Некоторые свойства почти всех n -квазигрупп

А.В. Галатенко, В.В. Галатенко, А.Е. Панкратьев

Аннотация. Изучается “типичность” свойств простоты, неаффинности и полиномиальной полноты конечных n -квазигрупп. Показано, что при фиксированном n почти все n -квазигруппы сильно неаффинны, т. е. не изотопны аффинным. Найдено точное значение числа простых, аффинных и одновременно простых и аффинных n -квазигрупп порядка 4. Как следствие, показано, что почти все n -квазигруппы порядка 4 полиномиально полны и сильно неаффинны.

Ключевые слова: квазигруппа, n -квазигруппа, простота, аффинность, полиномиальная полнота.

DOI: 10.26907/2949-3919.2024.4.35-50

Введение

Конечные квазигруппы и их n -арные обобщения – конечные n -квазигруппы – становятся перспективной платформой для реализации различных криптографических примитивов (см., например, квазигрупповые обзоры [1,2]). Для обеспечения высокой стойкости к используемым объектам предъявляются дополнительные требования, такие как бесформенность [3] и нефрактальность [4]. В.А. Артамоновым с соавторами было предложено использовать полиномиально полные квазигруппы (см., например, [5]), так как задача проверки разрешимости уравнений над полиномиально полными алгебрами NP-полна [6]. Известно, что полиномиальная полнота конечных n -квазигрупп эквивалентна одновременной простоте и неаффинности. Для случая квазигрупп порядка 4 в работе [7] были найдены мощности классов, определенных наличием и/или отсутствием свойств простоты и/или аффинности, однако некоторые из указанных в работе [7] значений требуют корректировки. Имеется ряд результатов о “типичности” свойства полиномиальной полноты. В.Л. Мурским было установлено, что при фиксированной значности логики почти все алгебры полиномиально полны [8]. Кэмерон доказал, что почти любая квазигрупповая операция и множество всех констант порождают знакопеременную группу [9], откуда по теореме Саломеа [10] следует, что почти все квазигруппы полиномиально полны. В работе [11] этот результат был усилен: оказалось, что почти все квазигруппы не изотопны квазигруппам, не являющимся полиномиально полными.

В нашей работе сперва изучается задача “типа Кэмерона”, когда арность n является фиксированной, а значность логики растет. В этом случае удается показать, что почти все n -квазигруппы являются сильно неаффинными, т.е. не изотопны аффинным n -квазигруппам. Отметим, что с точки зрения криптографических приложений именно неаффинность является ключевым аспектом полиномиальной полноты, так как разрешимость систем уравнений над аффинными квазигруппами полиномиальна, а над неаффинными NP-полна [12]; кроме того, в ряде случаев (например, для n -квазигрупп простого порядка) свойство простоты заведомо выполнено. Затем исследуется задача “типа Мурского”, когда значность логики k фиксируется, а арность операции растет. В случае $k = 2$ задача тривиальна: для любого n имеется ровно две n -квазигруппы, являющиеся простыми и аффинными; при $k = 3$ ситуация аналогична: число n -квазигрупп равно $3 \cdot 2^n$ и все они простые и аффинные. Первый нетривиальный случай возникает при $k = 4$. Здесь удалось найти точные значения для чисел простых, аффинных и одновременно простых и аффинных квазигрупп, откуда следуют утверждения о полиномиальной полноте и сильной неаффинности почти всех n -квазигрупп порядка 4, а также исправленные значения мощностей классов квазигрупп, обладающих или не обладающих соответствующими свойствами. Отметим, для случая n -квазигрупп порядка 4 в работе [13] было доказано, что такие квазигруппы либо изотопны n -квазигруппам, не являющимся простыми, либо разложимы в неповторную суперпозицию n -квазигрупп меньшей арности.

Дальнейшее изложение имеет следующую структуру. В разделе 1 вводятся основные определения. В разделе 2 устанавливается сильная неаффинность почти всех n -квазигрупп при фиксированном n . В разделе 3 изучается случай n -квазигрупп порядка 4. Раздел 4 является заключением.

1. Основные определения и обозначения

Пусть $k, n \in \mathbb{N}$, $k, n \geq 2$.

Определение 1. n -квазигруппой порядка k называется пара (Q, f) , где $|Q| = k$, а $f: Q^n \rightarrow Q$ обратима по каждому аргументу.

В дальнейшем для краткости мы будем использовать термин “ n -квазигруппа”, а при $n = 2$ – термин “квазигруппа”. Без ограничения общности можно считать, что $Q = E_k = \{0, 1, \dots, k-1\}$, а f – функция k -значной логики арности n .

Пусть $x \oplus y$ обозначает сложение по модулю 2. Легко увидеть, что имеется ровно две n -квазигруппы порядка 2, для которых операция $f(x_1, \dots, x_n)$ имеет вид $x_1 \oplus x_2 \oplus \dots \oplus x_n \oplus c$, $c \in E_2$.

Для n -квазигрупп порядка 3 верен аналогичный результат: число n -квазигрупп равно $3 \cdot 2^n$, а операция $f(x_1, \dots, x_n)$ задается соотношением $c_0 + c_1 x_1 + c_2 x_2 + \dots + c_n x_n \pmod{3}$, где $c_0, c_1, \dots, c_n \in E_3$, $c_1, \dots, c_n \neq 0$ (см., например, [14]).

