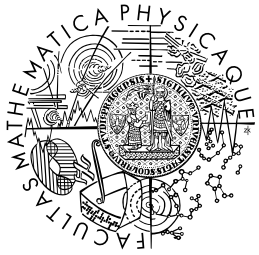

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

Tomáš Nagy

Selfdistributive quasigroups of size 2^k

Department of Algebra

Supervisor of the master thesis: Doc. RNDr. David Stanovský, Ph.D.

Study programme: Mathematics

Study branch: Mathematical Structures

Prague 2019

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources.

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 ..... signature of the author

I would like to thank my supervisor David Stanovský for the possibility of working on the topic of this thesis, for his willingness to consult every problem that I encounter during the work and for his help during my study.

I would also like to thank my parents for smaller hints about programming with that they helped me during my work on this thesis and for their support during my whole study.

Because Master's study is the last regular form of study, I would also like to thank all my teachers and professors that I had the pleasure to meet at the ground school, at the high school and at the university for their enthusiasm and patience and for all the inspirations and ideas that they gave me.

Finally, I would like to thank the One who is because all things were made through him and without him was not any thing made that was made (John 1,3).

Title: Selfdistributive quasigroups of size 2^k

Author: Tomáš Nagy

Department: Department of Algebra

Supervisor: Doc. RNDr. David Stanovský, Ph.D., Department of Algebra

Abstract: We present the theory of selfdistributive quasigroups and the construction of non-affine selfdistributive quasigroup of size 2^{16} that was presented by Onoi in 1970 and which was the least known example of such structure of size 2^k. Based on this construction, we introduce the notion of Onoi structures and Onoi mappings between them which generalizes Onoi's construction and which allows us to construct non-affine selfdistributive quasigroups of size 2^{2k} for $k \geq 3$.

We present and implement algorithm for finding central extensions of selfdistributive quasigroups which enables us to classify non-affine selfdistributive quasigroups of size 2^k and prove that those quasigroup exists exactly for $k \geq 6$, $k \neq 7$. We use this algorithm also in order to better understand the structure of non-affine selfdistributive quasigroups of size 2^6.

Keywords: quasigroups non-affine quandles selfdistributivity medial quasigroups enumeration

Contents

Introduction

Sudoku is maybe one of the most popular logical games worldwide. We can ask ourselves as mathematicians, how would it be possible to transform solving sudoku into some mathematical problem. One of the possible ways is to ask in how many ways can we fill an $n \times n$ square with numbers from 1 to n such that each number appears in each row and each column exactly once.

This approach still seems to be rather combinatorial (such structures are called *latin squares* in combinatorics). But if we will understand latin squares as multiplication tables of an operation $*$ on a set with n elements, we will obtain the notion of well-known algebraical object - a *quasigroup*. As one of the most important aspects of studying mathematics is finding beauty (e.g. studying *beautiful* objects, properties or proofs), we can ask ourselves further: Which properties of quasigroups are particulary beautiful?

Wouldn't be a quasigroup whose translations are homomorphisms really nice? We can consider either left or right translations and we obtain *left* or *right selfdistributive quasigroups*. In this thesis, we will be interested in the left selfdistributive ones and hence we will usually omit the adjective "left", the case of right selfdistributive is dual.

It turns out that selfdistributive quasigroups can be further divided into two subclasses - *affine* ones can easily be obtained from abelian groups, while the non-affine ones are in no easy correspondence with any well-known class of structures.

The history of non-affine selfdistributive quasigroups of size 2^k is quite interesting: One of the first examples of such a structure was introduced by Onoi in 1970 in his article [6] and this example has size 2^{16}. But since then, Onoi's example is still the least known example of non-affine selfdistributive quasigroup of size 2^k. On the other hand, a lot of new results was presented in the theory of selfdistributive quasigroups (for example, it was proven that the least non-affine selfdistributive quasigroup has 15 elements and it is known for many primes p which is the least k such that there exists non-affine selfdistributive quasigroup of size p^k).

Our main aim in this thesis will be to examine non-affine selfdistributive quasigroups of size 2^k - to construct the least example of such a quasigroup and possibly also to classify all such quasigroups, e.g. to find out for which k's there exists an example of such a structure.

In order to reach our goal, we will use Onoi's construction and also the new developed commutator theory for selfdistributive quasigroups.

1. Basic notions

In this chapter, we will introduce some basic concepts for studying quandles. More related definitions and theorems can be found in [5] and in [1].

1.1 Quasigroups, quandles and loops

An *algebraical structure* is a non-empty set with a collection of operations of arbitrary finite arity. In the whole thesis, we will consider only finite structures without explicitly mentioning this.

Let $(Q, *)$ be an algebraical structure with a binary operation $*$. Let us define for $a \in Q$ the *left translation* $L_a : Q \to Q$ by $L_a(b) = a * b$.

Definition 1 (left quasigroup)**.** *We say that the binary structure $(Q, *)$ is a* left quasigroup *if all its left translations are bijective.*

In a left quasigroup we can define the *left division* $\backslash$ by $a\backslash b = L_a^{-1}(b)$. For a left quasigroup Q we define the *displacement group* and the *left multiplication group* by

$$Dis(Q) = \langle L_a L_b^{-1} \mid a, b \in Q \rangle,$$
$$LMlt(Q) = \langle L_a \mid a \in Q \rangle.$$

We can define *right translation*, *right quasigroup* and *right division* $/$ in a similar way. We say that $(Q, *)$ is a *quasigroup* if it is both left and right quasigroup. In order to express that the structure $(Q, *)$ has both left and right translation bijective (i.e. it is a quasigroup), we use also the adjective *latin*.

It is easy to see that each group is a quasigroup (with $a\backslash b = a^{-1}b$ and $b/a = ba^{-1}$) which means that we can see the concept of quasigroup as a non-associative generalization of groups without identity element.

From the combinatorial point of view, we can describe quasigroup as a set Q with binary operation $*$ whose multiplication table is a latin square (i.e. each number appears in each row and each column exactly once).

We say that a left quasigroup $(Q, *)$ is connected if $LMlt(Q)$ acts transitively on Q. If $(Q, *)$ is a quasigroup, then $L_{b/a}(a) = (b/a) * a = (R_a^{-1}(b)) * a = R_a R_a^{-1}(b) = b$, i.e. $(Q, *)$ is connected.

Definition 2 (rack)**.** *Let $(Q, *)$ be a left quasigroup. We say that $(Q, *)$ is a rack if all its left translations are automorphisms, i.e. if $a * (b * c) = (a * b) * (a * c)$ for all $a, b, c \in Q$ (we call this property the* left-selfdistributivity*).*

We will often omit the adjective left and we will call left-selfdistributive quasigroups just selfdistributive quasigroups (it would be also possible to replace left-selfdistributivity by right-selfdistributivity and this case would be dual).

Definition 3 (quandle)**.** *We say that a rack $(Q, *)$ is a quandle if it is idempotent, i.e. the identity $a * a = a$ holds for all $a \in Q$.*

We say that a quandle Q is *medial* if the identity $(a*b)*(c*d) = (a*c)*(b*d)$ holds for all $a, b, c, d \in Q$, we say that it is *(left) involutory* if $a * (a * b) = b$ holds for all $a, b \in Q$.

It is easy to see that left-distributive quasigroups are exactly latin quandles, because from $a * (a * a) = (a * a) * (a * a)$ we get that $(a * (a * a))/(a * a) = ((a * a) * (a * a))/(a * a)$, i.e. $a = a * a$. On the other hand, latin quandle is a selfdistributive quasigroup by definition.

The concept of selfdistributivity appeared for the first time already in the 19th century in the work of logicians Peirce and Schröder and nowadays it appears in many areas of mathematics including low-dimensional topology (knot and braid invariants), theory of symmetric spaces and set theory (a nice historical overview of selfdistributivity can be found e.g. in [8]).

There are nice examples of selfdistributive operations in many areas of mathematics, some of them are listed below:

- *Group conjugation:* Let $(G, \cdot)$ be a group and let us define an operation $*$ on the set G by $a * b = aba^{-1}$. Then $(G, *)$ is a quandle (but rarely a latin one).
- *Reflection in (Euclidean) geometry*: We can define an operation $*$ on the set of points (on some surface) such that $a * b$ is the reflection of b over a. This gives us also a quandle (but not necessarily a latin quandle, e.g. on a sphere).
- *Convex combination:* Let V be a real vector space and $s \in [0, 1)$. Let us define an operation $*$ on V by $u * v = s \cdot u + (1 - s) \cdot v$. This is a quandle once more and for $s \neq 0$ it is also a selfdistributive quasigroup.

Definition 4 (loop)**.** *A quasigroup $(Q, *)$ is called a* loop *if it has a neutral element* 1 *(i.e. $1 * a = a = a * 1$ for all $a \in Q$).*

We list here a few identities for loops which we will use later. We use the notation ab instead of $a \cdot b$ and $ab \cdot c$ instead of $(a \cdot b) \cdot c$. A loop $(Q, \cdot)$ is called:

- *Moufang* if $(ab \cdot a)c = a(b \cdot ac)$ for all $a, b, c \in Q$;
- *commutative* if $ab = ba$ for all $a, b \in Q$;
- *(left) Bol* if $(a \cdot ba)c = a(b \cdot ac)$;
- *with two-sided inverses* if for all $a \in Q$ there exists $a^{-1} \in Q$ such that $aa^{-1} = 1 = a^{-1}a$;
- *with automorphic inverse property* if it has two-sided inverses and $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in Q$;
- *Bruck* (or only B-loop) if it is a Bol loop with automorphic inverse property;
- *uniquely 2-divisible* if the mapping $a \mapsto a^2$ is a bijection.

1.2 Affine quandles

Let G be a group, $f \in Aut(G)$ and let H be some subgroup of $Fix(f) = \{x \in G \mid f(x) = x\}$. Let us denote by G/H the set of left cosets of G by H, i.e. $G/H = \{gH \mid g \in G\}$. Let us define an operation $*$ on G/H by $g_1H * g_2H = g_1f(g_1^{-1}g_2)H$. Then, $(G/H, *)$ is a quandle, called the *coset quandle*. If G is abelian and $H = 1$, then $(G/1, *)$ is called *affine* and we will denote it by $Aff(G, f)$.

Definition 5 (affine quandle)**.** *A quandle $(Q, *_1)$ is called* affine *if it is isomorph to some affine coset quandle $Aff(G, f)$.*

It is easy to see that an affine quandle is a quandle: It is a left quasigroup because if $(1-f)(a) + f(x) = a * x = b$ then $x = f^{-1}(b - (1-f)(a))$, moreover, $a*(b*c) = a*((1-f)(b)+f(c)) = (1-f)(a)+f(b)-f^2(b)+f^2(c) = (1-f)((1-f)(a)+f(b))+f((1-f)(a)+f(c)) = (a*b)*(a*c)$ and $a*a = (1-f)(a)+f(a) = a$.

