# Об индексе ассоциативности конечных квазигрупп

К. Д. Царегородцев[1]

В статье рассматриваются результаты, связанные с оценками числа ассоциативных троек в произвольных квазигруппах и в квазигруппах из некоторых классов. Приведены результаты исследований, описывающие количество ассоциативных троек в квазигруппах, задаваемых правильными семействами булевых функций малых размеров.

**Ключевые слова:** ассоциативная тройка, квазигруппа, правильное семейство булевых функций.

## 1. Введение

Квазигруппы — одни из базовых структур в алгебре. Таблицы умножения квазигрупп, более известные под названием «латинские квадраты», с древнейших времен и по настоящее время используются в различных областях математики [1]: при планировании статистических экспериментов, в играх и головоломках, в теории кодирования и криптографии. Из общих обзоров криптографических приложений квазигрупп можно отметить следующие источники:

- статья [2], в которой приводятся примеры кодов аутентификации, шифров и однонаправленных функций на основе квазигрупповых преобразований, а также недавний обзор [3], затрагивающий тематику построения симметричных криптопримитивов на основе квазигрупповых операций;
- монография [4], в которой довольно подробно освещена тематика использования квазигрупп в криптографии; в частности, в работе рассматриваются следующие темы: поточные шифры и их криптоанализ, хэш-функции и односторонние функции, схемы разделения секрета; а также смежная тематика теории кодирования (в частности, рекурсивные МДР-коды);
- монография [1] и статья [5], посвященные общим обзорам тематики латинских квадратов, их использованию в докомпьютерный этап развития криптографии и современным приложениям.

[1] *Царегородцев Кирилл Денисович* — старший специалист-исследователь Лаборатории Криптографии, АО «НПК «Криптонит» e-mail: kirill94_12@mail.ru.
Tsaregorodtsev Kirill Denisovich — senior researcher, JSRPC "Kryptonite".

Для того, чтобы некоторые криптографические примитивы, основанные на квазигрупповом умножении, были стойкими к криптоанализу, необходимо, чтобы в квазигруппе было как можно меньше ассоциативных троек, то есть, чтобы квазигрупповая операция была как можно менее ассоциативна. Так, например, большое количество ассоциативных троек может быть использовано при нахождении коллизий и вторых прообразов для некоторых хэш-функций, построенных на основе квазигруппового умножения [6]. Следовательно, с практической точки зрения интересны следующие вопросы:

- каково минимально возможное (и достижимое) число ассоциативных троек для квазигрупп заданного размера?
- можно ли построить классы квазигрупп с заданным малым числом ассоциативных троек?
- можно ли найти квазигруппы с малым числом ассоциативных троек и компактным описанием (в частности, для которых не нужно было бы хранить всю таблицу умножения в компьютере, а вычислять результат квазигрупповой операции более эффективно)?

Указанные вопросы, а также тесно связанные с ними (например, каково *минимально возможное* число неассоциативных троек в неассоциативной квазигруппе заданного порядка?) изучались с 1980-х годов и в отрыве от практических приложений (см. работы [7, 8, 9, 10, 11], а также задачу 1.1 в [1]). Таким образом, сформулированные вопросы интересны как с точки зрения практики, так и чисто теоретически. В данной работе мы рассматриваем большинство полученных на данный момент результатов по количеству ассоциативных троек в квазигруппах, а также приводим результаты исследований, описывающих количество ассоциативных троек в квазигруппах, задаваемых правильными семействами булевых функций малых размеров.

## 2. Предварительные сведения

Приведем стандартные определения из теории квазигрупп (более подробно см., например, [1, 12]).

**Определение 1.** Квазигруппой $(Q, \circ)$ называется множество $Q$ с заданной на нем бинарной операцией $\circ\colon Q \times Q \to Q$, удовлетворяющей следующему условию: для любых $a, b \in Q$ найдутся единственные элементы $x, y \in Q$ — решения уравнений $a \circ x = b,\ y \circ a = b$.

Далее мы будем рассматривать конечные квазигруппы $|Q| < \infty$, для краткости слово «конечный» будем опускать. Также иногда будем писать

«квазигруппа $Q$» без явного упоминания операции $\circ$, если она понятна из контекста.

**Замечание 1.** *Пусть $(Q, \circ)$ — квазигруппа, тогда для каждого $a \in Q$ можно задать операции левого $L_a$ и правого $R_a$ сдвига:*

$$L_a \colon Q \to Q,\ L_a(x) = a \circ x,$$
$$R_a \colon Q \to Q,\ R_a(y) = y \circ a.$$

*Операции $L_a$ и $R_a$ задают биективные отображения на множестве $Q$.*

**Определение 2.** Латинский квадрат размера $k$ — это квадратная таблица размера $k \times k$, заполненная некоторыми $k$ различными элементами таким образом, что в каждой строке и в каждом столбце каждый элемент встречается ровно один раз.

**Определение 3.** Пусть $(Q, \circ)$ — квазигруппа, $Q = \{q_1, \ldots, q_k\}$. Таблицей умножения $Q$ будем называть квадратную таблицу размера $k \times k$, заполненную элементами $q \in Q$ таким образом, что на пересечении $i$-й строки и $j$-го столбца записывается произведение $(q_i \circ q_j) \in Q$.

**Замечание 2.** *Латинские квадраты являются таблицами умножения квазигруппы. Это следует из того факта, что левые и правые сдвиги являются биекциями.*

Далее мы будем отождествлять квазигруппу с латинским квадратом, задающим ее таблицу умножения.

**Определение 4.** Пусть $(Q, \circ)$ — квазигруппа. Ее изотопом называется квазигруппа $(Q_{\alpha\beta\gamma}, *)$ с операцией $*$, заданной на том же множестве $Q$ по правилу $a * b = \gamma^{-1}(\alpha(a) \circ \beta(b))$, где $\alpha, \beta, \gamma \in \mathcal{S}_Q$ — биекции на $Q$.

**Определение 5.** Главным изотопом $Q_{\alpha\beta}$ называется изотоп квазигруппы $Q$ с дополнительным условием $\gamma = \mathsf{id}$, где $\mathsf{id}$ — тождественное отображение на $Q$.

**Определение 6.** Биекция $\sigma \in \mathcal{S}_Q$ называется ортоморфизмом квазигруппы $(Q, \circ)$, если отображение $\theta$, задаваемое правилом $x \circ \theta(x) = \sigma(x)$ также является биекцией на множестве $Q$.