В работе [15] показано, что мощность Q_4 множества всех n -квазигрупп порядка 4 удовлетворяет соотношению

$$Q_4 = 4 \cdot 3^{n+1} \cdot 2^{2^n+1}(1 + o(1)), \quad n \rightarrow \infty. \quad (1)$$

В общем случае известные оценки существенно менее точные. В работе [16] получена следующая нижняя оценка на число $Q(n, k)$ n -квазигрупп порядка $k > 3$:

$$Q(n, k) \geq \begin{cases} 2^{(k/2)^n} & \text{при четных } k, \\ 2^{n(k/3)^n} & \text{при } k \text{ кратных } 3, \\ 2^{3^{n/3-c}} & \text{при } k = 5, \text{ где } c < 0.072 \text{ зависит от } n \bmod 3, \\ 2^{1.5 \lfloor k/3 \rfloor^n} & \text{в остальных случаях.} \end{cases} \quad (2)$$

Для случая нечетных $k \geq 5$ эта оценка была уточнена в [17] следующим образом:

$$\log_2 Q(n, k) > \left(\frac{k-3}{2} \right)^{\frac{n}{2}} \left(\frac{k-1}{2} \right)^{\frac{n}{2}}. \quad (3)$$

В той же работе [17] была получена верхняя оценка

$$Q(n, k) \leq 2^{c_k(k-2)^n}, \quad \text{где } c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}.$$

В статье [18] была доказана асимптотическая оценка

$$Q(n, k) \lesssim \left((1 + o(1)) \frac{k}{e^n} \right)^{k^n},$$

при фиксированном n и $k \rightarrow \infty$, а в статье [19] была приведена нижняя оценка, из которой следует, что $\log Q(n, k) = \Theta(k^n \log k)$ при тех же предположениях.

Определение 2. Две n -квазигруппы (E_k, f_1) и (E_k, f_2) назовем изотопными, если существуют перестановки $\sigma_0, \sigma_1, \dots, \sigma_n$ на множестве E_k такие, что

$$f_1(x_1, \dots, x_n) \equiv \sigma_0^{-1}(f_2(\sigma_1(x_1), \dots, \sigma_n(x_n))).$$

Пусть $m \in \mathbb{N} \cup \{0\}$. Множество всех функций из E_k^m в E_k обозначим через P_k^m (в частности, P_k^0 – множество всех констант), $\bigcup_{m=0}^{\infty} P_k^m$ обозначим через P_k .

Определение 3. Пусть $f \in P_k^m$, а $\sim$ – отношение эквивалентности на множестве E_k . Функция f сохраняет отношение $\sim$, если для любых двух наборов $\alpha = (a_1, \dots, a_m)$, $\beta = (b_1, \dots, b_m) \in E_k^m$ таких, что $a_i \sim b_i$ для $i = 1, \dots, m$, выполнено $f(\alpha) \sim f(\beta)$.

Определение естественным образом обобщается на произвольное множество функций $F \subseteq P_k$.

Определение 4. n -квазигруппа (E_k, f) называется простой, если не существует нетривиального отношения эквивалентности, сохраняемого f . В противном случае n -квазигруппа называется непростой.

Несложно показать, что в случае n -квазигрупп сохраняться могут только отношения эквивалентности, все классы которых равномоцны. В дальнейшем мы будем рассматривать только отношения эквивалентности с равномоцными классами без явного указания на это предположение. Кроме того, известно (см. [20]), что n -квазигруппа (E_k, f) сохраняет нетривиальное отношение эквивалентности тогда и только тогда, когда это отношение сохраняется всеми унарными функциями, полученными из f произвольной подстановкой констант вместо всех переменных, кроме одной.

Определение 5. n -квазигруппа (E_k, f) называется аффинной, если существует абелева группа $(E_k, +)$, автоморфизмы $\alpha_1, \dots, \alpha_n$ этой группы и элемент $c \in E_k$ такие, что

$$f(x_1, x_2, \dots, x_n) \equiv \alpha_1(x_1) + \alpha_2(x_2) + \dots + \alpha_n(x_n) + c. \quad (4)$$

В противном случае n -квазигруппа называется неаффинной.

В работе [20] показано, что без ограничения общности можно считать, что нейтральным элементом группы $(E_k, +)$ является 0.

Определение 6. n -квазигруппа (E_k, f) называется сильно неаффинной, если она не изотопна n -квазигруппам, являющимся аффинными.

На множестве P_k стандартным образом введем операцию суперпозиции, порожденную удалением и добавлением фиктивных переменных, переименованием переменных без отождествления, отождествлением пары переменных и подстановкой одной функции в другую. Суперпозиция естественным образом индуцирует операцию замыкания множества функций: замыкание представляет собой множество всех функций, которые могут быть получены конечными цепочками суперпозиций из функций замыкаемого множества. Замыкание множества $F \subseteq P_k$ обозначим через $[F]$. Более подробное описание операций суперпозиции и замыкания можно найти, например, в монографии [21].

Определение 7. n -квазигруппа (E_k, f) называется полиномиально полной, если $[\{f\} \cup P_k^0] = P_k$. В случае, если (E_k, f) не изотопна n -квазигруппам, не являющимся полиномиально полными, она называется сильно полиномиально полной.

Из теоремы Розенберга (см., например, [21]) следует, что n -квазигруппа полиномиально полна тогда и только тогда, когда она одновременно проста и неаффинна.

