FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Martina Lehká

Nonassociativity in two operations

Department of Algebra

Supervisor of the bachelor thesis:	prof. RNDr. Aleš Drápal, CSc., DSc.
Study programme:	Mathematics
Study branch:	General Mathematics

Prague 2023

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In .... date ....

Author's signature

I wish to thank my supervisor prof. RNDr. Aleš Drápal, CSc., DSc. for introducing me to this topic, for the amount of time he devoted to me and for his guidance and patience throughout the whole process of writing this thesis.

Title: Nonassociativity in two operations

Author: Martina Lehká

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of Algebra

Abstract: This thesis follows up mainly on the research of Drápal and Valent, who in [1], [2] and [3] studied the nonassociativity of one quasigroup operation. Its central objective is to examine the number of triples $(x, y, z) \in Q^3$ such that $(x * y) \circ z = x * (y \circ z)$, where $(Q, *)$ and $(Q, \circ)$ are two quasigroups, $|Q| = n$. Let $a_2(C)$ be the number of such triples in a quasigroup couple C. Call it the associativity index. Denote by $a_2(n)$ the minimal $a_2(C)$, where C is a couple of order n. By averaging the associativity index over all the principal isotopes of a quasigroup couple, we prove that $a_2(n) \leq n^2(1 + 1/(n - 1))$, $n > 2$. We then characterize the couples C that, on average, attain $a_2(C) = n^2$ and we prove that this value is an improved upper bound on $a_2(n)$, $n > 2$. Furthermore, we begin research on couples of quasigroups isotopic to groups. Lastly, we present computational results with examples, including $a_2(4) = 8$ and $a_2(5) = 9$.

Keywords: associative triple, quasigroup, isotopy, associativity index

Contents

Introduction

Though they may seem different, quasigroups and latin squares are two sides of the same coin. Whereas the first notion refers to an algebraic structure resembling a group but lacking the neutral element and the associativity, the second has a more combinatorial nature. However, they interconnect tightly since bordering any latin square yields a multiplication table of a quasigroup and vice versa. In this thesis, we focus on quasigroups and their associativity, and the other viewpoint gives us a way to represent the structure on a computer.

If $(Q, \cdot)$ is a quasigroup, then we say that a triple $(a, b, c) \in Q^3$ is associative if it fulfils the condition $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. We call the total number of such triples the associativity index of Q and denote it by $a(Q)$. Also, let $a(n)$ be the minimal associativity index that a quasigroup of order n can attain. Quasigroups with small associative indices have been studied by Drápal and Valent in [1], [2], [3], by Drápal and Wanless in [4] and by many more, most of the relevant papers are listed in the references of the last article. These quasigroups are of interest, since they have potential applications in constructions of hash functions as explained in [6].

The first three chapters of this thesis modify approaches from previously mentioned [1] and from [12] to obtain similar results, but in a situation where we consider two quasigroup operations instead of one. In other words, we are interested in the number of triples $(a, b, c) \in Q^3$ such that $(a * b) \circ c = a * (b \circ c)$, where $*$ and $\circ$ are two quasigroup operations on a set Q. We fully analyze the average number of such triples and as a result we establish an upper bound on the number of these triples. The remaining two chapters report on our partial results. They were motivated by the questions of whether it is possible to find a couple of quasigroups with a relatively small number of triples fulfilling the condition above as isotopes of groups and what are the possible numbers of these triples for a couple of quasigroups of order n. Overall, the associativity of two quasigroup operations offers fascinating problems that, once solved, could potentially lead to applications in cryptography since some cryptographical systems based on quasigroups, take [5] for example, use multiple operations.

The outline of this thesis is as follows. Chapter 1 summarizes definitions and important facts about quasigroups and introduces a new algebraic structure called the quasigroup couple, which can also be interpreted as two quasigroups on the same set in a fixed order. The following two parts, Chapter 2 and Chapter 3, aim to find an upper bound on the associativity index of quasigroup couples of a given order. That is achieved firstly by finding the average value of the associativity index over all the principal isotopes of one of the quasigroups in the couple and secondly by averaging the index over all the principal isotopes of the quasigroup couple itself. Chapter 3 then generalizes the first result and contains a characterization of the situation in which the minimal average index is attained. Chapter 4 analyzes several special cases of quasigroup couples principally isotopic to group couples. We focus on finding the lower bound on the associativity index of these couples and on determining whether this minimal value is achievable. Computational results – all possible associativity indices of couples up to order 5 – are presented in Chapter 5.

1. Quasigroup couples

The main objective of this chapter is to state well-known facts about quasigroups. For further information on their properties, we recommend the first chapter of [10]. Also, we formally introduce a new algebraic structure, a quasigroup couple, that we can view as a pair of quasigroups on the same set in a fixed order.

1.1 General properties of quasigroups

Definition. A *quasigroup* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ defined on Q such that for every two elements $a, b \in Q$ each of the equations $a \cdot x = b$ and $y \cdot a = b$ has exactly one solution.
The *order* of $(Q, \cdot)$, denoted by $|Q|$, is the number of elements of Q. Throughout this thesis, unless written otherwise, we shall assume that $|Q| = n$, for $n \in \mathbb{N}$.

Definition. A *latin square* of order n is a square matrix consisting of n^2 entries using n different symbols, each of which does not repeat in any row and column.

Remark. The body of a multiplication table of any quasigroup is a latin square of the same order. Conversely, we can border any latin square (in many different ways) to get a multiplication table of a quasigroup.

Definition. Let $(Q, \cdot)$ be a quasigroup. For every $a \in Q$, define the *left and right translations* as follows

$$L_a(x) = a \cdot x \quad \text{and} \quad R_a(x) = x \cdot a, \text{ for all } x \in Q.$$

The inverse mappings are the *left and right divisions*, defined by

$$L_a^{-1}(x) = a \backslash x \quad \text{and} \quad R_a^{-1}(x) = x/a, \text{ for all } x \in Q.$$

Remark. By the definition

$$\begin{aligned} L_a L_a^{-1}(x) = x = L_a^{-1} L_a(x), \\ R_a R_a^{-1}(x) = x = R_a^{-1} R_a(x), \end{aligned}$$

from which we obtain the following identities describing the relationship between quasigroup multiplication and division

$$\begin{aligned} a \cdot (a \backslash x) = x = a \backslash (a \cdot x), \\ (x/a) \cdot a = x = (x \cdot a)/a. \end{aligned}$$

The following two definitions will give us ways of talking about relationships between quasigroups.

Definition. Let $(Q, *)$ and $(R, \circ)$ be two quasigroups. A triple (θ, ϕ, ψ) of bijections $\theta, \phi, \psi : Q \to R$ is called an *isotopy* of $(Q, *)$ upon $(R, \circ)$ if

$$\theta(x) \circ \phi(y) = \psi(x * y), \text{ for all } x, y \in Q.$$

Such quasigroups are then said to be *isotopic*.

Definition. Let $(Q, *)$ and $(R, \circ)$ be quasigroups. An isotopy (θ, ϕ, ψ) of $(Q, *)$ upon $(R, \circ)$ such that $\theta = \phi = \psi$ is called an *isomorphism.* An isomorphism of a quasigroup onto itself is called an *automorphism.*

It is worth remarking that there exist equivalent notions for latin squares. An isotopy of a latin square L permutes the rows of L, permutes the columns of L and permutes the symbols of L. Further details can be found in [10], chapter Elementary properties. We shall talk more about latin square isotopy and isomorphism in Chapter 5 of this thesis.

Now, let us define a special case of an isotopy: a principal isotopy.

Definition. Let $(Q, *)$ be a quasigroup. For each pair of permutations $\alpha, \beta \in S_Q$ define $(Q, *_{\alpha,\beta})$ by

$$x *_{\alpha,\beta} y = \alpha(x) * \beta(y), \text{ for all } x, y \in Q.$$

Such quasigroup is isotopic to $(Q, *)$ and we call it a *principal isotope* of $(Q, *)$.

A connection between isotopes and principal isotopes of a quasigroup is described in the next theorem. For the proof see the first chapter of [10].

Theorem 1.1. *Every isotope $(R, \circ)$ of a quasigroup $(Q, *)$ is isomorphic to a principal isotope of the quasigroup.*

The following lemma borrowed from [12] relates translations of a quasigroup to translations of its principal isotope.

Lemma 1.2. *Let $(Q, *)$ be a quasigroup, $(Q, *_{\alpha,\beta})$ its principal isotope and L_a, R_a and $L_a^{\alpha,\beta}, R_a^{\alpha,\beta}$ their translations. Then $L_a^{\alpha,\beta} = L_{\alpha(a)}\beta$ and $R_a^{\alpha,\beta} = R_{\beta(a)}\alpha$, for all $a \in Q$.*

Proof. Let $x \in Q$, then $L_a^{\alpha,\beta}(x) = a *_{\alpha,\beta} x = \alpha(a) * \beta(x) = L_{\alpha(a)}(\beta(x))$. Analogously for every $x \in Q$: $R_a^{\alpha,\beta}(x) = x *_{\alpha,\beta} a = \alpha(x) * \beta(a) = R_{\beta(a)}(\alpha(x))$. □

1.2 Associativity of quasigroup couples

Definition. We define a *quasigroup couple* $C = (Q, *, \circ)$ as a set Q with two binary operations $*$ and $\circ$ on Q such that $(Q, *)$ and $(Q, \circ)$ are quasigroups. The order of C, denoted by $|C|$, is the order of the quasigroups of C.

