In memoriam: Galina B. Belyavskaya (1940 – 2015)

Galina Borisovna Belyavskaya (19.04.1940–07.05.2015)

Galina Borisovna Belyavskaya, the greatest woman-mathematician in Moldova, passed away at a hospital on May 7, 2015, as a result of cerebral hemorrhage.

She has been active professionally until her last days. She left a lot of unpublished notes. Her last finished work is a website dedicated to V. D. Belousov (see https://ru.wikipedia.org/wiki).

For more than fifty years Galina Belyavskaya worked in the Institute of Mathematics and Computer Science at the Academy of Sciences of Moldova. She started working there immediately after finishing her studies in Moldova State University where she graduated with honors. Her PhD dissertation was prepared under the supervision of Valentin D Belousov.

Her scientific interests were connected with the theory of binary and n-ary quasigroups. List of publications and a brief overview of her results were presented in vol. 18 (2010), no. 2 of *Quasigroups and Related Systems.*

In the last five years Galina Belyavskaya studied various problems connected with the orthogonality of binary and n-ary quasigroups, especially paratrophy orthogonality, r-differentiable quasigroups and their transformations. She has also investigated parastrophically equivalent identities characterizing quasigroups isotopic to abelian groups.

In [77] she proved these two theorems.

Theorem 1. *A quasigroup $(Q,\cdot)$ is isotopic to a group if and only if the following identity is true*

$$R_a^{-1}(x\cdot L_b^{-1}y)\cdot z = x\cdot L_b^{-1}(R_a^{-1}y\cdot z).$$

Theorem 2. *A quasigroup $(Q,\cdot)$ is isotopic to an abelian group if and only if the following identity is true*

$$R_a^{-1}(y\cdot x)\cdot z = R_a^{-1}(y\cdot z)\cdot x.$$

Since M.M. Glukhov proved (unpublished result), that no balanced identities (in the Belousov's sense) exist with three variables that guarantee that a quasigroup is isotopic to an abelian group, the last result (three variables and one fixed element) seem to be the best possible.

Another well-known result proved by G. Belyavskaya (see *Quasigroups and Related Systems* vol. 1 (1994)) is the following theorem, in literature known as the Belyavskaya's Theorem.

Theorem 3. *A quasigroup is central* (*in the sense of Belyavskaya and Smith*) *if and only if it is a T-quasigroup.*

Galina put much of her attention to various applications of quasigroups to the construction of Latin squares (prolongation and contraction) and, in the last years, to the coding theory, in particular to sharing systems and check character systems.

Wieslaw A. Dudek
Victor A. Shcherbacov

Below we present the list of last publications of Galina B. Belyavskaya. It is a continuation of the list published in *Quasigroups and Related Systems* 18 (2010), 109 – 112.

References

[68] *Identities with permutations leading to the linearity of quasigroups*, (with A. Kh. Tabarov), Discrete Math. Appl. **19** (2009), 173 – 190 (translation from Diskr. Mat. **21** (2009), 36 – 51.

[69] *Groupoids with the identity defining commutative Moufang loops*, (with A. Th. Tabarov), J. Math. Sci. (N. Y.) **164** (2010), 21 – 25 (translation from Fundam. Prikl. Mat. **14** (2008), no. 6, 33 – 39).

[70] *Conjugate-orthogonality and the complete multiplication group of a quasigroup*, (with A. Diordiev), Bul. Acad. Ştiinţe Republ. Mold. Mat. **1(59)** (2009), 22 – 30.

[71] *Secret-sharing schemes and orthogonal systems of k-ary operations*, Quasigroups Related Systems **17** (2009), 161 – 176.

[72] *Check character systems and totally conjugate orthogonal T-quasigroups*, Quasigroups Related Systems **18** (2010), 7 – 16.

[73] *Polynomial k-ary operations, matrices, and k-mappings*, J. Gen. Lie Theory Appl. **4** (2010), Article IDG100301.

[74] *Totally conjugate-orthogonal quasigroups and complete groups*, (with T. V. Popovich), J. Math. Sci. (N. Y.) **185** (2012), 184 – 191 (translation from Fundam. Prikl. Mat. **16** (2010), no. 8, 17 – 26).

[75] *Recursively r-differentiable quasigroups within S-systems and MDS-codes*, Quasigroups Related Systems **20** (2012), 157 – 168.

[76] *Conjugate sets of loops and quasigroups: DC-quasigroups*, (with T. Popovich), Bul. Acad. Ştiinţe Repub. Mold., ser. Math. **1(68)** (2012), 21 – 31.

[77] *Identities with permutations and quasigroups isotopic to groups and abelian groups*, Discrete Math. Appl. **23** (2013), 369 – 384 (translation from Diskret. Mat. **25** (2013), no. 2, 68 – 81).

[78] *Quasigroups: identities with permutations, linearity and nucleus*, (Russian), Lambert Academic Publishing, Saarbrucken, (2013), 71pp. ISNB 973-3-659-39143-9.

[79] *About graphs connected with quasigroups*, (Russian), (with T. Popovich), in "Topics in Graph Theory", University of Illinois (2013), 187 – 193.

[80] *Parastrophically equivalent identities characterizing quasigroups isotopic to abelian groups*, Quasigroups Related Systems **22** (2014), 19 – 32.

[81] *Successively orthogonal systems of k-ary operations*, Quasigroups Related Systems **22** (2014), 165 – 178.

[82] *Near-totally conjugate orthogonal quasigroups*, (with T. Popovich), Bul. Acad. Ştiinţe Repub. Mold., ser. Math. **3(76)** (2014), 89 – 96.

Quasigroups and Related Systems **23** (2015), 5 − 30

Applications of complete mappings and orthomorphisms of finite groups

Anthony B. Evans

Abstract. For a finite group G a permutation of G is a *complete mapping* of G if the mapping $g \mapsto g\theta(g)$ is a permutation, and an *orthomorphism* of G if the mapping $g \mapsto g^{-1}\theta(g)$ is a permutation. Complete mappings of a finite group G correspond to transversals of the Cayley table M of G, and orthomorphisms of G correspond to permutations of the columns of M that yield latin squares orthogonal to M.

Complete mappings and orthomorphisms have been used in constructions of mutually orthogonal sets of latin squares and in constructions of latin squares with particular properties. They and related mappings have also been used in many other algebraic and combinatorial constructions. In this paper we will survey the applications of complete mappings, orthomorphisms, near complete mappings, and near orthomorphisms in the construction of orthogonal latin squares, group sequencings, and neofields.

1. Introduction

Let G be a finite group and let $\theta\colon G \to G$ be a permutation. We call θ a *complete mapping* of G if the mapping $\sigma\colon g \mapsto g\theta(g)$ is a permutation, an *orthomorphism* of G if the mapping $\delta\colon g \mapsto g^{-1}\theta(g)$ is a permutation, and a *strong complete mapping* of G if it is both a complete mapping and an orthomorphism of G. Complete mappings and orthomorphisms are very closely related as a permutation θ is a complete mapping of G if and only if the mapping $g \mapsto g\theta(g)$ is an orthomorphism of G and an orthomorphism of G if and only if the mapping $g \mapsto g^{-1}\theta(g)$ is a complete mapping of G. While either complete mappings or orthomorphisms can be used in applications, we will see that in some applications one is more natural than the other. For example, in describing transversals of latin squares complete mappings are more natural, whereas in constructing mutually orthogonal latin squares by permuting the columns of the Cayley table of a finite group orthomorphisms are more natural. In the special case in which G is the additive group of the finite field $GF(q)$, any permutation of G can be represented by a permutation polynomial of $GF(q)$. Those permutation polynomials that represent orthomorphisms are called *orthomorphism polynomials*, and those permutation polynomials that represent complete mappings are called *complete mapping polynomials* or *complete permu-*

2010 Mathematics Subject Classification: 05B15
Keywords: Complete mapping, orthomorphism, orthogonal latin square, group sequencing, neofield.

tation polynomials. A complete mapping or orthomorphism θ of G is said to be *normalized* or in *canonical form* if $\theta(1) = 1$. If θ is a complete mapping (orthomorphism) of G, then the mapping $\theta_0 \colon g \mapsto \theta(g)\theta(1)^{-1}$ is a normalized complete mapping (orthomorphism) of G: θ_0 is the *normalization* of θ.

Closely related to complete mappings and orthomorphisms are near complete mappings and near orthomorphisms, mappings that just fail to be complete mappings or orthomorphisms. By a *near complete mapping* of G we mean a bijection $\theta : G \setminus \{h\} \to G \setminus \{1\}$, $h \neq 1$, for which the mapping $\sigma : g \mapsto g\theta(g)$ is a bijection $\theta : G \setminus \{h\} \to G \setminus \{k\}$, for some $k \in G$, $k \neq h$. A *near orthomorphism* of G is a bijection $\theta : G \setminus \{h\} \to G \setminus \{1\}$, $h \neq 1$, for which the mapping $\delta \colon g \mapsto g^{-1}\theta(g)$ is a bijection $\theta : G \setminus \{h\} \to G \setminus \{k\}$, for some $k \in G$, $k \neq h^{-1}$. A near complete mapping (near orthomorphism) θ is *normalized* or in *canonical form* if $k = 1$, in which case h is the *exdomain element* of θ. Near complete mappings and near orthomorphisms are closely related as, if θ is a normalized near complete mapping with exdomain element h, then the mapping $g \mapsto g\theta(g)$ is a normalized near orthomorphism with exdomain element h; and, if θ is a normalized near orthomorphism with exdomain element h, then the mapping $g \mapsto g^{-1}\theta(g)$ is a normalized near complete mapping with exdomain element h.

In Section 2 we will discuss the relationship between complete mappings of groups and transversals of the Cayley tables of groups; and we will also discuss the use of orthomorphisms in constructing sets of mutually orthogonal latin squares. In Section 3 we will discuss group sequencings and its variations that can be constructed using (near) complete mappings or (near) orthomorphisms; and in Section 4 we wlll discuss the use of orthomorphisms and near orthomorphisms in the construction of neofields.

2. Latin squares and orthogonality

Complete mappings and orthomorphisms were first introduced in constructions of sets of mutually orthogonal latin squares (MOLS). Complete mappings were introduced by Mann [44] in 1944; and orthomorphisms were introduced by Johnson, Dulmage and Mendelsohn [36] in 1961, and under the name orthogonal mappings by Bose, Chakravarti, and Knuth [6] in 1960. A *latin square of order* n is an $n \times n$ matrix with entries chosen from a set of n *symbols*, such that each symbol appears exactly once in each row and exactly once in each column. Latin squares in general are covered in the books by Dénes and Keedwell ([12] and [13]) and the forthcoming book by Keedwell [42]. Two latin squares of the same order are *orthogonal* if each ordered pair of symbols appears exactly once when the squares are superimposed: each square is then an *orthogonal mate* of the other. A set of k *mutually orthogonal latin squares* (MOLS) of order n is a set of k latin squares of order n, each pair of which is orthogonal. We use $N(n)$ to denote the largest k for which a set of k MOLS of order n exists.