**Определение 7.** Идемпотентом в квазигруппе $(Q, \circ)$ называется элемент $x \in Q$ со свойством $x \circ x = x$.

**Определение 8.** Ассоциативной тройкой называется тройка элементов квазигруппы $a, b, c \in Q$ таких, что выполнено равенство:

$$(a \circ b) \circ c = a \circ (b \circ c).$$

**Определение 9** ([10]). Индексом ассоциативности $a(Q)$ квазигруппы $Q$ называется число ассоциативных троек в ней.

Индекс ассоциативности, как было отмечено выше, является важной характеристикой квазигруппы, которая, в частности, показывает, насколько квазигрупповая операция близка к групповой. В дальнейшем изложении нам понадобятся следующие обозначения:

- $a(Q)$: индекс ассоциативности для квазигруппы $Q$;
- $b(Q)$: число неассоциативных троек в квазигруппе $Q$;
- $a(n)$: минимальное число ассоциативных троек среди всех квазигрупп порядка $n$;
- $a(n, C)$: минимальное число ассоциативных троек среди всех квазигрупп из класса $C$ порядка $n$;
- $b(n)$: минимальное число неассоциативных троек среди всех неассоциативных квазигрупп порядка $n$;
- $b(n, C)$: минимальное число неассоциативных троек среди всех квазигрупп из класса $C$ порядка $n$.

## 3. Оценки на число ассоциативных троек

Очевидно, что число ассоциативных троек в квазигруппе не может превышать $|Q|^3$ — общего числа всех троек элементов в квазигруппе. Данная оценка достижима при условии что $Q$ — группа. Можно легко получить следующую универсальную для всех квазигрупп оценку.

**Утверждение 1** ([13]). *Выполняется следующее двойное неравенство:*

$$n \leq a(n) \leq n^3.$$

Утверждение следует из того факта, что в квазигруппе $Q$ для каждого элемента $x \in Q$ существуют левая и правая единицы $le(x), re(x) \in Q$ со свойством $le(x) \circ x = x = x \circ re(x)$. Тогда для каждого $x \in Q$ тройка $(le(x), x, re(x))$ является ассоциативной:

$$(le(x) \circ x) \circ re(x) = x = le(x) \circ (x \circ re(x)).$$

Одной из первых работ, в которых изучалось число ассоциативных троек в алгебраических структурах, является работа [8], автор которой

исследовал коммутативные группоиды. В [8] показано, что для коммутативного неассоциативного группоида $Q$ порядка $n$ верны оценки:

$$n^2 \leq a(Q) \leq n^3 - 2,$$

причем каждая из границ достижима в классе коммутативных группоидов (при $n \geq 3$). Также в [8] рассмотрены классы коммутативных квазигрупп, изотопных группам, коммутативных медиальных квазигрупп и несколько других классов, для каждого из которых получены похожие оценки ($\Theta(n^2)$ для нижней границы и $\Theta(n^3)$ для верхней).

Работа [7] также посвящена группоидам (а именно, классу группоидов с сокращением, частными случаями которых являются квазигруппы). Следствием результатов из работы [7] является неравенство $b(n) \geq n$ (т.е. число неассоциативных троек в группоидах $Q$ с сокращениями не может быть меньше, чем $|Q|$).

Работы [9, 11] посвящены смежному вопросу: каково минимальное число неассоциативных троек в неассоциативной квазигруппе? В работе [9] был рассмотрен класс квазигрупп, изотопных группам, и на него были расширены некоторые результаты из работы [8]. Общим результатом этих работ является следующее наблюдение.

**Утверждение 2** ([9, теорема 5.1]). *Пусть $C$ — класс всех неассоциативных квазигрупп $Q$, изотопных группам. Тогда:*

$$b(n, C) \geq \begin{cases} 4n^2 - 6n, & n \geq 3,\ n \text{ нечетно;} \\ 4n^2 - 8n, & n \text{ четно.} \end{cases}$$

В [11] для исследования величины $b(Q)$ вводится следующая характеристика квазигрупповой операции.

**Определение 10.** Для квазигруппы $(Q, \circ)$ определим расстояние до множества групп $\mathsf{gdist}(Q)$ как минимум среди чисел $\mathsf{dist}(Q, G)$, где $G = (Q, \cdot)$ — группа, заданная на том же множестве, что и квазигруппа $(Q, \circ)$, а функция $\mathsf{dist}$ определена следующим образом:

$$\mathsf{dist}(Q, G) = |\{(x, y) \in Q^2 \mid x \circ y \neq x \cdot y\}|.$$

**Утверждение 3** ([11, утверждение 4.1]). *Пусть $Q$ — квазигруппа порядка $n$, $t = \mathsf{gdist}(Q)$. Тогда выполнены следующие неравенства:*

*1)* $4tn - 2t^2 - 24t \leq b(Q) \leq 4tn$;

*2) если* $t \geq 24$, *то* $b(Q) \geq 4tn - 2t^2 - 16t$.

Также в [11] показано, что для всех $n \geq 6$ выполняется неравенство

$$b(n) \leq 16n - 64.$$

Обозначим через $i(Q) = |\{x \in Q \mid x \circ x = x\}|$ — количество идемпотентов (см. определение 7) в квазигруппе $Q$. Основным результатом работы [14] является связь чисел $i(Q)$ и $a(Q)$.

**Утверждение 4** ([14, теорема 1.1]). *Для квазигруппы $Q$ выполняется следующее неравенство:*

$$a(Q) \geq 2n - i(Q).$$

В частности, из утверждения 4 следует, что если в квазигруппе $Q$ порядка $n$ число ассоциативных троек $a(Q)$ также равно $n$ (т.е. достигается нижняя граница на число ассоциативных троек для квазигруппы порядка $n$), то каждый элемент квазигруппы является идемпотентом.

**Замечание 3.** *Заметим, что с криптографической точки зрения это требование входит в противоречие с требованием отсутствия подквазигрупп [15, 16] (в частности, подквазигрупп размера 1).*

Дальнейшие продвижения были получены в работе [17]. Обозначим через $\delta_L(Q)$ число элементов $a \in Q$, для которых подстановка $L_a$ (см. замечание 1) не имеет неподвижных точек, через $\delta_R(Q)$ число элементов $a \in Q$, для которых подстановка $R_a$ не имеет неподвижных точек.

**Утверждение 5** ([17, теорема 2.5]). *Выполнено следующее неравенство:*

$$a(Q) \geq 2n - i(Q) + \delta_L(Q) + \delta_R(Q).$$

Таким образом, если для квазигруппы $Q$ порядка $n$ достигается минимально возможное число ассоциативных троек $a(Q) = n$, то в $Q$ каждый элемент является идемпотентом (т.е., $i(Q) = n$), и у отображений $L_a$, $R_a$ нет неподвижных точек.

## 4. Примеры квазигрупп с заданным числом ассоциативных троек

В работах [10, 13] приведены несколько примеров классов квазигрупп с малым числом ассоциативных троек, что позволяет получить верхние оценки на минимальное число ассоциативных троек $a(n)$.