Definition. Let $C = (Q, *, \circ)$ be a quasigroup couple. We say that a triple $(a, b, c) \in Q^3$ is *associative in C* (shortly, *associative*) if

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

We will call the total number of such triples in C *the associativity index of* C and denote it by $a_2(C)$. We also put

$$a_2(n) = \min\{a_2(C) \mid C \text{ is a quasigroup couple of order } n\}.$$

For a set X and a permutation $\varphi \in S_X$, we shall denote the set of fixed points of φ by $\mathrm{Fix}(\varphi) = \{x \in X \mid \varphi(x) = x\}$. Following a convention of group theory, $[\varphi, \psi] = \varphi^{-1}\psi^{-1}\varphi\,\psi$ will denote the commutator of permutations φ and ψ. Then the associativity index of a quasigroup couple can be expressed in the following way:

Lemma 1.3. *Suppose that $C = (Q, *, \circ)$ is a quasigroup couple. For all $a \in Q$, let L_a, R_a and λ_a, ρ_a be the left and right translations of the quasigroups $(Q, *)$ and $(Q, \circ)$. Then*

$$a_2(C) = \sum_{a,c \in Q} |\mathrm{Fix}([L_a, \rho_c])|.$$

Proof. $[L_a, \rho_c](b) = b \Leftrightarrow L_a^{-1}(\rho_c^{-1}(L_a(\rho_c(b)))) = b \Leftrightarrow L_a(\rho_c(b)) = \rho_c(L_a(b)) \Leftrightarrow a * (b \circ c) = (a * b) \circ c$. □

A lower bound on $a_2(n)$ can be found analogously as in the case of one quasigroup described, for example, in [1]. Before we proceed to determine it, let us introduce one more notion. If $(Q, *)$ is a quasigroup, then for every element $a \in Q$ there exist $e_*^a, f_*^a \in Q$ such that $e_*^a * a = a$ and $a * f_*^a = a$. We call them the *left and right local units of* a in $(Q, *)$. We shall talk more about local units and their connection to associative triples in Chapter 4.

Now, let $C = (Q, *, \circ)$ be a quasigroup couple of order n. Since for all $a \in Q$ we have $(e_*^a * a) \circ f_\circ^a = a \circ f_\circ^a = a = e_*^a * a = e_*^a * (a \circ f_\circ^a)$, the triple $(e_*^a, a, f_\circ^a)$ is always associative. Hence, $a_2(n) \geq n$, for all $n \in \mathbb{N}$.

As for an upper bound on $a_2(n)$, it follows from the case of one quasigroup that it, with finitely many exceptions, equals n whenever n is not of the form $n = 2p_1$ or $n = 2p_1p_2$ for primes p_1, p_2 with $p_1 \leq p_2 < 2p_1$ as proven in [4]. As a result of the following two chapters, we shall get general estimates on the index.

2. Average index over all principal isotopes

This chapter aims to find the average number of associative triples of a quasigroup couple over all its principal isotopes. First, we will prove some general observations about the newly defined structure.

2.1 Principal isotope of a quasigroup couple

Definition. We say, that a quasigroup couple C is the *principal isotope* of a quasigroup couple $(Q, *, \circ)$, if there exist permutations $\alpha, \beta, \gamma, \delta \in S_Q$, such that $C = (Q, *_{\alpha,\beta}, \circ_{\gamma,\delta})$.

Lemma 2.1. *Let α, β, γ and δ be permutations of Q and let $(Q, *, \circ)$ be a quasigroup couple. Denote by L_a, R_a and λ_a, ρ_a the left and right translations of $(Q, *)$ and $(Q, \circ)$. Then*

$$a_2((Q, *_{\alpha,\beta}, \circ_{\gamma,\delta})) = \sum_{x,y \in Q} |\mathrm{Fix}([L_x\beta, \rho_y\gamma])|.$$

Proof. Let $L_a^{\alpha,\beta}, R_a^{\alpha,\beta}$ and $\lambda_a^{\gamma,\delta}, \rho_a^{\gamma,\delta}$ be the translations of $(Q, *_{\alpha,\beta})$ and $(Q, \circ_{\gamma,\delta})$, respectively. Then by Lemma 1.2,

$$L_a^{\alpha,\beta} = L_{\alpha(a)}\beta \text{ and } \rho_a^{\gamma,\delta} = \rho_{\delta(a)}\gamma, \text{ for all } a \in Q.$$

Also, since $\alpha, \delta \in S_Q$, we get

$$\{(L_{\alpha(a)}\beta, \rho_{\delta(c)}\gamma) \,|\, a, c \in Q\} = \{(L_x\beta, \rho_y\gamma) \,|\, x, y \in Q\}, \text{ for all } \beta, \gamma \in S_Q.$$

Therefore, by Lemma 1.3 and by the previous steps,

$$\begin{aligned} a_2((Q, *_{\alpha,\beta}, \circ_{\gamma,\delta})) &= \sum_{a,c \in Q} |\mathrm{Fix}([L_a^{\alpha,\beta}, \rho_c^{\gamma,\delta}])| \\ &= \sum_{a,c \in Q} |\mathrm{Fix}([L_{\alpha(a)}\beta, \rho_{\delta(c)}\gamma])| \\ &= \sum_{x,y \in Q} |\mathrm{Fix}([L_x\beta, \rho_y\gamma])|. \end{aligned}$$

□

Corollary 2.2. *Let $(Q, *, \circ)$ be a quasigroup couple and let α, β, γ and δ be permutations of Q. Then for all $\sigma, \tau \in S_Q$ the following equality holds:*

$$a_2((Q, *_{\alpha,\beta}, \circ_{\gamma,\delta})) = a_2((Q, *_{\sigma,\beta}, \circ_{\gamma,\tau})).$$

Proof. By the previous lemma, the associativity index is not dependent on the permutations α and δ. They only permute the summands and therefore do not affect the final sum. □

2.2 Average associativity index

In the following lemmas, we will prove two identities from [1] and then use them to find the desired average index. We shall need a well-known theorem, here in a formulation from [9]:

Theorem 2.3 (Burnside's lemma)**.** *Let G be a finite group acting on a set X and let k denote the number of orbits of X. Then*

$$k = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|.$$

Lemma 2.4. *Let $f = |\mathrm{Fix}(\alpha)|$ for a permutation $\alpha \in S_n$. Then*

$$\sum_{\varphi\in S_n}|\mathrm{Fix}([\alpha,\varphi])| = n(n-2)!(f^2-2f+n).$$

Proof. Put $F = \mathrm{Fix}(\alpha)$ and $M = \{1, 2, ..., n\}$. The goal is to count the number of pairs (i, φ), where $i \in M$ and $\varphi \in S_n$, such that $\alpha\varphi(i) = \varphi\alpha(i)$.
First, let us prove the following observation: if (i, φ) is a pair fulfilling $\alpha\varphi(i) = \varphi\alpha(i)$, then

$$i \in F \Leftrightarrow \varphi(i) \in F.$$

Let $i \in F$, that is $\alpha(i) = i$. This condition yields the following equivalence

$$\alpha\varphi(i) = \varphi\alpha(i) \quad\Leftrightarrow\quad \alpha\varphi(i) = \varphi(i),$$

where the right side implies that $\varphi(i) \in F$. Therefore, $i \in F \Rightarrow \varphi(i) \in F$.
For the other implication, let $\varphi(i) \in F$, equivalently $\alpha(\varphi(i)) = \varphi(i)$. Then

$$\alpha\varphi(i) = \varphi\alpha(i) \quad\Leftrightarrow\quad \varphi(i) = \varphi\alpha(i) \quad\Leftrightarrow\quad i = \alpha(i),$$

and so by the last equation $i \in F$. Hence, $\varphi(i) \in F \Rightarrow i \in F$. This concludes the observation.

Therefore, the problem of counting pairs can be divided into two cases depending on whether the given permutation α preserves the elements i and $j = \varphi(i)$:

(a) Consider a pair of elements $(i, j) \in F^2$. There are exactly f^2 such pairs, since $|F| = f$.
For each selected pair, we want to count all $\varphi \in S_n$ such that $\varphi(i) = j$, because then from $\alpha(i) = i$ and $\alpha(j) = j$ follows that $\varphi(\alpha(i)) = \alpha(j)$, thus, $\varphi\alpha(i) = \alpha\varphi(i)$ as needed.
Clearly, there are $(n-1)!$ permutations $\varphi \in S_n$ such that $\varphi(i) = j$. Hence, in this case, there exist $f^2(n-1)!$ possible pairs (i, φ).