The following is well-known.

Theorem 1. *If $n > 1$, then the following hold.*

(1) $1 \leqslant N(n) \leqslant n-1$.

(2) $N(n) = 1$ *if and only if* $n = 2$ *or* $n = 6$.

(3) *If n is a prime power, then* $N(n) = n-1$.

Proof. See [12] for instance. □

For $n > 1$, a set of $n-1$ MOLS of order n is a *complete sets of MOLS* of order n. A set of k MOLS of order n is *maximal* if it cannot be extended to a larger set of MOLS of order n. A table of lower bounds for $N(n)$ up to $n = 10,000$ can be found in [11].

Cayley ([9] and [10]) pointed out that the multiplication/addition table of a group is a latin square. Let $G = \{g_1, \ldots, g_n\}$ be a group of order n. The *Cayley table* M of G is the $n \times n$ matrix with ijth entry g_ig_j, and for θ a permutation of G, M_θ denotes the $n \times n$ matrix with ijth entry equal to $g_i\theta(g_j)$. It is easy to see that M is a latin square, and that M_θ is obtained from M by permuting columns.

2.1. Complete mappings and transversals. A set of cells in a latin square, exactly one in each row and exactly one in each column, whose entries are distinct is called a *transversal* of the latin square. The transversals of a latin square determine whether the square has an orthogonal mate or not. To see this, let L_1 and L_2 be an orthogonal pair of latin squares and let a be a symbol in L_2: the cells in L_1 corresponding to cells in L_2 with entry a form a transversal in L_1. The set of transversals of L_1 corresponding to the symbols of L_2 partitions the cells of L_1. We obtain the following.

Theorem 2. *A latin square possesses an orthogonal mate if and only if its cells can be partitioned by transversals.*

For the Cayley table M of a finite group G, a single transversal suffices.

Theorem 3. *The Cayley table M of a finite group G possesses an orthogonal mate if and only if it possesses a transversal.*

Proof. Let $G = \{g_1, \ldots, g_n\}$ and let M be the Cayley table of G. If M does not possess a transversal, then it does not possess an orthogonal mate by Theorem 2.

Let us assume that M does possess a transversal. Let $\phi_k \colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ be defined by $\phi_k(j) = t$ if $g_jg_k = g_t$, and let the ij_ith cells of M, $i = 1, \ldots, n$ form a transversal T. For $k = 1, \ldots, n$, let T_k consist of the $i\phi_k(j_i)$th cells of M, $i = 1, \ldots, n$. Then $T_1, \ldots, T_n$ are transversals of M that partition the cells of M. It follows that M possesses an orthogonal mate by Theorem 2. □

There is a natural correspondence between complete mappings of a group and transversals of its Cayley table.

Theorem 4. *There is a on-one correspondence between the complete mappings of a finite group G and the transversals of the Cayley table M of G.*

Proof. Let $G = \{g_1, \dots, g_n\}$ and let M be the Cayley table of G. Let T be a transversal of M consisting of the ij_ith cells of M, $i = 1, \dots, n$, n the order of G, and define $\theta\colon G \to G$ by $\theta(g_i) = g_{j_i}$. Then θ is a complete mapping of G and this correspondence establishes a bijection between the set of complete mappings of G and the set of transversals of M. □

To illustrate the proof of Theorem 4, Figure 1 shows a pair of orthogonal latin squares of order 7. The square M is the Cayley table of $\mathbb{Z}_7 = \{0, 1, 2, \dots, 6\}$, the operation being addition modulo 7. The entries of the cells in M corresponding to the cells in L with entry 3 are shown in italics: these cells clearly form a transversal of M. Let us define $\theta\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ by $\theta(i) = j$ if the ijth entry of M is italicized: this mapping, depicted in Figure 2, is a complete mapping of $\mathbb{Z}_7$.

$$M = \begin{pmatrix} 0 & \mathit{1} & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & \mathit{0} \\ 2 & 3 & 4 & \mathit{5} & 6 & 0 & 1 \\ \mathit{3} & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & \mathit{6} & 0 & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & \mathit{2} & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & \mathit{4} & 5 \end{pmatrix}, \quad L = \begin{pmatrix} 0 & 3 & 6 & 1 & 5 & 4 & 2 \\ 1 & 4 & 0 & 2 & 6 & 5 & 3 \\ 2 & 5 & 1 & 3 & 0 & 6 & 4 \\ 3 & 6 & 2 & 4 & 1 & 0 & 5 \\ 4 & 0 & 3 & 5 & 2 & 1 & 6 \\ 5 & 1 & 4 & 6 & 3 & 2 & 0 \\ 6 & 2 & 5 & 0 & 4 & 3 & 1 \end{pmatrix}$$

Figure 1: A pair of orthogonal latin squares of order 4.

i	0	1	2	3	4	5	6
$\theta(i)$	1	6	3	0	2	4	5
$i + \theta(i)$	1	0	5	3	6	2	4

Figure 2: A complete mapping of $\mathbb{Z}_7$.

Finite groups that admit complete mappings have been characterized.

Theorem 5. *The Cayley table of a finite group G possesses a transversal, equivalently a finite group G admits complete mappings, if and only if the Sylow 2-subgroup of G is either trivial or noncyclic.*

Proof. See [7], [20], [26], and [60]. □

As an immediate corollary to Theorems 3 and 5 we obtain the following.

Corollary 1. *The Cayley table of a finite group G possesses an orthogonal mate if and only if the Sylow 2-subgroup of G is either trivial or noncyclic.*

The literature contains many results on the number of complete mappings of small groups. Computer searches have confirmed and extended earlier results. In particular in 2004 Hsiang, Hsu, and Shieh [30] computed the number of complete mappings of $\mathbb{Z}_n$ for $n \leqslant 23$; and in 2006 McKay, McLeod, and Wanless [45] computed the number of complete mappings for all groups of order at most 23.

2.2. Orthomorphisms and MOLS. Let us reconsider the pair of orthogonal latin squares shown in Figure 1. We know that M is the Cayley table of $\mathbb{Z}_7$ and we observe that L can be obtained from M by permuting columns. This permutation ϕ, essentially the first row of L as a permutation of the first row of M, is shown in Figure 3: it is an orthomorphism of $\mathbb{Z}_7$.

i	0	1	2	3	4	5	6
$\phi(i)$	0	3	6	1	5	4	2
$\phi(i) - i$	0	2	4	5	1	6	3

Figure 3: An orthomorphism of $\mathbb{Z}_7$.

Theorem 6. *If M is the Cayley table of a finite group G and θ a permutation of G, then M_θ is orthogonal to M if and only if θ is an orthomorphism of G. If θ and ϕ are two permutations of G, then M_θ and M_ϕ are orthogonal if and only if the mapping $g \mapsto \phi(g)^{-1}\theta(g)$ is a permutation of G.*

Proof. Routine. □

We say that two mappings $\theta, \phi \colon G \to G$ are *orthogonal* if the mapping $g \mapsto \phi(g)^{-1}\theta(g)$ is a permutation. Thus a mapping $\theta \colon G \to G$ is a complete mapping of G if it is orthogonal to the mappings $g \mapsto 1$ and $g \mapsto g^{-1}$, and an orthomorphism if it is orthogonal to the mapping $g \mapsto 1$ and the identity mapping $g \mapsto g$. Orthogonality is a symmetric relationship. Note that, if θ and ϕ are orthomorphisms of G and θ_0 and ϕ_0 are their respective normalizations, then θ and ϕ are orthogonal if and only if θ_0 and ϕ_0 are orthogonal. By Theorem 6, pairwise orthogonal sets of orthomorphisms can be used to construct MOLS.

Corollary 2. *From r pairwise orthogonal orthomorphisms of a group of order $n > 1$ we can construct a set of $r + 1$ MOLS of order n.*

Proof. Let M be the Cayley table of a group G of order $n > 1$, and let $\theta_1, \ldots, \theta_r$ be a pairwise orthogonal set of orthomorphisms of G.Then the squares M,$M_{\theta_1}, \ldots, M_{\theta_r}$ form a set of $r + 1$ MOLS of order n. □

2.3. Complete sets of MOLS. While complete sets of MOLS of prime power order were known long before the introduction of complete mappings and orthomorphisms, they are easily constructed from pairwise orthogonal sets of orthomorphisms.

Corollary 3. *If q is a prime power, then there exists a complete set of MOLS of order q.*

Proof. Let $G = GF(q)^+$, the additive group of the field of order q. Then the mappings $x \mapsto ax$, $a \neq 0, 1$, form a set of $q-2$ pairwise orthogonal orthomorphisms of G from which the result follows. □

The orthomorphisms used in the proof of Corollary 3 are called *linear orthomorphisms* and are represented by the orthomorphism polynomials ax, $a \neq 0, 1$, of $GF(q)$.

We define $\omega(G)$ to be the largest possible order of a set of pairwise orthogonal orthomorphisms of G. Theorems 1 and Corollary 2 yield bounds on $\omega(G)$ when $|G| > 1$.

Theorem 7. *If $|G| = n > 1$, then $0 \leqslant \omega(G) \leqslant n-2$.*

By Theorem 5, the lower bound in Theorem 7 can be improved to 1 if the Sylow 2-subgroup of G is either trivial or noncyclic. By the proof of Corollary 3 the upper bound in Theorem 7 is achieved when G is elementary abelian.

For a group G of order $n > 2$ a set of $n-2$ pairwise orthogonal orthomorphisms of G is called a *complete set of orthomorphisms* of G. By Corollary 2, a complete set of orthomorphisms of a group G of order n yields a complete set of MOLS of order n.