2. Сильная неаффинность почти всех n -квазигрупп

Теорема 8. Для любого фиксированного $n \in \mathbb{N}$, $n \geq 2$, доля сильно неаффинных n -квазигрупп порядка k стремится к 1 при $k \rightarrow \infty$.

Доказательство. Для доказательства теоремы скомбинируем несколько достаточно грубых оценок. Число автоморфизмов абелевой группы порядка k заведомо не превосходит $k!$, причем в представлении (4) требуется выбрать n автоморфизмов; число абелевых групп порядка k , изоморфных данной, также не превосходит $k!$; число способов выбора константы равно k . Число n -квазигрупп, изотопных данной, оценивается сверху величиной $(k!)^{n+1}$. Таким образом, число n -квазигрупп, не являющихся сильно неаффинными (т. е., изотопных аффинным), оценивается сверху величиной

$$S(k) = a(k) \cdot k \cdot (k!)^{2n+2},$$

где $a(k)$ – число различных (с точностью до изоморфизма) абелевых групп порядка k . Заметим, что при достаточно больших k выполняется неравенство

$$a(k) \leq k^4$$

(оно следует из асимптотической формулы Харди и Рамануждана [22] на значение $p(x)$ числа разбиений x). Таким образом,

$$S(k) \lesssim k^5 \cdot (k!)^{2n+2} < k^{k(2n+7)}.$$

При логарифмировании получаем верхнюю оценку $(2n + 7)k \log_2 k$. С другой стороны, из нижних оценок на число n -квазигрупп (2), (3) следует, что логарифм числа n -квазигрупп порядка k по порядку больше или равен k^n , откуда с учетом неравенства $n \geq 2$ следует утверждение теоремы. $\square$

Замечание 9. Полностью аналогичным образом можно показать, что доля сильно неаффинных n -квазигрупп порядка k стремится к 1 при фиксированном $k \geq 5$ и $n \rightarrow \infty$. Так как все n -квазигруппы простого порядка являются простыми, отсюда следует, что почти все n -квазигруппы простого порядка $k \geq 5$ сильно полиномиально полны.

3. Свойства n -квазигрупп порядка 4

В этом разделе сперва доказываются вспомогательные, а затем основные утверждения о свойствах n -квазигрупп порядка 4.

3.1. ВСПОМОГАТЕЛЬНЫЕ УТВЕРЖДЕНИЯ

Лемма 10. Пусть перестановка $\sigma \in S_4$ сохраняет два из трех отношений эквивалентности $0 \sim 1, 2 \sim 3; 0 \sim 2, 1 \sim 3; 0 \sim 3, 1 \sim 2$. Тогда σ сохраняет все три отношения эквивалентности, причем $\sigma(x) = x \oplus c$ для некоторой константы $c \in E_4$, где $\oplus$ – операция сложения в группе $\mathbb{Z}_2^2$.

Доказательство. Без ограничения общности рассмотрим случай, когда сохраняются первые два отношения эквивалентности. Пусть $\sigma(0) = c$ для некоторого элемента $c \in E_4$. Тогда из сохранения первого отношения эквивалентности следует, что $\sigma(1) = c \oplus 1$, из условия сохранения второго отношения эквивалентности – что $\sigma(2) = c \oplus 2$. Таким образом, $\sigma(3) = c \oplus 3$, и третье отношение эквивалентности также сохраняется. $\square$

Следствие 11. *Непростая n -квазигруппа порядка 4 сохраняет либо ровно одно нетривиальное отношение эквивалентности, либо все три нетривиальных отношения эквивалентности. Существует ровно четыре n -квазигруппы (E_4, f) порядка 4, сохраняющие все три отношения эквивалентности, причем f имеет вид $c \oplus x_1 \oplus \dots \oplus x_n$.*

Лемма 12. *Пусть $(E_4, +_i)$, $i = 1, 2, 3$, – абелевы группы с операциями, заданными следующими таблицами Кэли:*

$+_1$	0	1	2	3	$+_2$	0	1	2	3	$+_3$	0	1	2	3
0	0	1	2	3	0	0	1	2	3	0	0	1	2	3
1	1	2	3	0	1	1	0	3	2	1	1	3	0	2
2	2	3	0	1	2	2	3	1	0	2	2	0	3	1
3	3	0	1	2	3	3	2	0	1	3	3	2	1	0

Пусть $1 \leq i, j \leq 3$, $i \neq j$. Тогда если квазигруппа (E_4, f) аффинна относительно $(E_4, +_i)$, она не аффинна относительно $(E_4, +_j)$.

Заметим, что группы из условия леммы получены из группы $\mathbb{Z}_4$ переобозначением элемента порядка 2 и элемента порядка 4.

Доказательство. Рассмотрим случай $i = 1$, $j = 2$. Остальные случаи рассматриваются полностью аналогично. Заметим, что операция $+_1$, все константы и любой автоморфизм группы $(E_4, +_1)$ сохраняют предикат p арности 4, обращающийся в истину на всех наборах (x, y, z, w) , удовлетворяющих соотношению $x +_1 y = z +_1 w$, и только на них. Понятие сохранения предиката подробно описано, например, в монографии [21]. Содержательно сохранение предиката функцией арности t означает, что если рассмотреть произвольные t наборов, на которых предикат обращается в истину, записать их в виде столбцов матрицы и применить функцию к каждой строке, на выходе получится набор, также обращающий предикат в истину. Известно, что множество всех функций, сохраняющих заданный предикат, является замкнутым классом относительно операции суперпозиции. В случае предиката p этот класс отличен от множества всех функций. Примером функции, не сохраняющей предикат, является $g(x, y) = x +_2 y$. Действительно, рассмотрим набор $(2, 2, 0, 0)$. Так как $2 +_1 2 = 0$, он обращает p в истину, однако покомпонентное применение функции g к двум копиям этого набора дает $(1, 1, 0, 0)$, обращающий p в ложь.

