О взаимосвязи криптографически важных свойств конечных квазигрупп

Р. А. Жигляев[1]

В данной работе устанавливается взаимосвязь между некоторыми свойствами конечных квазигрупп. Доказывается, что в случае квазигрупп простого порядка из бесформенности следует полиномиальная полнота. Даны примеры, показывающие, что обратное утверждение и обобщение до составных порядков не являются верными.

Ключевые слова: конечная квазигруппа, полиномиальная полнота, бесформенность.

1. Введение

Некоммутативные и неассоциативные алгебраические структуры играют важную роль в построении криптографических алгоритмов [1]. Один из примеров таких структур – квазигруппы. В алгоритмах GAGE и InGAGE [2], участвовавших в конкурсе Lightweight Cryptography от NIST, используются e-преобразования и d-преобразования, основанные на одной из квазигрупп порядка 4. В конкурсе SHA-3 были квазигрупповые кандидаты Edon-R' [3] и NaSHA [4]. Основанное на квазигруппах табличное гаммирование обладает свойством совершенной секретности [5]. В работе [6] приводится обзор применения квазигрупп в построении однонаправленных функций, A-кодов, и методов шифрования. В [7] представлен более широкий обзор применения квазигрупп в криптографии.

У каждого криптографического алгоритма могут быть свои требования к используемым квазигруппам. Среди наиболее часто встречаемых требований можно выделить следующие: полиномиальная полнота, отсутствие собственных подквазигрупп, бесформенность [8, 9].

Полиномиальная полнота гарантирует NP-полноту задачи проверки разрешимости уравнений и систем уравнений [10, 11]. Ранее упомянутый алгоритм NaSHA требует квазигруппы больших размеров. Наличие подквазигрупп может снизить стойкость таких алгоритмов. Требование к отсутствию собственных подквазигрупп также является частью более общего набора требований, называемого бесформенностью. Аккуратные определения всех этих понятий будут даны в разделе 2.

[1] *Жигляев Родион Алексеевич* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: rzhiglyaev@mail.ru.

Zhigliaev Rodion Alekseevich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

В данной работе устанавливается взаимосвязь между понятиями бесформенности и полиномиальной полноты.

Все эксперименты в рамках данной работы проводились с использованием программы https://github.com/Gerror/Quasigroup.

Автор выражает благодарность А.В. Галатенко за постановку задачи и помощь в работе.

2. Основные определения

Введем основные определения.

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

Далее слово "конечная" будем опускать, предполагая, что речь всегда идет о конечных квазигруппах. Вместо символа f иногда для удобства будем обозначать квазигрупповую операцию символом умножения $*$.

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

Определение 3. *Квазигруппа (Q, f) называется аффинной, если на множестве Q можно ввести структуру абелевой группы $(Q, +)$, такую, что существуют автоморфизмы α, β группы $(Q, +)$ и элемент $c \in Q$, для которых выполнено тождество*

$$f(x, y) = \alpha(x) + \beta(y) + c.$$

Рассмотрим множество элементов квазигруппы $Q = \{q_1, ..., q_N\}$, $N \geq 2$ и некоторое разбиение α множества Q в объединение непересекающихся подмножеств $Q = A_1 \sqcup ... \sqcup A_m$. Будем называть разбиение α нетривиальным, если $m > 1$, $A_i \neq \emptyset$, $i = 1, ..., m$, и существует индекс j, $1 \leq j \leq m$, такой, что $|A_j| > 1$. В случае если $|A_1| = ... = |A_m|$, такое нетривиальное разбиение будем называть равномерным. Элементы a, b, которые принадлежат одному множеству A_i, далее назовем эквивалентными и будем использовать запись $a \sim b$.

Будем говорить, что f сохраняет разбиение α, если для любой пары наборов (a_1, b_1), $(a_2, b_2) \in Q^2$, таких, что $a_i \sim b_i$, $i = 1, 2$, выполнено $f(a_1, a_2) \sim f(b_1, b_2)$. Как можно заметить, квазигрупповые операции могут сохранять только равномерные разбиения.