It is well-known that a complete set of MOLS of order n corresponds to a projective plane of order n: see [11, 12, 13]. A *projective plane* is an incidence structure in which two distinct points are incident with exactly one line, two distinct lines meet in exactly one point, and there exist four points, no three of which are collinear. By removing one line of the projective plane and all the points on this line we obtain an *affine plane.* If π is a finite projective plane, then for some $n > 1$, each line of π is incident with $n+1$ points, and each point of π is incident with $n+1$ lines: n is the *order* of π and also the *order* of the corresponding affine plane. Given a group G of order n and a complete set of orthomorphisms $\theta_1, \ldots, \theta_{n-2}$ of G we can construct an affine plane of order n as follows. Without loss of generality we may assume that $\theta_1, \ldots, \theta_{n-2}$ are normalized. Treat G as an additive group with identity 0 whether abelian or not. We next form an affine plane $\mathcal{A}$ of order n. The points of $\mathcal{A}$ are the ordered pairs (x, y), $x, y \in G$. The lines of $\mathcal{A}$ are described by the equations $y = b$, $b \in G$; $y = x + b$, $b \in G$; $y = \theta_i(x) + b$, $b \in G$, $i = 1, \ldots, n-2$; and $x = c$, $c \in G$. Each class of equations describes a *parallel class* of $\mathcal{A}$. A *collineation* of a affine plane is a permutation of the points of the plane that preserves lines, and a *translation* of an affine plane is a collineation that fixes all parallel classes and fixes all the lines of a given parallel class. For each $g \in G$ the mapping $\tau_g \colon (x, y) \mapsto (x, y + g)$ is a translation of $\mathcal{A}$, and the set $\{\tau_g \mid g \in G\}$ is a group of translations of $\mathcal{A}$ that is transitive on the points of any line $x = c$. This construction can be reversed.

Theorem 8. *An affine plane admits a group G of translations that fixes all lines of a given parallel class and is transitive on the points of a line of this parallel class if and only if G admits a complete set of orthomorphisms.*

If a projective plane is constructed from a complete set of orthomorphisms of a group G, then the corresponding projective plane is (P, l)-transitive for some line l and some point P on l, the corresponding collineation group being isomorphic to G: see [11, 12, 13] for the definition of (P, l)-transitivity. The only groups known to admit complete sets of orthomorphisms are the elementary abelian groups. An unsolved problem:

Problem 1. *Does there exist a group G, $|G| = n > 1$, which is not elementary abelian, that admits a complete set of orthomorphisms?*

In particular, as it has long been conjectured that all finite affine and projective planes are of prime power order, we might ask:

Problem 2. *Does there exist a group G, $|G| = n > 1$, n not a prime power, that admits a complete set of orthomorphisms?*

While many finite projective planes can be constructed from complete sets of orthomorphisms, this approach is rarely used in the study of finite projective planes. As an example, translation planes are the projective planes that can be constructed from complete sets of orthomorphisms, each of which is a fixed-point-free automorphism of an elementary abelian group. However, translation planes are usually constructed from other algebraic structures such as spreads and quasifields. There are, however, some instances in which orthomorphisms have been used to establish the nonexistence of certain affine and projective planes. In 1973 Baumert and Hall [4] showed that no projective plane of order 10 or 12, if such existed, could be (P, l)-transitive for any point P on any line l: for the plane of order 10, this result can be derived from Theorem 5. In 1972 Studnicka [58] showed that no projective plane of order $2p^m$, if such existed, could be (P, l)-transitive for any point P on any line l: this result can also be derived from Theorem 5. In 2004 Lazebnik and Thomason [43], using orthomorphisms and a computer, were able to construct 3 of the 4 known projective planes of order 9 and 16 of the 22 known projective planes of order 16: they found no new projective planes.

It has long been conjectured that, if p is a prime, then there is only one affine (projective) plane of order p. This plane can be constructed from the linear orthomorphisms used in the proof of Corollary 3. It was shown in 1984 by Evans and McFarland [23] that the existence of a complete set of normalized orthomorphisms of $\mathbb{Z}_p$, p a prime, that are not all linear, would imply the existence of at least two affine (projective) planes of order p.

Theorem 9 (Evans, McFarland, 1984). *If, for a prime p, there exists more than one complete set of normalized orthomorphisms of $\mathbb{Z}_p$, then there exists more than one affine (projective) plane of order p.*

Problem 3. *Does there exist more than one complete set of normalized orthomorphisms of $\mathbb{Z}_p$ for any prime p?*

For primes 7 or less, Problem 3 is easily answered by hand: the answer is no. In 1961, via a computer search, Johnson, Dulmage, and Mendelsohn [36] showed that there was only one complete set of normalized orthomorphisms of $\mathbb{Z}_{11}$. Subsequent computer searches confirmed this; by Cates and Killgrove [8] in 1981; by Evans and McFarland [23] in 1984; and by Lazebnik and Thomason [43] in 2004. For $\mathbb{Z}_{13}$, in 1981 Cates and Killgrove [8] used a computer search to show that there was only one complete set of normalized orthomorphisms of this group. This was confirmed via computer searches by Mendelsohn and Wolk [46] in 1985, and by Lazebnik and Thomason [43] in 2004.

An alternative approach to searching for other complete sets of normalized orthomorphisms of $\mathbb{Z}_p$, p prime, was tried by Mendelsohn and Wolk [46] in 1985. They restricted themselves to quadratic orthomorphisms. For q an odd prime power, the *quadratic orthomorphism* $[A, B]$ of $GF(q)^+$ is defined by

$$[A,B](g) = \begin{cases} 0 & \text{if } g = 0, \\ Ag & \text{if } g \text{ is a nonzero square}, \\ Bg & \text{if } g \text{ is a nonsquare}, \end{cases}$$

where AB and $(A-1)(B-1)$ are both nonzero squares. Note that the quadratic orthomorphism $[A, B]$ of $GF(q)^+$ is represented by the orthomorphism polynomial $ax^{(q+1)/2} + bx$, where $a = (A - B)/2$ and $b = (A + B)/2$. The orthomorphism of $\mathbb{Z}_7$, depicted in Figure 3, is the quadratic orthomorphism $[3, 5]$. Mendelsohn and Wolk showed by a computer search that there is only one complete set of quadratic orthomorphisms of $GF(13)^+$ and of $GF(17)^+$, that is the known complete set of linear orthomorphisms. In 1987 Evans [14] extended this result to all primes $p \leqslant 47$ using simple hand calculations, and in 1989 Evans [15] extended this result to all primes.

2.4. Lower bounds for $N(n)$. A number of the best lower bounds for $N(n)$ have been obtained using difference matrices. For G a group of order n an $(n, r; \lambda)$-*difference matrix* over G is an $r \times \lambda n$ matrix $D = (d_{ij})$ with entries from G such that for any $i, k \in \{1, \ldots, r\}$, $i \neq k$, each element of G appears λ times in the form $d_{ij}^{-1} d_{kj}$. We call λ the *index* of D. An $(n, r; \lambda)$-*difference matrix* can be transformed into another $(n, r; \lambda)$-*difference matrix* by permuting columns, permuting rows, multiplying all the elements of a row on the right by an element of G, and multiplying all the elements of a column on the left by an element of G. Employing these operations we may transform any difference matrix into a *normalized* difference matrix, that is, one in which every entry in the first row and first column is the identity. Given a normalized $(n, r; 1)$-*difference matrix* over a group G, the second row is a listing of the elements of G and the third through rth rows, regarded as permutations of the second row, form a set of $r - 2$ pairwise orthogonal normalized orthomorphisms of G: this construction can be reversed.

Table 1 shows some of the lower bounds for $N(n)$ that have been obtained from difference matrices with the corresponding groups: this data is from [11].

n	$N(n) \geqslant$	The group
12	5	$GF(3)^+ \times GF(4)^+$
15	4	$GF(3)^+ \times GF(5)^+$
21	5	$GF(3)^+ \times GF(7)^+$
24	7	$GF(3)^+ \times GF(8)^+$
28	5	$GF(4)^+ \times GF(7)^+$
33	5	$GF(3)^+ \times GF(11)^+$
35	5	$GF(5)^+ \times GF(7)^+$
36	8	$GF(4)^+ \times GF(9)^+$
39	5	$GF(3)^+ \times GF(13)^+$
40	7	$GF(5)^+ \times GF(8)^+$
44	5	$GF(4)^+ \times GF(11)^+$
45	6	$GF(5)^+ \times GF(9)^+$
48	8	$GF(3)^+ \times GF(16)^+$

Table 1: MOLS from groups.

Problem 4. *For a finite group G determine $\omega(G)$ or improve bounds on $\omega(G)$.*

Problem 4 has only been completely answered for small groups, elementary abelian groups (see Corollary 3), and for groups with nontrivial, cyclic Sylow 2-subgroups (See Theorem 5).

2.5. Maximal sets of MOLS. Given a maximal set of pairwise orthogonal orthomorphisms of a group finite G, is the corresponding set of MOLS also maximal? The answer to this question is yes. This was implicitly proved by Ostrom [50] in 1966 in the language of nets.

Theorem 10 (Ostrom, 1966)**.** *Let G be a finite group of order n and let M be its Cayley table. If $\theta_1, \ldots, \theta_r$ is a maximal set of pairwise orthogonal orthomorphisms of G, then M, M_{θ_1}, …, M_{θ_r} is a maximal set of MOLS of order n.*

As an example, the orthomorphism of $\mathbb{Z}_7$, depicted in Figure 3, is not orthogonal to any other orthomorphism of $\mathbb{Z}_7$. Hence, by Theorem 10, the latin squares in Figure 1 form a maximal set of 2 MOLS of order 7. A difference matrix over a group G is *maximal* if it cannot be extended to a larger difference matrix over G by adding rows. As a corollary to Theorem 10 we obtain the following.

Corollary 4. *If there exists a maximal $(n, r; 1, G)$-difference matrix, then there exists a maximal set of $r - 1$ MOLS of order n.*

All maximal $(n, r; 1, G)$-difference matrices over groups of order at most 10 were determined by Jungnickel and Grams [37] in 1986. In 1991 Evans [17] generalized Corollary 4.

Theorem 11 (Evans, 1991). *If there exists an $(n, r; 1, G)$-difference matrix D for which $mD = (D \dots D)$, i.e., m consecutive copies of D, is maximal and if either $m = 1$ or there exist a set of $r - 1$ MOLS of order m, then there exists a maximal set of $r - 1$ MOLS of order nm.*

Theorem 11 was used to prove the following.

Theorem 12 (Evans, 1991). *If $n = mp^r$, p a prime, $\gcd(m, p) = 1$, and either $m = 1$ or there exist a set of $p - 1$ MOLS of order m then there exists a maximal set of $p - 1$ MOLS of order n.*

The proof of Theorem 12 was obtained by generalizing the construction of a maximal set of $p - 2$ pairwise orthogonal orthomorphisms of $\mathbb{Z}_{p^r}$, p a prime. In 1992 Evans [18] used quadratic orthomorphisms to construct two infinite classes of maximal sets of MOLS.