We can easily see that an affine quandle $Aff(G, f)$ is latin if and only if $(1-f) \in Aut(G)$. Hence, we can easily enumerate affine latin quandles (i.e. affine selfdistributive quasigroups) of size k by taking all abelian groups of this size with their automorphisms. The following theorem shows that the group G in $Aff(G, f)$ is determined uniquely up to isomorphism:

Theorem 1. *Let $Aff(G, f)$ be isomorph to $Aff(H, g)$. Then, $G \simeq H$.*

Proof. This is an easy consequence of [5, Theorem 5.6]. □

In the context of universal algebra, the adjective "latin" means "being essentially a module". This can be formalized as follows: Let $(A, f_1, f_2 \ldots)$ be an algebraical structure. We call an operation f on A a *term operation* if it can be obtained by composing the basic operations $f_1, f_2, \ldots$. A *polynomial operation* is an operation that is obtained from a term operation by substituting constants for some variables. Two algebras with the same underlying set are said to be *term (polynomially) equivalent* if they have the same term (polynomial) operations.

An algebraical structure is called *affine* if it is polynomially equivalent to a module.

An affine quandle $Aff(G, f)$ is polynomially equivalent to a module over the ring of Laurent polynomials $\mathbf{Z}[s, s^{-1}, t, t^{-1}]$ with the underlying additive structure $(G, +)$ where the actions of s and t correspond to the actions of $(1-f)$ and f respectively.

We will look at this correspondence for affine latin quandle considered as quasigroup: Let $Aff(G, f) = (G, *, \backslash, /)$. We can clearly write $a * b = (1-f)(a)+f(b) = sa+tb$. Moreover, $a\backslash b = t^{-1}(b-sa)$ and $b/a = s^{-1}(b-ta)$. Hence, polynomial operations of $(G, *, \backslash, /)$ are subset of polynomial operations of the module $(G, +)$.

We can show also the other inclusion: Actions of s, s^{-1}, t and t^{-1} are polynomial operations over $(G, *, \backslash, /)$ because: $sa = a * 0$, $ta = 0 * a$, $s^{-1}a = a/0$ and $t^{-1}a = 0\backslash a$. Finally, $a + b = (a/0) * (0\backslash b)$. We have showed that the quasigroup $(G, *, \backslash, /)$ and the module $(G, +)$ are polynomially equivalent.

For a group G we will denote by G' the commutator of this group, i.e. $G' = \langle g_1^{-1}g_2^{-1}g_1g_2 \mid g_1, g_2 \in G\rangle$.

The following theorem holds for connected quandles:

Theorem 2. *Let $(Q, *)$ be a connected quandle. Then, the following are equivalent:*

1. *Q is affine,*
2. *Q is medial,*
3. *$Dis(Q) = LMlt(Q)'$ is abelian.*

Proof. See [5, Theorem 7.3] (they prove it for right-selfdistributive quandles instead of left-selfdistributive, but this case is dual). □

Hence, we obtain correspondence between idempotent medial quasigroups and abelian groups with their automorphisms (we can use the previous theorem, each quasigroup is connected and idempotent medial quasigroups are quandles and hence are isomorphic to $Aff(G, f)$ for some abelian group G and $f \in Aut(G)$).

1.3 Correspondence between classes of quasigroups and loops

We have already seen in the previous section that there is an easy correspondence between medial idempotent quasigroups and abelian groups. Since the theory of abelian groups is well-developed, this correspondence enables us to easily enumerate all those quasigroups. We can ask ourselves if there exist similar correspondences also for other classes of quasigroups (or latin quandles). All results mentioned in this chapter comes from [8] and [11] where also deeper facts can be found.

First of all, we will show that it is possible to generalize the correspondence between idempotent medial quasigroups and abelian groups for medial quasigroups that are not necessarily idempotent:

A permutation φ of Q is called *affine* over $(Q, \cdot)$ if there exist an automorphism $\tilde{\varphi}$ of $(Q, \cdot)$ and $q \in Q$ such that $\varphi(a) = q \cdot \tilde{\varphi}(a)$ or $\varphi(a) = \tilde{\varphi}(a) \cdot q$ for all $a \in Q$. A quasigroup $(Q, *)$ is called *affine* over a loop $(Q, \cdot)$ if for every $a, b \in Q$ it holds that $a * b = \varphi(a) \cdot \psi(b)$, where φ, ψ are affine mappings over $(Q, \cdot)$ such that $\tilde{\varphi}\tilde{\psi} = \tilde{\psi}\tilde{\varphi}$.

We have the following correspondence:

Theorem 3. *Let $(Q, *)$ be a quasigroup. Then, the following are equivalent:*

1. *$(Q, *)$ is medial,*
2. *$(Q, *)$ is affine over an abelian group.*

Proof. See [8, Theorem 3.1]. □

There is a similar correspondence between distributive quasigroups (i.e. quasigroups that are also right-selfdistributive) and commutative Moufang loops. But this corerspondence is not of our particular interest because the only non-medial distributive quasigroups are of size 3^k for $k \geq 4$ (see [8, Theorem 3.5]).

We can obtain similar correspondence also between involutory latin quandles and uniquely 2-divisible Bruck loops:

Theorem 4. *Let Q be a set and $e \in Q$. Then, there is a one-to-one correspondence between involutory latin quandles on Q and uniquely 2-divisible Bruck loops on Q with identity element e. This correspondence is given by:*

- *If $(Q, *)$ is an involutory latin quandle, then $(Q, +)$ is a uniquely 2-divisible Bruck loop with identity element e, where $+$ is defined by $a + b = (x/e) * (e\backslash y)$.*
- *If $(Q, +)$ is a uniquely 2-divisible Bruck loop with identity element e, then $(Q, *)$ is an involutory latin quandle, where $a * b = (a + a) - b$.*
- *Those mappings are mutual inverses.*

Proof. See [11, Theorem 3.1]. □

This correspondence is also not of our particular interest because there exists no involutory latin quandle of size 2^k (this is an easy consequence of Theorem 8.1 in [1]).

For general left-selfdistributive quasigroups, we will be able to obtain a correspondence with the class of Belousov-Onoi loops:

Let $(Q, \cdot)$ be a loop and $\psi \in Aut(Q)$. We will call $(Q, \cdot, \psi)$ a *Belousov-Onoi (or just BO-) module* if the identity $\varphi(ab) \cdot \psi(ac) = a \cdot \varphi(b)\psi(c)$ holds (φ is defined by $\varphi(a) = a/\psi(a)$). For example, group with its automorphism ψ is a BO-module and every Bruck loop with $\psi(x) = x^{-1}$ is a BO-module.

We can obtain a (latin) quandle from a BO-module in the following way:

Theorem 5. *Let $(Q, \cdot, \psi)$ be a BO-module and let us define an operation $*$ on Q by $a * b = \varphi(a)\psi(b)$. Then, $(Q, *)$ is a quandle. It is a quasigroup if and only if φ is a permutation.*

Proof. See [8, Proposition 5.2]. □

If (in the notation of the theorem) $(Q, *)$ is a quasigroup, then $(Q, \cdot)$ is called a *Belousov-Onoi (BO-) loop* with respect to ψ. If φ is an automorphism, the representation of $(Q, *)$ over $(Q, \cdot)$ is called *right linear*.

Theorem 6. *The following are equivalent for a quasigroup $(Q, *)$:*

1. *it is left self-distributive,*
2. *it is right linear over a BO-loop.*

Proof. See [8, Theorem 5.5]. □

As we already mentioned in the previous section, it is easy to use the correspondence between medial quasigroups and abelian groups in order to enumerate all medial quasigroups of a given size. The correspondence between involutory latin quandles and Bruck loops was used for enumeration of those quandles recently in [11].

On the other hand, it is hard to make use of the correspondence between selfdistributive quasigroups and Belousov-Onoi loops. This explains, why are we interested in the construction of non-medial (i.e. non-affine) selfdistributive

quasigroups and why we have to develop other tools in order to construct those quasigroups.

It is harder to enumerate latin quandles than to enumerate several classes of loops because (as we have already showed before) latin quandles are homogeneous while it is often possible to partition a given loop into non-trivial blocks that are preserved under homomorphism. Examples of this approach to enumeration of certain classes of loops can be found e.g. in [11] and in [2].

1.4 Abelian and central extensions of quandles

The terminology in this section comes from [1].

Definition 6 (extension)**.** *Let $(Q, *_Q)$ be a left quasigroup, $(A, +, -, 0)$ an abelian group and ϕ, ψ, θ the following mappings:*

$$\phi : Q \times Q \to End(A),$$
$$\psi : Q \times Q \to Aut(A),$$
$$\theta : Q \times Q \to A.$$

Let us define an operation $*$ on $Q \times A$ by $(a, x) * (b, y) = (a *_Q b, \phi_{a,b}(x) + \psi_{a,b}(y) + \theta_{a,b})$. Then, $Q \times_{\phi,\psi,\theta} A = (Q \times A, *)$ is a left quasigroup and we call it an abelian extension *of Q by ϕ, ψ, θ. If the mappings ϕ and ψ are constant, we will call it a* central extension*.*

Similar theory of central extensions for groups is described e.g. in [7, pages 201 - 216], theory of abelian extensions of loops was described in [9].

Abelian extensions of quandles are not necessarily quandles but we can easily derive conditions for ϕ, ψ and θ that are equivalent to the fact that this extension is a quandle:

Lemma 7. *Let $(Q, *)$ be a rack, $(A, +, -, 0)$ an abelian group and ϕ, ψ, θ as in Definition 6. Then, $Q \times_{\phi,\psi,\theta} A$ is a rack if and only if the following conditions are satisfied for all $a, b, c \in Q$:*

$$\psi_{a,b*c}(\theta_{b,c}) + \theta_{a,b*c} = \psi_{a*b,a*c}(\theta_{a,c}) + \phi_{a*b,a*c}(\theta_{a,b}) + \theta_{a*b,a*c}, \tag{1.1}$$
$$\psi_{a,b*c}\psi_{b,c} = \psi_{a*b,a*c}\psi_{a,c}, \tag{1.2}$$
$$\psi_{a,b*c}\phi_{b,c} = \phi_{a*b,a*c}\psi_{a,b}, \tag{1.3}$$
$$\phi_{a,b*c} = \phi_{a*b,a*c}\phi_{a,b} + \psi_{a*b,a*c}\phi_{a,c}. \tag{1.4}$$

Moreover, $Q \times_{\phi,\psi,*} A$ is a quandle if and only if, additionally, Q is a quandle and

$$\theta_{a,a} = 0, \tag{1.5}$$
$$\phi_{a,a} + \psi_{a,a} = 1_A, \tag{1.6}$$

for all $a \in Q$.