Предположим, что квазигруппа (E_4, f) аффинна относительно групп $(E_4, +_1)$ и $(E_4, +_2)$. Из аффинности относительно $(E_4, +_1)$ следует, что f и все функции, полученные суперпозициями из f , констант и операции $+_1$, сохраняют предикат p . Из аффинности f

относительно группы $(E_4, +_2)$ следует, что $f(x, y) = \alpha_1(x) +_2 \alpha_2(y) +_2 c$, где α_1, α_2 – автоморфизмы $(E_4, +_2)$. Пусть $a = \alpha_2^{-1}(\alpha_1^{-1}(-_2\alpha_1(c) -_2 \alpha_2(c) -_2 c))$. Рассмотрим функцию $h(x, y) = f(f(x, a), f(0, y))$. Покажем, что $h(x, y) = x +_2 y$. Действительно, с учетом того, что для любого автоморфизма α группы $\mathbb{Z}_4$ верно, что α^2 – тождественное отображение, получаем следующую цепочку равенств:

$$\begin{aligned} h(x, y) &= \alpha_1(\alpha_1(x) +_2 \alpha_2(\alpha_2^{-1}(\alpha_1^{-1}(-_2\alpha_1(c) -_2 \alpha_2(c) -_2 c))) +_2 c) \\ &+_2 \alpha_2(\alpha_1(0) +_2 \alpha_2(y) +_2 c) +_2 c = x +_2 -_2\alpha_1(c) -_2 \alpha_2(c) -_2 c +_2 \alpha_1(c) +_2 y +_2 \alpha_2(c) +_2 c = x +_2 y. \end{aligned}$$

Таким образом, суперпозиции функции f и констант породили функцию, не сохраняющую предикат p . Полученное противоречие завершает доказательство леммы. $\square$

3.2. ОСНОВНЫЕ УТВЕРЖДЕНИЯ

Теорема 13. *Для любого фиксированного $n \in \mathbb{N}$, $n \geq 2$, число n -квазигрупп порядка 4, не являющихся простыми, равно $3 \cdot 2^{2^n+1} - 8$.*

Доказательство. Есть три способа выбрать сохраняемое отношение эквивалентности, выбрав элемент $c \in E_4$, $c \neq 0$, и положив $0 \sim c$. Пусть (E_4, f) – n -квазигруппа, сохраняющая выбранное отношение. Тогда это отношение порождает разбиение множества входных наборов f на 2^n классов $C = \{(a_1, \dots, a_n)\}$ таких, что для любого i , $1 \leq i \leq n$, из условия $\alpha, \beta \in C$ вытекает эквивалентность i -х компонент наборов α и β , причем на любой паре аргументов из одного класса f принимает эквивалентные значения. Таким образом, есть 2 варианта выбора класса эквивалентности для значений на классе C , содержащем нулевой набор (классы значений на оставшихся C будут определены однозначно), и 2 варианта выбора значений на наборах внутри каждого класса C . Значит, при фиксированном отношении эквивалентности имеется ровно $2 \cdot 2^{2^n} = 2^{2^n+1}$ непростых n -квазигрупп, сохраняющих это отношение. Для доказательства теоремы осталось применить [следствие 11](#) и учесть, что четыре n -квазигруппы, сохраняющие все три отношения, были посчитаны трижды. $\square$

Из [теоремы 13](#) с учетом оценки (1) на мощность множества всех n -квазигрупп порядка 4 непосредственно вытекает следующий факт.

Следствие 14. *Доля простых n -квазигрупп порядка 4 стремится к 1 при $n \rightarrow \infty$.*

Теорема 15. *Для любого фиксированного $n \in \mathbb{N}$, $n \geq 2$, число n -квазигрупп порядка 4, являющихся аффинными, равно $3 \cdot 2^{n+2} (3^{n-1} + 1)$.*

Доказательство. Сперва заметим, что с точностью до изоморфизма абелева группа $(E_4, +)$ может быть выбрана двумя способами: $\mathbb{Z}_4$ и $\mathbb{Z}_2^2$. Также заметим, что из аффинности n -квазигруппы (E_k, f) следует аффинность квазигруппы (E_k, f') , где f' получена из f произвольной подстановкой констант вместо переменных $x_3, \dots, x_n$. Известно (см.,

например, [20]), что если квазигруппа аффинна относительно абелевой группы, то эти квазигруппа и группа изотопны. Так как группы $\mathbb{Z}_4$ и $\mathbb{Z}_2^2$ не являются изотопными, аффинность относительно первой означает неаффинность относительно второй, и наоборот.