Theorem 13 (Evans, 1992). *Let $p \geqslant 7$ be a prime.*

(1) *If $p \equiv 3 \pmod 4$, then there exists a maximal set of $(p - 3)/2$ MOLS of order p.*

(2) *If $p \equiv 1 \pmod 4$, then there exists a maximal set of $(p - 1)/2$ MOLS of order p.*

The maximal sets of MOLS, constructed in Theorem 13, are obtained from maximal sets of pairwise orthogonal orthomorphisms of $GF(p)^+$ that are constructed in the following way. If p is a prime and $[A, B]$ is a nonlinear, quadratic orthomorphism of $GF(p)^+$, then $[A, B]$ is orthogonal to precisely $(p-7)/2$ linear orthomorphisms of $GF(p)^+$, forming a set of $(p-5)/2$ pairwise orthogonal orthomorphisms of $GF(p)^+$. If $p \equiv 3 \pmod 4$, then this set is maximal. If $p \equiv 1 \pmod 4$, then $[B, A]$ must be included yielding a maximal set of $(p-3)/2$ pairwise orthogonal orthomorphisms of $GF(p)^+$. As examples, $[7, 7], [8, 8], [2, 6]$ is a maximal set of 3 pairwise orthogonal orthomorphisms of $GF(11)^+$, and $[6, 6], [7, 7], [10, 10], [2, 5]$, $[5, 2]$ is a maximal set of 5 pairwise orthogonal orthomorphisms of $GF(13)^+$.

In 1993 Pott [54] gave a simpler proof of Theorem 13 using a result of Rédei. Using a computer and cyclotomic orthomorphisms, a generalization of quadratic orthomorphisms, Pott found a maximal set of 2 MOLS of order 13, a maximal set of 4 MOLS of order 13, a maximal set of 3 MOLS of order 17, a maximal set of 4 MOLS of order 17, a maximal set of 3 MOLS of order 19, and a maximal set of 6 MOLS of order 19.

2.6. Strong complete mappings and Knut Vic designs. Let $G = \{g_1, \dots, g_n\}$ be a group of order n. The *normal multiplication table* of G is the $n \times n$ array with ijth entry $g_i g_j^{-1}$. Strong complete mappings are important in determining the existence of latin squares orthogonal to both N and the Cayley table M of G.

Theorem 14. *Let G be a finite group with Cayley table M and normal multiplication table N. There exists a latin square orthogonal to both M and N if and only if G admits a strong complete mapping.*

Proof. See [22]. □

In fact, if θ is a strong complete mapping of G, then M_θ is orthogonal to both M and N. In the special case $G = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, any latin square L orthogonal to both the Cayley table of G and the normal multiplication table of G is a *Knut Vic design*: these are characterized by each broken left and right diagonal being a transversal.

Problem 5. *Which finite groups admit strong complete mappings?*

Problem 5 was implicitly solved for cyclic groups in papers by Hedayat and Federer [28] in 1975 and Hedayat [27] in 1977.

Theorem 15 (Hedayat, Federer, 1975 & 1977)**.** $\mathbb{Z}_n$ *admits strong complete mappings if and only if* $\gcd(n, 6) = 1$.

As a consequence of Theorem 5, if the Sylow 2 subgroup of a finite group G is nontrivial and cyclic, then G cannot admit strong complete mappings. In 1990 Evans [16] and Horton [29] showed that the structure of the Sylow 3-subgroup also plays a role in determining the existence of strong complete mappings.

Theorem 16. *If a finite group G has a nontrivial, cyclic Sylow 3-subgroup that is a homomorphic image of G, then G does not admit strong complete mappings.*

The special case of Theorem 16, G abelian, was proved by Horton and the general case by Evans. For finite abelian groups the existence of strong complete mappings is completely determined by the structure of the Sylow 2-subgroups and the Sylow 3-subgroups: this was proved by Evans [21] in 2012.

Theorem 17 (Evans, 2012)**.** *A finite abelian group with a trivial or noncyclic Sylow 2-subgroup and a trivial or noncyclic Sylow 3-subgroup admits strong complete mappings.*

In light of Theorem 5, it is natural to ask whether it is true that a finite group with a nontrivial, cyclic Sylow 3-subgroup does not admit strong complete mappings. The answer to this question was shown to be no by Shieh, Hsiang, and Hsu [57], who described a strong complete mapping of D_{12}, the dihedral group of order 12. Since then, Evans [22] has shown a number of classes of dihedral groups and quaternion groups to admit strong complete mappings, as well as most groups of order at most 31. Let $D_{4k} = \langle a, b \mid a^{2k} = b^2 = 1, ab = ba^{-1} \rangle$ denote the dihedral group of order $4k$, and $Q_{4k} = \langle a, b \mid a^{2k} = 1, b^2 = a^k, bab^{-1} = a^{-1} \rangle$ the quaternion group of order $4k$. Evans' results are given in Theorems 18, 19, and 20.

Theorem 18. *D_8 does not admit strong complete mappings. If* $\gcd(m, 6) = 1$, *then D_{4m}, D_{12m}, D_{16m}, and D_{24m} admit strong complete mappings.*

Similar results hold for the quaternion groups.

Theorem 19. *Q_8 does not admit strong complete mappings. If $\gcd(m,6)=1$, then Q_{16m} and Q_{24m} admit strong complete mappings.*

The following is the result of a computer search for strong complete mappings.

Theorem 20. *All groups of order at most 31 admit strong complete mappings with the following exceptions:*

(1) *any group with nontrivial, cyclic Sylow 2-subgroups,*
(2) *any group G with a nontrivial, cyclic Sylow 3-subgroup that is a homomorphic image of G,*
(3) *D_8, and*
(4) *Q_8.*

3. Group labeling problems

In this section we will discuss group sequencings, which can be constructed from a class of near complete mappings: these arose in the construction of complete latin squares. We will also discuss two variants of group sequencings, R-sequencings and harmonious orderings, both of which can be constructed from classes of orthomorphisms.

3.1. Group sequencings. A *sequencing* of a group G of order n is an ordering $a_0=1,a_1,a_2,\dots,a_{n-1}$ of the elements of G such that the *partial products* $b_0=a_0=1,\ b_1=a_0a_1,\ b_2=a_0a_1a_2\ ,\dots,b_{n-1}=a_0a_1a_2\cdots a_{n-1}$ are distinct. We say that a group is *sequenceable* if it possesses a sequencing.

Group sequencings were introduced by Gordon [25] in 1961 in the construction of complete latin squares. A latin square $L=\{l_{ij}\}$ of order n is *row complete* if the $n(n-1)$ ordered pairs $(l_{ij},l_{i,j+1})$, $i=1,\dots,n$ and $j=1,\dots,n-1$, are distinct, *column complete* if the $n(n-1)$ ordered pairs $(l_{ij},l_{i+1,j})$, $i=1,\dots,n-1$ and $j=1,\dots,n$, are distinct, and *complete* if it is both row complete and column complete.

Theorem 21 (Gordon, 1961)**.** *Let $a_0,a_1,a_2,\dots,a_{n-1}$ be a sequencing of a group G of order n and let $b_0,b_1,b_2,\dots,b_{n-1}$ be the corresponding sequence of partial products. Then the $n\times n$ matrix with ijth entry $\{b_i^{-1}b_j\}$ is a complete latin square of order n.*

Proof. See Theorem 2 in [25]. □

Example 1. *Let $0,1,8,3,6,5,4,7,2,9$ be an ordering of the elements of $\mathbb{Z}_{10}$. As the partial sums $0,1,9,2,8,3,7,4,6,5$ are distinct this is a sequencing of $\mathbb{Z}_{10}$. The associated complete latin square is shown in Figure 4.*

The sequencing of Example 1 can be generalized: the ordering

$$0,1,-2,3,-4,\dots,2n-3,-(2n-2),2n-1$$

is a sequencing of $\mathbb{Z}_{2n}$ as the partial sums are

$$0, 1, -1, 2, -2, \ldots, n-1, -(n-1), n.$$

$$\begin{pmatrix}
0 & 1 & 9 & 2 & 8 & 3 & 7 & 4 & 6 & 5 \\
9 & 0 & 8 & 1 & 7 & 2 & 6 & 3 & 5 & 4 \\
1 & 2 & 0 & 3 & 9 & 4 & 8 & 5 & 7 & 6 \\
8 & 9 & 7 & 0 & 6 & 1 & 5 & 2 & 4 & 3 \\
2 & 3 & 1 & 4 & 0 & 5 & 9 & 6 & 8 & 7 \\
7 & 8 & 6 & 9 & 5 & 0 & 4 & 1 & 3 & 2 \\
3 & 4 & 2 & 5 & 1 & 6 & 0 & 7 & 9 & 8 \\
6 & 7 & 5 & 8 & 4 & 9 & 3 & 0 & 2 & 1 \\
4 & 5 & 3 & 6 & 2 & 7 & 1 & 8 & 0 & 9 \\
5 & 6 & 4 & 7 & 3 & 8 & 2 & 9 & 1 & 0
\end{pmatrix}$$

Figure 4: A complete latin square of order 10.

It should be noted that the complete latin square in Figure 4 can be obtained from the Cayley table of $\mathbb{Z}_{10}$ by permuting rows and columns. This was observed by Keedwell [38] in 1976.

Theorem 22. *A complete latin square can be obtained from the Cayley table of a finite group G, by permuting rows and columns, if and only if G is sequenceable.*

From a sequencing of a group we can construct a near complete mapping of the group.

Theorem 23. *Let $a_0, a_1, a_2, \ldots, a_{n-1}$ be a sequencing of a group G of order n and let $b_0, b_1, b_2, \ldots, b_{n-1}$ be the partial products. Define $\theta\colon G \setminus \{b_{n-1}\} \to G \setminus \{1\}$ by*

$$\theta(b_i) = a_{i+1}, i = 0, \ldots, n-2.$$

Then θ is a near complete mapping of G with exdomain element b_{n-1}.

Proof. First note that $\{b_0, \ldots, b_{n-2}\} = G \setminus \{b_{n-1}\}$.

Now

$$\{\theta(b_0), \ldots, \theta(b_{n-2})\} = \{a_1, \ldots, a_{n-1}\} = G \setminus \{1\}$$

and

$$\{b_0\theta(b_0), \ldots, b_{n-2}\theta(b_{n-2})\} = \{b_1, \ldots, b_{n-1}\} = G \setminus \{1\},$$

from which the result follows. □

As an example, the near complete mapping derived from the sequencing of $\mathbb{Z}_{10}$, described in Example 1, is shown in Figure 5. The exdomain element of this near complete mapping is 5.

g	0	1	2	3	4	5	6	7	8	9
$\theta(g)$	1	8	6	4	2	.	9	7	5	3
$g+\theta(g)$	1	9	8	7	6	.	5	4	3	2

Figure 5: A near complete mapping from a sequencing of $\mathbb{Z}_{10}$.