(b) Now, similarily as above, let us consider a pair (i, j) such that $i, j \in M\backslash F$. There are $(n-f)^2$ such pairs.
Next, we need to count all $\varphi \in S_n$ such that $\varphi(i) = j$ and also $\varphi\alpha(i) = \alpha(j)$. Clearly, substituting for j in the second equality yields the desired condition. The two requirements on φ give us $(n-2)!$ possibilities for choosing the permutation. Therefore, the second case leaves us with $(n-f)^2(n-2)!$ more pairs (i, φ).

$$\begin{tikzcd} i \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & i \arrow[d, "\varphi"] \\ j \arrow[r, "\alpha"] & j = \varphi(i) \end{tikzcd}$$

(a) First case

$$\begin{tikzcd} i \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & \alpha(i) \neq i \arrow[d, "\varphi"] \\ j \arrow[r, "\alpha"] & \alpha(j) = \varphi(\alpha(i)) \end{tikzcd}$$

(b) Second case

Figure 2.1: Commutative diagrams illustrating the proof of Lemma 2.4

Thus, in total, there are $f^2(n-1)! + (n-f)^2(n-2)! = (n-2)!(f^2n - f^2 + n^2 - 2fn + f^2) = (n-2)!n(f^2 + n - 2f)$ pairs (i, φ) fulfilling our condition. □

Remark. Lemma 2.4 with switched positions of α and φ in the commutator also holds since $[\varphi, \alpha] = \varphi^{-1}\alpha^{-1}\varphi\alpha = (\alpha^{-1}\varphi^{-1}\alpha\varphi)^{-1} = ([\alpha, \varphi])^{-1}$ and $|\mathrm{Fix}(\psi)| = |\mathrm{Fix}(\psi^{-1})|$ for all $\psi \in S_n$.

Lemma 2.5. *The following equation holds:*

$$\sum_{\varphi, \psi \in S_n} |\mathrm{Fix}([\varphi, \psi])| = n^3(n-1)!(n-2)!.$$

Proof.

$$\begin{aligned} \sum_{\varphi, \psi \in S_n} |\mathrm{Fix}([\varphi, \psi])| &= \sum_{\varphi \in S_n} \sum_{\psi \in S_n} |\mathrm{Fix}([\varphi, \psi])| \\ &= \sum_{\varphi \in S_n} n(n-2)!(|\mathrm{Fix}(\varphi)|^2 - 2|\mathrm{Fix}(\varphi)| + n) \\ &= n(n-2)! \left(\sum_{\varphi \in S_n} |\mathrm{Fix}(\varphi)|^2 - 2 \sum_{\varphi \in S_n} |\mathrm{Fix}(\varphi)| + nn! \right), \end{aligned}$$

where the second equality follows from Lemma 2.4.
Next, consider an action of the group S_n on a set $M = \{1, 2, ..., n\}$; the symmetric group acts on the set by permuting its elements. Clearly, an element of M can be mapped by a permutation to any of the elements of M. Thus, the orbit of any x is $[x] = \{\pi(x) \mid \pi \in S_n\} = M$ or, in other words, all elements belong to the same orbit. Therefore this action has a single orbit.
Now, by Burnside's lemma 2.3 and by the fact that $|S_n| = n!$, we get

$$\sum_{\varphi \in S_n} |\mathrm{Fix}(\varphi)| = n!.$$

Analogously, consider an action of S_n on a set M^2. In this case, the group acts on the set by permuting its elements coordinatewise, that is $\pi((x, y)) = (\pi(x), \pi(y))$ for $(x, y) \in M^2$ and $\pi \in S_n$. Clearly, all elements $(x, x) \in M^2$ form an orbit $[(x, x)] = \{\pi((x, x)) \mid \pi \in S_n\}$. Also, since any pair $(a, b) \in M^2$, $a \neq b$, can be mapped to any pair $(c, d) \in M^2$, $c \neq d$, by any permutation mapping a to c and b to d, all the remaining elements belong to $[(x, y)] = \{\pi((x, y)) \mid x \neq y, \pi \in S_n\}$. Therefore this action has two orbits.
Thus, Burnside's lemma 2.3 gives

$$\sum_{\varphi \in S_n} |\mathrm{Fix}_{M^2}(\varphi)| = 2n!,$$

where $\mathrm{Fix}_{M^2}(\varphi) = \{(x,y) \in M^2 \mid \varphi((x,y)) = (\varphi(x),\varphi(y)) = (x,y)\}$. For each $\varphi \in S_n$, the set of points $\mathrm{Fix}_{M^2}(\varphi) \subseteq M^2$ fixed by the action of S_n on M^2 consists of all possible couples of elements from the set of points $\mathrm{Fix}(\varphi) \subseteq M$ fixed by the action of S_n on M, since $\mathrm{Fix}(\varphi) = \{x \in M \mid \varphi(x) = x\}$. Hence, we get that $|\mathrm{Fix}_{M^2}(\varphi)| = |\mathrm{Fix}(\varphi)|^2$, for all $\varphi \in S_n$, and so

$$\sum_{\varphi \in S_n} |\mathrm{Fix}(\varphi)|^2 = 2n!.$$

Therefore,

$$\begin{aligned}\sum_{\varphi,\psi \in S_n} |\mathrm{Fix}([\varphi,\psi])| &= n(n-2)!\,(2n! - 2n! + nn!)\\ &= n^3(n-1)!(n-2)!.\end{aligned}$$

□

After preparing the auxiliary lemmas, we can start calculating the average index. Firstly, consider a situation when one of the operations is fixed and the other quasigroup of the couple runs through all its principal isotopes.

Proposition 2.6. *Suppose that $(Q,*,\circ)$ is a quasigroup couple, $|Q| = n$, and L_a, R_a and λ_a, ρ_a are the left and right translations of $(Q,*)$ and $(Q,\circ)$. Then*

$$\begin{aligned}\frac{1}{(n!)^2}\sum_{\alpha,\beta \in S_Q} a_2((Q,*_{\alpha,\beta},\circ)) &= \frac{1}{n!}\sum_{\beta \in S_Q} a_2((Q,*_{\mathrm{id},\beta},\circ))\\ &= \frac{n}{n-1}\left(\sum_{y \in Q}|\mathrm{Fix}(\rho_y)|^2 - 2n + n^2\right).\end{aligned}$$

Proof. By using an equivalent notation $(Q,*_{\alpha,\beta},\circ) = (Q,*_{\alpha,\beta},\circ_{\mathrm{id},\mathrm{id}})$, we get that

$$\begin{aligned}\frac{1}{(n!)^2}\sum_{\alpha,\beta \in S_Q} a_2((Q,*_{\alpha,\beta},\circ_{\mathrm{id},\mathrm{id}})) &= \frac{1}{n!}\sum_{\beta \in S_Q} a_2((Q,*_{\mathrm{id},\beta},\circ_{\mathrm{id},\mathrm{id}}))\\ &= \frac{1}{n!}\sum_{\beta \in S_Q}\sum_{x,y \in Q}|\mathrm{Fix}([L_x\beta,\rho_y])|\\ &= \frac{1}{n!}\sum_{y \in Q}\sum_{\beta \in S_Q}\sum_{x \in Q}|\mathrm{Fix}([L_x\beta,\rho_y])|,\end{aligned}$$

where the first equality follows from Corollary 2.2, the second from Lemma 2.1 and the last one holds due to the finiteness of the sums. Since for each $\psi \in S_Q$ and each $x \in Q$ the equation $L_x\beta = \psi$ has a unique solution $\beta \in S_Q$, the commutator $[\psi,\rho_y]$ can be written in exactly n ways as $[L_x\beta,\rho_y]$. Therefore,

$$\frac{1}{(n!)^2}\sum_{\alpha,\beta \in S_Q} a_2((Q,*_{\alpha,\beta},\circ_{\mathrm{id},\mathrm{id}})) = \frac{1}{n!}\sum_{y \in Q}\sum_{\psi \in S_Q} n|\mathrm{Fix}([\psi,\rho_y])|.$$

Next, put $f_y = |\mathrm{Fix}(\rho_y)|$. Since $\rho_y \in S_Q$ for all $y \in Q$, the remark after Lemma 2.4 yields:

$$\begin{aligned}\frac{1}{(n!)^2}\sum_{\alpha,\beta \in S_Q} a_2((Q,*_{\alpha,\beta},\circ_{\mathrm{id},\mathrm{id}})) &= \frac{n}{n!}\sum_{y \in Q}(n(n-2)!(f_y^2 - 2f_y + n))\\ &= \frac{n}{n-1}\left(\sum_{y \in Q} f_y^2 - 2\cdot\sum_{y \in Q} f_y + n^2\right).\end{aligned}$$