Proof. Because $Q \times_{\phi,\psi,\theta} A = (Q \times A, *_1)$ is a left quasigroup, it is a rack if and only if it is left-selfdistributive, i.e. if for all $a, b, c \in Q$ and $x, y, z \in A$ it holds that:

$$(a, x) *_1 ((b, y) *_1 (c, z)) = ((a, x) *_1 (b, y)) *_1 ((a, x) *_1 (c, z)).$$

This gives us the following equation:

$$\begin{aligned}(a * (b * c), \phi_{a,b*c}(x) + \psi_{a,b*c}(\phi_{b,c}(y) + \psi_{b,c}(z) + \theta_{b,c}) + \theta_{a,b*c} = \\ ((a * b), (a * c), \phi_{a*b,a*c}(\phi_{a,b}(x) + \psi_{a,b}(y) + \theta_{a,b}) + \\ \psi_{a*b,a*c}(\phi_{a,c}(x) + \psi_{a,c}(z) + \theta_{a,c}) + \theta_{a*b,a*c}.\end{aligned}$$

By equating coefficients, we get the equations from Lemma 7. Moreover, $Q \times_{\phi,\psi,\theta} A$ is a quandle if and only if for all $a \in Q$ and $x \in A$:

$$(a, x) *_1 (a, x) = (a, x).$$

This means that

$$(a * a, \phi_{a,a}(x) + \psi_{a,a}(x) + \theta_{a,a}) = (a, x).$$

But, obviously, this happens if and only if Q is a quandle and the conditions 1.4 and 1.5 are satisfied. □

Let $Q \times_{\phi,\psi,\theta} A$ be a central extension that is a quandle. Then, we have the following two homomorphisms of quandles:

- An injective homomorphism $f : Aff(A, \psi) \longrightarrow Q \times_{\phi,\psi,\theta} A$ defined by $f(a) = (q, a)$ where q is a fixed element of Q. This is a homomorphism because $f(a * b) = f((1-\phi)(a) + \phi(b)) = (q, (1-\phi)(a) + \phi(b)) = (q * q, \psi(a) + \phi(b) + \theta_{q,q}) = f(a) * f(b)$ (we use the condition 1.6).
- A surjective homomorphism $g : Q \times_{\phi,\psi,\theta} A \longrightarrow Q$ defined by $g(q, a) = q$.

We can also easily obtain conditions that are equivalent to the fact that an abelian extension is a latin (or medial) quandle.

Lemma 8. *Let $Q \times_{\phi,\psi,\theta} A$ be an abelian extension that is a quandle as in the previous lemma. Then, it is a latin quandle if and only if $\phi_{a,b} \in Aut(A)$ for all $a, b \in Q$.*
$Q \times_{\phi,\psi,\theta} A$ is medial if and only if the following conditions hold for all $a, b, c, d \in Q$:

$$\phi_{a*b,c*d}(\theta_{a,b}) + \psi_{a*b,c*d}(\theta_{c,d}) + \theta_{a*b,c*d} = \phi_{a*c,b*d}(\theta_{a,c}) + \psi_{a*c,b*d}(\theta_{b,d}) + \theta_{a*c,b*d}, \tag{1.7}$$

$$\phi_{a*b,c*d}(\phi_{a,b}) = \phi_{a*c,b*d}(\phi_{a,c}), \tag{1.8}$$

$$\psi_{a*b,c*d}(\phi_{c,d}) = \phi_{a*c,b*d}(\psi_{a,c}), \tag{1.9}$$

$$\phi_{a*b,c*d}(\psi_{a,b}) = \psi_{a*c,b*d}(\phi_{b,d}), \tag{1.10}$$

$$\psi_{a*b,c*d}(\psi_{c,d}) = \psi_{a*c,b*d}(\psi_{b,d}). \tag{1.11}$$

Proof. If there exist $a, b \in Q$ and $x, y \in A$, $x \neq y$ such that $\phi_{a,b}(x) = \phi_{a,b}(y)$ (i.e. $\phi_{a,b}$ is not a bijection) then $(a, x) *_1 (b, z) = (a * b, \phi_{a,b}(x) + \psi_{a,b}(z) + \theta_{a,b}) = (a, y) *_1 (b, z)$. But this means that $R_{(b,z)}$ is not a bijection, i.e. $Q \times_{\phi,\psi,\theta} A$ is not latin.
If, on the other hand, $\phi_{a,b} \in Aut(A)$ for all $a, b \in Q$, we can easily define $L^{-1}_{(a,x)}$ and $R^{-1}_{(a,x)}$ for all $a \in Q$, $x \in A$ and hence, $Q \times_{\phi,\psi,\theta} A$ is latin.
We can obtain the rest of the lemma similarly as in the Lemma 7 using the equations that define mediality. □

Lemma 9. *Let $Q \times_{\phi,\psi,\theta} A$ be an abelian extension and let $\alpha \in Aut(A)$ then, $Q \times_{\phi,\psi,\theta} A$ is isomorph to $Q \times_{\alpha^{\phi}\alpha^{-1},\alpha\psi\alpha^{-1},\alpha\theta} A$.*

Proof. Let us consider the mapping $\Phi : Q \times_{\phi,\psi,\theta} A \to Q \times_{\alpha^{-1}\phi\alpha,\alpha^{-1}\psi\alpha,\alpha\theta} A$ defined by $\Phi((a, x)) = (a, \alpha(x))$. This is clearly a bijection. Moreover, we have $\Phi((a, x) * (b, y)) = \Phi((a *_Q b, \phi_{a,b}(x) + \psi_{a,b}(y) + \theta_{a,b})) = (a *_Q b, \alpha(\phi_{a,b}(x)) + \alpha(\psi_{a,b}(y)) + \alpha(\theta_{a,b})) = (a *_Q b, (\alpha\phi_{a,b}\alpha^{-1})(\alpha(x)) + (\alpha\psi_{a,b}\alpha^{-1})(\alpha(y)) + \alpha\theta_{a,b} = \Phi((a, x)) * \Phi((b, y))$. Hence, Φ is an isomorphism. □

The importance of the notion of central extensions of quandles for construction of selfdistributive quasigroups of prime power size can be clearly seen from the following theorem:

Theorem 10. *Let Q be a latin quandle of prime power size. Then, there exists a latin quandle E (with $|E| < |Q|$) and an abelian group A such that $Q \simeq E \times_{\phi,\psi,\theta} A$ for some abelian group A and ϕ, ψ, θ as in Definition 6.*

Proof. According to [1, Corollary 6.6] Q is nilpotent and hence there exists a chain of congruences $0_Q \leq \alpha_1 \leq \ldots \leq \alpha_n = 1_Q$ such that α_{i+1}/α_i is a central congruence of Q/α_i.
Let us assume that $\alpha_{i+1} \neq \alpha_i$ for all $i \in 0, 1, \ldots, n$ (otherwise, we can forget some of the congruences).
Then, $\alpha_1/\alpha_0 = \alpha_1$ is a central congruence of Q/α_1 and $|Q/\alpha_1| < |Q|$. Moreover, Q/α_1 is connected (because it is a latin quandle) and $Dis_{\alpha_1} = \langle L_a L_b^{-1} | a\alpha_1 b \rangle$ acts transitively on every block of α_1 because blocks of each congruence of an affine latin quandle are connected by the comment above [1, Proposition 7.8].
Then, $Q \simeq Q/\alpha_1 \times_{\phi,\psi,\theta} A$ for some abelian group A by [1, Proposition 7.8]. □

If we consider non-affine latin quandles, they are not central extensions of a trivial quandle (i.e. of a quandle with one element) because those extensions are only affine quandles as we can easily see from the conditions of Lemma 7.

There is surely no central extension of an arbitrary quandle Q by an abelian group of size 2 because there is only one abelian group of this size, namely $\mathbb{Z}_2$ and there is no $f \in Aut(\mathbb{Z}_2)$ such that $(1 - f) \in Aut(\mathbb{Z}_2)$. We know all the latin quandles of size ≤ 47 (all those quandles are stored in the RIG library [10]). Hence, we are able to obtain all non-affine latin quandles of size 2^k for $k \leq 7$ by constructing central extensions of smaller latin quandles that we already know. We will use this approach later in Chapter 3.

2. Construction of latin quandles of size 2^k

In this chapter, we will introduce the notion of Onoi structure. Then, we will use Onoi structures to construct several affine and non-affine latin quandles of size 2^k.

2.1 Onoi structures

Definition 7 (Onoi structure)**.** *We will say that an algebraical structure* $\mathbf{A} = (A, +, 0, \cdot, \alpha)$ *with two binary operations* $+, \cdot$*, a constant* 0 *and an unary operation* α *is an* Onoi structure *if it satisfies the following properties:*

- $(A, +, 0)$ *is an abelian group and* $a + a = 0$ *for all* $a \in A$*,*
- $\cdot$ *is left- and right-distributive with respect to* $+$*, i.e.* $a \cdot (b+c) = (a \cdot b)+(a \cdot c)$ *and* $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ *for all* $a, b, c \in A$*,*
- α *is an automorphism of the structure* $(A, +, 0, \cdot)$*,*
- $\alpha^2(a) + \alpha(a) + a = 0$ *for all* $a \in A$*,*
- $(\alpha(a) \cdot b) = (a \cdot \alpha(b))$ *for all* $a, b \in A$*.*

We call this structure an Onoi structure in honour of V. I. Onoi, who constructed two Onoi structures in 1970 (see [6]). We will introduce these examples later.

From the definition of an Onoi structure, we can obtain several properties of this structure that are summarized in the following lemma:

Lemma 11. *Let* $\mathbf{A} = (A, +, 0, \cdot, \alpha)$ *be an Onoi structure. Then following properties hold for all* $a, b, c \in A$*:*

- $0 \cdot a = a \cdot 0 = 0$*,*
- $\alpha^2(a) + \alpha(a) = a$*,*
- $\alpha^3 = 1_A$*,*
- *if* $|A| > 1$*, then* α, α^2 *and* 1_A *are different mappings,*
- $\alpha^2(a \cdot b) = (\alpha(a) \cdot b)$*,*
- $\alpha^2(a) \cdot b = a \cdot \alpha^2(b)$*,*
- $\alpha(a) \cdot (\alpha(b) \cdot c)) = a \cdot (b \cdot c)$*.*

Proof. Straightforward computation, we will show only the last property:
$\alpha(a) \cdot (\alpha(b) \cdot c)) = \alpha(a) \cdot (\alpha(b) \cdot \alpha^3(c)) = \alpha(a) \cdot \alpha(b \cdot \alpha^2(c)) = \alpha^2(a) \cdot (\alpha(b) \cdot \alpha(c)) = \alpha^2(a) \cdot \alpha(b \cdot c) = \alpha^3(a) \cdot (b \cdot c) = a \cdot (b \cdot c)$. □

From the properties in lemma 11, we can easily derive the following corollary:

Corollary. Let $\mathbf{A} = (A, +, 0, \cdot, \alpha)$ be an Onoi structure. Then, $(A, +, 0, \cdot, \alpha^2)$ is also an Onoi structure.

Obviously, the smallest non-trivial Onoi structure (i.e. $|A| > 1$) has at least 4 elements (we are not able to define 3 different automorphisms on an abelian group of smaller size then 4). We will construct a four-element Onoi structure in the following example:

Example (Onoi, 1970). Let $S = \{0, 1, 2, 3\}$ and let us define the operations $+, \cdot$ by the following tables:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	3	2
2	0	3	2	1
3	0	2	1	3

Let us define α as the permutation $(1, 2, 3)$, i.e. α is defined as follows: $\alpha(0) = 0$, $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 1$.
Obviously, $(S, +, 0)$ is an abelian group, because $(S, +, 0) \simeq \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$. We can easily verify also the rest of the axioms from definition 7 (we have a small commutative structure, therefore it is also possible to simply examine all possibilities for a, b and c).