Just as the cycle $(c_0\ c_1\ \cdots\ c_{k-1})$ is used to represent the mapping $c_i \mapsto c_{i+1}$, $i = 0, \ldots, k-1$, the subscripts being added modulo k, the sequence $[c_0\ c_1\ \cdots\ c_{k-1}]$ is used to denote the mapping is used to represent the mapping $c_i \mapsto c_{i+1}$, $i = 0, \ldots, k-2$. Any complete mapping, orthomorphism, near complete mapping, or near orthomorphism can be written as a product of disjoint cycles and sequences. The near orthomorphism, $g \mapsto g+\theta(g)$, associated with the near complete mapping in Figure 5 can be written as the sequence [0 1 9 2 8 3 7 4 6 5].

In 1984 Hsu and Keedwell [34] characterized the normalized near orthomorphisms from which group sequencings can be constructed.

Theorem 24 (Hsu, Keedwell, 1984). *A group G of order n is sequenceable if and only if it admits a normalized near orthomorphism that consists of one sequence of length n.*

Proof. Let $a_0, a_1, a_2, \ldots, a_{n-1}$ be a sequencing of a group G of order n and let $b_0, b_1, b_2, \ldots, b_{n-1}$ be the partial products. Then $[b_0\ b_1\ \cdots\ b_{n-1}]$ is a normalized near orthomorphism of G.

If $[b_0\ b_1\ \cdots\ b_{n-1}]$ is a normalized near orthomorphism of G, then setting

$$a_i = \begin{cases} 1 & \text{if } i = 0, \\ b_{i-1}^{-1} b_i & \text{if } i = 1, \ldots, n-1, \end{cases}$$

yields a sequencing $a_0, \ldots, a_{n-1}$ of G. □

Problem 6. *Which groups are sequenceable?*

Problem 6 was answered for abelian groups by Gordon [25] in 1961.

Theorem 25 (Gordon, 1961). *An abelian group is sequenceable if and only if it has a unique element of order* 2.

Proof. See Theorem 1 in [25]. □

The situation is different for nonabelian groups. Order 10 appears to be a dividing line.

Theorem 26. *No nonabelian group of order less than* 10 *is sequenceable.*

Proof. See Gordon [25]. □

However, the nonabelian group of order 10, the dihedral group $D_{10} = \langle a, b \mid a^5 = b^2 = 1, ab = ba^{-1}\rangle$ is sequenceable. $1, ba, a^4, ba^2, b, ba^4, a^2, a, ba^3, a^3$ is a sequencing for this group. In 1983 Keedwell [40] conjectured that nonabelian groups of order less that 10 were the only nonsequenceable nonabelian groups.

Conjecture 1 (Keedwell). *All nonabelian groups of order at least* 10 *are sequenceable.*

Keedwell's conjecture has been proved true for many classes of groups.

Theorem 27 (Anderson, 1987). *All nonabelian groups of order n,* $10 \leqslant n \leqslant 32$ *are sequenceable.*

Proof. See [1] and [2]. □

Theorem 28 (Anderson, 1987). *A_5 and S_5 are sequenceable.*

Proof. See [1]. □

The proof that the dihedral groups satisfy Keedwell's conjecture is the result of work by several mathematicians, whose work is described in the dynamic survey [49] by Ollis.

Theorem 29. *The dihedral group of order $2n$, D_{2n}, $n \geqslant 5$, is sequenceable.*

There are a number of results for binary groups: a group is *binary* if it has exactly one involution. Theorem 25 can be restated as, a finite abelian group is sequenceable if and only if it is a binary group. Keedwell's conjecture has been proved for binary solvable groups.

Theorem 30 (Anderson and Ihrig, 1993). *All binary solvable groups, except the quaternion group of order* 8*, are sequenceable.*

Proof. See [3]. □

Anderson and Ihrig actually proved the stronger result that solvable groups with a unique element of order 2 are symmetrically sequenceable. A *symmetric sequencing* of a group G of order $2n$, with a unique element u of order 2, is a sequencing $a_0 = 1, a_1, a_2, \ldots, a_{2n-1}$ of G for which $a_n = u$ and $a_{n-i} = a_{n+i}^{-1}$, $i = 1, 2, \ldots, n-1$. A group is *symmetrically sequenceable* if it possesses a symmetric sequencing. A number of other groups have been shown to be sequenceable including many binary groups and groups of odd order: see [49] for details.

3.2. R-sequencings. An *R-sequencing* of a group G of order n is an ordering $a_0 = 1, a_1, a_2, \ldots, a_{n-1}$ of the elements of G such that the *partial products* $b_0 = a_0 = 1$, $b_1 = a_0a_1$, $b_2 = a_0a_1a_2$ $, \ldots, b_{n-2} = a_0a_1a_2 \cdots a_{n-2}$ are distinct and $a_0a_1a_2 \cdots a_{n-1} = 1$. A group is *R-sequenceable* if it possesses an R-sequencing. R-sequencings were introduced by Paige [53] in 1951 as a sufficient condition for a group to admit complete mappings, equivalently orthomorphisms. they were also used by Ringel [55] in 1974 in his solution of the map coloring problem for all compact 2-dimensional manifolds except the sphere. Note that in and R-sequencing of a finite group G exactly one element of G does not appear as a partial product.

Theorem 31. *Let $a_0, a_1, a_2, \ldots, a_{n-1}$ be an R-sequencing of a group G of order n, let $b_0, b_1, b_2, \ldots, b_{n-2}$ be the corresponding sequence of partial products, and let c be the element of G that is not in the list of partial products. Then, the mapping $\theta\colon G \to G$ defined by*

$$\theta(g) = \begin{cases} b_{i+1} & \textit{if } g = b_i, i = 0, 1, \ldots, n-3, \\ b_0 & \textit{if } g = b_{n-2}, \\ c & \textit{if } g = c, \end{cases}$$

is an orthomorphism of G.

Proof. Routine. □

An immediate consequence of Theorems 5 and 31.

Corollary 5. *If G is a finite R-sequenceable group, then its Sylow 2 subgroup is either trivial or non-cyclic.*

As an example $0, 12, 2, 10, 4, 8, 6, 5, 9, 3, 11, 1, 7$ is an R-sequencing of $\mathbb{Z}_{13}$. The partial sums are $0, 12, 1, 11, 2, 10, 3, 8, 4, 7, 5, 6$, missing 9. The associated orthomorphism is shown in Figure 6.

g	0	1	2	3	4	5	6	7	8	9	10	11	12
$\theta(g)$	12	11	10	8	7	6	0	5	4	9	3	2	1
$\theta(g) - g$	12	10	8	5	3	1	7	11	9	0	6	4	2

Figure 6: An orthomorphism of $\mathbb{Z}_{13}$.

The orthomorphism in Figure 6 is the cycle (0 12 1 11 2 10 3 8 4 7 5 6). In 1984 Hsu and Keedwell [34] characterized the normalized orthomorphisms from which R-sequencings can be constructed.

Theorem 32 (Hsu, Keedwell, 1984)**.** *A group G of order n is R-sequenceable if and only if it admits a normalized orthomorphism that consists of one cycle of length $n - 1$.*

Proof. Similar to the proof of Theorem 24. □

Problem 7. *Which finite groups are R-sequenceable?*

Cyclic groups of odd order were shown to be R-sequenceable groups by Friedlander, Gordon, and Miller [24] in 1978.

Theorem 33 (Friedlander, Gordon and Miller, 1978)**.** *If n is odd, then $\mathbb{Z}_n$ is R-sequenceable.*

Proof.

$$\begin{aligned}0, -1, 2, -3, 4, \dots, -(2n-1), 2n, 2n-1, -(2n-2),\\ 2n-3, -(2n-4), \dots, 3, -2, 1, -2n\end{aligned}$$

is an R-sequencing of $\mathbb{Z}_{4n+1}$, and

$$\begin{aligned}0, -1, 2, -3, 4, \dots, -(2n-1), 2n, -(2n+2), 2n+3,\\ -(2n+4), \dots, -4n, 4n+1, -(4n+2), 2n+2\end{aligned}$$

is an R-sequencing of $\mathbb{Z}_{4n+3}$. □

There are many other classes of R-sequenceable groups known: see Ollis [49].

3.3. Harmonious groups. A *harmonious ordering* of a group G of order n is an ordering $a_0 = 1, a_1, a_2, \dots, a_{n-1}$ of the elements of G such that the products a_0a_1, a_1a_2, $a_2a_3, \dots,$ $a_{n-1}a_0$ are distinct. G is a *harmonious* group if it possesses a harmonious ordering. Harmonious groups were introduced by Beals, Gallian, Headley, and Jungreis [5] in 1991.

Theorem 34. *If $a_0 = 1, a_1, a_2, \dots, a_{n-1}$ is a harmonious ordering of a group G, of order n, then the mapping $a_i \mapsto a_ia_{i+1}$, indices added modulo n, is an orthomorphism of G.*

Proof. Routine. □

As an example, $0, 1, 2, \dots, n-1$ is a harmonious ordering of $\mathbb{Z}_n$ if n is odd. The associated orthomorphism is $i \mapsto 2i + 1$. Note that this orthomorphism is not normalized, and that its associated complete mapping $i \mapsto i + 1$ is a cycle of length n. Beals, Gallian, Headley, and Jungreis characterized complete mappings from which harmonious orderings can be constructed.

Theorem 35. *A group G of order n is harmonious if and only if it admits a complete mapping that consists of one cycle of length n.*

Proof. Routine. □

An immediate corollary of Theorems 5 and 34.

Corollary 6. *Finite groups with nontrivial cyclic 2-groups are not harmonious.*

Beals, Gallian, Headley, and Jungreis [5] discovered an additional class of non-harmonious groups.

Theorem 36 (Beals, Gallian, Headley, and Jungreis, 1991)**.** *The additive group of the finite field $GF(2^n)$ is not harmonious.*

Problem 8. *Which finite groups are harmonious?*

Beals, Gallian, Headley, and Jungreis [5] completely characterized finite abelian harmonious groups and showed all groups of odd order to be harmonious.

Theorem 37 (Beals, Gallian, Headley, and Jungreis, 1991)**.** *Groups of odd order are harmonious.*

Theorem 38 (Beals, Gallian, Headley, and Jungreis, 1991)**.** *Abelian groups, except $GF(2^n)^+$, with trivial or noncyclic 2-groups, are harmonious.*

In addition, several dihedral and quaternion groups have been shown to be harmonious: See Ollis [49]

4. Neofields

Neofields were first introduced in 1949 by Paige [52]: they were also the subject of his 1947 Ph.D thesis [51]. A *left neofield* is a set N with two binary operations, addition and multiplication, satisfying the following:

1. The elements of N form a loop under addition, with identity 0.
2. The nonzero elements of N form a group under multiplication, with identity 1.
3. The left distributive law holds: $a(b+c) = ab + ac$ for all $a, b, c \in N$.