Recall that $\mathrm{Fix}(\rho_y) = \{x \in Q \,|\, x \circ y = x\}$, for each $y \in Q$. By the definition of a quasigroup, for all $x \in Q$ the equation $x \circ y = x$ has a single solution $y \in Q$. Hence, $\sum_{y \in Q} |\mathrm{Fix}(\rho_y)| = n$.
Finally,

$$\frac{1}{(n!)^2} \sum_{\alpha,\beta \in S_Q} a_2((Q, *_{\alpha,\beta}, \circ_{\mathrm{id},\mathrm{id}})) = \frac{n}{n-1} \left(\sum_{y \in Q} f_y^2 - 2n + n^2 \right).$$

□

Remark. By the previous proposition and by the triangle inequality

$$n = \sum_{y \in Q} |\mathrm{Fix}(\rho_y)| \leq \sum_{y \in Q} |\mathrm{Fix}(\rho_y)|^2 \leq \left(\sum_{y \in Q} |\mathrm{Fix}(\rho_y)| \right)^2 = n^2,$$

for all $n \in \mathbb{N}$. Thus, we get the following estimates on the average

$$n^2 \leq \frac{1}{(n!)^2} \sum_{\alpha,\beta \in S_Q} a_2((Q, *_{\alpha,\beta}, \circ)) \leq 2n^2.$$

We will discuss the case where the average attains the minimum in the following chapter. As for the maximum, if a quasigroup $(Q, \circ)$ has an identity element $e \in Q$, then $|\mathrm{Fix}(\rho_e)| = n$ and $|\mathrm{Fix}(\rho_x)| = 0$ for all $e \neq x \in Q$. Thus, such a quasigroup attains the maximal average. Quasigroups with an identity element are called *loops*, and in contrast to groups, loops need not be associative.

Next, we focus on a case where the average is taken over all the principal isotopes of a quasigroup couple.

Proposition 2.7. *Let $(Q, *, \circ)$ be a quasigroup couple of order n with translations defined as in Proposition 2.6. Then*

$$\begin{aligned} \frac{1}{(n!)^4} \sum_{\alpha,\beta,\gamma,\delta \in S_Q} a_2((Q, *_{\alpha,\beta}, \circ_{\gamma,\delta})) &= \frac{1}{(n!)^2} \sum_{\beta,\gamma \in S_Q} a_2((Q, *_{\mathrm{id},\beta}, \circ_{\gamma,\mathrm{id}})) \\ &= \frac{n^3}{n-1} = n^2 \left(1 + \frac{1}{n-1}\right). \end{aligned}$$

Proof. The first equality follows directly from Corollary 2.2. By Lemma 2.1 then

$$\frac{1}{(n!)^2} \sum_{\beta,\gamma \in S_Q} a_2((Q, *_{\mathrm{id},\beta}, \circ_{\gamma,\mathrm{id}})) = \frac{1}{(n!)^2} \sum_{\beta,\gamma \in S_Q} \sum_{x,y \in Q} |\mathrm{Fix}([L_x\beta, \rho_y\gamma])|.$$

For each $\varphi \in S_Q$ and for each $x \in Q$ the equation $L_x\beta = \varphi$ has exactly one solution $\beta \in S_Q$. Similarly for $\psi \in S_Q$. Therefore, for each $[\varphi, \psi]$ there are exactly n^2 ways of expressing it in the form of $[L_x\beta, \rho_y\gamma]$.
Hence,

$$\begin{aligned} \frac{1}{(n!)^2} \sum_{\beta,\gamma \in S_Q} a_2((Q, *_{\mathrm{id},\beta}, \circ_{\gamma,\mathrm{id}})) &= \frac{1}{(n!)^2} \sum_{\varphi,\psi \in S_Q} n^2 |\mathrm{Fix}([\varphi, \psi])| \\ &= \frac{n^2}{(n!)^2} n^3 (n-1)!(n-2)! \\ &= \frac{n^3}{n-1}, \end{aligned}$$

where the second equality follows from Lemma 2.5. □

Similarly, as [1] and [12] have found the average number of associative triples of a single quasigroup over all its principal isotopes, we have obtained analogous results for a quasigroup couple. As the earlier mentioned papers have noted, the average associativity index of one quasigroup over all its principal isotopes does not depend on the structure of the quasigroup but solely on its order. We now know that the same applies when considering two operations.

Proposition 2.7 also gives us an upper bound on $a_2(n)$, which is, for $n > 2$, equal to $n^2\left(1 + 1/(n-1)\right)$. However, we will improve this estimate in the next chapter.

3. Nonassociativity and orthomorphisms

In this chapter, we shall first introduce the notion of an orthomorphism, then use it to generalize the situation from Proposition 2.6 and characterize the quasigroup couples for which the average associativity index taken over the principal isotopes of one of the quasigroups in the couple attains its minimum.

Definition. Let $(Q, \cdot)$ be a quasigroup. A permutation φ of Q is a *(left) complete mapping* if the mapping $x \mapsto \vartheta(x)$ defined by $\vartheta(x) = x \cdot \varphi(x)$ is again a permutation of Q. The associated mapping ϑ is called a *(left) orthomorphism*.

Remark. By the definition, $\vartheta(x) = x \cdot \varphi(x)$, thus, also $\varphi(x) = x \backslash \vartheta(x)$. Clearly, there is a one-to-one correspondence between complete mappings and orthomorphisms of a quasigroup.

Throughout this thesis, only the left versions of the definitions above shall be considered. However, similarily, we could define the right orthomorphism by $\vartheta(x) = \varphi(x) \cdot x$, with the right complete mapping fulfilling $\varphi(x) = \vartheta(x)/x$, and work with those instead.

We shall follow an approach similar to the one used in [12]. We will first prove a combinatorial lemma from [12], that shall later be useful in our estimations.

Lemma 3.1. *For a permutation $\alpha \in S_n$ put $f = |\mathrm{Fix}(\alpha)|$. Then*

$$\sum_{\varphi \in S_n} |\mathrm{Fix}([\alpha, \varphi])| = n! \iff f = 1.$$

Proof. By Lemma 2.4

$$\sum_{\varphi \in S_n} |\mathrm{Fix}([\alpha, \varphi])| = n(n-2)!(f^2 - 2f + n),$$

therefore the reverse implication holds.
To prove the forward direction of the equivalence, consider a function $h(x) = n(n-2)!(x^2 - 2x + n)$, $n \geq 2$, $x \in \mathbb{R}$, and its derivatives $h'(x) = n(n-2)!(2x-2)$ and $h''(x) = 2n(n-2)!$, $n \geq 2$, $x \in \mathbb{R}$. Clearly, $h'(x) = 0$ if and only if $x = 1$. Also, $h''(x) > 0$ in $\mathbb{R}$. Thus, the function h is convex and has its global minimum at $x = 1$ with a value $h(1) = n!$. Therefore, by Lemma 2.4 and by the observations above, the statement is true. □

Lemma 3.2. *Let $(Q, *, \circ)$ be a quasigroup couple of order n with the translations defined as in Proposition 2.6 and let $\gamma \in S_Q$. For every $y \in Q$ put $f_y = |\mathrm{Fix}(\rho_y \gamma)|$. Then*

$$\frac{1}{(n!)^2} \sum_{\alpha,\beta,\delta \in S_Q} a_2((Q, *_{\alpha,\beta}, \circ_{\gamma,\delta})) = \sum_{\beta \in S_Q} a_2((Q, *_{\mathrm{id},\beta}, \circ_{\gamma,\mathrm{id}}))$$

$$= n^2(n-2)! \left(n^2 + \sum_{y \in Q} (f_y^2 - 2f_y) \right) \geq n^2 n!.$$

Proof.

$$\begin{aligned}\frac{1}{(n!)^2}\sum_{\alpha,\beta,\delta\,\in S_Q} a_2((Q,*_{\alpha,\beta},\circ_{\gamma,\delta})) &= \sum_{\beta\,\in S_Q} a_2((Q,*_{\mathrm{id},\beta},\circ_{\gamma,\mathrm{id}}))\\ &= \sum_{\beta\in S_Q}\sum_{x,y\,\in Q} |\mathrm{Fix}([L_x\beta,\rho_y\gamma])|,\end{aligned}$$

as follows from the Corollary 2.2 and Lemma 2.1. Since for each $\varphi\in S_Q$ and each $x\in Q$ the equation $\varphi = L_x\beta$ holds for exactly one $\beta\in S_Q$, the commutator $[\varphi,\rho_y\gamma]$ can be expressed in n ways in the form of $[L_x\beta,\rho_y\gamma]$. Hence,

$$\begin{aligned}\frac{1}{(n!)^2}\sum_{\alpha,\beta,\delta\,\in S_Q} a_2((Q,*_{\alpha,\beta},\circ_{\gamma,\delta})) &= \sum_{\varphi\in S_Q}\sum_{y\,\in Q} n|\mathrm{Fix}([\varphi,\rho_y\gamma])|\\ &= n\cdot\sum_{y\,\in Q}\sum_{\varphi\in S_Q}|\mathrm{Fix}([\varphi,\rho_y\gamma])|.\end{aligned}$$