Так, для случая $n \neq 2 \mod 4$ существует коммутативная группа $(G, +)$ и автоморфизм $\phi \in Aut(G)$ со свойством

$$\forall x \in G \setminus \{0\} \quad \phi(x) \neq x.$$

Если $n$ нечетно, то положим $G = \mathbb{Z}_n$, $\phi(x) = 2x$. В случае $n = 2^m$ рассмотрим группу $G = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$ и автоморфизм

$$\phi(x_1, \ldots, x_m) = (x_1 + x_2, x_3, \ldots, x_m, x_1).$$

Наконец, в случае $n = 2^m \cdot d$, где $m \geq 2$, $d$ нечетное, рассмотрим группу $G = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2 \times \mathbb{Z}_d$ и автоморфизм

$$\phi(x_1, \ldots, x_m, z) = (x_1 + x_2, x_3, \ldots, x_m, x_1, 2z).$$

Зададим квазигрупповую операцию $\circ$ на множестве $G$ по правилу:

$$x \circ y = \phi(x + y), \quad x, y \in G.$$

В таком случае все тройки $(x, y, x)$ в $(G, \circ)$ являются ассоциативными:

$$\begin{aligned}(x \circ y) \circ x = \phi\left(\phi(x + y) + x\right) = \phi^2(x) + \phi^2(y) + \phi(x) = \\ = \phi\left(x + \phi(x + y)\right) = x \circ (y \circ x).\end{aligned}$$

Других ассоциативных троек в $(G, \circ)$ нет: если $(x, y, z)$ — ассоциативная тройка, то выполняются следующие равенства:

$$\begin{aligned}(x \circ y) \circ z = \phi^2(x) + \phi^2(y) + \phi(z) = \phi(x) + \phi^2(y) + \phi^2(z) = x \circ (y \circ z) \Rightarrow \\ \Rightarrow \phi^2(x - z) = \phi(x - z).\end{aligned}$$

Поскольку $\phi(x) = x$ только при $x = 0$, мы имеем $x = z$.

Для полученной квазигруппы $Q = (G, \circ)$ верно равенство $a(Q) = n^2$, а следовательно, мы имеем:

$$a(n) \leq n^2, \quad n \neq 2 \mod 4.$$

Для случая $n = 2 \mod 4$ можно построить квазигруппу $Q$ с индексом ассоциативности $a(Q) = 2n^2$. Для этого представим $n$ в виде $n = 2d$, $d$ нечетное. Положим $G = \mathbb{Z}_2 \times \mathbb{Z}_d$ и введем операцию покомпонентного сложения в $G$. Рассмотрим автоморфизм $\phi$ группы $G$, заданный по правилу $\phi(a, b) = (a, 2b)$, и операцию $\circ$ на множестве $G$:

$$(x_1, x_2) \circ (y_1, y_2) = \phi(x_1, x_2) + (y_1, y_2).$$

Операция $\circ$ задает структуру квазигруппы $Q$ на множестве $G$. Для ассоциативных троек должно выполняться равенство:

$$(x \circ y) \circ z = \phi^2(x) + \phi(y) + z = \phi(x) + \phi(y) + z = x \circ (y \circ z).$$

Следовательно, любая тройка $(x, y, z)$ с условием $\phi(x) = x$ является ассоциативной. Указанное условие выполняется для элементов

$$x = (x_1, 0), \quad x_1 \in \mathbb{Z}_2,$$

$y, z$ — любые элементы $G$. Следовательно, $a(n) \leq 2n^2$, $n = 2 \bmod 4$.

В работе [10] приведен пример класса квазигрупп размера $n$, где $n \geq 6$, $n = 0, 2 \bmod 6$, с количеством ассоциативных троек $a(Q) = n^2 - 3n + 3$. Таким образом, в случае $n \geq 6$, $n = 0, 2 \bmod 6$ мы получаем оценку

$$a(n) \leq n^2 - 3n + 3.$$

В ряде статей [18, 19, 20] были получены примеры классов **максимально неассоциативных** квазигрупп, т.е. квазигрупп, для которых $a(Q) = |Q|$. В [18] была дана конструкция на основе т.н. почтиполей (см., например, [21]), из которой следует, что $a(n) = n$ для $n = 2^{6k} \cdot r^2$, где $k \geq 0$, $r$ нечетное. В частности, $a(p^2) = p^2$ для всех нечетных простых $p$.

Указанный результат был расширен в [19, 20]. Обозначим через $\nu_p(n)$ степень вхождения $p$ в разложение $n$ на простые сомножители. В статье [20] показано, что для $n$, удовлетворяющих условиям:

$$\nu_p(n) \neq 1, \ p \in \{3, 5, 7, 11\}, \quad \nu_2(n) \neq 2, 4 \text{ и четно},$$

существует максимально неассоциативная квазигруппа порядка $n$.

В статье [19] показано, что максимально неассоциативная квазигруппа существует для всех достаточно больших порядков $n$, которые **не имеют** вид $n = 2p_1$ или $n = 2p_1p_2$, где $p_1$, $p_2$ — нечетные простые, $p_1 \leq p_2 < 2p_1$. В частности, существует максимально неассоциативная квазигруппа для простых порядков $p \geq 13$.

## 5. Оценка среднего числа ассоциативных троек

В работе [22] предложен еще один подход к подсчету числа ассоциативных троек в квазигруппах. Как известно (см., например, [23]), ассоциативные тройки можно рассматривать как неподвижные точки коммутатора отображений $[L_a, R_b]$, где $[x, y] = x^{-1}y^{-1}xy$: если $(a, x, b)$ — ассоциативная тройка, то выполняется условие

$$(a \circ x) \circ b = R_b(L_a(x)) = a \circ (x \circ b) = L_a(R_b(x)),$$

то есть $x$ является неподвижной точкой коммутатора: $[L_a, R_b](x) = x$.

В работе [22] предложено оценивать среднее число ассоциативных троек в квазигруппе, где усреднение берется по всем главным изотопам. Обозначим через $Q_{\alpha\beta}$ главный изотоп $Q$, заданный операцией

$$a * b = \alpha(a) \circ \beta(b).$$

**Утверждение 6** ([22, утверждение 2.1]). *Для $n \geq 2$ выполнено следующее равенство:*

$$\frac{1}{(n!)^2} \sum_{\alpha,\beta \in \mathcal{S}_Q} a(Q_{\alpha\beta}) = \frac{n^3}{n-1}.$$

Идея доказательства состоит в подсчете числа неподвижных точек всех коммутаторов $[L_a, R_b]$ для всех главных изотопов, что, в свою очередь, сводится к задаче подсчета суммы $\sum_{\phi,\psi \in \mathcal{S}_Q} |Fix([\phi, \psi])|$, где $Fix(\pi) = \{x \in Q \mid \pi(x) = x\}$ — множество неподвижных точек подстановки $\pi$.