We will denote the Onoi structure constructed in Example 2.1 by $\mathbf{S}$.

Let us denote the set of permutations on a set X by Σ_X. For a given Onoi structure $\mathbf{O} = (O, +, 0, \cdot, \alpha)$, $n \in \mathbb{N}$ and $\sigma \in \Sigma_{\{1,\dots,n\}}$ we can construct a structure $\mathbf{O}^n_\sigma = (O^n, +_n, 0_n, \cdot_\sigma, \alpha_n)$ as follows:

- $O^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in O, i = 1, 2, \dots, n\}$,
- $(a_1, a_2, \dots, a_n) +_n (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$,
- $0_n = (0, 0, \dots, 0)$,
- $(a_1, a_2, \dots, a_n) \cdot_\sigma (b_1, b_2, \dots, b_n) = (a_{\sigma(1)} \cdot b_1, a_{\sigma(2)} \cdot b_2, \dots, a_{\sigma(n)} \cdot b_n)$,
- $\alpha_n((a_1, a_2, \dots, a_n)) = (\alpha(a_1), \alpha(a_2), \dots, \alpha(a_n))$.

Lemma 12. *Let $n \in \mathbb{N}$, $\sigma \in S_n$. Then, $\mathbf{O}^n_\sigma$ is an Onoi structure.*

Proof. $(O^n, +_n, 0_n)$ is clearly an abelian group, because it is a product of abelian groups. All other properties from the definition 7 can be checked straightforward, we will show only the last one:

$$\begin{aligned}
&\alpha_n((a_1, a_2, \dots, a_n)) \cdot_\sigma (b_1, b_2, \dots, b_n) \\
&= (\alpha(a_1), \alpha(a_2), \dots, \alpha(a_n)) \cdot_\sigma (b_1, b_2, \dots, b_n) \\
&= (\alpha(a_{\sigma(1)}) \cdot b_1, \alpha(a_{\sigma(2)}) \cdot b_2, \dots, \alpha(a_{\sigma(n)}) \cdot b_n) \\
&= (a_{\sigma(1)} \cdot \alpha(b_1), a_{\sigma(2)} \cdot \alpha(b_2), \dots, a_{\sigma(n)} \cdot \alpha(b_n)) \\
&= (a_1, a_2, \dots, a_n) \cdot_\sigma \alpha_n((b_1, b_2, \dots, b_n))
\end{aligned}$$

□

Let $n \leq m$, $\sigma_1 \in \Sigma_{\{1,\dots,n\}}$, $\sigma_2 \in \Sigma_{\{n,\dots,m\}}$. Then, we can see the Onoi structure $\mathbf{O}^n_{\sigma_1}$ as a substructure of $\mathbf{O}^m_{\sigma_1 \cup \sigma_2}$ by taking an injective homomorphism $\iota : O^n \to O^m$ defined by $\iota(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_n, 0, \dots, 0)$ (it is clearly an injective mapping and it is easy to check that it is also a homomorphism). From now on, we will understand $\mathbf{O}^n_{\sigma_1}$ as an substructure of $\mathbf{O}^m_{\sigma_1 \cup \sigma_2}$ without explicitly mentioning it.

We will mention also another example of an Onoi structure that was constructed by Onoi in [6]:

Example (Onoi, 1970). Let $M_2(\mathbf{S})$ be the set of all 2×2 matrices over $\mathbf{S}$ (i.e. the matrix addition $+_2$ and multiplication $\cdot_2$ is given in the obvious way using the addition and multiplication in $\mathbf{S}$). Let us define $\alpha_2 : M_2(\mathbf{S}) \to M_2(\mathbf{S})$ by $\alpha_2((x_{ij})) = (\alpha(x_{ij}))$. Then, $(M_2(\mathbf{S}), +_2, 0_{2\times 2}, \cdot_2, \alpha_2)$ is an Onoi structure.

We can generalize this construction in a natural way for an arbitrary Onoi structure $\mathbf{O} = (O, +, 0, \cdot, \alpha)$, $n \in \mathbb{N}$ and $\sigma \in \Sigma_{\{1,\dots,n\}\times\{1,\dots,n\}}$: We will define the Onoi structure $M^\sigma_n(\mathbf{O}) = (M_n(O), +_n, 0_{n\times n}, \cdot^\sigma_n, \alpha_n)$ by taking the standard matrix addition $+_n$, $\alpha_n(x_{ij}) = (\alpha(x)_{ij})$ and $((x_{ij}) \cdot^\sigma_n (y_{kl})) = ((\sum_{j=1}^n x_{\sigma(i,j)} \cdot y_{jk})_{ik})$. We will not prove that this is in fact an Onoi structure but the proof is straightforward and similar to the proof of Lemma 12.

2.2 Construction of latin quandles from Onoi structures

Let $\mathbf{O}$ be an Onoi structure and let $Aff(O, \alpha) = (O, *)$ be an affine quandle. Then, $a * b = (1 - \alpha)(a) + \alpha(b) = a + \alpha(a) + \alpha(b) = \alpha^2(a) + \alpha(a)$ (we use the properties of an Onoi structure). Moreover, $(O, *)$ is a latin quandle because $(1 - \alpha) = \alpha^2 \in Aut((O, +, 0))$.

Let $\mathbf{O} = (O, +, 0, \cdot, \alpha)$ be an Onoi structure and let us define the mapping $\theta : O^3 \to O$ by $\theta(a, b, c) = a \cdot (b \cdot c)$. Then, we can easily show (using definition 7 and lemma 11) that θ has the following properties (for all $a, b, c, d \in O$):

- $\theta(a + b, c, d) = \theta(a, c, d) + \theta(b, c, d)$, $\theta(a, b + c, d) = \theta(a, b, d) + \theta(a, c, d)$, $\theta(a, b, c + d) = \theta(a, b, c) + \theta(a, b, d)$,
- $\theta(0, b, c) = \theta(a, 0, c) = \theta(a, b, 0) = 0$,
- $\alpha(\theta(a, b, c)) = \theta(\alpha(a), \alpha(b), \alpha(c))$,
- $\theta(\alpha(a), b, c) = \theta(a, \alpha(b), \alpha(c))$,
- $\theta(a, \alpha(b), c) = \theta(a, b, \alpha(c))$.

We will generalize those properties for mappings between two Onoi structures in the following definition:

Definition 8 (Onoi mapping)**.** *Let* $\mathbf{O_1}$ *and* $\mathbf{O_2}$ *be two Onoi structures. We say that a mapping* $\theta : O_1^3 \to O_2$ *is an* Onoi mapping *if it has the following properties*

for all $a, b, c, d \in O_1$*:*

$$\begin{aligned}\theta(a +_1 b, c, d) &= \theta(a, c, d) +_2 \theta(b, c, d),\\ \theta(a, b +_1 c, d) &= \theta(a, b, d) +_2 \theta(a, c, d),\\ \theta(a, b, c +_1 d) &= \theta(a, b, c) +_2 \theta(a, b, d),\end{aligned} \tag{2.1}$$

$$\alpha_2(\theta(a, b, c)) = \theta(\alpha_1(a), \alpha_1(b), \alpha_1(c)), \tag{2.2}$$

$$\theta(\alpha_1(a), b, c) = \theta(a, \alpha_1(b), \alpha_1(c)), \tag{2.3}$$

$$\theta(a, \alpha_1(b), c) = \theta(a, b, \alpha_1(c)). \tag{2.4}$$

It holds also that $\theta(0, b, c) = \theta(a, 0, c) = \theta(a, b, 0) = 0$ because $\theta(0, b, c) = \theta(0 + 0, b, c) = \theta(0, b, c) + \theta(0, b, c)$ and by subtracting $\theta(0, b, c)$ from both sides we get that $\theta(0, b, c) = 0$ and we can show similarly that $\theta(a, 0, c) = \theta(a, b, 0)$. It is also easy to show that the properties from the previous definition hold for α_1^2 and α_2^2 instead of α_1 and α_2.

Lemma 13. *Let* $\mathbf{O_1} = (O_1, +_1, 0_1, \cdot_1, \alpha_1)$ *and* $\mathbf{O_2} = (O_2, +_2, 0_2, \cdot_2, \alpha_2)$ *be two Onoi structures and let* $\theta : O_1^3 \to O_2$ *be an Onoi mapping. Let us define* $A(\mathbf{O_2}) = (O_2, +_2, 0_2)$ *and* $\theta^*_{a,b} = \theta(a, a +_1 b, a +_1 b)$ *for* $a, b \in O_1$*. Then, the central extension* $Aff(O_1, \alpha_1) \times_{\alpha_2^2, \alpha_2, \theta^*} A(\mathbf{O_2}) = (O_1 \times O_2, *)$ *is a latin quandle.*

Proof. For simplicity, we will not use the indexes by α and $\cdot$ if it will be clear, in which structure are we working. Let us also denote the quandle operation in $Aff(O_1, \alpha)$ by $\circ$. We will verify the conditions from lemma 7:

For (1.1) we have for all $a, b, c \in O_1$:

$$\begin{aligned}&\alpha_2(\theta^*_{b,c}) +_2 \theta^*_{a,b\circ c}\\ &= \alpha(\theta(b, b + c, b + c)) + \theta(a, a + \alpha^2(b) + \alpha(c), a + \alpha^2(b) + \alpha(c)\\ &= \theta(\alpha^2(b), b + c, b + c) + \theta(a, a + \alpha^2(b) + \alpha(c), a + \alpha^2(b) + \alpha(c)\\ &= \theta(\alpha^2(b), b + c, b + c) + \theta(a, a, a) + \theta(a, a, \alpha^2(b))\\ &+\theta(a, a, \alpha(c)) + \theta(a, \alpha^2(b), a) + \theta(a, \alpha^2(b), \alpha^2(b)) + \theta(a, b, c)\\ &+\theta(a, \alpha(c), a) + \theta(a, c, b) + \theta(a, \alpha(c), \alpha(c))\\ &= \theta(\alpha^2(b), b + c, b + c)\\ &+\theta(\alpha^2(a), c, c) + \theta(\alpha^2(a), c, a) + \theta(\alpha^2(a), a, c) + \theta(\alpha^2(a), a, a)\\ &+\theta(\alpha(a), a, a) + \theta(\alpha(a), a, b) + \theta(\alpha(a), b, a) + \theta(\alpha(a), b, b)\\ &+\theta(a, c, c) + \theta(a, c, b) + \theta(a, b, c) + \theta(a, b, b)\\ &= \theta(\alpha^2(a), c + a, c + a) + \theta(\alpha(a), a + b, a + b)\\ &+\theta(\alpha^2(b), b + c, b + c) + \theta(a, b + c, b + c)\\ &= \alpha(\theta(a, a + c, a + c)) + \alpha^2(\theta(a, a + b, a + b))\\ &+\theta(\alpha^2(a) + \alpha(b), \alpha^2(a) + \alpha(c) + \alpha^2(a) + \alpha(b), \alpha^2(a) + \alpha(c) + \alpha^2(a) + \alpha(b))\\ &= \alpha_2(\theta^*_{a,c}) +_2 \alpha_2^2(\theta^*_{a,b}) +_2 \theta^*_{a\circ b, a\circ c}\end{aligned}$$

(1.2) holds automatically because $\psi_{a,b}$ (from definition 6) is equal to α_2 and hence it is a constant mapping (i.e. the same mapping for all $a, b \in O_1$).