Определение 4. *Квазигруппа (Q, f) называется простой, если операция f не сохраняет никакое нетривиальное разбиение Q.*

Для фиксированного (конечного) множества A обозначим через $\mathcal{O}_n(A)$ совокупность всех n-арных операций на A ($n \geq 0$). Под 0-арными операциями будем подразумевать константы. Пусть $\mathcal{O}(A) = \bigcup_{n=0}^{\infty} \mathcal{O}_n(A)$. Далее под множеством A понимается множество элементов квазигруппы, поэтому будем использовать упрощённую запись: $\mathcal{O}_n$ и $\mathcal{O}$.

Стандартным образом введем операции суперпозиции и замыкания [12]. Обозначим замыкание множества F через $[F]$.

Определение 5. *Квазигруппа Q называется полиномиально полной, если $[\{f\} \cup \mathcal{O}_0] = \mathcal{O}$.*

Известно, что полиномиальная полнота эквивалентна одновременной простоте и неаффинности [13].

Определение 6. *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 элементов $e_1, e_2 \in Q$, т.ч. $\forall x \in Q\ e_1 * x = x$, $x * e_2 = x$;*
- *квазигруппа не содержит собственных подквазигрупп;*
- *не существует $k < 2N$, при котором выполняются тождества*

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

Определение 7. *Автоморфизм группы G называется регулярным, если он оставляет неподвижным только тривиальный элемент из G.*

3. Сложность проверки свойств

В данном разделе при подсчете сложности будем предполагать, что квазигруппы заданы таблично, а вычисление умножения в квазигруппе – это элементарная операция.

Сложность проверки бесформенности зависит от самого сложного из проверяемых свойств. Очевидно, идемпотентность легко проверить со сложностью $O(N)$, перебрав все элементы квазигруппы. Для проверки коммутативности достаточно перебрать все пары элементов квазигруппы. Сделать это можно со сложностью $O\left(N^2\right)$. Для проверки ассоциативности можно воспользоваться процедурой, называемой тестом Лайта.

Теорема 1 ([14]). *Пусть G — множество с заданной операцией умножения $*$, и у G есть порождающее множество S. Тогда для проверки ассоциативности операции $*$ достаточно проверить тождества $x*(g*y)$ и $(x*g)*y$ для всех $x, y \in G$ и $g \in S$.*

Теорема 2 ([15]). *Пусть G — квазигруппа порядка N. Тогда в G можно выделить порождающее множество S размером не больше $\lfloor \log_2 N \rfloor + 1$.*

Из этих утверждений нетрудно установить, что ассоциативность проверяется со сложностью $O\left(N^2 \log_2 N\right)$.

Проверить что какой-то элемент квазигруппы является левой или правой единицей можно со сложностью $O(N)$. Таким образом, для квазигруппы порядка N алгоритм нахождения левой или правой единицы можно реализовать за $O\left(N^2\right)$, проверив каждый элемент квазигруппы.

Для поиска собственных подквазигрупп можно использовать следующее утверждение.

Теорема 3 ([16]). *Существует алгоритм, который устанавливает наличие собственных подквазигрупп в квазигруппе порядка N с временной сложностью $O\left(N^{7/3} \cdot (\log N)^{2/3}\right)$ и пространственной сложностью $O\left(N^2\right)$, $N \to \infty$.*

В работе [17] было анонсировано, что временную сложность поиска подквазигрупп можно понизить до $O\left(N^{7/3}\right)$.

Проверку тождеств из определения бесформенности можно произвести явно. Для вычисления одного равенства с m операциями умножения требуется m действий. Чтобы проверить одно тождество с m умножениями необходимо перебрать все пары элементов квазигруппы и для каждой пары вычислить произведение длины m. В худшем случае придется проверить все тождества, т.е. выполнить $N^2 + 2N^2 + 3N^2 + ... + 2N * N^2$ действий. Таким образом, сложность проверки тождеств из определенеия квазигруппы составляет $O\left(N^4\right)$. Поскольку этот шаг является наиболее сложным, мы получаем следующее утверждение.

Теорема 4. *Сложность процедуры проверки бесформенности $O\left(N^4\right)$, где N — порядок квазигруппы.*

Отметим, что тождества можно проверять более оптимальным образом. Если для каждого тождества с m операциями умножения хранить результаты вычисления тождества с $m-1$ операцией умножения, то временную сложность алгоритма можно понизить до $O\left(N^3\right)$. Это также повысит пространственную сложность до $O\left(N^2\right)$. Однако, в случае табличного задания квадратичная память требуется на задание операции, поэтому такая пространственная сложность алгоритма не является существенной. Таким образом, можно сформулировать следующее утверждение.