Следующее утверждение следует из предыдущего.

**Утверждение 7.** *Для $n \geq 2$ выполнено следующее равенство:*

$$\frac{1}{(n!)^3} \sum_{\alpha,\beta,\gamma \in \mathcal{S}_Q} a(Q_{\alpha\beta\gamma}) = \frac{n^3}{n-1}.$$

Таким образом, для каждой квазигруппы среднее число ассоциативных троек (при усреднении по всем изотопам) примерно равно $n^2$.

**Утверждение 8** ([22, утверждение 2.3]). *Для $n \geq 2$ выполнено следующее неравенство:*

$$\frac{1}{n!} \sum_{\beta} a(Q_{\alpha\beta}) \geq n^2,$$

*и равенство достигается тогда и только тогда, когда $\alpha^{-1}$ — ортоморфизм квазигруппы $Q$.*

## 6. Минимальное число ассоциативных троек в квазигруппах малого порядка

В ряде работ [13, 14, 22] путем перебора были получены точные значения минимального числа ассоциативных троек $a(n)$ для квазигрупп порядка $n \leq 7$ (см. Табл. 1). Для квазигрупп порядка $n = 8, 9$ число $a(n)$ уже не может быть получено путем полного перебора, поэтому в работах [17, 24] был предложен способ сократить перебор. С помощью ограниченного перебора были получены точные значения чисел $a(8)$, $a(9)$ и получена оценка снизу для $a(10)$ (а именно, было показано, что не существует квазигрупп порядка 10 с индексом ассоциативности 10). Полученные результаты отображены в Табл. 1. Заметим, что полученные значения меньше существующих теоретических оценок, приведенных в разделе 3.

Таблица 1. Минимальное число ассоциативных троек длквазигрупп порядка $n \leq 10$

| $n$ | $a(n)$ | Работа |
|---|---|---|
| 1 | 1 | [13] |
| 2 | 8 | [13] |
| 3 | 9 | [13] |
| 4 | 16 | [13] |
| 5 | 15 | [13] |
| 6 | 16 | [13] |
| 7 | 17 | [22] |
| 8 | 16 | [17] |
| 9 | 9 | [17] |
| 10 | $> 10$ | [24] |

# 7. Индексы ассоциативности квазигрупп, заданных правильными семействами функций

В цикле работ [25, 26, 27] было предложено задавать таблицу умножения квазигруппы с помощью правильных семейств функций. В настоящем разделе мы рассмотрим один способ задания квазигрупп с помощью правильных семейств и приведем результаты численных экспериментов по вычислению индексов ассоциативности полученных квазигрупп.

## 7.1. Правильные семейства функций

**Определение 11.** Пусть $Q_1, \ldots, Q_n$ — набор непустых конечных множеств. Под семейством функций $F_n$ на $Q_1 \times \ldots \times Q_n$ будем понимать отображение $F_n \colon Q_1 \times \ldots \times Q_n \to Q_1 \times \ldots \times Q_n$ вида

$$F_n \colon \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \begin{bmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{bmatrix}, \; f_i(x_1, \ldots, x_n) \colon Q_1 \times \ldots \times Q_n \to Q_i.$$

Число $n$ будем называть размером семейства. Иногда мы будем опускать размер семейства $n$ из обозначения $F_n$, если он понятен из контекста.

**Замечание 4.** *Если $Q_1 = \ldots = Q_n = \mathbb{E}_2$, где $\mathbb{E}_2 = \{0, 1\}$, то $F_n$ будем называть семейством булевых функций.*

**Определение 12.** Семейство функций $F_n$ на $Q_1 \times \ldots \times Q_n$ называется правильным, если для любых двух неравных наборов

$$\alpha = (\alpha_1, \ldots, \alpha_n), \quad \beta = (\beta_1, \ldots, \beta_n), \quad \alpha \neq \beta,$$

выполняется следующее условие:

$$\exists i\colon \alpha_i \neq \beta_i,\ f_i(\alpha) = f_i(\beta).$$

## 7.2. Критерий правильности в терминах регулярности

Для семейств булевых функций выполняется следующий критерий правильности.

**Утверждение 9** ([27, теорема 2]). *Семейство булевых функций $F_n(x)$ является правильным тогда и только тогда, когда для любого набора отображений $\Psi = (\psi_1, \ldots, \psi_n)$, $\psi_i\colon \mathbb{E}_2 \to \mathbb{E}_2$ отображение*

$$x \to x \oplus \Psi(F_n(x)) = \begin{bmatrix} x_1 \oplus \psi_1(f_1(x_1, \ldots, x_n)) \\ \vdots \\ x_n \oplus \psi_n(f_n(x_1, \ldots, x_n)) \end{bmatrix}$$

*является биекцией $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$.*

Указанное утверждение допускает следующее обобщение.

**Теорема 1.** *Семейство $F_n$ на $Q_1 \times \ldots \times Q_n$, где $(Q_i, \circ_i)$ — квазигруппы, является правильным тогда и только тогда, когда для любого набора отображений $\psi_i\colon Q_i \to Q_i$ следующее отображение биективно:*

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to x \circ \Psi(F_n(x)) = \begin{bmatrix} x_1 \circ_1 \psi_1(f_1(x_1, \ldots, x_n)) \\ \vdots \\ x_n \circ_n \psi_n(f_n(x_1, \ldots, x_n)) \end{bmatrix},\ x_i \in Q_i.$$

*Док-во.* Пусть $F_n$ — правильное семейство на $Q_1 \times \ldots \times Q_n$. Покажем, что отображение $x \to x \circ \Psi(F_n(x))$ инъективно. Пусть $x \neq y$, $x, y \in Q_1 \times \ldots \times Q_n$, тогда по условию правильности найдется такой индекс $i$, что $x_i \neq y_i$, но $f_i(x) = f_i(y)$, а значит,

$$x_i \circ_i \psi_i(f_i(x)) \neq y_i \circ_i \psi_i(f(y)).$$

Из конечности $Q_1 \times \ldots \times Q_n$ и инъективности отображения следует его биективность.

Пусть $F$ не является правильным. Построим отображение $\Psi$ таким образом, чтобы $x \to x \circ \Psi(F_n(x))$ не было биекцией. Поскольку $F$ не является правильным, то найдутся две точки $x \neq y$, для которых для всех индексов $i$ со свойством $x_i \neq y_i$ следует $f_i(x) \neq f_i(y)$. Рассмотрим все индексы, в которых наборы $x$ и $y$ различаются. Для каждого «плохого» индекса зададим $\psi_i$ таким образом, чтобы $x_i \circ_i \psi_i(f_i(x)) = y_i \circ_i \psi_i(f_i(y))$; это можно сделать, зафиксировав $\psi_i(f_i(x))$ как угодно и доопределить

$\psi_i(f_i(y))$ из уравнения (из условия на «плохие» индексы мы имеем $f_i(x) \neq f_i(y)$, а значит, определение $\psi_i$ корректно). В тех индексах, где $x_i = y_i$, зададим $\psi_i$ как правый нейтральный элемент для $x_i$ для любого значения аргумента.