For (1.3): $\alpha_2 \circ \alpha_2^2 = \alpha_2^3 = \alpha_2^2 \circ \alpha_2$.

For (1.4): $\alpha_2^2 = \alpha_2 + 1_{O_2} = \alpha_2^2 \circ \alpha_2^2 + \alpha_2 \circ \alpha_2^2$.

For (1.5): $\theta^*_{a,a} = \theta(a, a+a, a+a) = \theta(a, 0, 0) = 0$ for all $a \in O_1$.

For (1.6): $\alpha_2^2 + \alpha_2 = 1_{O_2}$ by the definition of Onoi structure.

Hence, $(O_1 \times O_2, *)$ is a quandle by the Lemma 7 and since α_2^2 is an automorphism, it is also a latin quandle by Lemma 8. □

We will denote the quandle constructed in lemma 13 by $\mathscr{Q}(\mathbf{O_1}, \mathbf{O_2}, \theta)$.

Let us examine the inverse to $L_{(b,y)}$ in $(O_1 \times O_2, *)$ from the previous lemma (this inverse exists since $(O_1 \times O_2, *)$ is a (latin) quandle): Let us define $M_{(b,y)} : O_1 \times O_2 \to O_1 \times O_2$ by $M_{(b,y)}(a, x) = (\alpha_1(b) + \alpha_1^2(a),$
$\alpha_2(y) + \alpha_2^2(x) + \theta(b, a+b, a+b))$. We will prove that $M_{(b,y)}$ is a left inverse to $L_{(b,y)}$ (where $L_{(b,y)}(a, x) = (b, y) * (a, x)$) for all $(b, y) \in O_1 \times O_2$:

Let $(a, x), (b, y) \in O_1 \times O_2$. Then:

$$\begin{aligned} &M_{(b,y)}(L_{(b,y)}(a, x)) \\ &= M_{(b,y)}(\alpha_1^2(b) + \alpha_1(a), \alpha_2^2(y) + \alpha_2(x) + \theta(b, a+b, a+b)) \\ &= (\alpha_1(b) + \alpha_1(b) + a, \alpha_2(y) + \alpha_2(y) + x \\ &+\alpha_2^2(\theta(b, a+b, a+b)) + (\theta(b, \alpha_1^2(b) + \alpha_1(a) + b, \alpha_1^2(b) + \alpha_1(a) + b))) \\ &= (a, x + \theta(\alpha_1(a), \alpha_1(a+b), \alpha_1(a+b)) + \theta(\alpha_1(a), \alpha_1(a+b), \alpha_1(a+b))) = (a, x) \end{aligned}$$

Hence, $M_{(b,y)}$ is the desired inverse to $L_{(b,y)}$, i.e. $L^{-1}_{(b,y)} = (\alpha_1(b) + \alpha_1^2(a), \alpha_2(y) + \alpha_2^2(x) + \theta(b, a+b, a+b))$.

Lemma 14. *Let* $\mathbf{O_1} = (O_1, +_1, 0_1, \cdot_1, \alpha_1)$ *and* $\mathbf{O_2} = (O_2, +_2, 0_2, \cdot_2, \alpha_2)$ *be two Onoi structures and let* $\theta : O_1^3 \to O_2$ *be an Onoi mapping. Then, the quandle* $\mathscr{Q}(\mathbf{O_1}, \mathbf{O_2}, \theta)$ *is affine if and only if the following two equations hold for all* $a, b, c \in O_1$*:*

$$\theta(a, b, b) = \theta(b, a, a), \tag{2.5}$$

$$\theta(a, b, c) = \theta(a, c, b). \tag{2.6}$$

Proof. For simplicity, we will not use the indexes by α and $\cdot$ in the whole proof if it will be clear, in which structure are we working.

We will use lemma 7 and prove that $Dis(\mathscr{Q}(\mathbf{O_1}, \mathbf{O_2}, \theta))$ is abelian if and only if the conditions 2.5 and 2.6 hold. A group is abelian if and only if all its generators commute. Hence, the quandle $\mathscr{Q}(\mathbf{O_1}, \mathbf{O_2}, \theta)$ is affine if and only if for all $a, b, c, d, u \in O_1$, $w, x, y, z, v \in O_2$:

$$L_{(a,w)} \circ L^{-1}_{(b,x)} \circ L_{(c,y)} \circ L^{-1}_{(d,z)}(u, v) = L_{(c,y)} \circ L^{-1}_{(d,z)} \circ L_{(a,w)} \circ L^{-1}_{(b,x)}(u, v)$$

Let $a, b, c, d, u \in O_1$, $w, x, y, z, v \in O_2$ be arbitrary. Then, the left side gives us:

$$
\begin{aligned}
&L_{(a,w)} \circ L^{-1}_{(b,x)} \circ L_{(c,y)} \circ L^{-1}_{(d,z)}((u,v)) \\
&= L_{(a,w)} \circ M_{(b,x)} \circ L_{(c,y)} \circ M_{(d,z)}((u,v)) \\
&= L_{(a,w)} \circ M_{(b,x)} \circ L_{(c,y)}((\alpha(d)+\alpha^2(u), \alpha(z)+\alpha^2(v)+\theta(d,d+u,d+u)) \\
&= L_{(a,w)} \circ M_{(b,x)}(\alpha^2(c)+\alpha^2(d)+u, \alpha^2(y)+\alpha^2(z)+v+\theta(\alpha^2(d),d+u,d+u)) \\
&\quad +\theta(c,\alpha(d)+\alpha^2(u)+c,\alpha(d)+\alpha^2(u)+c))) \\
&= L_{(a,w)}((\alpha(b)+\alpha(c)+\alpha(d)+\alpha^2(u), \alpha(x)+\alpha(y)+\alpha(z)+\alpha^2(v) \\
&\quad +\theta(d,d+u,d+u)) + \theta(\alpha(c),\alpha(d)+\alpha^2(u)+c,\alpha(d)+\alpha^2(u)+c)) \\
&\quad +\theta(b,b+\alpha^2(c)+\alpha^2(d)+u,b+\alpha^2(c)+\alpha^2(d)+u))) \\
&= (\alpha^2(a)+\alpha^2(b)+\alpha^2(c)+\alpha^2(d)+u, \alpha^2(w)+\alpha^2(x)+\alpha^2(y)+\alpha^2(z)+v \\
&\quad +\theta(\alpha^2(d),d+u,d+u)) + \theta(c,\alpha(d)+\alpha^2(u)+c,\alpha(d)+\alpha^2(u)+c)) \\
&\quad +\theta(\alpha^2(b),b+\alpha^2(c)+\alpha^2(d)+u,b+\alpha^2(c)+\alpha^2(d)+u) \\
&\quad +\theta(a,a+\alpha(b)+\alpha(c)+\alpha(d)+\alpha^2(u),a+\alpha(b)+\alpha(c)+\alpha(d)+\alpha^2(u)))
\end{aligned}
$$

Similarly, the right side gives:

$$
\begin{aligned}
&L_{(a,w)} \circ L^{-1}_{(b,x)} \circ L_{(c,y)} \circ L^{-1}_{(d,z)}((u,v)) \\
&= (\alpha^2(c)+\alpha^2(d)+\alpha^2(a)+\alpha^2(b)+u, \alpha^2(y)+\alpha^2(z)+\alpha^2(w)+\alpha^2(x)+v \\
&\quad +\theta(\alpha^2(b),b+u,b+u)) + \theta(a,\alpha(b)+\alpha^2(u)+a,\alpha(b)+\alpha^2(u)+a)) \\
&\quad +\theta(\alpha^2(d),d+\alpha^2(a)+\alpha^2(b)+u,d+\alpha^2(a)+\alpha^2(b)+u) \\
&\quad +\theta(c,c+\alpha(d)+\alpha(a)+\alpha(b)+\alpha^2(u),c+\alpha(d)+\alpha(a)+\alpha(b)+\alpha^2(u)))
\end{aligned}
$$

These expressions are equal if and only if:

$$
\begin{aligned}
&\theta(\alpha^2(b),\alpha(c),c) + \theta(\alpha^2(b),\alpha(d),d) + \theta(\alpha^2(b),\alpha^2(c),u) + \theta(\alpha^2(b),\alpha(c),d) \\
&+\theta(\alpha^2(b),\alpha^2(c),b) + \theta(\alpha^2(b),u,\alpha^2(c)) + \theta(\alpha^2(b),u,\alpha^2(d)) + \theta(\alpha^2(b),\alpha(d),c) \\
&+\theta(\alpha^2(b),\alpha^2(d),u) + \theta(\alpha^2(b),\alpha^2(d),b) + \theta(\alpha^2(b),b,\alpha^2(c)) + \theta(\alpha^2(b),b,\alpha^2(d)) \\
&+\theta(a,\alpha^2(c),c) + \theta(a,\alpha^2(d),d) + \theta(a,c,u) + \theta(a,\alpha^2(c),d) \\
&+\theta(a,\alpha^2(c),b) + \theta(a,\alpha(c),a) + \theta(a,u,c) + \theta(a,u,d) \\
&+\theta(a,\alpha^2(d),c) + \theta(a,d,u) + \theta(a,\alpha^2(d),b) + \theta(a,\alpha(d),a) \\
&+\theta(a,\alpha^2(b),c) + \theta(a,\alpha^2(b),d) + \theta(a,a,\alpha(c)) + \theta(a,a,\alpha(d)) \\
&= \theta(\alpha^2(d),\alpha(a),a) + \theta(\alpha^2(d),\alpha(b),b) + \theta(\alpha^2(d),\alpha^2(a),u) + \theta(\alpha^2(d),\alpha(a),b) \\
&+\theta(\alpha^2(d),\alpha^2(a),d) + \theta(\alpha^2(d),u,\alpha^2(a)) + \theta(\alpha^2(d),u,\alpha^2(b)) + \theta(\alpha^2(d),\alpha(b),a) \\
&+\theta(\alpha^2(d),\alpha^2(b),u) + \theta(\alpha^2(d),\alpha^2(b),d) + \theta(\alpha^2(d),d,\alpha^2(a)) + \theta(\alpha^2(d),d,\alpha^2(b)) \\
&+\theta(c,\alpha^2(a),a) + \theta(c,\alpha^2(b),b) + \theta(c,a,u) + \theta(c,\alpha^2(a),b) \\
&+\theta(c,\alpha^2(a),d) + \theta(c,\alpha(a),c) + \theta(c,u,a) + \theta(c,u,b) \\
&+\theta(c,\alpha^2(b),a) + \theta(c,b,u) + \theta(c,\alpha^2(b),d) + \theta(c,\alpha(b),c) \\
&+\theta(c,\alpha^2(d),a) + \theta(c,\alpha^2(d),b) + \theta(c,c,\alpha(a)) + \theta(c,c,\alpha(b))
\end{aligned}
\tag{2.7}
$$

Assume that $\mathscr{Q}(\mathbf{O_1}, \mathbf{O_2}, \theta)$ is affine, i.e. $Dis(\mathscr{Q}(\mathbf{O_1}, \mathbf{O_2}, \theta))$ is abelian. Then, the equation 2.7 holds for all a, b, c, d, u.