A left neofield is called a *neofield* if the right distributive law is also satisfied. For a neofield or left neofield we will use N^+ to denote the additive loop and N^* to denote the multiplicative group of nonzero elements.

Loops that can be the additive loop of a left neofield can be characterized by their automorphism groups.

Theorem 39. *A loop can be the additive loop of a left neofield if and only if it admits an automorphism group that acts sharply transitively on its nonidentity elements.*

Proof. Let N be a left neofield and, for each $g \in N^*$, define $\tau_g \colon N \to N$ by $\tau_g(a) = ga$. Then $\{\tau_g \mid g \in N^*\}$ is an automorphism group of N^+ that acts sharply transitively on the nonzero elements of N.

Conversely, let L be a loop written additively with identity 0. Let us assume that G is an automorphism group of L that acts sharply transitively on the nonzero elements of L. We will use G to define multiplication on L. Pick a nonzero element of L and denote it 1 and for each nonzero element $a \in L$, let τ_a denote the unique element of G satisfying $\tau_a(1) = a$. Define multiplication on L by:

$$ab = \begin{cases} 0 & \text{if } \ a = 0 \text{ or } b = 0, \\ \tau_a(b) & \text{if } \ a, b \neq 0. \end{cases}$$

With this multiplication L is a left neofield. □

An *automorphism* of a left neofield N is a bijection $\alpha : N \to N$ for which $\alpha(a+b) = \alpha(a)+\alpha(b)$, and $\alpha(ab) = \alpha(a)\alpha(b)$, for all $a, b \in N$. Clearly the automorphism group $Aut(N)$ of a left neofield N is a subgroup of the automorphism group of N^*, as well as a subgroup of the automorphism group of N^+.

4.1. Orthomorphisms and near orthomorphisms. The *presentation function* of a left neofield N is the mapping $\theta\colon N \to N$ defined by $\theta(x) = 1 + x$. A left neofield N is complete determined by its multiplicative group N^* and its presentation function θ as, if $a, b \neq 0$, then

$$a + b = a(1 + a^{-1}b) = a\theta(a^{-1}b).$$

The presentation function of a left neofield N is essentially an orthomorphism or near orthomorphism of N^* depending on whether $1 + 1 = 0$ in N or not. Bruck (see [52], Theorem I.1) implicitly established the connection between neofields with multiplicative group G and orthomorphisms and near orthomorphisms of G. Later in 1984 Hsu and Keedwell [34] generalized this result to establish a correspondence between left neofields with multiplicative group G and orthomorphisms and near orthomorphisms of G. Neofields in which $1 + 1 = 0$ can be constructed from orthomorphisms.

Theorem 40 (Hsu, Keedwell, 1984)**.** *Let G be a group, written multiplicatively with identity 1, let θ be a normalized orthomorphism of G, and define $\theta'\colon G\cup\{0\} \to G \cup \{0\}$ by*

$$\theta'(g) = \begin{cases} 0 & \textit{if } \ g = 1, \\ 1 & \textit{if } \ g = 0, \\ \theta(g) & \textit{if } \ g \neq 0, 1. \end{cases}$$

Then θ' is the presentation function of a left neofield in which $1 + 1 = 0$.

Proof. Let $N = G \cup \{0\}$ and define addition and multiplication in N as follows. Multiplication is as in G except that $0a = a0 = 0$ for all $a \in N$. To define addition,

$$x + y = \begin{cases} y & \text{if } \ x = 0, \\ x\theta'(x^{-1}y) & \text{if } \ x \neq 0. \end{cases}$$

N is then a left neofield, with presentation function θ', in which $1+1 = 0$. □

This construction can be reversed.

Theorem 41 (Hsu, Keedwell, 1984)**.** *Let θ be the presentation function of a left neofield, in which $1 + 1 = 0$, with multiplicative group G. Define $\theta'\colon G \to G$ by*

$$\theta'(g) = \begin{cases} 1 & \textit{if } \ g = 1, \\ \theta(g) & \textit{if } \ g \neq 1. \end{cases}$$

Then θ' is a normalized orthomorphism of G.

Proof. Routine. □

The constructions of Theorems 40 and 41 establish a one-one correspondence.

Corollary 7. *There is a one to one correspondence between the set of normalized orthomorphisms of a group G and the set of left neofields, in which $1+1=0$, with multiplicative group G.*

Neofields in which $1+1\neq 0$ can be constructed from near orthomorphisms.

Theorem 42 (Hsu, Keedwell, 1984)**.** *Let G be a group, written multiplicatively with identity 1, let θ be a normalized near orthomorphism of G, with exdomain element t, and define $\theta'\colon G\cup\{0\}\to G\cup\{0\}$ by*

$$\theta'(g)=\begin{cases}0 & \text{if } g=t,\\ 1 & \text{if } g=0,\\ \theta(g) & \text{if } g\neq 0,t.\end{cases}$$

Then θ' is the presentation function of a left neofield in which $1+t=0$.

Proof. Similar to the proof of Theorem 40. □

This construction can be reversed.

Theorem 43 (Hsu, Keedwell, 1984)**.** *If θ is the presentation function of a left neofield, in which $1+t=0$, $t\neq 1$, with multiplicative group G, then θ, restricted to $G\setminus\{t\}$, is a normalized near orthomorphism of G with exdomain element t.*

Proof. Similar to the proof of Theorem 41. □

The constructions of Theorems 42 and 43 establish a one-one correspondence.

Corollary 8. *There is a one to one correspondence between normalized near orthomorphisms of a group G and left neofields, in which $1+1\neq 0$, with multiplicative group G.*

4.2. Properties of left neofields. We have associated to each neofield N a normalized orthomorphism of N^* if $1+1=0$ or a normalized near orthomorphism with exdomain element t if $1+t=0$ and $t\neq 1$. Thus properties of neofields and their additive loops can, in principle, be determined from their associated normalized orthomorphisms or normalized near orthomorphisms.

For normalized orthomorphisms of a group G the following maps will prove useful. For $\alpha\in Aut(G)$ the *homology* H_α is defined by $H_\alpha[\theta]=\alpha\theta\alpha^{-1}$; the *reflection* R is defined by $R[\theta](x)=x\theta(x^{-1})$; and the *inversion* I is defined by $I[\theta](x)=\theta^{-1}(x)$. All of these mappings map normalized orthomorphisms to normalized orthomorphisms. Homologies, and reflections preserve orthogonality, but inversion does not. However, if θ is a normalized orthomorphism, then there is a one-one correspondence between the normalized orthomorphisms orthogonal to θ and the normalized orthomorphisms orthogonal to $I[\theta]$ that preserves orthogonality. For more information about these and other mappings that map orthomorphisms into orthomorphisms see [19].

For normalized near orthomorphisms these same maps will be useful. The homologies and reflection are defined as for normalized orthomorphisms, but inversion must be defined differently. If θ is a normalized near orthomorphism of a group G with exdomain element t, then $I[\theta]$ is defined by $I[\theta](x) = t^{-1}\theta^{-1}(tx)$. The exdomain element for H_α is $\alpha(t)$, and the exdomain element for both $R[\theta]$ and $I[\theta]$ is t^{-1}.

Theorem 44. *When acting on the set of normalized orthomorphisms of a group, the following relationships hold between homologies, reflection and inversion.*

(1) $H_\alpha H_\beta = H_{\alpha\beta}$,
(2) $R^2 = 1$,
(3) $H_\alpha R = RH_\alpha$,
(4) $I^2 = 1$,
(5) $H_\alpha I = IH_\alpha$,
(6) $(IR)^3 = 1$.

Proof. Routine. □

The relationships in Theorem 44 still hold for actions on the set of normalized near orthomorphisms of a group except, possibly, for the last $(IR)^3 = 1$. If θ is a normalized near orthomorphism with exdomain element t, then $(IR)^3[\theta] = \theta$ if $t \in Z(G)$ and $t^2 = 1$.

The homologies that fix the normalized orthomorphism or normalized near orthomorphism associated with a left neofield determine automorphisms of the left neofield and instances of the right distributive law.

Theorem 45. *Let θ be a normalized orthomorphism or normalized near orthomorphism of a group G, let N be the left neofield constructed from θ, and let $\alpha \in Aut(G)$.*

(1) *α extends to an automorphism of N, by setting $\alpha(0) = 0$, if and only if $H_\alpha[\theta] = \theta$.*
(2) *If $\alpha(x) = c^{-1}xc$ then $H_\alpha[\theta] = \theta$ if and only if $(a+b)c = ac + bc$ for all $a, b \in N$.*

Proof. (1). If $a, b \neq 0$ then $\alpha(a+b) = \alpha(a) + \alpha(b)$ if and only if $\alpha(a\theta(a^{-1}b)) = \alpha(a)\theta(\alpha(a^{-1}b))$ if and only if $\alpha(\theta(a^{-1}b)) = \theta(\alpha(a^{-1}b))$. By setting $x = \alpha(a^{-1}b)$, this is seen to be true if and only if $\alpha\theta\alpha^{-1}(x) = \theta(x)$. Hence the result.

(2). If any of a, b, or c is zero then $(a+b)c = ac + bc$. If $a, b, c \neq 0$ then $(a+b)c = a\theta(a^{-1}b)c$ and $ac + bc = ac\theta(c^{-1}a^{-1}bc)$ and $a\theta(a^{-1}b)c = ac\theta(c^{-1}a^{-1}bc)$ if and only if $H_\alpha[\theta] = \theta$. □

An immediate corollary.

Corollary 9. *If N is the left neofield constructed from a normalized orthomorphism or a normalized near orthomorphisms θ of a group G, then*
$$Aut(N) = \{\alpha \in Aut(G) \mid H_\alpha[\theta] = \theta\}.$$

Theorem 45 yields a characterization of those normalized orthomorphisms and normalized near orthomorphisms that correspond to neofields.

Corollary 10. *Let θ be a normalized orthomorphism or normalized near orthomorphism of a group G, and let N be the left neofield constructed from θ. Then N is a neofield if and only if $H_\alpha[\theta] = \theta$ for all $\alpha \in Inn(G)$.*

Corollary 11. *If θ is a normalized near orthomorphism of a group G with exdomain element t corresponding to a neofield, then the $t \in Z(G)$.*

Proof. By Corollary 10, $H_\alpha[\theta] = \theta$ for all $\alpha \in Inn(G)$. As the exdomain element of $H_\alpha[\theta]$ is $\alpha(t)$, $\alpha(t) = t$ for all $\alpha \in Inn(G)$. The result follows. □

Let N be a left neofield. N is *commutative* if N^+ is commutative and *abelian* if N^* is abelian. N has the *right inverse property* if for all $a \in N$ there exists $(-a)_R \in N$ such that $(x + a) + (-a)_R = x$ for all $x \in N$. N has the *left inverse property* if for all $a \in N$ there exists $(-a)_L \in N$ such that $(-a)_L + (a + x) = x$ for all $x \in N$. N has the inverse property if it has both the left and right inverse properties. N has the exchange inverse property if for all $a \in N$ there exists $(-a)_L \in N$ such that $(-a)_L + (x+a) = x$ for all $x \in N$. If a left neofield N is constructed from a normalized orthomorphism or normalized near orthomorphism θ, then the properties N satisfies are determined by which elements of $\langle R, I\rangle$ fix θ.