Если мы зададим $\psi_i$ обозначенным выше образом, то получим

$$x \neq y, \quad x \circ \Psi(F_n(x)) = y \circ \Psi(F_n(y)),$$

а значит, отображение не может быть биективным. □

## 7.3. Один способ построения квазигрупп с помощью правильных семейств

Заметим, что с помощью теоремы 1 можно предложить следующий способ задания квазигруппы. Пусть $F$, $G$ — два правильных семейства функций размера $n$ над группой $(H^n, +)$ (группа $H$ не обязана быть абелевой). Для $x, y \in H^n$ зададим операцию $\circ$ следующим образом:

$$x \circ y = x + F(x) + y + G(y).$$

Поскольку отображение $x \to \pi_F(x) = x + F(x)$, где $F$ — правильное, является биекцией, то операция $\circ$ задает главный изотоп группы $H^n$ (а значит, задает квазигрупповую операцию).

**Замечание 5.** *Указанный способ задания квазигруппы отличается от «стандартного» построения на основе одного правильного семейства (см., например, [25, 26]).*

Потребуем дополнительно, чтобы группа $H^n$ была коммутативной, и рассмотрим условие на ассоциативность тройки $(x, y, z)$ в квазигруппе $Q$, построенной по паре правильных семейств $(F, G)$:

$$(x \circ y) \circ z = (x + F(x)) + (y + G(y)) + (z + G(z)) + F\left(x + F(x) + y + G(y)\right),$$
$$x \circ (y \circ z) = (x + F(x)) + (y + F(y)) + (z + G(z)) + G\left(y + F(y) + z + G(z)\right),$$

и из условия $(x \circ y) \circ z = x \circ (y \circ z)$ получаем, что:

$$F(y) - G(y) = F\left(x + F(x) + y + G(y)\right) - G\left(y + F(y) + z + G(z)\right). \quad (1)$$

Из подобного эквивалентного представления относительно легко следуют два наблюдения, которые могут быть доказаны прямой проверкой.

**Утверждение 10.** *Тройка $(x, y, z)$ является ассоциативной в квазигруппе $Q$, построенной по паре семейств $(F, G)$, тогда и только тогда, когда тройка $(z, y, x)$ является ассоциативной в квазигруппе $Q'$, построенной по паре семейств $(G, F)$.*

В частности, индексы ассоциативности квазигрупп, построенных по парам семейств $(F, G)$ и по парам семейств $(G, F)$, совпадают.

**Утверждение 11.** *Пусть $\mathcal{A}$ — такое обратимое линейное отображение (т.е. $\mathcal{A}(x+y) = \mathcal{A}(x) + \mathcal{A}(y)$), что семейства*

$$F'(x) = \mathcal{A}^{-1}\left(F\left(\mathcal{A}(x)\right)\right), \quad G'(y) = \mathcal{A}^{-1}\left(G\left(\mathcal{A}(y)\right)\right)$$

*также являются правильными (так, в качестве $\mathcal{A}$ можно рассмотреть преобразование обратимой линейной перекодировки, см. [28]). В таком случае $(x, y, z)$ является ассоциативной тройкой для квазигруппы, построенной по паре правильных семейств $(F, G)$, тогда и только тогда, когда тройка $\left(\mathcal{A}^{-1}(x), \mathcal{A}^{-1}(y), \mathcal{A}^{-1}(z)\right)$ является ассоциативной для квазигруппы, построенной по паре правильных семейств $(F', G')$.*

В частности, индексы ассоциативности квазигрупп, построенных по парам семейств $(F, G)$ и $(F', G')$, совпадают.

В случае $A^n = \mathbb{Z}_2^n$ выполняется несколько дополнительных свойств.

**Утверждение 12.** *Тройка $(x, y, z)$ является ассоциативной для квазигруппы, построенной по паре правильных семейств $(F, G)$, тогда и только тогда, когда она является ассоциативной для квазигруппы, построенной по паре правильных семейств $(F \oplus \alpha, G \oplus \alpha)$, где $\alpha \in \mathbb{Z}_2^n$.*

**Утверждение 13.** *Количество ассоциативных троек в квазигруппе, построенной по паре правильных булевых семейств $(F, G)$, четно.*

*Док-во.*Зафиксируем значения $x$, $y$ и найдем все значения $z$, которые удовлетворяют требованию ассоциативности (1):

$$F(y) \oplus G(y) = F\left(x \oplus F(x) \oplus y \oplus G(y)\right) \oplus G\left(y \oplus F(y) \oplus z \oplus G(z)\right).$$

После фиксации $x$, $y$, мы получим уравнение на $z$ вида

$$G\left(z \oplus G(z) \oplus \alpha\right) = \beta, \quad \alpha, \beta \in \mathbb{Z}_2^n. \tag{2}$$

Как было показано ранее [29, теорема 7], уравнение вида $G(t) = \beta$ всегда имеет четное число решений для булевых правильных семейств. Поскольку отображение $z \to z \oplus G(z) \oplus \alpha$ является биекцией, для каждой фиксации переменных $x$, $y$ уравнение (2) будет иметь четное число решений $z$. Тем самым мы получим четное число ассоциативных троек. □

Указанные свойства могут быть использованы при исследовании индексов ассоциативности квазигрупп, построенных по различным парам правильных семейств.

## 7.4. Индексы ассоциативности для квазигрупп, построенных по правильным булевым семействам малых размеров

Приведем результаты численных экспериментов. Для $n = 2$ имеется 12 правильных булевых семейств, с помощью которых можно задать $12^2 = 144$ квазигруппы (используя конструкцию, описанную в разделе 7.3). Для $n = 3$ имеется 744 правильных булевых семейства, с помощью которых можно задать $744^2 = 553536$ квазигрупп. Все порождаемые квазигруппы будут попарно различны: если $F \neq G$, то для некоторого $x$ имеем $\pi_F(x) = x \oplus F(x) \neq x \oplus G(x) = \pi_G(x)$. Результаты численных экспериментов для $n = 2$ приведены в Табл. 2, для $n = 3$ — приведены в Табл. 3 и на рис. 1.