Теорема 5. *Существует процедура проверки бесформенности, имеющая временную сложность $O\left(N^3\right)$ и пространственную сложность $O\left(N^2\right)$. Здесь N — порядок квазигруппы.*

Теорема 6 ([18])**.** *Сложность процедуры проверки аффинности $O\left(N^3\right)$, где N — порядок квазигруппы.*

Отметим, что наибольшую сложность в алгоритме проверки аффинности имеет этап проверки ассоциативности. Воспользовавшись ранее упомянутым тестом Лайта можно понизить сложность проверки аффинности до $O\left(N^2 \log_2 N\right)$.

Теорема 7 ([18, 19])**.** *Сложность процедуры проверки простоты $O\left(N^3\right)$, где N — порядок квазигруппы.*

Таким образом, полиномиальную полноту можно проверить со сложностью $O\left(N^3\right)$.

4. Взаимосвязь криптографически важных свойств

Теорема 8. *Пусть $(Q,*)$ квазигруппа порядка p, где p – простое число, $p \geq 5$. Если $(Q,*)$ бесформенна, то она полиномиально полна.*

Доказательство. Предположим противное. Тогда существует биективное отображение $\varphi : Q \to \mathbb{Z}_p$, такое что $\varphi(x*y) = a\varphi(x) + b\varphi(y) + c$, где $a, b \in \mathbb{Z}_p \backslash \{0\}$, а сложение и умножение на скаляры ведутся по модулю p [20]. Несложно проверить, что

$$\varphi(\underbrace{x*(x...*(x}_{k}*y))) = a\varphi(x) + c + \textstyle\sum_{i=1}^{k-1} b^i(a\varphi(x)+c) + b^k\varphi(y).$$

Возьмем $k = p-1$. По малой теореме Ферма $b^k = 1 \pmod p$. Обозначим

$$\alpha(x) = a\varphi(x) + c + \textstyle\sum_{i=1}^{k-1} b^i(a\varphi(x)+c).$$

Перепишем $a\varphi(x)+c$ как $b^k(a\varphi(x)+c)$ и вынесем b за скобки. Тогда

$$\alpha(x) = b\alpha(x).$$

Отсюда либо $b = 1$, либо $\alpha(x) \equiv 0$. Рассмотрим оба случая.

1) Пусть $b = 1$. Поскольку $(Q, *)$ бесформенна, то она не содержит левой единицы. Значит для любого x можно найти y, такой, что $x * y \neq y$. Т.е. $\varphi(x * y) = a\varphi(x) + \varphi(y) + c \neq \varphi(y)$. Значит для любого x верно, что $a\varphi(x) + c \neq 0$. Но поскольку φ биекция, такой x всегда можно найти. Таким образом, если $b = 1$, то $(Q, *)$ содержит левую единицу и не может быть бесформенной.

2) Пусть теперь $\alpha(x) \equiv 0$. Тогда $\varphi(\underbrace{x * (x... * (x}_{p-1} * y))) = \varphi(y)$. Но это значит, что $\underbrace{x * (x... * (x}_{p-1} * y)) = y$. Длина этого произведения $p - 1 < 2p$. Следовательно, квазигруппа не будет бесформенной.

Аналогично доказывается, что либо $a = 1$ и тогда квазигруппа содержит правую единицу, либо верно тождество $y = ((y * \underbrace{x) * ...x) * x}_{k}$. Следовательно, квазигруппа не может не быть полиномиально полной. □

Замечание 1. *При $p = 2, 3$ все квазигруппы не полиномиально полные и не бесформенные. Поэтому, формально, теорема верна при любом простом порядке.*

Покажем, что в обратную сторону теорема не верна.

Рассмотрим квазигруппу $(Q, *)$ порядка 5, где $Q = \{0, 1, 2, 3, 4\}$, а умножение задано таблицей:

*	0	1	2	3	4
0	2	4	3	1	0
1	3	0	4	2	1
2	4	3	1	0	2
3	1	2	0	4	3
4	0	1	2	3	4

Очевидно, эта квазигруппа простая, поскольку её порядок простое число. Воспользуемся алгоритмом проверки аффинности из работы [18] и покажем, что эта квазигруппа неаффинна. Построим латинский квадрат L', в котором при каждом $i = 1, 2, 3, 4, 5$ строка с номером i содержит перестановку $\sigma_i \cdot \sigma_1^{-1}$, где σ_i – перестановка, соответствующая i-й строке