Now, Lemma 2.4 applied for $\alpha=\rho_y\gamma$ yields:

$$\begin{aligned}\frac{1}{(n!)^2}\sum_{\alpha,\beta,\delta\,\in S_Q} a_2((Q,*_{\alpha,\beta},\circ_{\gamma,\delta})) &= n\cdot\sum_{y\,\in Q}\Big(n(n-2)!(f_y^2-2f_y+n)\Big)\\ &= n^2(n-2)!\left(n^2+\sum_{y\,\in Q}(f_y^2-2f_y)\right)\geq n^2n!,\end{aligned}$$

where the final inequality follows from the fact that $f_y^2-2f_y\geq -1$ for all $y\in Q$ and $n^2+\sum_{y\,\in Q}(f_y^2-2f_y)\geq n^2-n=n(n-1)$. □

Lemma 3.3. *Let* $(Q,*,\circ)$ *be defined as in the previous lemma and let* $\gamma\in S_Q$ *be a permutation. For every* $y\in Q$ *put* $f_y=|\mathrm{Fix}(\rho_y\gamma)|$*. Then*

$$\frac{1}{(n!)^2}\sum_{\alpha,\beta,\delta\,\in S_Q} a_2((Q,*_{\alpha,\beta},\circ_{\gamma,\delta})) = n^2n! \iff f_y=1 \textit{ for every } y\in Q.$$

Proof. From the proof of Lemma 3.2 follows that

$$\frac{1}{(n!)^2}\sum_{\alpha,\beta,\delta\,\in S_Q} a_2((Q,*_{\alpha,\beta},\circ_{\gamma,\delta})) = n\cdot\sum_{y\,\in Q}\sum_{\varphi\in S_Q}|\mathrm{Fix}([\varphi,\rho_y\gamma])|,$$

and by Lemma 3.1, for each $y\in Q$,

$$\sum_{\varphi\in S_Q}|\mathrm{Fix}([\alpha,\rho_y\gamma])| = n! \iff f_y=1.$$

Therefore,

$$\frac{1}{(n!)^2}\sum_{\alpha,\beta,\delta\,\in S_Q} a_2((Q,*_{\alpha,\beta},\circ_{\gamma,\delta})) = n\cdot\sum_{y\,\in Q} n! = n^2n! \iff f_y=1 \text{ for every } y\in Q.$$

□

For the proof of the following equivalence see Lemma 4.7 of [12].

Lemma 3.4. *Suppose that $(Q, \circ)$ is a quasigroup of order n with the translations λ_a, ρ_a, for all $a \in Q$, and $\gamma \in S_Q$. Then $|\mathrm{Fix}(\rho_y \gamma)| = 1$ for every $y \in Q$ if and only if γ^{-1} is an orthomorphism.*

Proposition 3.5. *Let $(Q, *, \circ)$ be a quasigroup couple of order n and let $\gamma \in S_Q$. Then*

$$\frac{1}{(n!)^3} \sum_{\alpha,\beta,\delta \in S_Q} a_2((Q, *_{\alpha,\beta}, \circ_{\gamma,\delta})) = \frac{1}{n!} \sum_{\beta \in S_Q} a_2((Q, *_{\mathrm{id},\beta}, \circ_{\gamma,\mathrm{id}})) \geq n^2$$

and the equality holds if and only if γ^{-1} is an orthomorphism in $(Q, \circ)$.

Proof. The first statement was already proven in Lemma 3.2. The equivalence follows directly from Lemma 3.3 and Lemma 3.4. □

We say that a quasigroup $(Q, *)$ is *idempotent* if for all its elements $a \in Q$: $a * a = a$. By [10] (Theorem 1.5.6), there exists an idempotent quasigroup of order n iff $n \neq 2$. Furthermore, it is easy to see that for every idempotent quasigroup, identity mapping is an orthomorphism. Therefore, Proposition 3.5 gives us an improved upper bound on $a_2(n)$, that is $a_2(n) \leq n^2$ for $n > 2$.

4. Quasigroups isotopic to groups

Since the impracticality of computer representation of quasigroups as multiplication tables is increasing with their growing order, it is desirable to research quasigroups principally isotopic to groups. Due to the potential cryptographical applications, the couples of low associativity indices are of particular interest.

4.1 Groups and associativity

For starting, we shall make several observations about a couple of groups. Denote by 1_* the identity of the group $(G,*)$ and by x_*^{-1} the inverse of x in the group $(G,*)$.

Lemma 4.1. *Let $(G,*)$ be a group and let $u \in G$ be any element in G. Then the operation defined by $x \circ y = x * u_*^{-1} * y$ for all $x, y \in G$ is a group operation on G and the groups are isomorphic.*

Proof. Firstly, verify that $(G,\circ)$ is a group. It is associative, since

$$(x \circ y) \circ z = (x * u_*^{-1} * y) * u_*^{-1} * z = x * u_*^{-1} *(y * u_*^{-1} * z) = x \circ(y \circ z).$$

Also, since

$$x \circ u = x * u_*^{-1} * u = x * 1_* = x \quad \text{and} \quad u \circ x = u * u_*^{-1} * x = 1_* * x = x,$$

the neutral element in $(G,\circ)$ is $1_\circ = u$. Lastly, the inverse of x in $(G,\circ)$ has the form of $x_\circ^{-1} = u * x_*^{-1} * u$, because

$$x \circ x_\circ^{-1} = x * u_*^{-1} * u * x_*^{-1} * u = x * 1_* * x_*^{-1} * u = x * x_*^{-1} * u = 1_* * u = u$$

and similarly

$$x_\circ^{-1} \circ x = u * x_*^{-1} * u * u_*^{-1} * x = u.$$

Thus $(G,\circ)$ is a group. Next, consider a bijection:

$$\begin{aligned} L_{u_*^{-1}} :\ & G \to G \\ & x \mapsto u_*^{-1} * x. \end{aligned}$$

Since for all $x, y \in G$:

$$\begin{aligned} L_{u_*^{-1}}^{-1}(L_{u_*^{-1}}(x) * L_{u_*^{-1}}(y)) &= L_u(L_{u_*^{-1}}(x) * L_{u_*^{-1}}(y)) = u *((u_*^{-1} * x) *(u_*^{-1} * y)) \\ &= (u * u_*^{-1}) * x * u_*^{-1} * y = x * u_*^{-1} * y = x \circ y, \end{aligned}$$

it is an isomorphism from $(G,\circ)$ to $(G,*)$. □

Lemma 4.2. *Let $(G,*)$ and $(G,\circ)$ be two groups. Then $(x * y) \circ z = x *(y \circ z)$, for all $x, y, z \in G$, if and only if there exists $u \in G$ such that $x \circ y = x * u_*^{-1} * y$, for all $x, y \in G$.*

Proof. We start with the forward implication. Since the equation $(x * y) \circ z = x * (y \circ z)$ holds for all $x, y, z \in G$, put $y = 1_\circ$. Then:

$$\begin{aligned}(x * 1_\circ) \circ z &= x * (1_\circ \circ z)\\ (x * 1_\circ) \circ z &= x * z\end{aligned}$$

We are only interested in the number of solutions of this equation and a right translation is a permutation. Hence, we can put $x = x * (1_\circ)_*^{-1}$. Then:

$$x \circ z = (x * (1_\circ)_*^{-1}) * z.$$

Thus, for all $x, y \in G : x \circ y = x * u_*^{-1} * y$, where $u = 1_\circ$.
The reverse direction follows directly from:

$$(x * y) \circ z = (x * y) * u_*^{-1} * z = x * (y * u_*^{-1} * z) = x * (y \circ z).$$

□

Corollary 4.3. *Let $(G, *)$ and $(G, \circ)$ be two groups. If for all $x, y, z \in G$: $(x * y) \circ z = x * (y \circ z)$, then the groups are isomorphic.*

As will soon become evident, the reverse implication of the corollary does not hold.

4.2 Lower bounds on associativity indices

In this section, we pose several questions concerning the associativity of couples of quasigroups isotopic to groups and provide partial solutions.