We can express this equation as $g^1_{a,b,c,d}(u) + f^1_{a,b,c,d} = g^2_{a,b,c,d}(u) + f^2_{a,b,c,d}$ for some mappings $g^1_{a,b,c,d}$ and $g^2_{a,b,c,d}$ and constants $f^1_{a,b,c,d}$, $f^2_{a,b,c,d}$ depending on $a, b, c, d,$

where $g^1_{a,b,c,d}(0) = g^2_{a,b,c,d}(0) = 0$. If the quandle $\mathscr{Q}(\mathbf{O_1}, \mathbf{O_2}, \theta)$ is affine, then $g^1_{a,b,c,d} = g^2_{a,b,c,d}$ and $f^1_{a,b,c,d} = f^2_{a,b,c,d}$. We will compare $g^1_{a,b,c,d}$ and $g^2_{a,b,c,d}$:

$$\begin{aligned}
&\theta(\alpha^2(b), \alpha^2(c), u) + \theta(\alpha^2(b), u, \alpha^2(c)) + \theta(\alpha^2(b), u, \alpha^2(d)) + \theta(\alpha^2(b), \alpha^2(d), u) \\
&\qquad + \theta(a, c, u) + \theta(a, u, c) + \theta(a, u, d) + \theta(a, d, u) \\
&= \theta(\alpha^2(d), u, \alpha^2(a)) + \theta(\alpha^2(d), \alpha^2(a), u) + \theta(\alpha^2(d), u, \alpha^2(b)) + \theta(\alpha^2(d), \alpha^2(b), u) \\
&\qquad + \theta(c, a, u) + \theta(c, u, a) + \theta(c, u, b) + \theta(c, b, u)
\end{aligned}$$

This has to hold for all $a, b, c, d \in O_1$, i.e. we can set $a = 0$ and $c = \alpha(d)$:

$$\begin{aligned}
&\theta(\alpha^2(b), d, u) + \theta(\alpha^2(b), u, d) + \theta(\alpha^2(b), u, \alpha^2(d)) + \theta(\alpha^2(b), \alpha^2(d), u) \\
&= \theta(\alpha^2(d), u, \alpha^2(b)) + \theta(\alpha^2(d), \alpha^2(b), u) + \theta(\alpha(d), u, b) + \theta(\alpha(d), b, u)
\end{aligned}$$

This holds if and only if:

$$\theta(\alpha^2(b), \alpha(d), u) + \theta(\alpha^2(b), u, \alpha(d)) = \theta(\alpha(d), u, \alpha^2(b)) + \theta(\alpha(d), \alpha^2(b), u)$$

By setting $e = \alpha^2(b)$ and $f = \alpha(d)$ (α is an automorphism) we get that the equation

$$\theta(e, f, u) + \theta(e, u, f) = \theta(f, u, e) + \theta(f, e, u) \tag{2.8}$$

holds for all $e, f, u \in O_1$

Now, we are able to simplify (2.7) (we use also the identity $\theta(a, b, a) = \theta(a, a, b)$ which can easily be derived from (2.8)):

$$\begin{aligned}
&\theta(\alpha^2(b), \alpha(c), c) + \theta(\alpha^2(b), \alpha(d), d) + \theta(\alpha^2(b), \alpha(c), d) + \theta(\alpha^2(b), \alpha(d), c) \\
&\qquad + \theta(a, \alpha^2(c), c) + \theta(a, \alpha^2(d), d) + \theta(a, \alpha^2(d), b) + \theta(a, \alpha^2(b), d) \\
&= \theta(\alpha^2(d), \alpha(a), a) + \theta(\alpha^2(d), \alpha(b), b) + \theta(\alpha^2(d), \alpha(a), b) + \theta(\alpha^2(d), \alpha(b), a) \\
&\qquad + \theta(c, \alpha^2(a), a) + \theta(c, \alpha^2(b), b) + \theta(c, \alpha^2(b), d) + \theta(c, \alpha^2(d), b)
\end{aligned} \tag{2.9}$$

We set $b = 0$, $c = 0$ and we get that: $\theta(a, \alpha^2(d), d) = \theta(\alpha^2(d), \alpha(a), a)$ and hence $\theta(a, \alpha(d), \alpha(d) = (\theta(\alpha(d), a, a)$ and hence (2.5) holds.

We will simplify (2.9) further:

$$\begin{aligned}
&\theta(\alpha^2(b), \alpha(c), d) + \theta(\alpha^2(b), \alpha(d), c) + \theta(a, \alpha^2(d), b) + \theta(a, \alpha^2(b), d) \\
&= \theta(\alpha^2(d), \alpha(a), b) + \theta(\alpha^2(d), \alpha(b), a) + \theta(c, \alpha^2(b), d) + \theta(c, \alpha^2(d), b)
\end{aligned}$$

We set $c = 0$ and we get:

$$\theta(a, \alpha^2(d), b) + \theta(a, \alpha^2(b), d) = \theta(\alpha^2(d), \alpha(a), b) + \theta(\alpha^2(d), \alpha(b), a) \tag{2.10}$$

By (2.8) we get that:

$$\theta(a, \alpha^2(d), b) + \theta(a, \alpha^2(b), d) = \theta(\alpha^2(d), a, b) + \theta(\alpha^2(d), b, a)$$

And therefore we get from (2.10) that $\theta(\alpha^2(d), \alpha^2(a), b) = \theta(\alpha^2(d), b, \alpha^2(a))$ and hence (2.6) holds.

On the other hand, if (2.5) and (2.6) hold, we can easily simplify the equation (2.7) to the form $0 = 0$ and therefore in this case $Dis(\mathscr{Q}(\mathbf{O_1}, \mathbf{O_2}, \theta))$ is abelian and hence is $\mathscr{Q}(\mathbf{O_1}, \mathbf{O_2}, \theta)$ an affine quandle. The lemma is proven.

□

Now, we are able to construct non-affine latin quandle of size 2^{2k} for $k = 4, 5, 6, 7, \ldots$:

Recall that $\mathbf{S}$ denotes the Onoi structure constructed in example 2.1 and that $\mathbf{O}^{\mathbf{n}}_{\sigma}$ denotes the Onoi structure constructed from an Onoi structure $\mathbf{O}$ by taking the set O^n, where all the operations are given by operations in $\mathbf{O}$ and the multiplication is given by $(a_1, a_2, \ldots, a_n) \cdot_\sigma (b_1, b_2, \ldots, b_n) = (a_{\sigma(1)} \cdot b_1, a_{\sigma(2)} \cdot b_2, \ldots, a_{\sigma(n)} \cdot b_n)$, where $\cdot$ denotes multiplication in $\mathbf{O}$.

Let $k \in \mathbb{N}$, $k \geq 4$. Let $m, n \in \mathbb{N}$, $m, n \geq 2$ such that $m \leq n$ and $m+n = k$. Let us denote by e^l_i the element of S^l that consists of zeros except on the i-th position where it has 1. Let $\sigma_1 \in \Sigma_{\{1,2,\ldots,m\}}$, $\sigma_2 \in \Sigma_{\{n+1,\ldots,m\}}$ such that $\sigma_1 \neq 1_{\{1,2,\ldots,m\}}$. Let us define $\theta : S^m \times S^m \times S^m \to S^n$ by $\theta(a, b, c) = a \cdot_{\sigma_1} (b \cdot_{\sigma_1} c)$. Then, $\mathscr{Q}(\mathbf{S}^{\mathbf{m}}_{\sigma_1}, \mathbf{S}^{\mathbf{n}}_{\sigma_1 \cup \sigma_2}, \theta)$ is a latin quandle by lemma 13 (because θ is clearly an Onoi mapping by the comment above the definition 8).

Let $i \in \{1, 2, \ldots, n\}$ be such that $\sigma_1(i) \neq i$. Then, $\theta(e^m_i, e^m_i, e^m_{\sigma_1(i)}) = e^m_i \cdot_{\sigma_1} (e^m_i \cdot_{\sigma_1} e^m_{\sigma_1(i)}) = e^m_i \cdot_{\sigma_1} e^m_{\sigma_1(i)} = e^m_{\sigma_1(i)} \neq (0, \ldots, 0)$. If $\sigma_1^2(i) = i$ then $\theta(e^m_i, e^m_{\sigma_1(i)}, e^m_i) = e^m_i \cdot_{\sigma_1} (e^m_{\sigma_1(i)} \cdot_{\sigma_1} e^m_i) = e^m_i \cdot_{\sigma_1} e^m_i = (0, \ldots, 0)$ (because $\sigma_1(i) \neq i$). Otherwise (i.e. $\sigma_1^2(i) \neq i$), $\theta(e^m_i, e^m_{\sigma_1(i)}, e^m_i) = e^m_i \cdot_{\sigma_1} (e^m_{\sigma_1(i)} \cdot_{\sigma_1} e^m_i) = e^m_i \cdot_{\sigma_1} (0, \ldots, 0) = (0, \ldots, 0)$. This means that the condition (2.6) from lemma 14 is not satisfied and hence $\mathscr{Q}(\mathbf{S}^{\mathbf{m}}_{\sigma_1}, \mathbf{S}^{\mathbf{n}}_{\sigma_1 \cup \sigma_2}, \theta)$ is a non-affine latin quandle.

We are able to construct also a non-affine quandle of size 2^6:

Let us define $\theta : S^2 \times S^2 \times S^2 \to S$ by $\theta((a, b), (c, d), (e, f)) = b \cdot (d \cdot e)$, where $\cdot$ denotes multiplication in $\mathbf{S}$. We will prove that this is an Onoi mapping. Let $a, b, c, d, e, f, g, h \in S$. Then:

- For (2.1) we have: $\theta((a, b) +_2 (c, d), (e, f), (g, h)) = (b + d) \cdot (f \cdot g) = b \cdot (f \cdot g) + d \cdot (f \cdot g) = \theta((a, b), (e, f), (g, h)) + \theta((c, d), (e, f), (g, h))$, we can easily show this property also for the other components of θ,
- for (2.2): $\alpha(\theta((a, b), (c, d), (e, f))) = \alpha(b \cdot (d \cdot e)) = (\alpha(b)) \cdot (\alpha(d) \cdot (\alpha(e)) = \theta(\alpha_2((a, b)), \alpha_2((c, d)), \alpha_2((e, f)))$,
- for (2.3): $\theta(\alpha_2((a, b)), (c, d), (e, f)) = \alpha(b) \cdot (d \cdot e) = b \cdot \alpha(d \cdot e) = b \cdot (\alpha(d) \cdot \alpha(e)) = \theta((a, b), \alpha_2((c, d)), \alpha_2((e, f)))$,
- for (2.4): $\theta((a, b), \alpha_2((c, d)), (e, f)) = b \cdot (\alpha(d) \cdot e) = b \cdot (d \cdot \alpha(e))$ $= \theta((a, b), (c, d), \alpha_2((e, f)))$.