Рассмотрим случай n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_2^2$. Как отмечалось выше, без ограничения общности можно считать, что нейтральным элементом группы является 0. Таким образом, имеется шесть вариантов абелевой группы, полученных из $\mathbb{Z}_2^2$ перестановкой элементов, сохраняющей 0. Легко увидеть, что любая такая перестановка σ является автоморфизмом группы $\mathbb{Z}_2^2$. Обозначим через $\oplus$ сложение в группе $\mathbb{Z}_2^2$, через $+$ сложение в изоморфном образе. Предположим, что n -квазигруппа (E_4, f) аффинна относительно $(E_4, +)$, т.е. $f(x_1, \dots, x_n) = \alpha_1(x_1) + \dots + \alpha_n(x_n) + c$, где $\alpha_1, \dots, \alpha_n$ – автоморфизмы $(E_4, +)$. Тогда верна следующая цепочка равенств:

$$\begin{aligned} f(x_1, \dots, x_n) &= \sigma(\alpha_1(\sigma^{-1}(x_1))) \oplus \dots \oplus \alpha_n(\sigma^{-1}(x_n)) \oplus \sigma^{-1}(c) = \\ &= \sigma(\alpha_1(\sigma^{-1}(x_1))) \oplus \dots \oplus \sigma(\alpha_n(\sigma^{-1}(x_n))) \oplus c, \end{aligned}$$

причем $\sigma \circ \alpha_i \circ \sigma^{-1}$ являются автоморфизмами группы $\mathbb{Z}_2^2$. Таким образом, без ограничения общности можно считать, что в рассматриваемом случае все n -квазигруппы аффинны относительно $\mathbb{Z}_2^2$. Легко увидеть, что разным автоморфизмам и константам в представлении (4) соответствуют разные n -квазигруппы. Значит, число n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_2^2$, равно $4 \cdot 6^n$ (четыре способа выбора константы и шесть способов выбора каждого из n автоморфизмов).

Рассмотрим случай n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_4$. Заметим, что если изоморфизм между двумя такими группами переставляет элементы порядка 4, то, аналогично предыдущему случаю, легко показать, что множества n -квазигрупп, аффинных относительно этих групп, совпадают. Таким образом, с учетом [леммы 12](#) имеется ровно три непересекающихся множества n -квазигрупп, аффинных относительно групп $(E_4, +_1)$, $(E_4, +_2)$ и $(E_4, +_3)$. Значит, число n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_4$, равно $3 \cdot 4 \cdot 2^n$ (три способа выбора операции абелевой группы, четыре способа выбора константы и два способа выбора каждого из n автоморфизмов).

Для завершения доказательства остается сложить оценки из первого и второго случаев:

$$3 \cdot 4 \cdot 2^n + 4 \cdot 6^n = 3 \cdot 2^{n+2} (3^{n-1} + 1). \quad \square$$

Заметим, что число n -квазигрупп, получаемых из некоторой n -квазигруппы (E_4, f) с помощью изотопий, очевидным образом оценивается сверху величиной $(4!)^{n+1}$. Таким образом, из [теоремы 15](#) и оценки (1) вытекает следующий факт.

Следствие 16. *Доля сильно неаффинных n -квазигрупп порядка 4 стремится к 1 при $n \rightarrow \infty$.*

Следующее утверждение напрямую выводится из теорем 13, 15 и критерия полиномиальной полноты.

Следствие 17. Доля полиномиально полных n -квазигрупп порядка 4 стремится к 1 при $n \rightarrow \infty$.

Теорема 18. Для любого фиксированного $n \in \mathbb{N}$, $n \geq 2$, число n -квазигрупп порядка 4, являющихся одновременно простыми и аффинными, равно $24 \cdot 2^n - 8$.

Доказательство. Выше мы показали, что множество аффинных n -квазигрупп порядка 4 разбивается в объединение двух непересекающихся подмножеств: n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_4$, и n -квазигрупп, аффинных относительно групп, изоморфных $\mathbb{Z}_2^2$. Покажем, что в первом случае все аффинные n -квазигруппы не являются простыми. Рассмотрим подслучай группы $(E_4, +_1)$, остальные подслучаи рассматриваются полностью аналогично. Зафиксируем отношение эквивалентности $0 \sim 2$, $1 \sim 3$. Заметим, что множество функций, сохраняющих это отношение, является замкнутым классом, т. е. любая суперпозиция таких функций сохраняет отношение $\sim$. Также заметим, что все константы, все автоморфизмы абелевой группы и операция $+_1$ сохраняет отношение $\sim$. Значит, в силу представления (4), любая n -квазигруппа, аффинная относительно $(E_4, +_1)$, также сохраняет искомое отношение эквивалентности, т. е. не является простой.

Перейдем к случаю n -квазигрупп (E_4, f) , аффинных относительно групп, изоморфных $\mathbb{Z}_2^2$. Выше было показано, что без ограничения общности можно считать, что группа совпадает с $\mathbb{Z}_2^2$. Проанализируем, каким критериям должны удовлетворять автоморфизмы α_i в представлении (4), чтобы получающаяся n -квазигруппа не была простой. Для этого необходимо и достаточно, чтобы все унарные функции, полученные из f всевозможными подстановками констант, сохраняли какое-то нетривиальное фиксированное отношение эквивалентности (см. [20]). В следствии 11 было показано, что если все автоморфизмы тривиальны, получающиеся n -квазигруппы сохраняют все три возможных отношения эквивалентности.