Problem 4.1. *What is the lower bound on the associativity index of a quasigroup couple $C = (Q, *, \circ)$ of order n such that $(Q, *)$ and $(Q, \circ)$ are groups?*

Lemma 4.4. *Let $C = (Q, *, \circ)$ be a quasigroup couple of order n such that $(Q, *)$ and $(Q, \circ)$ are groups. Then $a_2(C) \geq 2n^2 - n$.*

Proof. For a triple $(x, y, z) \in Q^3$:

$$(x * y) \circ z = x * y = x * (y \circ z) \tag{4.1}$$

iff $z = 1_\circ$, and so, to satisfy the condition on the right-hand side, we have n^2 choices for $(x, y) \in Q^2$. Also, for a triple $(x, y, z) \in Q^3$:

$$(x * y) \circ z = y \circ z = x * (y \circ z) \tag{4.2}$$

iff $x = 1_*$. The latter condition leaves us with n^2 options for $(y, z) \in Q^2$. However, we have counted the triples $(1_*, y, 1_\circ)$ twice for each $y \in Q$. Therefore, it is neccessary to subtract n triples. □

After determining the lower bound theoretically, we may inquire if the value agrees with the computed minima in small orders or if there is a scope for improvement. We first focus on a special case where the two groups are isomorphic. The computationally found minimal associativity indices are listed in Table 4.1. However, all these values are higher than the expected lower bound $2n^2 - n$.

n	$2n^2 - n$	$\min\{a_2((Q, *, \circ))\}$
3	15	27
4	28	36
5	45	61
6	66	84
7	91	115
8	120	146
9	153	201

Table 4.1: Computed minima of $a_2((Q, *, \circ))$, where $|Q| = n$ and $*, \circ$ are two isomorphic group operations

In a general situation with one quasigroup operation, if we have a quasigroup $(Q, \cdot)$, then for a triple $(x, y, z) \in Q^3$

$$(x \cdot y) \cdot z = x \cdot y = x \cdot (y \cdot z) \iff z = f_{\cdot}^{y} = f_{\cdot}^{(x \cdot y)},$$
$$(x \cdot y) \cdot z = y \cdot z = x \cdot (y \cdot z) \iff x = e_{\cdot}^{y} = e_{\cdot}^{(y \cdot z)},$$

and it can also fulfill

$$(x \cdot y) \cdot z = x \cdot z = x \cdot (y \cdot z) \iff f_{\cdot}^{x} = y = e_{\cdot}^{z},$$

where the conditions on the right-hand side use the local units defined at the end of Chapter 1. Further analysis of this case can be found in [2].

Thus, returning to our scenario with two groups, one might start wondering whether the minimal number of triples such that

$$(x * y) \circ z = x * z = x * (y \circ z) \text{ or} \tag{4.3}$$
$$(x * y) \circ z = x \circ z = x * (y \circ z) \tag{4.4}$$

can be described similarly.

However, that seems to be a rather complicated question. Our computations on the couples of isomorphic groups of orders 3 to 8 having the minimal indices from Table 4.1 suggest that these triples might always be present, and their number can vary within each order. The results are listed in Table 4.2. Note that each of the two last equations can be fulfilled by a different number of associative triples. Also, let us emphasize that these equations do not determine disjoint subsets of triples. We shall describe the intersections of these sets in a general scenario with two quasigroups in the following section.

Furthermore, by our computations on couples of isomorphic groups, it seems that there are always some associative triples that fulfill neither of the four equations mentioned above and their number is also not fixed. All the computed numbers can be found in Table 4.3. Therefore, it is possible that even if we managed to include the triples fulfilling the equations (4.3) and (4.4) in our lower bound from Lemma 4.4, there still might not exist couples with such minimal indices.

n	(4.1)	(4.2)	(4.3)	(4.4)
3	9	9	9	9
4	16	16	9	9
5	25	25	$\{12, 13\}$	$\{12, 13\}$
6	36	36	$\{13, 14, 15\}$	$\{13, 14, 15\}$
7	49	49	$\{16, 19\}$	$\{16, 19\}$
8	64	64	$\{17, 18, 19, 22\}$	$\{17, 18, 19, 22\}$

Table 4.2: Computed possible numbers of associative triples fulfilling given equations over couples of isomorphic groups attaining the minimal indices from Table 4.1

n	number of triples
3	$\{4, 8\}$
4	$\{4, 6\}$
5	$\{9, 10, 12, 13\}$
6	$\{10, 11, 12, 13, 14, 15, 16\}$
7	$\{15, 18, 21\}$
8	$\{12, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24\}$

Table 4.3: Computed possible numbers of associative triples that fulfill neither of (4.1), (4.2), (4.3) and (4.4) over couples of isomorphic groups attaining the minimal indices from Table 4.1

We can also generalize the situation by letting $C = (Q, *, \circ)$ be a quasigroup couple of two groups in general. We shall refer to it as a *group couple.* Our computations on orders $4, 6$ and 8 found that the minimal values of $a_2(C)$ correspond with the minima previously listed in Table 4.1. Thus, judging by results on the small orders, it seems that the minimal indices may not be attainable by any group couple unless the two groups are isomorphic.

Problem 4.2. *Consider a quasigroup couple $C = (Q, *, \circ_{\gamma,\delta})$ of order n such that $(Q, *)$ is a group and $(Q, \circ_{\gamma,\delta})$ is a principal isotope of a group $(Q, \circ)$. What can we say about the lower bound on $a_2(C)$ in this scenario?*

The lower bound on $a_2(C)$ for such couples is at least n^2, since the triple $(1_*, y, z) \in Q^3$ is associative for all $y, z \in Q$.

Let $C = (Q, \circ, \circ_{\gamma,\delta})$ be a quasigroup couple of order n such that $(Q, \circ)$ is a group and $(Q, \circ_{\gamma,\delta})$ is its principal isotope. Then, $a_2(C)$ can be obtained as the number of solutions of the equation:

$$\begin{gathered}(x \circ y) \circ_{\gamma,\delta} z = x \circ (y \circ_{\gamma,\delta} z)\\ \gamma(x \circ y) \circ \delta(z) = x \circ \gamma(y) \circ \delta(z)\\ \gamma(x \circ y) = x \circ \gamma(y).\end{gathered}$$

We can computationally verify that minimum $a_2(C) = n^2$ is attainable even for small orders. Several examples of all orders 3 to 8, except for order 6, were found and some are presented in Appendix, see A.1 and A.2.

It turns out that this case corresponds to the situation where we consider a single quasigroup $(Q, \circ_{\gamma,\mathrm{id}})$ isotopic to a group $(Q, \circ)$ of order n and count $a((Q, \circ_{\gamma,\mathrm{id}}))$ as the number of solutions of:

$$\begin{gathered}
(x \circ_{\gamma,\delta} y) \circ_{\gamma,\delta} z = x \circ_{\gamma,\delta}(y \circ_{\gamma,\delta} z) \\
\gamma(\gamma(x) \circ y) \circ z = \gamma(x) \circ(\gamma(y) \circ z) \\
\gamma(x \circ y) = x \circ \gamma(y).
\end{gathered}$$

By [1], $a((Q, \circ_{\gamma,\delta})) = n^2$ for a group $(Q, \circ)$ of order n iff γ is a left orthomorphism or δ is a right orthomorphism. Also, by [7], a complete mapping, and therefore an orthomorphism, of a finite group of even order exists only if its Sylow 2-subgroup is non-cyclic, and this condition is sufficient for solvable groups. Thus, we could not find an example of order 6.

If $C = (Q, *, \circ_{\gamma,\delta})$, $|Q| = n$, is a quasigroup couple defined as in Problem 4.2 then the associativity index of C can be calculated as the number of solutions of the equation:

$$\begin{gathered}
(x * y) \circ_{\gamma,\delta} z = x *(y \circ_{\gamma,\delta} z) \\
\gamma(x * y) \circ \delta(z) = x *(\gamma(y) \circ \delta(z)) \\
\gamma(x * y) \circ z = x *(\gamma(y) \circ z).
\end{gathered}$$

However, it still remains to discuss this situation in which the quasigroup couple consists of a group and a group isotope in general in more detail.

Problem 4.3. *Let $C = (Q, *_{\alpha,\beta}, \circ_{\gamma,\delta})$ be a quasigroup couple of order n such that both $(Q, *_{\alpha,\beta})$ and $(Q, \circ_{\gamma,\delta})$ are principal isotopes of groups. Can C attain the associativity index of n?*

In this scenario, the lower bound on the associativity index is at least n by the argument with local units mentioned at the end of Chapter 1.

First, let $C = (Q, *_{\alpha,\beta}, *_{\gamma,\delta})$ be a quasigroup couple, $|Q| = n$, such that both $(Q, *_{\alpha,\beta})$ and $(Q, *_{\gamma,\delta})$ are principal isotopes of a group $(Q, *)$. Then the number of associative triples is the number of solutions of the equation:

$$\begin{gathered}
(x *_{\alpha,\beta} y) *_{\gamma,\delta} z = x *_{\alpha,\beta} (y *_{\gamma,\delta} z) \\
\gamma(\alpha(x) * \beta(y)) * \delta(z) = \alpha(x) * \beta(\gamma(y) * \delta(z)) \\
\gamma(x * \beta(y)) * z = x * \beta(\gamma(y) * z).
\end{gathered}$$

However, this is an equivalent problem to the one with a single operation where we consider a quasigroup $(Q, *_{\gamma,\beta})$ isotopic to a group $(Q, *)$ and count how many associative triples it has. This case was already studied in [1] and it was proven that the lower bound n can never be attained. Therefore, neither two isotopes of the same group can achieve the associativity index n.

