посещённым
$t \leftarrow 1$; $B_1 \leftarrow \{a\}$; $P_1 \leftarrow [(a, a)]$
while true **do**
    if $P_t = \emptyset$ **then**
        return «существует», если $|B_t| < N$; иначе «не существует»
    end if
    извлечь (x, y) из P_t; $z \leftarrow x * y$
    if $z \notin B_t$ **then**
        if z не посещён **then**
            пометить z посещённым; $t \leftarrow t + 1$
            $B_t \leftarrow \{z\}$; $P_t \leftarrow [(z, z)]$
        else
            найти $i < t$ с $z \in B_i$
            $B \leftarrow \bigcup_{j=i}^{t} B_j$
            $P \leftarrow$ очереди $P_i, \ldots, P_t$, объединённые без копирования
            добавить в P все пары $(u, v) \in B_p \times B_q$, где $i \le p, q \le t$ и $p \ne q$
            $t \leftarrow i$; $B_t \leftarrow B$; $P_t \leftarrow P$
        end if
    end if
end while

Приведем также алгоритм проверки тождества $\underbrace{x * (x \ ... * (x}_{k} * y)) = y$. Для второго тождества алгоритм выглядит аналогичным образом.

Алгоритм 2 Проверка левого тождества

$k \leftarrow 1$
for all $x \in Q$ **do**
    пометить все элементы непосещёнными
    for all $y \in Q$ **do**
        if y посещён **then continue**
        end if
        $z \leftarrow x * y$, $len \leftarrow 1$
        while $z \ne y$ **do**
            пометить z посещённым; $z \leftarrow x * z$, $len \leftarrow len + 1$
        end while
        пометить y посещённым; $k \leftarrow \mathrm{lcm}(k, len)$
        if $k \ge 2N$ **then return** «не выполняется при $0 < k < 2N$»
        end if
    end for
end for
return «выполняется при найденном k»

Теорема 1. *Существует алгоритм проверки бесформенности конечной квазигруппы со сложностью $O(N^2)$ по времени и памяти, где N – порядок квазигруппы.*

Список литературы

[1] D. Gligoroski, R. S. Ødegård, M. Mihova, S. J. Knapskog, A. Drapal, V. Klíma, J. Amundsen, M. El-Hadedy, "Cryptographic hash function EDON-R'", *Proceedings of the 1st International Workshop on Security and Communication Networks*, IEEE, 2009, 1–9.

[2] S. Markovski, A. Mileva, "NaSHA — family of cryptographic hash functions", *The First SHA-3 Candidate Conference* (K.U. Leuven, Belgium, February 25–28, 2009), 2009.

[3] М. М. Глухов, "О применениях квазигрупп в криптографии", *Прикладная дискретная математика*, 2008, №2(2), 28–32. DOI: 10.17223/20710410/2/7.

[4] R. Beals, "Testing Whether a Table Defines a Group", *The American Mathematical Monthly*, **133**:5 (2026), 472–477. DOI: 10.1080/00029890.2025.2557077.

Статья поступила 8 ноября 2026 г.

Quadratic algorithm for checking shapelessness of finite quasigroups

R. A. Zhigliaev

The paper presents an algorithm for checking the shapelessness of finite quasigroups that has quadratic time and space complexity in the order of the quasigroup. In particular, a quadratic algorithm is presented for checking the absence of proper subquasigroups as one of the properties comprising the concept of shapelessness.

Keywords: quasigroup, subquasigroup, shapelessness .

References

[1] D. Gligoroski, R. S. Ødegård, M. Mihova, S. J. Knapskog, A. Drapal, V. Klíma, J. Amundsen, M. El-Hadedy, "Cryptographic hash function EDON-R'", *Proceedings of the 1st International Workshop on Security and Communication Networks*, IEEE, 2009, 1–9.

[2] S. Markovski, A. Mileva, "NaSHA — family of cryptographic hash functions", *The First SHA-3 Candidate Conference* (K.U. Leuven, Belgium, February 25–28, 2009), 2009.

[3] M. M. Glukhov, "On applications of quasigroups in cryptography", *Prikladnaya Diskretnaya Matematika*, 2008, №2(2), 28–32 (In Russian. DOI: 10.17223/20710410/2/7).

[4] R. Beals, "Testing Whether a Table Defines a Group", *The American Mathematical Monthly*, **133**:5 (2026), 472–477. DOI: 10.1080/00029890.2025.2557077.

Received on November 8, 2026