Lemma 1. *Let N be a left neofield in which $1+t = 0$, $t \neq 1$. If N is commutative, satisfies the left inverse property, or satisfies the right inverse property, then $t^2 = 1$.*

Proof. If N is commutative, then $t + 1 = 0$ and so $t(1 + t^{-1}) = 0$, from which it follows that $t^{-1} = t$.

If N has the right inverse property then $(-t)_R = 1$ as $(1 + t) + (-t)_R = 1$ and then $(0 + t) + 1 = 0$, which again implies that $t^2 = 1$.

If N has the left inverse property then $(-1)_L = t$ as $(-1)_L + (1 + t) = t$ and then $t + (1 + 0) = 0$, which again implies that $t^2 = 1$. □

Theorem 46. *Let θ be a normalized orthomorphism of a group G, or a normalized near orthomorphism of G with exdomain element t, and let N be the left neofield constructed from θ.*

(1) *N is commutative if and only if $R[\theta] = \theta$.*
(2) *If $t \in Z(G)$ then N has the right inverse property if and only if $IRI[\theta] = \theta$.*
(3) *N has the left inverse property if and only if $I[\theta] = \theta$.*
(4) *If $t \in Z(G)$ then N has the inverse property if and only if $I[\theta] = \theta$ and $IRI[\theta] = \theta$.*
(5) *N has the exchange inverse property if and only if $RI[\theta] = \theta$.*

Proof. We will give the proof for the special case θ a normalized orthomorphism: thus $a + a = 0$ for all $a \in N$. The proof for the case θ a normalized near orthomorphism is similar except that it requires Lemma 1.

N is commutative if and only if $a + b = b + a$, for all $a, b \neq 0$, if and only if $a\theta(a^{-1}b) = b\theta(b^{-1}a)$, for all $a, b \neq 0$, if and only if $\theta(a^{-1}b) = (a^{-1}b)\theta((a^{-1}b)^{-1})$, for all $a, b \neq 0$, if and only if $R[\theta](a^{-1}b) = \theta(a^{-1}b)$, for all $a, b \neq 0$, if and only if $R[\theta] = \theta$.

If N has the right inverse property, then, as $(0+a)+(-a)_R = 0$, $(-a)_R = a$. If $a, x \neq 0$, then $(x + a) + a = x$ if and only if $\theta(\theta(x^{-1}a)^{-1}x^{-1}a) = \theta(x^{-1}a)^{-1}$ if and only if $\theta(y\theta^{-1}(y^{-1})) = y$, where $y = \theta(x^{-1}a)^{-1}$, if and only if $y\theta^{-1}(y^{-1}) = \theta^{-1}(y)$ if and only if $RI[\theta](y) = I[\theta](y)$ if and only if $IRI[\theta] = \theta$.

A similar proof shows that N has the left inverse property if and only if $I[\theta] = \theta$.

N has the inverse property if and only if N has both the right and left inverse properties, if and only if $I[\theta] = \theta$ and $IRI[\theta] = \theta$.

If N has the exchange inverse property then $(-a)_L = a$. If $a, x \neq 0$, then $a + (x + a) = x$ if and only if $a\theta(a^{-1}x\theta(x^{-1}a)) = x$ if and only if $RI[\theta](a^{-1}x) = \theta(a^{-1}x)$, if and only if $RI[\theta] = \theta$. □

Further correspondences between the properties of neofields and properties of the corresponding near orthomorphisms can be found in [39]. These properties were used in Hsu [31] in 1980 to classify cyclic neofields, i.e. neofields in which the multiplicative group is cyclic.

5. Final remarks

This survey of applications of complete mappings and orthomorphisms, and the related near complete mappings and near orthomorphisms is not exhaustive. We have tended to emphasize applications in which there is a clear relationship between properties of the mappings and properties of the algebraic and combinatorial structures constructed from them.

In Section 3, there are a number of variants of group sequencings that we did not cover: symmetrically harmonious orderings, R^*-sequencings, and 2-sequencings for instance. Readers interested in pursuing these topics should consult Ollis [49] or the chapter on sequenceable and R-sequenceable groups in Dénes and Keedwell's book [13].

Readers who want to know more about neofields should consult the papers by Hsu and Keedwell [34, 35] or the more recentpaper by Keedwell [41].

A number of applications are described in the papers in the reprint volumes [32, 33], edited by Hsu, and in the papers by Hsu and Keedwell [34, 35]. Other applications include the construction of Bol loops by Niederreiter and Robinson [48], Mittenthal's [47] use of orthomorphic mappings in cryptography, Wanless' [59] use of cyclotomic orthomorphisms in the construction of atomic latin squares, and Shaheen and Winterhof's [56] use of complete permutation polynomials to construct check digit systems.

References

[1] **B.A. Anderson**, *S_5, A_5 and all non-abelian groups of order* 32 *are sequenceable*, Congr. Numer. **58** (1987), 53–68.

[2] **B.A. Anderson**, *A fast method for sequencing low order non-abelian groups*, Ann. Discrete Math. **34** (1987), 27–42.

[3] **B.A. Anderson and E.C. Ihrig**, *Every finite solvable group with a unique element of order two, except the quaternion group, has a symmetric sequencing*, J. Combin. Des. **1** (1993), 3–14.

[4] **L. Baumert and M. Hall Jr.**, *Nonexistence of certain planes of order* 10 *and* 12, J. Combin. Theory Ser. A **14** (1973), 273–280.

[5] **R. Beals, J.A. Gallian, P. Headley and D. Jungreis**, *Harmonious groups*, J. Combin. Theory Ser. A **56** (1991), 223–238.

[6] **R.C. Bose, I.M. Chakravarti and D.E. Knuth**, *On methods of constructing sets of mutually orthogonal latin squares using a computer I*, Technometrics **2** (1960), 507–516.

[7] **J.N. Bray**, personal communication.

[8] **M.L. Cates and R.B. Killgrove**, *One-directional translation planes of order* 13, Congr. Numer. **32** (1981), 173–180.

[9] **A. Cayley**, *On the theory of groups as depending on the symbolical equation* $\theta^n = 1$, Phil. Mag. **7** (1854), 40–47.

[10] **A. Cayley**, *On the theory of groups*, Proc. London Math. Soc. **9** (1877/78), 126–133.

[11] **C.J. Colbourn and J.H. Dinitz (ed.)**, *Handbook of combinatorial designs*, 2nd ed. Chapman and Hall, CRC, Florida (2007).

[12] **J.Dénes and A.D. Keedwell**, *Latin squares and their applications*, English Universities Press, London (1974).

[13] **J.Dénes and A.D. Keedwell**, *Latin squares: New developments in the theory and applications*, Annals Discrete Math. **46**, North Holland (1991).

[14] **A.B. Evans**, *Orthomorphisms of Z_p*, Discrete Math. **64** (1987), 147–156.

[15] **A.B. Evans**, *On planes of prime order with translations and homologies*, J. Geom. **34** (1989), 36–41.

[16] **A.B. Evans**, *On strong complete mappings*, Congr. Numer. **70** (1990), 241–248.

[17] **A.B. Evans**, *Maximal sets of mutually orthogonal Latin squares I*, Europ. J. Combinatorics **12** (1991), 477–482.

[18] **A.B. Evans**, *Maximal sets of mutually orthogonal Latin squares II*, Europ. J. Combinatorics **13** (1992), 345–350.

[19] **A.B. Evans**, *Orthomorphism graphs of groups*, Lecture Notes Math. **1535**, Springer-Verlag (1992).

[20] **A.B. Evans**, *The admissibility of sporadic simple groups*, J. Algebra **321** (2009), 105–116.

[21] **A.B. Evans**, *The existence of strong complete mappings*, Electronic J. Combin. **19** (2012), # P34.

[22] **A.B. Evans**, *The strong admissibility of finite groups: an update*, submitted.

[23] **A.B. Evans and R.L. Mcfarland**, *Planes of prime order with translations*, Congr. Numer. **44** (1984), 41–46.

[24] **R.J. Friedlander, B. Gordon and M.D. Miller**, *On a group sequencing problem of Ringel*, Congr. Numer. **21** (1978), 307?-321.

[25] **B. Gordon**, *Sequences in groups with distinct partial products*, Pacific J. Math. **11** (1961), 1309–1313.

[26] **M. Hall and L.J. Paige**, *Complete mappings of finite groups*, Pacific J. Math. **5** (1955), 541–549.

[27] **A. Hedayat**, *A complete solution to the existence and non-existence of Knut Vic designs and orthogonal Knut Vic designs*, J. Combin. Theory Ser. A **22** (1977), 331–337.

[28] **A. Hedayat and W.T. Federer**, *On the non-existence of Knut Vic designs for all even orders*, Ann. Statist. **3** (1975), 445–447.

[29] **J.D. Horton**, *Orthogonal starters in finite abelian groups*, Discrete Math. **79** (1990), 265–278.

[30] **J. Hsiang, D.F. Hsu, and Y.-P. Shieh**, *On the hardness of computing problems of complete mappings*, Discrete Math. **277** (2004), 87–100.

[31] **D.F. Hsu**, *Cyclic neofields and combinatorial designs*, Springer-Verlag, Lecture Notes Math. **824** (1980).

[32] **D.F. Hsu (ed.)**, *Advances in discrete mathematics and computer science*, vol I, *Neofields and combinatorial designs*, Hadronic Press (1985).

[33] **D.F. Hsu (ed.)**, *Advances in discrete mathematics and computer science*, vol. II, *Generalized complete mappings*, Hadronic Press (1987).

[34] **D.F. Hsu and A.D. Keedwell**, *Generalized complete mappings, neofields, sequenceable groups and block designs. I*, Pacific J. Math. **111** (1984), 317–332.

[35] **D.F. Hsu and A.D. Keedwell**, *Generalized complete mappings, neofields, sequenceable groups and block designs. II*, Pacific J. Math. **117** (1985), 291–312.