исходного латинского квадрата. Тогда L':

*'	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	0	4	1	3
3	3	4	1	0	2
4	4	3	0	2	1

Следующим шагом необходимо построить матрицу L'' из матрицы L' перестановкой строк, такой, что первый столбец L'' совпадает с первой строкой. Но в матрице L' уже первая строка совпадает с первым столбцом. Поэтому матрицы L' и L'' и задаваемые ими операции совпадают. Эта матрица не симметрична: $1 *'' 2 \neq 2 *'' 1$. Следовательно, квазигруппа $(Q, *)$ неаффинна. Поскольку квазигруппа простая и не аффинная, то она является полиномиально полной. При этом она не удовлетворяет сразу нескольким свойствам из определения бесформенности:

- 4 является левой и правой единицей;
- верно тождество $((((((y * x) * x) * x) * x) * x) * x) = y$;
- $4 * 4 = 4$, т.е. $\{4\}$ является подквазигруппой.

Аналогично можно привести пример полиномиально полной идемпотентной квазигруппы:

*	0	1	2	3	4
0	0	4	3	1	2
1	2	1	4	0	3
2	3	0	2	4	1
3	4	2	1	3	0
4	1	3	0	2	4

и пример полиномиально полной коммутативной квазигруппы:

*	0	1	2	3	4
0	1	3	2	0	4
1	3	4	0	1	2
2	2	0	3	4	1
3	0	1	4	2	3
4	4	2	1	3	0

При помощи ранее упомянутой программной реализации алгоритма проверки полиномильной полноты было выявлено, что знакопеременная

группа A_5 является полиномиально полной. При этом, A_5, очевидно, ассоциативна. Эксперимент осуществлялся с использованием ранее упомянутых алгоритмов проверки аффинности, простоты и бесформенности.

Покажем, что в случае составного порядка можно построить бесформенную квазигруппу, не являющуюся полиномиально полной. Рассмотрим следующую квазигруппу порядка 4:

*	0	1	2	3
0	2	0	3	1
1	1	2	0	3
2	0	3	1	2
3	3	1	2	0

Возьмем 4 вспомогательных квазигруппы порядка 4:

$*_0$	0	1	2	3
0	1	3	2	0
1	2	0	3	1
2	0	2	1	3
3	3	1	0	2

$*_1$	4	5	6	7
4	7	5	6	4
5	6	4	5	7
6	4	6	7	5
7	5	7	4	6

$*_2$	8	9	10	11
8	9	8	10	11
9	10	11	9	8
10	8	10	11	9
11	11	9	8	10

$*_3$	12	13	14	15
12	13	15	12	14
13	14	12	13	15
14	12	14	15	13
15	15	13	14	12

Несложно проверить, что все 5 квазигрупп являются бесформенными. Заменим в исходной таблице умножения элемент 0 на таблицу умножения $*_0$, элемент 1 на таблицу $*_1$, элемент 2 на таблицу $*_2$, элемент 3 на таблицу $*_3$. Получим следующую квазигруппу порядка 16:

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	9	8	10	11	1	3	2	0	13	15	12	14	7	5	6	4
1	10	11	9	8	2	0	3	1	14	12	13	15	6	4	5	7
2	8	10	11	9	0	2	1	3	12	14	15	13	4	6	7	5
3	11	9	8	10	3	1	0	2	15	13	14	12	5	7	4	6
4	7	5	6	4	9	8	10	11	1	3	2	0	13	15	12	14
5	6	4	5	7	10	11	9	8	2	0	3	1	14	12	13	15
6	4	6	7	5	8	10	11	9	0	2	1	3	12	14	15	13
7	5	7	4	6	11	9	8	10	3	1	0	2	15	13	14	12
8	1	3	2	0	13	15	12	14	7	5	6	4	9	8	10	11
9	2	0	3	1	14	12	13	15	6	4	5	7	10	11	9	8
10	0	2	1	3	12	14	15	13	4	6	7	5	8	10	11	9
11	3	1	0	2	15	13	14	12	5	7	4	6	11	9	8	10
12	13	15	12	14	7	5	6	4	9	8	10	11	1	3	2	0
13	14	12	13	15	6	4	5	7	10	11	9	8	2	0	3	1
14	12	14	15	13	4	6	7	5	8	10	11	9	0	2	1	3
15	15	13	14	12	5	7	4	6	11	9	8	10	3	1	0	2