Пусть некоторый автоморфизм является транспозицией (i, j) , $1 \leq i < j \leq 3$. Обозначим через s ненулевой элемент E_4 , отличный от i и j . Автоморфизм (i, j) сохраняет отношение эквивалентности $i \sim j$, $0 \sim s$. Так как все константы и сложение в группе $\mathbb{Z}_2^2$ также сохраняют это отношение эквивалентности, все n -квазигруппы, аффинные относительно $\mathbb{Z}_2^2$ и такие, что каждый автоморфизм в представлении (4) либо тривиален, либо представляет собой транспозицию (i, j) , не являются простыми. С другой стороны, транспозиция (i, j) не сохраняет нетривиальное отношение эквивалентности такое, что $0 \sim i$ или $0 \sim j$. Действительно, в этом случае эквивалентные аргументы $0 \sim i$ ($0 \sim j$, соответственно) переходят в неэквивалентные $0 \not\sim j$ ($0 \not\sim i$, соответственно). Из этого наблюдения следует, что n -квазигруппа, аффинная относительно группы $\mathbb{Z}_2^2$ и имеющая по крайней мере два различных автоморфизма-транспозиции в представлении (4), проста. Действительно, пусть для определенности $\alpha_u = (i, j)$, $\alpha_v = (i, s)$. Из определения n -квазигруппы следует, что можно так зафиксировать значения всех переменных, кроме

x_u (x_v , соответственно), что получившаяся функция одной переменной будет совпадать с транспозицией (i, j) ((i, s) , соответственно). Так как первая унарная функция сохраняет только отношение эквивалентности, включающее пару $0 \sim s$, а вторая – только отношение эквивалентности, включающее пару $0 \sim j$, $j \neq s$, множество унарных функций, порожденных подстановкой констант в f , не сохраняет никакое нетривиальное отношение эквивалентности, т. е. n -квазигруппа проста.

Наконец, пусть некоторый автоморфизм α является циклом длины 3. Тогда он не сохраняет никакое нетривиальное отношение эквивалентности. Действительно, если предположить, что сохраняется отношение, для которого $0 \sim i$, то $\alpha(0) = 0$, $j = \alpha(i) \neq i$, т. е. отношение не сохраняется.

Таким образом, доказано, что n -квазигруппа, аффинная относительно группы $\mathbb{Z}_2^2$, не является простой тогда и только тогда, когда каждый автоморфизм в представлении (4) либо тривиален, либо представляет собой транспозицию (i, j) . Отсюда общее число таких n -квазигрупп равно $4 \cdot (3 \cdot 2^n - 2)$ (четыре варианта выбора константы, три варианта выбора транспозиции, два варианта выбора автоморфизма для каждой из n позиций, при этом случай, когда все автоморфизмы тривиальны, посчитан трижды).

Для завершения доказательства осталось сложить оценки для двух случаев:

$$3 \cdot 4 \cdot 2^n + 4 \cdot (3 \cdot 2^n - 2) = 24 \cdot 2^n - 8. \quad \square$$

В заключение раздела приведем сводную таблицу числа n -квазигрупп порядка 4 различных типов для наиболее интересных для практике случаев $n = 2$ (таблица 1) и $n = 3$ (таблица 2). Значения для числа простых и непростых аффинных n -квазигрупп получены с помощью теорем 15 и 18, число неаффинных непростых n -квазигрупп получено с помощью теорем 13 и 18, оставшиеся значения были найдены с использованием информации о числе n -квазигрупп порядка 4 (576 для $n = 2$, 55296 для $n = 3$; см., например, [17]). Дополнительная валидация результатов была проведена с помощью программных реализаций алгоритмов проверки простоты и неаффинности из работы [20].

простые	аффинные	
	да	нет
да	104	384
нет	88	0

Таблица 1. Число квазигрупп различных типов порядка 4.

простые	аффинные	
	да	нет
да	776	52992
нет	184	1344

Таблица 2. Число 3-квазигрупп различных типов порядка 4.

4. Заключение

В работе изучается “типичность” свойств простоты, неаффинности и полиномиальной полноты n -квазигрупп. Установлено, что при фиксированном n почти все n -квазигруппы сильно неаффинны, т. е. не изотопны аффинным. Найдено точное значение числа простых, аффинных и одновременно простых и аффинных n -квазигрупп порядка 4. Как следствие, показано, что почти все n -квазигруппы порядка 4 полиномиально полны и сильно неаффинны.

В дальнейшем планируется установить сильную простоту и сильную полиномиальную полноту почти всех n -квазигрупп при фиксированном значении n , а также при $k = 4$ и $n \rightarrow \infty$.

Авторы благодарят М.В. Волкова за привлечение внимания к задаче, Р.Б. Халитову за ряд интересных наблюдений, на основе которых удалось получить приведенные в работе оценки, рецензента за ценные и конструктивные замечания и предоставленные ссылки.

Материалы данной работы являются продолжением исследований, проводившихся авторами в рамках проекта под руководством В.А. Артамонова.