Next, consider a quasigroup couple $C = (Q, *_{\alpha,\beta}, \circ_{\gamma,\delta})$ of order n, where $(Q, *_{\alpha,\beta})$ and $(Q, \circ_{\gamma,\delta})$ are principal isotopes of groups $(Q, *)$ and $(Q, \circ)$, respectively. Then $a_2(C)$ can be found as the number of solutions of:

$$\begin{gathered}(x *_{\alpha,\beta} y) \circ_{\gamma,\delta} z = x *_{\alpha,\beta} (y \circ_{\gamma,\delta} z)\\ \gamma(\alpha(x) * \beta(y)) \circ \delta(z) = \alpha(x) * \beta(\gamma(y) \circ \delta(z))\\ \gamma(x * \beta(y)) \circ z = x * \beta(\gamma(y) \circ z).\end{gathered}$$

As for now, we can only say that based on our computations presented in Chapter 5, we have $a_2(C) > n$, for all $1 < n \leq 5$.

Further research is required on this topic, as we have not fully answered all the questions. Especially interesting might be the most general scenario introduced in Problem 4.3 since two group isotopes could possibly attain the maximal nonassociativity by having the associativity index of n, which is unachievable for one group isotope. However, for now, it remains an open question.

4.3 Intersections of associative triple types

In this section, we shall return to the equations (4.1) to (4.4) from the previous section and describe the intersections of the associative triple subsets they determine. We will work in two general quasigroups, but the propositions can also be easily applied to the group setting described in Problem 4.1.

Firstly, let us introduce some notation adapted from [2]. Let $(Q, *)$ be a quasigroup. We say that an element $a \in Q$ is *idempotent* if $a * a = a$. The *set of idempotent elements* of a quasigroup $(Q, *)$ shall be denoted by $I((Q, *))$.

Also, consider mappings $e_*, f_* : Q \to Q$ such that $e_*(x) = e_*^x$ and $f_*(x) = f_*^x$, for all $x \in Q$. To a given element $x \in Q$, these mappings assign the left and right local units in $(Q, *)$, respectively. Then for all $x, y \in Q$ we have

$$x \in e_*^{-1}(y) \iff y * x = x \quad \text{and} \quad x \in f_*^{-1}(y) \iff x * y = x. \tag{4.5}$$

Let $(Q, *, \circ)$ be a quasigroup couple. Put $L = (x * y) \circ z$ and $R = x * (y \circ z)$. Using (4.5), the equations (4.1) to (4.4) can be expressed in the following way:

$$\begin{aligned} L = x * y = R &\iff y, (x * y) \in f_\circ^{-1}(z), && (4.6)\\ L = y \circ z = R &\iff y, (y \circ z) \in e_*^{-1}(x), && (4.7)\\ L = x * z = R &\iff y = e_\circ(z) \wedge (x * y) \circ z = x * z, && (4.8)\\ L = x \circ z = R &\iff y = f_*(x) \wedge x * (y \circ z) = x \circ z. && (4.9)\end{aligned}$$

Now, we can describe the intersections.

Proposition 4.5. *Let $C = (Q, *, \circ)$ be a quasigroup couple and let $(x, y, z) \in Q^3$ be a triple in C. Then:*

(i) $L = x * y = y \circ z = R \iff y \in e_*^{-1}(x) \cap f_\circ^{-1}(z)$,

(ii) $L = x * y = x * z = R \iff y = z \in I((Q, \circ)) \wedge (x * y) \in f_\circ^{-1}(y)$,

(iii) $L = x \circ z = y \circ z = R \iff x = y \in I((Q, *)) \wedge (y \circ z) \in e_*^{-1}(y)$,

(iv) $L = x * y = x \circ z = R \iff x, y \in f_\circ^{-1}(z) \wedge x \in f_*^{-1}(y)$,

(v) $L = x * z = y \circ z = R \iff y, z \in e_*^{-1}(x) \wedge z \in e_\circ^{-1}(y)$,

(vi) $L = x * z = x \circ z = R \iff x * z = x \circ z \wedge f_*(x) = y = e_\circ(z)$,

(vii) $L = x * y = y \circ z = x * z = R \iff (x * y) = y = z \in I((Q, \circ))$,

(viii) $L = x * y = y \circ z = x \circ z = R \iff (y \circ z) = x = y \in I((Q, *))$,

(ix) $L = x * y = x * z = x \circ z = R \iff f_*(x) = f_\circ(x) = y = z \in I((Q, \circ))$,

(x) $L = y \circ z = x * z = x \circ z = R \iff e_*(z) = e_\circ(z) = x = y \in I((Q, *))$,

(xi) $L = x * y = y \circ z = x * z = x \circ z = R \iff x = y = z \in I((Q, *)) \cap I((Q, \circ))$.

Proof. (i) The forward implication follows from (4.6) and (4.7). For the other direction, let $y \in e_*^{-1}(x) \cap f_\circ^{-1}(z)$, then by (4.5) we get $x * y = y = y \circ z$, and thus $(x * y) \circ z = y \circ z = x * y = x * (y \circ z)$.
(ii) By (4.6) and (4.8), $y \in f_\circ^{-1}(z)$ and $y = e_\circ(z)$. Thus $y \circ z = y$ and $y \circ z = z$, and so $y = z \in I((Q, \circ))$. Therefore from $(x * y) \circ z = x * z$ follows $(x * y) \circ y = x * y$, and thus $x * y \in f_\circ^{-1}(y)$. For the reverse implication, let $y = z \in I((Q, \circ))$ and $(x * y) \in f_\circ^{-1}(y)$. Then, $(x * y) \circ z = (x * y) \circ y = x * y = x * z = x * (z \circ z) = x * (y \circ z)$.
(iv) By (4.6) and (4.9), $y \in f_\circ^{-1}(z)$ and $y = f_*(x)$, thus $y \circ z = y$, $x * y = x$ and $x \in f_*^{-1}(y)$. Hence, $x = x * y = x * (y \circ z) = (x * y) \circ z = x \circ z$, and so $x \in f_\circ^{-1}(z)$. To prove the other implication, let $x, y \in f_\circ^{-1}(z)$ and $x \in f_*^{-1}(y)$, then $(x * y) \circ z = x \circ z = x = x * y = x * (y \circ z)$.
(vi) Clearly holds.
(vii) By (i), $y \in e_*^{-1}(x)$, so $x * y = y$. From (ii), $y = z \in I((Q, \circ))$ and $(x * y) \in f_\circ^{-1}(y)$, thus $(x * y) \circ y = x * y = y$. For the other implication, let $x * y = y = z \in I((Q, \circ))$. Then $(x * y) \circ z = y \circ z = y \circ y = y = x * y = x * z = x * (z \circ z) = x * (y \circ z)$.
(ix) By (ii), $y = z \in I((Q, \circ))$ and $(x * y) \in f_\circ^{-1}(z)$, thus $(x * y) \circ z = x * y$. Since from (iv) also $x \in f_*^{-1}(y)$, so $y = f_*(x)$ and $x * y = x$. Hence, we have $x \circ z = x$, so $z = f_\circ(x)$. To prove the reverse implication, let $f_*(x) = f_\circ(x) = y = z \in I((Q, \circ))$. Then $(x * y) \circ z = x \circ z = x = x * z = x * y = x * (y \circ y) = x * (y \circ z)$.
(xi) The forward direction follows directly from (ix) and (x). For reverse implication, let $x = y = z \in I((Q, *)) \cap I((Q, \circ))$. Then $x * (y \circ z) = x * (y \circ y) = x * y = x * z = x * x = x = x \circ y = x \circ z = (x * x) \circ z = (x * y) \circ z$.
Points $(iii), (v), (viii)$ and (x) follow by mirror arguments. □

Similarly, as an analogous lemma for a single operation that can be found in [2], Proposition 4.5 might be the first step towards determining an improved lower bound on the number of associative triples for a general quasigroup couple.

5. Computational results for small quasigroup couples

We observed that the problem of finding the value of $a_2(n)$ for an arbitrary $n \in \mathbb{N}$ is difficult. However, for quasigroup couples of small orders, these numbers can be obtained by computer evaluations, which might give us a better idea about the behaviour of $a_2(n)$ as a function of n.

5.1 2-associativity spectra

For each $n \in \mathbb{N}$, denote by $\operatorname{assspec}_2(n)$ the set of all $a_2(C)$, where C is a quasigroup couple of order n. We shall refer to this set as the *2-associativity spectrum of n*. We have computed that:

$$\operatorname{assspec}_2(1) = \{1\}$$
$$\operatorname{assspec}_2(2) = \{8\}$$
$$\operatorname{assspec}_2(2) = \{9, 27\}$$
$$\operatorname{assspec}_2(4) = \{8, 12, 16, 24, 32, 36, 48, 64\}$$
$$\operatorname{assspec}_2(5) = \{9, 11, ..., 63, 65, 67, 68, 69, 71, 74, 76, 77, 79, 80, 89, 125\}$$

The resulting values of $a_2(n)$ along with values of $a(n)$ determined by Ježek and Kepka in [8] are listed in Table 5.1. Two examples of found extremal quasigroup couples are presented in Table 5.2 and Table 5.3.

In the next section, we shall explain how we arrived at these results.