Эта квазигруппа не будет простой, так как квазигрупповая операция сохраняет разбиение $\{0,1,2,3\} \cup \{4,5,6,7\} \cup \{8,9,10,11\} \cup \{12,13,14,15\}$. Однако, она состоит из бесформенных блоков, а значит некоммутативна, неассоциативна, не содержит левых и правых единиц и неидемпотентна. Несложно проверить, что она также не содержит подквазигрупп и в ней не выполняются тождества $\underbrace{x * (x... * (x}_{k} * y)) = y$, $y = (\underbrace{(y * x) * ...x) * x}_{k}$ $\forall k < 32$. Следовательно, это бесформенная, но не полиномиально полная квазигруппа.

Однако, в случае составного порядка можно сформулировать ряд утверждений, когда отсутствие полиномиальной полноты влечет за собой отсутствие бесформенности.

Утверждение 1. *Пусть $(Q, *)$ аффинная квазигруппа над абелевой группой $(Q, +)$. Тогда $(Q, *)$ содержит правую единицу тогда и только тогда, когда α тривиальный автоморфизм.*

Доказательство. Квазигруппа $(Q, *)$ содержит правую единицу тогда и только тогда, когда существует элемент e, такой, что $x * e = x$ $\forall x \in Q$. Поскольку квазигруппа аффинна, это значит, что $\alpha(x) + \beta(e) + c = x$ $\forall x \in Q$. В частности, это верно для нейтрального элемента e' группы $(Q, +)$. Следовательно, $\beta(e) = -c$ и $\alpha(x) = x$. Таким образом, из существования правой единицы, следует, что α тождественный автоморфизм. А если α тождественный автоморфизм, то элемент $\beta^{-1}(-c)$ является правой единицей. □

Утверждение 2. *Пусть $(Q, *)$ аффинная квазигруппа над абелевой группой $(Q, +)$. Тогда $(Q, *)$ содержит левую единицу тогда и только тогда, когда β тривиальный автоморфизм.*

Доказательство. Аналогично предыдущему утверждению. □

Утверждение 3. *Пусть $(Q, *)$ аффинная квазигруппа над абелевой группой $(Q, +)$. Тогда $(Q, *)$ ассоциативна тогда и только тогда, когда α и β тождественные автоморфизмы.*

Доказательство. Известно, что квазигруппа ассоциативна тогда и только тогда, когда она группа [21]. В частности, это значит, что в ассоциативной квазигруппе есть единица. По предыдущим утверждениям это возможно только в том случае, когда α и β тождественные автоморфизмы. И наоборот, если α и β, то, очевидно, элемент $-c$ является единицей в квазигруппе. □

Утверждение 4. *Пусть* $(Q,*)$ *аффинная квазигруппа над абелевой группой* $(Q,+)$. *Тогда* $(Q,*)$ *коммутативна тогда и только тогда, когда* $\alpha \equiv \beta$.

Доказательство. Аффинная квазигруппа $(Q,*)$ коммутативна тогда и только тогда, когда $\alpha(x)+\beta(y)+c=\alpha(y)+\beta(x)+c\ \forall x,y\in Q$. Отсюда следует, что $\alpha(x-y)=\beta(x-y)\ \forall x,y\in Q$. Любой элемент из Q можно представить как разность некоторых элементов x,y из Q. Следовательно, α и β это один и тот же автоморфизм. □

Утверждение 5. *Пусть* $(Q,*)$ *аффинная квазигруппа над абелевой группой* $(Q,+)$. *Тогда* $(Q,*)$ *идемпотентна тогда и только тогда, когда* $\alpha(x)=x-\beta(x)$, *а* c *– единица группы* $(Q,+)$.