Таблица 2. Число квазигрупп с заданным $a(Q)$ для квазигрупп, построенных по правильным булевым семействам размера $n = 2$

| $a(Q)$ | Кол-во $Q$ |
|---|---|
| 16 | 32 |
| 32 | 96 |
| 64 | 16 |

Для $n = 4$ был проведен статистический эксперимент. Случайно равновероятно (среди всех возможных пар) выбирались $N = 10^5$ пар правильных семейств, по каждой паре строилась квазигруппа, подсчитывался индекс ассоциативности полученной квазигруппы. Была построена ядерная оценка плотности полученной случайной величины, результат приведен на рис. 2.

Заметим, что при $n = 2$ достигается минимально возможное значение индекса ассоциативности для квазигрупп порядка 4 (а именно 16). При $n \geq 3$ все полученные индексы ассоциативности существенно превышают теоретически возможные для квазигрупп заданного порядка. Отметим также, что во всех исследованных случаях $n = 2, 3, 4$ минимально достижимый индекс ассоциативности у построенных квазигрупп оказался равным квадрату порядка квазигруппы, в связи с чем можно выдвинуть гипотезу, что у квазигрупп, построенным по парам правильных булевых семейств размера $n$ число ассоциативных троек не может быть меньше, чем $2^{2n}$.

Для $n = 3$ также был проведен следующий эксперимент. Все 744 правильных семейства были разбиты на 10 классов эквивалентности относительно изометрий пространства Хэмминга (см. [28]). Затем для каждой пары классов эквивалентности $(\mathcal{F}, \mathcal{G})$ перебирались все пары представителей $F \in \mathcal{F}$, $G \in \mathcal{G}$ и вычислялся индекс ассоциативности

Таблица 3. Число квазигрупп с заданным $a(Q)$ для квазигрупп, построенных по правильным булевым семействам размера $n = 3$

| $a(Q)$ | Кол-во $Q$ |
|---|---|
| 64 | 27648 |
| 80 | 103424 |
| 88 | 18432 |
| 96 | 82944 |
| 104 | 33792 |
| 112 | 21504 |
| 120 | 21504 |
| 128 | 116352 |

| $a(Q)$ | Кол-во $Q$ |
|---|---|
| 144 | 3072 |
| 160 | 84480 |
| 176 | 6144 |
| 192 | 18432 |
| 208 | 3072 |
| 256 | 10368 |
| 320 | 2304 |
| 512 | 64 |

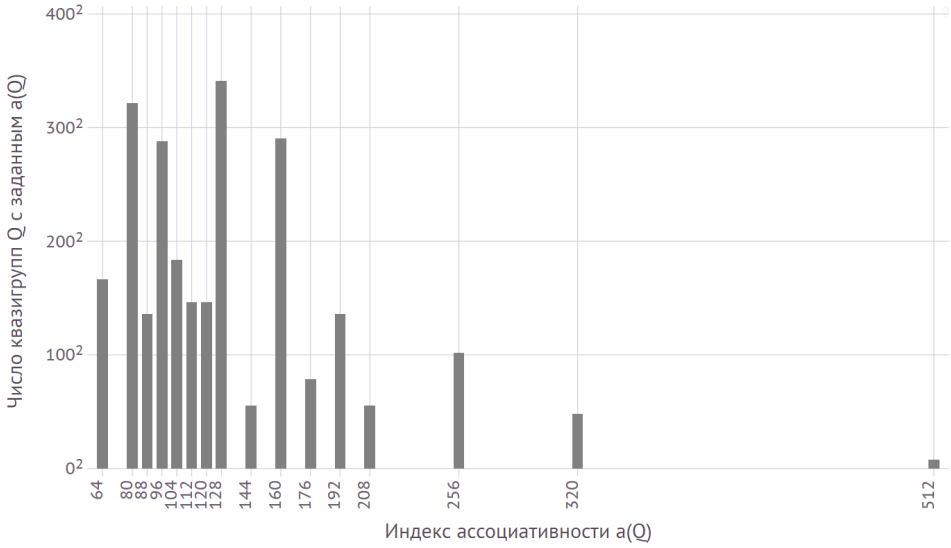


Рисунок 1. Распределение числа квазигрупп с заданным $a(Q)$ для $n = 3$

квазигруппы, порождаемой парой правильных булевых семейств $(F, G)$, после чего вычислялся «средний индекс ассоциативности» для пары классов эквивалентности $(\mathcal{F}, \mathcal{G})$. Результаты эксперимента отображены на рис. 3. Из приведенной тепловой карты видно, что наиболее неассоциативные квазигруппы порождаются при использовании 6-го класса эквивалентности, представителем которого является, например, семейство

$$(x_2x_3,\ x_1 \oplus x_1x_3,\ x_1 \oplus x_2 \oplus x_1x_2)\,. \tag{3}$$

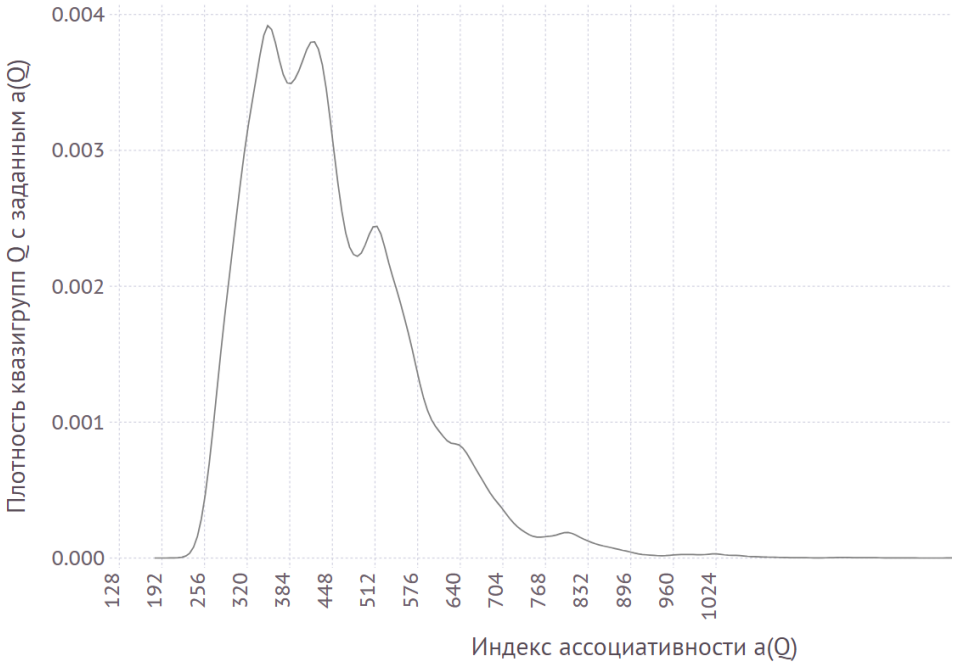


Рисунок 2. Оценка плотности распределения квазигрупп, построенных по парам правильных булевых семейств, с заданным $a(Q)$ для $n = 4$

Заметим, что класс правильных семейств, к которому принадлежит указанный представитель, отдельно изучался ранее (см. [29, раздел 4]); в частности, было отмечено, что «канонические» представители рассматриваемого семейства сильно квадратичны при нечетных $n$ [30, теорема 1] и имеют полный граф существенной зависимости.