5.2 Computations

All programs were written in Python using library NumPy and run on a computer with 1.8 GHz Intel Core i7 processor, using 4 GB of RAM, with macOS version 10.13.

n	$a_2(n)$	$a(n)$
1	1	1
2	8	8
3	9	9
4	8	16
5	9	15

Table 5.1: A comparison of minimal associativity indices of one and two operations

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

$\circ$	0	1	2	3
0	1	3	0	2
1	3	1	2	0
2	2	0	3	1
3	0	2	1	3

Table 5.2: Multiplication tables of a quasigroup couple $C = (Q, *, \circ)$ of order 4 with $a_2(C) = 8$

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

$\circ$	0	1	2	3	4
0	3	0	1	4	2
1	4	2	0	1	3
2	2	1	4	3	0
3	0	4	3	2	1
4	1	3	2	0	4

Table 5.3: Multiplication tables of a quasigroup couple $C = (Q, *, \circ)$ of order 5 with $a_2(C) = 9$

5.2.1 Exhaustive search

The values of $\text{assspec}_2(n)$ for $n = 1, ..., 4$ were obtained by performing an exhaustive search of the space of all quasigroup couples. Firstly, using a recursive algorithm, we generated all latin squares (and thus multiplication tables of all quasigroups) of a given order and saved them to a file. Then, we iterated through all the quasigroups in the file and for each one, we again looped through the same file, thus getting all the possible couples. Afterwards, we counted the associative triples of each couple.

However, this approach very soon proved to be ineffective due to the enormous search space. For instance, there are 576 latin squares of order 4, therefore we had to go through $576^2 = 331,776$ couples to aquire $\text{assspec}_2(4)$, which took less than 20 seconds. But, if we tried to apply the same algorithm to order 5, the computations would last approximately 24 days on a personal computer since there are $161,280$ latin squares of this order, and so $161,280^2 = 26,011,238,400$ couples.

5.2.2 Using isomorphism class representatives

Before we proceed to explain the second method, we need to talk briefly about the classification of latin squares. We will mention several useful definitions and theorems from the first and the fourth chapter of [10]. For further details and proofs, you can refer to that source.

The isotopy and isomorphism of latin squares are equivalence relations, as can be verified easily. Thus, we define:

Definition. An *isotopy class* of a latin square is an equivalence class for the isotopy relation. Similarily, an *isomorphism class* of a latin square is an equivalence class for the isomorphism relation.

Every latin square $L = (a_{ij})_{i,j=1}^n$ of order n can be represented as a set of n^2 triples $T_L = \{(i, j, a_{ij}) \,|\, i, j = 1, ..., n\}$. By permuting the entries within all the triples by a permutation $\sigma \in S_3$, we obtain a representation of a latin square, that is called *a parastrophe* of L.

Two latin squares are said to be *paratopic*, if one is isotopic to a parastrophe of the other. The set of all latin squares paratopic to L is called *the main class* of L.

Theorem 5.1. *The set of all latin squares of a given order is a disjoint union of main classes. Each main class is a disjoint union of isotopy classes. And finally, each isotopy class is a disjoint union of isomorphism classes.*

Each isomorphism class of a latin square determines a unique quasigroup up to isomorphism. Therefore, by generating a representative of each isomorphism class, we significantly reduce the amount of duplicit work, that we have done in the previous method.

For each generated isomorphism class representative, we looped through the earlier generated file of all quasigroups. Finally, we counted the associative triples of all the created couples. Since for order 5 there are $1,411$ isomorphism classes, we only had to go through $1,411 \cdot 161,280 = 227,566,080$ couples, which we finished in around 15 hours.

The isomorphism class representatives were obtained in the following way. First, we created all principal isotopes of isotopy class representatives that we downloaded from an online combinatorial data collection [11]. By Theorem 1.1, it is sufficient to generate only the principal isotopes. Then, we presorted them using isomorphism class invariants, like the number of elements on the main diagonal, the number of latin subsquares of order 2 (also called intercalates) and the number of transversals (a set of n cells of the latin square, one in each row, one in each column, each containing a different symbol). Lastly, we finished sorting by finding the isomorphisms, and finally, we selected our representatives.

Obtaining results for greater orders would require optimizing our algorithms and using greater computational power. However, even that would not get us much further, as with the current technology, this problem is very challenging even for a single operation.

Conclusion

The main purpose of this thesis was to adapt the methods used by Drápal and Valent in studying the nonassociativity of one quasigroup operation, apply them to a scenario with two quasigroups and obtain similar results. We succeeded in modifying their approaches and examined the newly defined algebraic structure called a quasigroup couple from two different angles.

Firstly, using the altered techniques, we thoroughly explored the average value of the associativity index of a quasigroup couple of order n over the principal isotopes of the quasigroup couple. As a result, we established an upper bound on the associativity index of a quasigroup couple.

We calculated that the average over the principal isotopes of one of the quasigroups in the couple lies between n^2 and $2n^2$. Then we took the average over all the principal isotopes of the quasigroup couple and obtained the value $n^2(1 + 1/(n-1))$, which can be regarded as an upper bound on $a_2(n)$ for $n > 2$. In Chapter 3, we again returned to the average over the principal isotopes of one of the quasigroups in the couple, and we characterized the setting in which the minimal average value n^2 is attained. As a result, we proved that it is an improved upper bound on the associativity index, that is $a_2(n) \leq n^2$.

Secondly, we began studying couples of quasigroups isotopic to groups. We presented observations about a couple of groups and isomorphism, then posed several questions concerning nonassociativity.

In the case of a group couple C of order n, we proposed that $a_2(C) \geq 2n^2 - n$ and presented computations on small orders that suggest that this lower bound might be higher as there exist types of associative triples that we have not accounted for. As a first step in addressing this problem, we described the intersections of the types of associative triples in a general scenario with two quasigroups.

In the more general scenarios that feature quasigroups isotopic to groups, we then reported on partial solutions that follow from the situation with one quasigroup operation and pointed out areas where more research is required.

Lastly, we also determined all possible values of associativity indices for orders $n \leq 5$ by performing computations on quasigroup couples of small orders. In addition, we presented examples of quasigroup couples attaining the minimal indices.

Bibliography

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

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

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

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

[5] D. Gligoroski, S. Markovski, and S. J. Knapskog. The Stream Cipher Edon80. In M. Robshaw and O. Billet, editors, *New Stream Cipher Designs: The eSTREAM Finalists*, volume 4986 of *LNCS*, pages 152–169. Springer, Berlin, 2008.

[6] O. Grošek and P. Horák. On quasigroups with few associative triples. *Designs, Codes and Cryptography*, 64:221–227, 2012.

[7] M. Hall and L. J. Paige. Complete mappings of finite groups. *Pacific Journal of Mathematics*, 5(4):541–549, 1955.

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

[9] T. W. Judson. *Abstract Algebra*, chapter Burnside's Counting Theorem, pages 180–185. Annual Edition 2022. PreTeXt, 2022. `http://abstract.ups.edu/download/aata-20220728.pdf` (Accessed: 22-02-2023).

[10] A. D. Keedwell and J. Dénes. *Latin Squares and Their Applications*. Second edition. Elsevier, Amsterdam, 2015. ISBN 978-0-444-63555-6.

[11] Brendan McKay. Latin squares. `https://users.cecs.anu.edu.au/~bdm/data/latin.html` (Accessed: 10-03-2023).

[12] V. Valent. Quasigroups with few associative triples. Bachelor thesis, Charles University, Faculty of Mathematics and Physics, Prague, 2016.

A. Appendix

$\circ$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\circ_{\gamma,\mathrm{id}}$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	2	3	4	5	6	0	1
2	5	6	0	1	2	3	4
3	1	2	3	4	5	6	0
4	6	0	1	2	3	4	5
5	4	5	6	0	1	2	3
6	3	4	5	6	0	1	2

Table A.1: Multiplication tables of a quasigroup couple $C = (Q, \circ, \circ_{\gamma,\mathrm{id}})$ of order 7 with $a_2(C) = 49$, $(Q, \circ) = \mathbb{Z}_7$ and $(Q, \circ_{\gamma,\mathrm{id}})$ is isotopic to $\mathbb{Z}_7$

$\circ$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	3	4	5	6	0	7	2
2	2	7	3	6	1	4	0	5
3	3	5	6	0	7	1	2	4
4	4	2	5	7	3	6	1	0
5	5	0	7	1	2	3	4	6
6	6	4	0	2	5	7	3	1
7	7	6	1	4	0	2	5	3

$\circ_{\gamma,\mathrm{id}}$	0	1	2	3	4	5	6	7
0	3	5	6	0	7	1	2	4
1	2	7	3	6	1	4	0	5
2	0	1	2	3	4	5	6	7
3	1	3	4	5	6	0	7	2
4	4	2	5	7	3	6	1	0
5	7	6	1	4	0	2	5	3
6	5	0	7	1	2	3	4	6
7	6	4	0	2	5	7	3	1

Table A.2: Multiplication tables of a quasigroup couple $C = (Q, \circ, \circ_{\gamma,\mathrm{id}})$ of order 8 with $a_2(C) = 64$, $(Q, \circ)$ is the quaternion group and $(Q, \circ_{\gamma,\mathrm{id}})$ is its isotope