Доказательство. Аффинная квазигруппа $(Q,*)$ идемпотентна тогда и только тогда, когда $\alpha(x)+\beta(x)+c=x$. Подставив в это тождество единичный элемент e группы $(Q,+)$ получим, что $c=e$. Таким образом, квазигруппа идемпотентна только в тех случаях, когда $c=e$ и $\alpha(x)+\beta(x)=x$. □

Теорема 9. *Пусть* $(Q,*)$ *аффинная квазигруппа над абелевой группой* $(Q,+)$ *порядка* N, *а* α *и* β *– регулярные автоморфизмы. Тогда* $(Q,*)$ *небесформенна.*

Доказательство. По индукции несложно показать, что

$$\underbrace{x*(x...*(x}_{k}*y))=\alpha(x)+c+\textstyle\sum_{i=1}^{k-1}(\beta^{(i)}(\alpha(x)+c))+\beta^{(k)}(y).$$

Возьмем $k=|\beta|$, где $|\beta|$ – порядок автоморфизма β. Тогда $\beta^{(k)}(y)=y$. Обозначим

$$\gamma(x)=\alpha(x)+c+\textstyle\sum_{i=1}^{k-1}(\beta^{(i)}(\alpha(x)+c)).$$

Запишем $\alpha(x)+c$ как $\beta^{(k)}(\alpha(x)+c)$ и воспользуемся тем, что β гомоморфизм. Тогда $\gamma(x)=\beta(\gamma(x))$. Поскольку β регулярный автоморфизм, то $\gamma(x)\equiv 0$. Следовательно, $\underbrace{x*(x...*(x}_{k}*y))=y$. Аналогично можно показать, что при $k=|\alpha|$ верно тождество $y=((y*\underbrace{x)*...x)*x}_{k}$. Здесь $|\alpha|$ – порядок автоморфизма α. Поскольку $|\alpha|,\ |\beta|<N-1<2N$ [22] квазигруппа небесформенна. □

С поиском бесформенных не полиномиально полных квазигрупп также был проведен эксперимент. Алгоритмом Джейкобсона-Мэтьюза [23] было

сгенерировано по 1000000 случайных квазигрупп порядков 6, 8 и 10. Все бесформенные квазигруппы среди них были полиномиально полными.

Существует всего 576 квазигрупп порядка 4. В ходе эксперимента было установлено, что среди них 384 полиномиально полных квазигруппы и 48 бесформенных квазигрупп. Более подробная классификация:

- 48 бесформенных полиномиально полных;
- 0 бесформенных не полиномиально полных;
- 336 не бесформенных полиномиально полных;
- 192 не бесформенных не полиномиально полных.

На основании результатов экспериментов можно предположить, что значительная часть бесформенных квазигрупп являются полиномиально полными. Обоснование этого вывода для квазигрупп составного порядка является направлением дальнейших исследований.

5. Заключение

В работе было установлено, что все бесформенные квазигруппы простого порядка являются полиномиально полными. Был приведен пример, показывающий, что обобщение этого утверждения на составные порядки невозможно. Однако, эксперименты показывают, что такие примеры по всей видимости являются исключительными ситуациями и значительное число бесформенных квазигрупп являются полиномиально полными. Кроме того, было показано, что существуют полиномиально полные квазигруппы, не являющиеся бесформенными. Для каждого свойства из определения бесформенности был приведен пример полиномиально полной квазигруппы, которая этим свойством не обладает.

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] Gligoroski D., “On the S-box in GAGE and InGAGE”, 2019, http://gageingage.org/upload/LWC2019NISTWorkshop.pdf.

[3] Gligoroski D., Ødegård R. S., Mihova M., Knapskog S. J., Drápal A., Klima V., Amundsen J., El-Hadedy M., “Cryptographic hash function

EDON-R'", *Proceedings of the 1st International Workshop on Security and Communication Networks*, 2009, 1–9.

[4] Markovski S., Mileva A., "NaSHA — family of cryptographic hash functions", *The First SHA-3 Candidate Conference*, 2009.

[5] Shannon C., "Communication theory of secrecy systems", *Bell System Technical Journal*, **28**:4 (1949), 656–715.

[6] Глухов М. М., "О применениях квазигрупп в криптографии", *Прикладная дискретная математика*, 2008, № 2(2), 28–32.

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

[8] Artamonov V. A., Chakrabarti S., Pal S. K., "Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations", *Discrete Applied Mathematics*, **200** (2016), 5–17.

[9] Markovski S., "Design of crypto primitives based on quasigroups", *Quasigroups and Related Systems*, **23** (2015), 41–90.

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

[11] Larose B., Zadori L., "Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras", *International Journal of Algebra and Computation*, **16** (2006), 563–581.

[12] Яблонский С. В., "Введение в дискретную математику", *Наука*, 1986.

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

[14] Clifford A., Preston G., "Light's associativity test", *The Algebraic Theory of Semigroups*, **1** (1961), 7–8.