Список литературы

- [1] V.A. Shcherbacov, *Quasigroups in cryptology*, Comput. Sci. J. Mold. **17** (2), 193–228 (2009).
- [2] D. Chauhan, I. Gupta, R. Verma, *Quasigroups and their applications in cryptography*, Cryptologia **45** (3), 227–265 (2021).
DOI: <https://doi.org/10.1080/01611194.2020.1721615>
- [3] A. Mileva, S. Markovski, *Shapeless quasigroups derived by Feistel orthomorphisms*, Glas. Mat. Ser. III **47** (2), 333–349 (2012).
DOI: <http://dx.doi.org/10.3336/gm.47.2.09>
- [4] V. Dimitrova, S. Markovski, *Classification of quasigroups by image patterns*, Proceedings of the Fifth International Conference for Informatics and Information Technology, 152–160 (2007).
- [5] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, *On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups Relat. Syst. **21** (2), 117–130 (2013).
- [6] G. Horváth, C.L. Nehaniv, Cs. Szabó, *An assertion concerning functionally complete algebras and NP-completeness*, Theoret. Comput. Sci. **407** (1–3), 591–595 (2008).
DOI: <https://doi.org/10.1016/j.tcs.2008.08.028>

- [7] V.A. Artamonov, S. Chakrabarti, S.K. Pal, *Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations*, Discrete Appl. Math. **200**, 5–17 (2016).
DOI: <https://doi.org/10.1016/j.dam.2015.06.033>
- [8] В.Л. Мурский, *Конечная базлируемость тождеств и другие свойства “почти всех” алгебр*, Проблемы кибернетики **30**, 43–56 (1975).
- [9] P.J. Cameron, *Almost all quasigroups have rank 2*, Discrete Math. **106–107**, 111–115 (1992).
DOI: [https://doi.org/10.1016/0012-365X\(92\)90537-P](https://doi.org/10.1016/0012-365X(92)90537-P)
- [10] A. Salomaa, *Some completeness criteria for sets of functions over a finite domain II*, Annales Universitatis Turkuensis. Series AI **63**, 19 pp. (1963).
- [11] А.В. Галатенко, В.В. Галатенко, А.Е. Панкратьев, *О сильной полиномиальной полноте почти всех квазигрупп*, Матем. заметки **111** (1), 8–14 (2022).
DOI: <https://doi.org/10.4213/mzm13229>
- [12] B. Larose, L. Zádori, *Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras*, Int. J. Algebra Comput. **16** (3), 563–581 (2006).
DOI: <https://doi.org/10.1142/S0218196706003116>
- [13] D.S. Krotov, V.N. Potapov, *n -ary quasigroups of order 4*, SIAM J. Discrete Math. **23** (2), 561–570 (2009).
DOI: <https://doi.org/10.1137/070697331>
- [14] C.F. Laywine, G.L. Mullen, *Discrete mathematics using Latin squares*, Wiley, New York, 1998.
- [15] В.Н. Потапов, Д.С. Кротов, *Асимптотика числа n -квазигрупп порядка 4*, Сиб. матем. журн. **47** (4), 873–887 (2006).
URL: <https://www.mathnet.ru/rus/smj902>
- [16] D.S. Krotov, V.N. Potapov, P.V. Sokolova, *On reconstructing reducible n -ary quasigroups and switching subquasigroups*, Quasigr. Relat. Syst. **16** (1), 55–67 (2008).
- [17] В.Н. Потапов, Д.С. Кротов, *О числе n -арных квазигрупп конечного порядка*, Дискрет. матем. **24** (1), 60–69 (2012).
DOI: <https://doi.org/10.4213/dm1172>
- [18] N. Linial, Z. Luria, *An upper bound on the number of high-dimensional permutations*, Combinatorica **34** (4), 471–486 (2014).
DOI: <https://doi.org/10.1007/s00493-011-2842-8>
- [19] V.N. Potapov, *On the number of SQSs, latin hypercubes and MDS codes*, J. Combin. Des. **26** (5), 237–248 (2018).
DOI: <https://doi.org/10.1002/jcd.21603>

- [20] А.В. Галатенко, А.Е. Панкратьев, В.М. Староверов, *Алгоритмы проверки некоторых свойств n -квазигрупп*, Программирование (1), 40–53 (2022).
DOI: <https://doi.org/10.31857/s0132347422010046>
- [21] D. Lau, *Function algebras on finite sets: a basic course on many-valued logic and clone theory*, Springer-Verlag, Berlin, 2006.
DOI: <https://doi.org/10.1007/3-540-36023-9>
- [22] G.H. Hardy, S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. **17**, 75–115 (1918).
DOI: <https://doi.org/10.1112/plms/s2-17.1.75>

Алексей Владимирович Галатенко

МГУ имени М.В.Ломоносова,
механико-математический факультет,
Ленинские горы, д. 1, г. Москва, 119991, Россия,
e-mail: agalat@msu.ru

Владимир Владимирович Галатенко

МГУ имени М.В.Ломоносова,
механико-математический факультет,
Ленинские горы, д. 1, г. Москва, 119991, Россия,
e-mail: vgalat@msu.ru

Антон Евгеньевич Панкратьев

МГУ имени М.В.Ломоносова,
механико-математический факультет,
Ленинские горы, д. 1, г. Москва, 119991, Россия,
e-mail: apankrat@intsys.msu.ru

Some properties of almost all n -quasigroups

A.V. Galatenko, V.V. Galatenko, A.E. Pankratiev

Abstract. We study the generic nature of simplicity, non-affinity and polynomial completeness of finite n -quasigroups. It is shown that for fixed n almost all n -quasigroups are strongly non-affine, i.e., not isotopic to affine n -quasigroups. Exact number of simple, affine and simultaneously simple and affine n -quasigroups of the order 4 is established. As a corollary, it is proven that almost all n -quasigroups of the order 4 are polynomially complete and strongly non-affine.

Keywords: quasigroup, n -quasigroup, simplicity, affinity, polynomial completeness.