## 8. Заключение

В настоящей работе были рассмотрены основные результаты, касающиеся оценок числа ассоциативных троек в квазигруппах. Также был рассмотрен один способ построения квазигрупп на основе правильных семейств функций и получен ряд утверждений об индексах ассоциативности получаемых квазигрупп, приведены результаты вычислительных экспериментов для размеров семейств $n = 2, 3, 4$.

В качестве дальнейших направлений исследований можно выделить следующие:

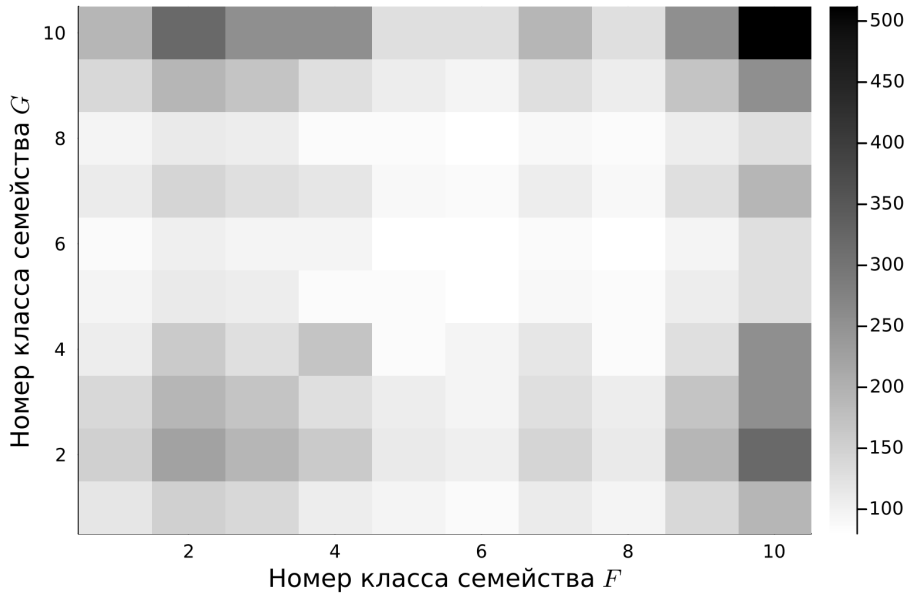


Рисунок 3. Тепловая карта для среднего индекса ассоциативности, усреднение берется по представителям классов эквивалентности, $n = 3$

- исследование алгебраических свойств квазигрупп, порождаемых семействами вида (3);
- исследование связи индекса ассоциативности и графа существенной зависимости семейства (чем «ближе» граф к полному на $n$ вершинах, тем меньше «тривиальных» соотношений в уравнении ассоциативности, а значит, меньше индекс ассоциативности);
- дальнейшее исследование связи индексов ассоциативности квазигрупп, построенных по эквивалентным (в некотором смысле) парам правильных семейств.

Автор выражает признательность научному руководителю А. Е. Панкратьеву и А. В. Галатенко за оказанную помощь при написании настоящей статьи.

## Список литературы

[1] J. Denes, A. Keedwell, *Latin squares and their applications (2nd Edition)*, North Holland, 2015, 428 pp.

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

[3] D. Chauhan, I. Gupta, R. Verma, “Quasigroups and their applications in cryptography”, *Cryptologia*, **45**:3 (2021), 227–265.

[4] V. A. Shcherbacov, *Elements of Quasigroup Theory and Applications (1st Edition)*, Chapman and Hall/CRC, 2017, 598 pp.

[5] М. Э. Тужилин, “Латинские квадраты и их применение в криптографии”, *Прикладная дискретная математика*, 2012, № 3(17), 47–52.

[6] V. Valent, *Quasigroups with few associative triples*, Bachelor thesis, Univerzita Karlova, Matematicko-fyzikální fakulta, 2016.

[7] T. Kepka, “A note on associative triples of elements in cancellation groupoids”, *Commentationes Mathematicae Universitatis Carolinae*, **21**:3 (1980), 479–487.

[8] T. Kepka, “Notes on associative triples of elements in commutative groupoids”, *Acta Universitatis Carolinae. Mathematica et Physica*, **22**:2 (1981), 39–47.

[9] A. Drбpal, T. Kepka, “A note on the number of associative triples in quasigroups isotopic to groups”, *Commentationes Mathematicae Universitatis Carolinae*, **22**:4 (1981), 735–743.

[10] A. Kotzig, C. Reischer, “Associativity index of finite quasigroups”, *Glasnik Matematicki Series III*, **18**:38 (1983), 243–253.

[11] A. Drбpal, “On quasigroups rich in associative triples”, *Discrete Mathematics*, **44**:3 (1983), 251–265.

[12] В.Д. Белоусов, *Основы теории квазигрупп и луп*, Наука, 1967, 224 с.

[13] J. Jeэek, T. Kepka, “Notes on the number of associative triples”, *Acta Universitatis Carolinae. Mathematica et Physica*, **31**:1 (1990), 15–19.

[14] O. Groўek, P. Horбk, “On quasigroups with few associative triples”, *Designs, Codes and Cryptography*, **64**:1-2 (2012), 221–227.

[15] D. Gligoroski, S. Markovski, L. Kocarev, “Edon-R, An Infinite Family of Cryptographic Hash Functions”, *International Journal of Security and Networks*, **8**:3 (2009), 293–300.

[16] В. А. Артамонов, “Квазигруппы и их приложения”, *Чебышевский сборник*, **19**:2 (2018), 111–122.

[17] A. Drбpal, V. Valent, “High nonassociativity in order 8 and an associative index estimate”, *Journal of Combinatorial Designs*, **27**:4 (2019), 205–228.

[18] A. Drбpal, P. Lisonжk, “Maximal nonassociativity via nearfields”, *Finite Fields and Their Applications*, **62** (2020), 101610.

[19] A. Drбpal, I. Wanless, “Maximally nonassociative quasigroups via quadratic orthomorphisms”, *Algebraic Combinatorics*, **4**:3 (2021), 501–515.

[20] P. Lisonжk, “Maximal nonassociativity via fields”, *Designs, Codes and Cryptography*, **88**:12 (2020), 2521–2530.

[21] Ю. Ионин, “Конечные проективные плоскости”, *Математическое просвещение*, **13** (2009), 50–79.

[22] A. Drбpal, V. Valent, “Few associative triples, isotopisms and groups”, *Designs, Codes and Cryptography*, **86**:3 (2018), 555–568.