This means that θ is an Onoi mapping. Hence, $\mathscr{Q}(\mathbf{S}^{\mathbf{2}}_{\mathbf{id}}, \mathbf{S}, \theta)$ is a latin quandle by lemma 13.

We have $\theta((0, 1), (0, 1), (1, 0)) = 1 \cdot (1 \cdot 1) = 1 \cdot 1 = 1$. On the other hand, $\theta((0, 1), (1, 0), (0, 1)) = 1 \cdot (0 \cdot 0) = 1 \cdot 0 = 0$. Hence, the condition (2.6) from Lemma 14 is not satisfied and therefore $\mathscr{Q}(\mathbf{S}^{\mathbf{2}}_{\mathbf{id}}, \mathbf{S}, \theta)$ is a non-affine latin quandle.

We have proved the following key theorem:

Theorem 15. *Let $k \in \mathbb{N}$, $k \geq 3$. Then, there exists a non-affine latin quandle of size 2^{2k}.*

Proof. If $n \geq 4$, we can take $m = 2$, $n = k - 2$ and $\sigma_1 = (1, 2)$. Then, $\mathscr{Q}(\mathbf{S}^{\mathbf{m}}_{\sigma_1}, \mathbf{S}^{\mathbf{n}}_{\sigma_1 \cup \sigma_2}, \theta)$ is a non-affine latin quandle as we showed above. If $n = 3$ then $\mathscr{Q}(\mathbf{S}^{\mathbf{2}}_{\mathbf{id}}, \mathbf{S}, \theta)$, where $\theta((a, b), (c, d), (e, f)) = b \cdot (d \cdot e)$, is a non-affine latin quandle (see construction above). □

3. Classification of non-affine latin quandles of size 2^k

We saw in the previous chapter that there exists non-affine latin quandle of size 2^{2k} for $k \geq 3$.

By looking into the RIG library [10] where all quandles of size ≤ 47 are stored we can see that there exists no non-affine latin quandle of size 2^k for $k \leq 5$. Hence, the quandle constructed above the Theorem 15 is the smallest non-affine latin quandle of size 2^k.

We can also easily construct non-affine latin quandle of size 2^k for k odd, $k \geq 9$ by taking one of the affine latin quandles of size 2^3 from the RIG library and non-affine latin quandle of size 2^{k-3} that exists by Theorem 15 and constructing their direct product. The existence of non-affine latin quandle of size 2^k for k even, $k \geq 6$ follows directly from this theorem.

Now, we are left with the question whether there exists also a non-affine latin quandle of size 2^7. In order to answer this question, we will use central extensions that were introduced in the first chapter. With the help of central extensions, we will be also able to better understand the structure of non-affine latin quandles of size 2^6.

3.1 Algorithm for finding central extensions

By Theorem 10 and by the comment under this theorem, we are able to construct all non-affine latin quandles of size 2^7 by constructing central extensions of latin quandles of size 2^k for $k \leq 5$.

We will introduce algorithm for finding central extensions that are latin quandles of size 2^7. This algorithm can easily be modified also for quandles of size 2^k for arbitrary $k \in \mathbb{N}$.

Let us denote the cyclic group with k elements by $\mathbf{C_k}$ and we will denote its elements by $0, 1, \ldots, k-1$.

Lemma 7 and Lemma 8 says that we can construct a central extension that is a latin quandle only from abelian groups A that have an automorphism ϕ such that $\psi = 1_A - \phi$ is also an automorphism.

This is certainly not possible for groups of the type $\mathbf{C}_{2^{k_1}} \times \mathbf{C}_{2^{k_2}} \times \ldots \mathbf{C}_{2^{k_n}}$ where $k_1 > k_2 \geq \ldots \geq k_n$ because each automorphism ϕ has to map the element $(1, 0, \ldots, 0)$ of order 2^{k_1} to another element of order 2^{k_1} and all such elements are obviously of the form $(a_1, a_2, \ldots, a_n)$ with a_1 odd. Hence, $\phi(1, 0, \ldots, 0) = (a_1, \ldots, a_n)$ where a_1 is odd. But $(1_A - \phi)(1, 0, \ldots, 0) = (1 - a_1, -a_2, \ldots, -a_n)$ and $1 - a_1$ is clearly even and hence $1_A - \phi$ is not an automorphism.

Hence, the only abelian groups that could provide us with a central extension that is a non-affine latin quandle of size 2^7 are $\mathbf{C}_2^k$ for $1 < k \leq 5$, $\mathbf{C}_4 \times \mathbf{C}_4$ and $\mathbf{C}_4 \times \mathbf{C}_4 \times \mathbf{C}_2$. We can exclude the case $A = \mathbf{C}_4 \times \mathbf{C}_4 \times \mathbf{C}_2$ either by looking on all automorphisms of A (up to conjugation) and finding out that there is no $\phi \in Aut(A)$ such that $(1 - \phi) \in Aut(A)$ or by using the canonical embedding mentioned above Lemma 8, using the fact that there is no affine

quandle $Aff(A, f)$ (it can be seen in the RIG library) and using that $Aff(A, f)$ is determined uniquely by the group A (see Theorem 1).

3.1.1 Abelian groups $\mathbf{C}_2^k$

The automorphism group of $\mathbf{C}_2^k$ is exactly the group $GL_k(2)$ of regular $k \times k$ matrices over $\mathbb{Z}_2$. By Lemma 9, we can examine only representatives of conjugation classes of $GL_k(2)$, as we want to examine non-affine latin quandles only up to isomorphism (we actually want to find out whether there exists any non-affine latin quandle of size 2^7). Moreover, by 8 we have to examine only matrices $A \in GL_k(2)$ that are representatives of conjugation classes for that it holds that $(I_k - A) \in GL_k(2)$, where I_k denotes the identity matrix.

Hence, given an affine quandle Q of size 2^k and $A \in GL_k(2)$, Lemma 7 provides us with a set of equations for $\theta_{a,b} \in C_2^{7-k}$, $a, b \in Q$. This means that we are actually solving a system of linear equations for the vector $\theta = ((\theta_{1,1})_1, \ldots, (\theta_{1,1})_{7-k}, (\theta_{1,2})_1, \ldots, (\theta_{2^k,2^k})_{7-k})$ that has $2^{2k}(7-k)$ elements over C_2. These equations are given by the condition $\theta_{a,a} = 0$, i.e. $(\theta_{a,a})_i = 0$ for all $a \in Q$, $i \in 1, \ldots, 7-k$ and by the equation (1.1) (we set $\phi = A$, $\psi = I_k - A$), i.e. $(I_k - A)(\theta_{b,c}) + \theta_{a,b*c} = (I_k - A)(\theta_{a,c}) + A(\theta_{a,b}) + \theta_{a*b,a*c}$ for all $a, b, c \in Q$. The rest of the equations from Lemma 7 is clearly satisfied.

We can solve this system efficiently on the computer (we implemented it using the GAP system [4], this system enabled us also to work easily with representatives of conjugation classes). We will get a vector space consisting of all solutions θ of this system. Now, we have to find out, if each basis element of this space satisfies also all the equations from Lemma 8 stating that the central extension $Q \times_{A, I_k - A, \theta}$ is an affine quandle, i.e. equations $A(\theta_{a,b}) + (I_k - A)(\theta_{c,d}) + \theta_{a*b,c*d} = A(\theta_{a,c}) + (I_k - A)(\theta_{b,d}) + \theta_{a*c,b*d}$ for all $a, b, c, d \in Q$ (the other equations from Lemma 8 are clearly satisfies).

If those equations are satisfied by all basis elements, there exists no central extension of Q by A that is a non-affine latin quandle, otherwise we find such a quandle.

3.1.2 Abelian group $\mathbf{C}_4^2$

We can use the same method as in the previous subsection. The only difference is that we will be working with matrices over $\mathbf{C}_4$ (automorphisms of $\mathbf{C}_4^2$ are given by some 2×2 matrices over $\mathbf{C_4}$). This means that we are not able to use the methods for solving linear equations over fields.

We are able to solve this problem by transforming it to solving linear equations over integers (the algorithm for solving those equations is provided in the GAP system) as we can see from the following lemma (it is a simplification of the approach described in [3, Chapter 3]):

Lemma 16. *Let $A \in \mathbf{C}_k^{m \times n}$ be a matrix representing a system of linear equations $A\mathbf{x} = \mathbf{o}$ over $\mathbf{C}_k$. Then, $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is a solution of this system if and only if there exists a solution $\mathbf{y} = (y_1, y_2, \ldots, y_{n+m})$ of the integral system of linear equations $B\mathbf{y} = \mathbf{o}$, where B is obtained by concatenating A and the diagonal matrix $k \cdot I_m$, such that $x_i = y_i$ for $i \in \{1, 2, \ldots, n\}$.*

Proof. If $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is a solution of $A\mathbf{x} = \mathbf{o}$ then, for all $i \in \{1, 2, \ldots, m\}$ $a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n = 0 \ mod\ 4$, i.e. there exists $k_i \in \mathbb{N}_0$ such that $a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n = 4k_i$. Hence, $\mathbf{y} = (x_1, x_2, \ldots, x_n, k_1, \ldots, k_m)$ is a solution of $B\mathbf{y} = \mathbf{o}$.

If, on the other hand, for all $i \in 1, \ldots, m$, $a_{i,1}y_1 + a_{i,2}y_2 + \cdots + a_{i,n}y_n + 4y_{n+i} = 0$, surely $a_{i,1}y_1 + a_{i,2}y_2 + \cdots + a_{i,n}y_n = 0 \ mod\ 4$. for all $i \in 1, \ldots, m$. □

3.2 Existence of non-affine latin quandle of size 2^7

We implemented the algorithms from the previous subsections in the GAP system and after few days of computation time we were able to prove that there exists no non-affine latin quandle of size 2^7. The programs and their results can be found in the attachement of this thesis.

The results enable us to finish the classification of non-affine latin quandles of size 2^k:

Theorem 17. *There exists a non-affine latin quandle of size 2^k if and only if $k = 6$ or $k \geq 8$.*

Proof. If $k \geq 6$ is even, the existence of non-affine latin quandle follows from Theorem 15, if $k > 8$ is odd, we can form a direct product of the (affine) latin quandle of size 2^3 (provided by the RIG library, [10]) and the non-affine latin quandle of size 2^{k-3} that exists by Theorem 15.