[15] Tarjan R. E., "Determining whether a groupoid is a group", *Information Processing Letters*, **1** (1972), 120–124.

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

[17] Galatenko A. V., Mazurin A. D., Pankratiev A. E., Zhigliaev R. A., "Efficient verification of some properties of finite quasigroups", *Mathematics in Armenia: advances and perspectives*, 2023, 29–30.

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

[19] Galatenko A. V., Pankratiev A. E., Staroverov V. M., "Efficient verifiation of polynomial completeness of quasigroups", *Lobachevskii Journal of Mathematics*, 2020, 1444–1453.

[20] Галатенко А. В., Панкратьев А. Е., Родин С. Б., "О полиномиально полных квазигруппах простого порядка", *Алгебра и логика*, **57**:5 (2018), 509–521.

[21] Prasad V. B. V. N., Venkateswara Rao J., "Characterization of Quasigroups and Loop", *International Journal of Scientific and Innovative Mathematical Research*, **1**:2 (2013), 95–102.

[22] Хорошевский М. В., "Об автоморфизмах конечных групп", *Математический сборник*, **135**:4 (1974), 576–587.

[23] Jacobson M. T., Matthews P., "Generating uniformly distributed random Latin squares", *Journal of Combinatorial Designs*, **4**:6 (1996), 405–437.

On the relationship between cryptographically important properties of finite quasigroups
Zhigliaev R.A.

In this paper we establish a relationship between some properties of finite quasigroups. It is proved that in the case of quasigroups of prime order, all shapeless quasigroups are polynomially complete. Examples are given to show that the converse statement and the generalization to composite orders are not true.

Keywords: finite quasigroup, polynomial completeness, shapeless quasigroup.

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] Gligoroski D., "On the S-box in GAGE and InGAGE", 2019, http://gageingage.org/upload/LWC2019NISTWorkshop.pdf.

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

[4] Markovski S., Mileva A., "NaSHA — family of cryptographic hash functions", *The First SHA-3 Candidate Conference*, 2009.

[5] Shannon C., "Communication theory of secrecy systems", *Bell System Technical Journal*, **28**:4 (1949), 656–715.

[6] Glukhov M. M., "Some applications of quasigroups in cryptography", *Prikl. Diskr. Mat.*, 2008, №2(2), 28–32 (In Russian).

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

[8] Artamonov V. A., Chakrabarti S., Pal S. K., "Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations", *Discrete Applied Mathematics*, **200** (2016), 5–17.

[9] Markovski S., "Design of crypto primitives based on quasigroups", *Quasigroups and Related Systems*, **23** (2015), 41–90.

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

[11] Larose B., Zadori L., "Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras", *International Journal of Algebra and Computation*, **16** (2006), 563–581.

[12] Yablonskii S. V., "Introduction to discrete mathematics", *Nauka*, 1986 (In Russian).

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

[14] Clifford A., Preston G., "Light's associativity test", *The Algebraic Theory of Semigroups*, **1** (1961), 7–8.

[15] Tarjan R. E., "Determining whether a groupoid is a group", *Information Processing Letters*, **1** (1972), 120–124.

[16] 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).

[17] Galatenko A. V., Mazurin A. D., Pankratiev A. E., Zhigliaev R. A., "Efficient verification of some properties of finite quasigroups", *Mathematics in Armenia: advances and perspectives*, 2023, 29–30.

[18] Galatenko A. V., Pankratiev A. E., "The complexity of checking the polynomial completeness of finite quasigroups", *Discrete Mathematics and Applications*, **30**:3 (2020), 169–175.

[19] Galatenko A. V., Pankratiev A. E., Staroverov V. M., "Efficient verifiation of polynomial completeness of quasigroups", *Lobachevskii Journal of Mathematics*, 2020, 1444–1453.

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

[21] Prasad V. B. V. N., Venkateswara Rao J., "Characterization of Quasigroups and Loop", *International Journal of Scientific and Innovative Mathematical Research*, **1**:2 (2013), 95–102.

[22] Khoroshevskii M. V., "On automorphisms of finite groups", *Mathematics of the USSR-Sbornik*, **22**:4 (1974), 584–594.

[23] Jacobson M. T., Matthews P., "Generating uniformly distributed random Latin squares", *Journal of Combinatorial Designs*, **4**:6 (1996), 405–437.