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

[24] A. Drбpal, V. Valent, “Extreme nonassociativity in order nine and beyond”, *Journal of Combinatorial Designs*, **28**:1 (2020), 33–48.

[25] В. А. Носов, “Построение классов латинских квадратов в булевой базе данных”, *Интеллектуальные системы*, **4**:3–4 (1999), 307–320.

[26] В. А. Носов, “Построение параметрического семейства латинских квадратов в векторной базе данных”, *Интеллектуальные системы*, **8**:1–4 (2006), 517–529.

[27] В. А. Носов, А. Е. Панкратьев, “Латинские квадраты над абелевыми группами”, *Фундаментальная и прикладная математика*, **12**:3 (2006), 65–71.

[28] А. В. Галатенко, А. Е. Панкратьев, К. Д. Царегородцев, “Об одном критерии правильности семейства функций”, *Фундаментальная и прикладная математика*, **24**:4 (2023), 61–73.

[29] К. Д. Царегородцев, “О свойствах правильных семейств булевых функций”, *Дискретная математика*, **33**:1 (2021), 91–102.

[30] А. В. Галатенко, В. А. Носов, А. Е. Панкратьев, К. Д. Царегородцев, “О порождении $n$-квазигрупп с помощью правильных семейств функций”, *Дискретная математика*, **35**:1 (2023), 35–53.

**On the associativity index of finite quasigroups**
**Tsaregorodtsev K. D.**

In this paper we review the results on the number of associative triples in generic quasigroups and quasigroups from restricted classes. Lower and upper bounds on the number of triples are considered, and experimental results on the associativity index of quasigroups generated by proper families of boolean functions are provided.

*Keywords:* associative triple, quasigroup, proper family of boolean functions.

# References

[1] J. Denes, A. Keedwell, *Latin squares and their applications (2nd Edition)*, North Holland, 2015, 428 pp.

[2] M. M. Glukhov, "On the applications of quasi-groups in cryptography", *Applied Discrete Mathematics*, 2008, №2, 28–32 (In Russian).

[3] D. Chauhan, I. Gupta, R. Verma, "Quasigroups and their applications in cryptography", *Cryptologia*, **45**:3 (2021), 227–265.

[4] V. A. Shcherbacov, *Elements of Quasigroup Theory and Applications (1st Edition)*, Chapman and Hall/CRC, 2017, 598 pp.

[5] M. E. Tuzhilin, "Latin squares and their application in Cryptography", *Applied Discrete Mathematics*, 2012, №3(17), 47–52 (In Russian).

[6] V. Valent, *Quasigroups with few associative triples*, Bachelor thesis, Univerzita Karlova, Matematicko-fyzikální fakulta, 2016.

[7] T. Kepka, "A note on associative triples of elements in cancellation groupoids", *Commentationes Mathematicae Universitatis Carolinae*, **21**:3 (1980), 479–487.

[8] T. Kepka, "Notes on associative triples of elements in commutative groupoids", *Acta Universitatis Carolinae. Mathematica et Physica*, **22**:2 (1981), 39–47.

[9] A. Drápal, T. Kepka, "A note on the number of associative triples in quasigroups isotopic to groups", *Commentationes Mathematicae Universitatis Carolinae*, **22**:4 (1981), 735–743.

[10] A. Kotzig, C. Reischer, "Associativity index of finite quasigroups", *Glasnik Matematicki Series III*, **18**:38 (1983), 243–253.

[11] A. Drápal, "On quasigroups rich in associative triples", *Discrete Mathematics*, **44**:3 (1983), 251–265.

[12] V. D. Belousov, *Foundations of the theory of quasigroups and loops*, Nauka, 1967 (In Russian), 224 pp.

[13] J. Ježek, T. Kepka, "Notes on the number of associative triples", *Acta Universitatis Carolinae. Mathematica et Physica*, **31**:1 (1990), 15–19.

[14] O. Grošek, P. Horák, "On quasigroups with few associative triples", *Designs, Codes and Cryptography*, **64**:1-2 (2012), 221–227.

[15] D. Gligoroski, S. Markovski, L. Kocarev, "Edon-R, An Infinite Family of Cryptographic Hash Functions", *International Journal of Security and Networks*, **8**:3 (2009), 293–300.

[16] V. A. Artamonov, "Quasigroups and their applications", *Chebyshevskii Sbornik*, **19**:2 (2018), 111–122 (In Russian).

[17] A. Drápal, V. Valent, "High nonassociativity in order 8 and an associative index estimate", *Journal of Combinatorial Designs*, **27**:4 (2019), 205–228.

[18] A. Drápal, P. Lisoněk, "Maximal nonassociativity via nearfields", *Finite Fields and Their Applications*, **62** (2020), 101610.

[19] A. Drápal, I. Wanless, "Maximally nonassociative quasigroups via quadratic orthomorphisms", *Algebraic Combinatorics*, **4**:3 (2021), 501–515.

[20] P. Lisoněk, "Maximal nonassociativity via fields", *Designs, Codes and Cryptography*, **88**:12 (2020), 2521–2530.

[21] Y. Ionin, "Finite projective planes", *Matematicheskoye prosveshcheniye*, **13** (2009), 50–79 (In Russian).

[22] A. Drápal, V. Valent, "Few associative triples, isotopisms and groups", *Designs, Codes and Cryptography*, **86**:3 (2018), 555–568.

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

[24] A. Drápal, V. Valent, "Extreme nonassociativity in order nine and beyond", *Journal of Combinatorial Designs*, **28**:1 (2020), 33–48.

[25] V. A Nosov, "Construction of classes of Latin squares in a Boolean database", *Intelligent Systems (Intellektualnye Sistemy)*, **4**:3–4 (1999), 307–320 (In Russian).

[26] V. A Nosov, "Construction of a parametric family of Latin squares in a vector database", *Intelligent Systems (Intellektualnye Sistemy)*, **8**:1–4 (2006), 517–529 (In Russian).

[27] V. A. Nosov, A. E Pankratiev, "Latin squares over Abelian groups", *Journal of Mathematical Sciences*, **163**:5 (2009), 53–542.

[28] A. V. Galatenko, A. E Pankratiev, K. D. Tsaregorodtsev, "A Criterion of Properness for a Family of Functions", *Journal of Mathematical Sciences*, 2024.

[29] K. D. Tsaregorodtsev, "Properties of proper families of Boolean functions", *Discrete Mathematics and Applications*, **32**:5 (2022), 369–378.

[30] A. V. Galatenko, V. A. Nosov, A. E Pankratiev, K. D. Tsaregorodtsev, "On the generation of $n$-quasigroups using proper families of functions", *Diskretnaya Matematika*, **35**:1 (2023), 35–53 (In Russian).