If, on the other hand, $k \leq 5$, there exists no non-affine latin quandle of size 2^k as can be seen in the RIG library. We were able to prove the remaining case $k = 7$ on the computer using the implementation of the algorithms above. □

3.3 Non-affine latin quandles of size 2^6

We will use the algorithm for finding central extensions in order to better understand the structure of non-affine latin quandles of size 2^6. With the help of those algorithms, we are able to determine for which latin quandles Q and abelian groups A there exists $\theta : Q \times Q \longrightarrow A$ and $\psi \in Aut(A)$ such that $Q \times_{(1-\psi),\psi,\theta} A$ is a non-affine latin quandle of size 2^7.

We found out (using the algorithm above) that there exists no central extension of latin quandle of size 4 by the abelian group $\mathbf{C}_4 \times \mathbf{C}_4$. Hence, the only abelian groups A for that there exists a central extension that is a non-affine latin quandle are of the form $\mathbf{C}_2^{6-k}$ (where $k = |Q|$). The automorphisms $\psi \in Aut(A)$ for that there exists this central extension are listed in Table 3.1.

We could use the obtained results in order to enumerate all non-affine latin quandles of size 2^6 by simple isomorphism checking. The problem is that for some quandles Q and abelian groups $\mathbf{C}_2^k$ there are more than 2^{30} possibilities for θ and hence we would need to do too many isomorphism checkings.

3.4 Enumeration of latin quandles

In this section, we will sketch a possible approach to enumeration of non-affine latin quandles. One of the problems with enumeration of this kind of quandles is that they do not form a variety (they are defined by the invalidity of mediality). Hence, in order to enumerate all non-affine latin quandles of size 2^k, we would probably have to enumerate all latin quandles of this size and also all affine latin quandles of this size (the latter is quite an easy task due to the correspondence between affine quandles and abelian groups). The terminology and ideas used in this section come from the approach to enumeration of loops that was presented in [2].

Let $(Q, *)$ be a latin quandle, A an abelian group and $f \in Aut(A)$ such that $Aff(A, f)$ is a latin quandle. Let us denote by $C(Q, Aff(A, f))$ (*cocycles*) the set of all mappings $Q \times Q \longrightarrow A$ and by $Map(Q, Aff(A, f))$ the set of all mappings from Q to A. Let us define:

Quandle Q	**Automorphisms** $\psi \in Aut(\mathbf{C}_2^{6-log_2(\|Q\|)})$
4_1	none
8_2	$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$
8_3	$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
16_1	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
16_2	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
16_3	none
16_4	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
16_5	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
16_6	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
16_7	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
16_8	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
16_9	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
4_1 × 4_1	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

Table 3.1: Latin quandles Q (numbered as in RIG library [10]) and automorphisms $\psi \in Aut(\mathbf{C}_2^{6-log_2(|Q|)})$ for that there exists $\theta : Q \times Q \longrightarrow \mathbf{C}_2^{6-log_2(|Q|)}$ such that $Q \times_{(1-\psi),\psi,\theta} \mathbf{C}_2^{6-log_2(|Q|)}$ is a non-affine latin quandle of size 2^6.

$$Hom(Q, Aff(A,f)) = \{\tau : Q \longrightarrow Aff(A,f) | \tau \textit{ is a homomorphism of quandles}\},$$

Let us define the mapping $Map(Q, Aff(A,f)) \longrightarrow C(Q, Aff(A,f))$ by $\tau \mapsto \hat{\tau}$ where $\hat{\tau}_{a,b} = \tau(a * b) - (1-f)(\tau(a)) - f(\tau(b))$. Then, this defines a homomorphism of groups with kernel $Hom(Q, Aff(A,f))$. We denote its image by $B(Q, Aff(A,f)) \simeq Map(Q, Aff(A,f))/Hom(Q, Aff(A,f))$ and we will call its elements *coboundaries*.

Lemma 18. *Let A be an abelian group such that $Aff(A,f)$ is a latin quandle. Let $\hat{\tau} \in B(Q, Aff(A,f))$. Then $\phi : Q \times_{(1-f),f,\theta} A \longrightarrow Q \times_{(1-f),f,\theta+\hat{\tau}} A$ defined by $\phi(q,a) = (q, a + \tau(q))$ is an isomorphism of quasigroups.*

Proof. It is clearly a bijection. Moreover, $\phi((p,a) * (q,b)) = (p * q, (1-f)(a) + f(b) + \theta_{p,q} + \tau(p*q)) = (p*q, (1-f)(a) + f(b) + \theta_{p,q} + \hat{\tau}_{p,q} + (1-f)(\tau(a)) + f(\tau(b))) = \phi((p,a)) * \phi((q,b))$. □

Hence, in order to obtain all quasigroups that are central extensions of Q by A (in the sense of Definition 6) up to isomorphism, it is sufficient to consider only the *cohomology* $H(Q, Aff(A,f)) = C(Q, Aff(A,f))/B(Q, Aff(A,f))$.

Let $\mathbf{V}$ be a variety of quasigroups (e.g. a subset of quasigroups axiomatized by identities, an example are (medial) latin quandles). If $Q \times_{(1-f),f,\theta} A \in \mathbf{V}$, it is necessary that $Q, Aff(A,f) \in \mathbf{V}$ by the comment above Lemma 8. Let $Q, Aff(A,f) \in \mathbf{V}$, we will call $\theta \in C(Q, Aff(A,f))$ a $\mathbf{V}$-cocycle if $Q \times_{(1-f),f,\theta} A \in \mathbf{V}$ and we will denote the set of all $\mathbf{V}$-cocycles by $C_{\mathbf{V}}(Q, Aff(A,f))$.

By Lemma 18, it holds that $\theta \in C_{\mathbf{V}}(Q, Aff(A,f))$ if and only if $\theta + \hat{\tau} \in C_{\mathbf{V}}(Q, Aff(A,f))$ for some $\hat{\tau} \in B(Q, Aff(A,f))$.

We can define an action of the group $Aut(Q) \times (Aut(A) \cap Aut(Aff(A,f)))$ on $C(Q, Aff(A,f))$ for $\alpha \in Aut(Q)$ and $\beta \in Aut(Aff(A,f)) \cap Aut(A)$ by $\theta^{(\alpha,\beta)}_{p,q} = \beta^{-1}(\theta_{\alpha(p),\alpha(q)})$. Moreover, the following lemma holds:

Lemma 19. *Let Q and $Aff(A,f)$ be latin quandles, $\theta \in F(Q, Aff(A,f))$, $\alpha \in Aut(Q)$ and $\beta \in Aut(Aff(A,f)) \cap Aut(A)$. Then, $Q \times_{(1-f),f,\theta} A \simeq Q \times_{(1-f),f,\theta^{(\alpha,\beta)}} A$.*

Proof. We can define a bijection $Q \times_{(1-f),f,\theta^{(\alpha,\beta)}} A \longrightarrow Q \times_{(1-f),f,\theta} A$ by $(q,a) \mapsto (\alpha(q), \beta(a))$. It is straightforward to check that this is also an isomorphism. □

Hence, in order to enumerate all central extensions $Q \times_{(1-f),f,\theta} A$, it is sufficient to consider only representatives from the orbits of the action of $Aut(Q) \times (Aut(A) \cap Aut(Aff(A,f)))$.

We can see that the theory that we described above is slightly more complicated than the theory for enumeration of loops developed in [2]. Hence, the enumeration of latin quandles is really a non-trivial task that goes beyond the extent of this thesis.

Conclusion

We were able to reach our main aim from the introduction section and to classify non-affine selfdistributive quasigroups of size 2^k, this classification is given by Theorem 17. We were able to prove that the least k for that there exists such a quasigroup is $k = 6$ in two inependent ways - we constructed such a quasigroup explicitely (construcion above Theorem 15) and we found also several central extensions that provide us with such a quasigroup (in Table 3.1).

We developed also a generalization of Onoi's construction (presented in his article [6]) that provides us with an interesting examples of selfdistributive quasigroups of size 2^k for that we are able to determine whether they are affine or not (due to Lemma 14).

On the other hand, there are still many open questions in the area of classification and enumeration of non-affine selfdistributive quasigroups left. One of them is, whether there exists an indecomposable (e.g. such that Q is not isomorph to the direct product $Q_1 \times Q_2$ for any $Q_1, Q_2 \neq Q$) non-affine selfdistributive quasigroup of size 2^k for some odd k - the only quasigroups of this kind that we were able to construct were direct products of smaller affine and non-affine quasigroups.

Another open question is the enumeration of non-affine selfdistributive quasigroups - we were not able to say how many of them (up to isomorphism) exist of size 2^6 and the question is surely harder for greater k's. Another question for further research could be to classify quasigroups that are constructed from Onoi structures (or to classify Onoi structures itself), because the construction presented in section 2 seems to be quite easy and it enables us to compute multiplication tables of quite huge quasigroups efficiently. Maybe it is also possible to generalize the notion of Onoi structures in order to construct quasigroups of size p^k for other primes p.

It could be quite depressing to end up with more open questions than we had at the beginning. But this is probably quite normal and even quite nice aspect of exploring the world of mathematical ideas. When we are able to answer one question, the desire to understand, explore and answer other new questions grows. And it is surely good the way it is - because the provoked desire means that we are still capable of perceiving the beauty of the ideas. And the beauty raises love. And that is everything what matters.

Bibliography

[1] Bonatto, Marco, Stanovský, David. *Commutator theory for racks and quandles*. arXiv:1902.08980.

[2] Daly, Daniel, Vojtěchovský, Petr. *Enumeration of nilpotent loops via cohomology*. Journal of Algebra **322**, 2009, 4080–4098.

[3] Eick, Bettina. *Linear equations over finite abelian groups*. Report, available at http://www.icm.tu-bs.de/ beick/publ/solvsys.pdf.

[4] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.10.0*; 2018, Available at https://www.gap-system.org.

[5] Hulpke, Alexander, Stanovský, David, Vojtěchovský Petr. *Connected quandles and transitive groups*. J. Pure Appl. Algebra **220**, 2016, no. 2, 735-758.

[6] Onoi, V. I. *Left distributive quasigroups that are left homogeneous over a quasigroup*. (Russian) Bul. Akad. Štiince RSS Moldoven **1970**, 1970 no. 2, 24-31.

[7] Rotman, Joseph J. *An Introduction to the Theory of Groups*. New York: Springer-Verlag, Inc., 1995. ISBN 978-1-4612-8686-8.

[8] Stanovský, David. *A guide to self-distributive quasigroups, or latin quandles*. Quasigroups and Related Systems **23/1**, 2015, 91-128.

[9] Stanovský, David, Vojtěchovský, Petr. *Abelian extensions and solvable loops*. Results in Math. **66/3-4**, 2014, 367-384.

[10] Vendramin, L. *Rig, a GAP package for racks, quandles and Nichols algebras*. Available at http://github.com/vendramin/rig/.

[11] Vojtěchovský, Petr, Stuhl, Izabella. *Enumeration of involutory latin quandles, Bruck loops and commutative automorphic loops of odd prime power order*. accepted to Nonassociative Mathematics and its Applications, proceedings of the 4th Mile High Conference on Nonassociative Mathematics, Denver, Colorado.

A. Attachments

Compact disc with programs introduced in Section 3 and their results