DOI: 10.26907/2949-3919.2024.4.35-50

References

- [1] V.A. Shcherbacov, *Quasigroups in cryptology*, Comput. Sci. J. Mold. **17** (2), 193–228 (2009).
- [2] D. Chauhan, I. Gupta, R. Verma, *Quasigroups and their applications in cryptography*, Cryptologia **45** (3), 227–265 (2021).
DOI: <https://doi.org/10.1080/01611194.2020.1721615>
- [3] A. Mileva, S. Markovski, *Shapeless quasigroups derived by Feistel orthomorphisms*, Glas. Mat. Ser. III **47** (2), 333–349 (2012).
DOI: <http://dx.doi.org/10.3336/gm.47.2.09>
- [4] V. Dimitrova, S. Markovski, *Classification of quasigroups by image patterns*, Proceedings of the Fifth International Conference for Informatics and Information Technology, 152–160 (2007).
- [5] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, *On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups Relat. Syst. **21** (2), 117–130 (2013).
- [6] G. Horváth, C.L. Nehaniv, Cs. Szabó, *An assertion concerning functionally complete algebras and NP-completeness*, Theoret. Comput. Sci. **407** (1–3), 591–595 (2008).
DOI: <https://doi.org/10.1016/j.tcs.2008.08.028>

- [7] V.A. Artamonov, S. Chakrabarti, S.K. Pal, *Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations*, Discrete Appl. Math. **200**, 5–17 (2016).
DOI: <https://doi.org/10.1016/j.dam.2015.06.033>
- [8] V.L. Murskiy, *Finite basis of identities and other properties of “almost all” algebras*, Problemy kibernetiki **30**, 43–56 (1975) [in Russian].
- [9] P.J. Cameron, *Almost all quasigroups have rank 2*, Discrete Math. **106–107**, 111–115 (1992).
DOI: [https://doi.org/10.1016/0012-365X\(92\)90537-P](https://doi.org/10.1016/0012-365X(92)90537-P)
- [10] A. Salomaa, *Some completeness criteria for sets of functions over a finite domain II*, Annales Universitatis Turkuensis. Series AI **63**, 19 pp. (1963).
- [11] A.V. Galatenko, V.V. Galatenko, A.E. Pankrat'ev, *Strong polynomial completeness of almost all quasigroups*, Math. Notes **111** (1), 7–12 (2022).
DOI: <https://doi.org/10.1134/S0001434622010023>
- [12] B. Larose, L. Zádori, *Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras*, Int. J. Algebra Comput. **16** (3), 563–581 (2006).
DOI: <https://doi.org/10.1142/S0218196706003116>
- [13] D.S. Krotov, V.N. Potapov, *n -ary quasigroups of order 4*, SIAM J. Discrete Math. **23** (2), 561–570 (2009).
DOI: <https://doi.org/10.1137/070697331>
- [14] C.F. Laywine, G.L. Mullen, *Discrete mathematics using Latin squares*, Wiley, New York, 1998.
- [15] V.N. Potapov, D.S. Krotov, *Asymptotics for the number of n -quasigroups of order 4*, Siberian Math. J. **47** (4), 720–731 (2006).
DOI: <https://doi.org/10.1007/s11202-006-0083-9>
- [16] D.S. Krotov, V.N. Potapov, P.V. Sokolova, *On reconstructing reducible n -ary quasigroups and switching subquasigroups*, Quasigr. Relat. Syst. **16** (1), 55–67 (2008).
- [17] V. N. Potapov, D. S. Krotov, *On the number of n -ary quasigroups of finite order*, Discrete Math. Appl. **21** (5–6), 575–585 (2011).
DOI: <https://doi.org/10.1515/dma.2011.035>
- [18] N. Linial, Z. Luria, *An upper bound on the number of high-dimensional permutations*, Combinatorica **34** (4), 471–486 (2014).
DOI: <https://doi.org/10.1007/s00493-011-2842-8>
- [19] V.N. Potapov, *On the number of SQSs, latin hypercubes and MDS codes*, J. Combin. Des. **26** (5), 237–248 (2018).
DOI: <https://doi.org/10.1002/jcd.21603>

- [20] A.V. Galatenko, A.E. Pankratiev, V.M. Staroverov, *Algorithms for checking some properties of n -quasigroups*, Program. Comput. Softw. **48** (1), 36–48 (2022).
DOI: <http://doi.org/10.1134/s0361768822010042>
- [21] D. Lau, *Function algebras on finite sets: a basic course on many-valued logic and clone theory*, Springer-Verlag, Berlin, 2006.
DOI: <https://doi.org/10.1007/3-540-36023-9>
- [22] G.H. Hardy, S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. **17**, 75–115 (1918).
DOI: <https://doi.org/10.1112/plms/s2-17.1.75>

Alexei Vladimirovich Galatenko

Moscow State University,
Faculty of Mechanics and Mathematics,
1 Leninskie Gory, Moscow 119991, Russia,
e-mail: agalat@msu.ru

Vladimir Vladimirovich Galatenko

Moscow State University,
Faculty of Mechanics and Mathematics,
1 Leninskie Gory, Moscow 119991, Russia,
e-mail: vgalat@msu.ru

Anton Evgevievich Pankratiev

Moscow State University,
Faculty of Mechanics and Mathematics,
1 Leninskie Gory, Moscow 119991, Russia,
e-mail: apankrat@intsys.msu.ru