[36] **D.M. Johnson, A.L. Dulmage and N.S. Mendelsohn**, *Orthomorphisms of groups and orthogonal latin squares, I.* Canad. J. Math. **13** (1961), 356–372.

[37] **D. Jungnickel and G. Grams**, *Maximal difference matrices of order* $\leqslant 10$, Discrete Math. **58** (1986), 199–203.

[38] **A.D. Keedwell**, *Latin squares P-quasigroups and graph decompositions*, Recueil des Travaux de l'Institute Mathématique, Belgrade, N.S. **1(9)** (1976), 41–48.

[39] **A.D. Keedwell**, *The existence of pathological left neofields*, Ars Combinatoria **16B** (1983), 161–170.

[40] **A.D. Keedwell**, *Sequenceable groups, generalized complete mappings, neofields and block designs*, Lecture Notes Math. **1036** (1983), 49–71.

[41] **A.D. Keedwell**, *Construction, properties and applications of finite neofields*, Comment. Math. Univ. Carolin. **41** (2000), 283–297.

[42] **A.D. Keedwell**, *Latin squares and their applications*, 2nd edition (in press).

[43] **F. Lazebnik and A. Thomason**, *Orthomorphisms and the construction of projective planes*, Math. Comp. **73** (2004), 1547–1557.

[44] **H.B. Mann**, *On orthogonal latin squares*, Bull. Amer. Math. Soc. **50** (1944), 249–257.

[45] **B.D. McKay, J.C. McLeod and I.M. Wanless**, *The number of transversals in a latin square*, Des. Codes Cryptogr. **40** (2006), 269–284.

[46] **N.S. Mendelsohn and B. Wolk**, *A search for a nondesarguesian plane of prime order*, Lecture Notes Pure and Appl. Math. **103** (1985), 199–208.

[47] **L. Mittenthal**, *Block substitutions using orthomorphic mappings*, Adv. in Appl. Math. **16** (1995), 59–71.

[48] **H. Niederreiter and K.H. Robinson**, *Bol loops of order pq*, Math. Proc. Camb. Phil. Soc. **89** (1981), 241–256.

[49] **M. A. Ollis**, *Sequenceable groups and related topics. Dynamic survey*, Electronic J. Combin. **20**(2) (2013), #DS10v2.

[50] **T.G. Ostrom**, *Replaceable nets, net collineations, and net extensions*, Canad. J. Math. **18** (1966), 666–672.

[51] **L.J. Paige**, *Neofields*, PhD dissertation, University of Wisconsin, 1947.

[52] **L.J. Paige**, *Neofields*, Duke Math. J. **16** (1949), 39–60.

[53] **L.J. Paige**, *Complete mappings of finite groups*, Pacific J. Math. **1** (1951), 111–116.

[54] **A. Pott**, *Maximal difference matrices of order q*, J. Combin. Des. **1** (1993), 171–176.

[55] **G. Ringel**, *Cyclic arrangements of the elements of a group*, Notices Amer. Math. Soc. **21** (1974), A95–96.

[56] **R. Shaheen and A. Winterhof**, *Permutations of finite fields for check digit systems*, Des. Codes Cryptogr. **57** (2010), 361–371.

[57] **Y.-P. Shieh, J. Hsiang, and D.F. Hsu**, *On the existence problems of complete mappings*, preprint.

[58] **I. Studicka**, *Non-existence of Cartesian groups of order $2p^m$*, Comment. Math. Univ. Carolin. **13** (1972), 721–725.

[59] **I.M. Wanless**, *Atomic latin squares based on cyclotomic orthomorphisms*, Electronic J. Combin. **12** (2005), # R22.

[60] **S. Wilcox**, *Reduction of the Hall-Paige conjecture to sporadic simple groups*, J. Algebra **321** (2009), 1407–1428.

Received May 15, 2015

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio, USA
E-mail: anthony.evans@wright.edu

Quasigroups and Related Systems **23** (2015), 31 – 39

Describing cyclic extensions of Bol loops

Stephen M. Gagola III

Abstract. It was shown in [4] that if a Moufang loop G factorizes as $G = NH$ where N is a normal subloop and $H = \langle u \rangle = \langle u^3 \rangle$ is a cyclic group then the structure of G is determined by the binary operation of N, the intersection $N \cap H$ and how u permutes the elements of N as a semi-automorphism of N. Here it is shown that if G is Moufang with $H = \langle u \rangle \neq \langle u^3 \rangle$ or if G is a Bol loop, not necessarily Moufang, then the structure of G is determined by the binary operation of N, the intersection $N \cap H$, how u permutes the elements of N and either of the two binary operations $x *_1 y = (xu)(u \backslash y)$ or $x *_{-1} y = (xu^{-1})(u^{-1} \backslash y)$ of N.

1. Introduction

A *quasigroup* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that for any $a, b \in Q$, the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions $x, y \in Q$ respectively. A quasigroup is a *loop* if it contains a two-sided identity element. A *right Bol loop* is a loop Q which, for all $x, y, z \in Q$, satisfies the right Bol relation

$$((zx)y)x = z((xy)x).$$

Similarly, a loop Q is a *left Bol loop* provided it satisfies the right Bol relation

$$x(y(xz)) = (x(yx))z.$$

Recently the structure and construction of Bol loops has caught the attention of many including Chein and Goodaire [1, 2] along with Foguel, Kinyon and Phillips [3].

Here the focus will be on (right) Bol loops of the form $Q = NH$ where $N \trianglelefteq Q$ and $H = \langle u \rangle$ is cyclic. It is well known for groups that the binary operation of Q depends only on the binary operation of N, the intersection $N \cap H$ and how H acts on N. Likewise, it was shown in [4] that the same is true for Moufang loops as long as $H = \langle u \rangle = \langle u^3 \rangle$. Generalizing to Bol loops, it is shown here how such extensions depend on the maps

$$\begin{aligned} f_{m,n} &: N \longrightarrow N \\ &\quad g \longmapsto (u^m(gu^n))u^{-m-n}. \end{aligned}$$

2010 Mathematics Subject Classification: 20E22, 20E34, 20N05
Keywords: Extensions, semidirect products.

Furthermore, the structure of Q depends not only on the structure of N, the intersection $N \cap H$ and the maps $f_{n,m}$ but also on the Bol loops $(N, *_i)$ where

$$x *_i y = (xu^i)(u^i \backslash y).$$

For instance, there exists a nonassociative right Bol loop $Q = NH$ of order eight (the mirror version of the left Bol loop LeftBolLoop(8,2) in GAP [5]) where $N \cong C_2 \times C_2$, $H \cong C_2$ and $f_{m,n} : N \to N$ is the identity map for all $m, n \in \mathbb{Z}$. But since Q is nonassociative, $Q \ncong C_2 \times C_2 \times C_2$. This is because the cyclic extension also depends on the Bol loop $(N, *_1)$ which is not the Klein four-group but rather the cyclic group of order four.

2. Preliminaries

For every element, say a, of a quasigroup Q one can define the *right translation* $R_a : Q \longrightarrow Q$ by $(x)R_a = xa$ and the *left translation* $L_a : Q \longrightarrow Q$ by $(x)L_a = ax$. By definition of a quasigroup, all such translations are bijections of Q. Let

$$x \backslash y = yL_x^{-1} \quad \text{and} \quad x/y = xR_y^{-1}$$

and note that

$$x \backslash y = z \Longleftrightarrow y = xz \quad \text{and} \quad x/y = w \Longleftrightarrow x = wy.$$

Such operations \ and / are called the left and right divisions respectively. The *multiplication group* of Q, denoted by $\mathrm{Mlt}(Q)$, is the permutation group generated by all left and right translations of Q. If Q is a loop with an identity element 1 then the *inner mapping group* of Q, denoted by $\mathrm{Inn}(Q)$, is the stabilizer of 1 in $\mathrm{Mlt}(Q)$.

Two quasigroups $(Q_1, *)$ and $(Q_2, \circ)$ are called *isotopic* if there exist three bijections $f, g, h : Q_1 \longrightarrow Q_2$ such that $f(x * y) = g(x) \circ h(y)$ for any $x, y \in Q_1$.

Lemma 1. *Every quasigroup $(Q, *)$ is isotopic to a loop. For $a, b \in Q$, $(Q, *)$ is isotopic to $(Q, \circ)$ where*

$$x \circ y = (x)R_b^{-1} * (y)L_a^{-1}$$

or equivalently

$$(x * b) \circ (a * y) = x * y.$$

Here $(a * b) \circ x = x = x \circ (a * b)$ for any $x \in Q$.

A loop Q is said to be *power-associative* if for any element $x \in Q$, the subloop generated by x is a group. A loop Q is *diassociative* if for any $x, y \in Q$, the subloop generated by x and y is a group. A loop Q is *left power-alternative,* if for any $x, y \in Q$,

$$x^m(x^n y) = x^{m+n} y$$

for all integers m and n. Similarly, Q is *right power-alternative,* if for any $x, y \in Q$,

$$(yx^m)x^n = yx^{m+n}$$

for all integers m and n. A loop Q is *power-alternative* if it is both left and right power-alternative.

Robinson [6] made the simple observation that right (left) Bol loops are right (left) power-alternative. Let Q be a right Bol loop with $u \in Q$ and define $x *_i y = (xu^i)(u^i \backslash y)$ for any $x, y \in Q$. Since right Bol loops are right power-alternative,

$$\begin{aligned} x *_i y &= (xu^i)(u^i \backslash y) \\ &= (x/u^{-i})(u^i \backslash y) \end{aligned}$$

and $(Q, *_i)$ is a loop isotopic to Q.

Lemma 2. (cf. [7]) *Let Q be a (right) Bol loop. Then all loop isotopes of Q are isomorphic to Q.*

From this it follows that $(Q, *_i)$ is a right Bol loop isomorphic to the original loop Q.

3. Diassociative Bol loops

It is well known that a Bol loop is diassociative if and only if it is a Moufang loop. As mentioned in [4], cyclic extensions $Q = NH$ resulting in such loops depend on more than just how H acts on N when $\langle u^3 \rangle \subsetneqq \langle u \rangle = H$.

Theorem 1. *Let Q be a right Bol loop. Suppose $Q = NH$ where $N \trianglelefteq Q$ and $H = \langle u \rangle$. If Q is diassociative then for any $x, y \in N$ and any $m, n \in \mathbb{Z}$*

$$(xu^m)(yu^n) = (x *_{2m+n} f^m(y))u^{m+n} \tag{1}$$

where

$$\begin{aligned} f : N &\longrightarrow N \\ g &\longmapsto ugu^{-1} \end{aligned}$$

and $(Q, *_i)$ is a right Bol loop isomorphic to Q with $x *_i y = (xu^i)(u^i \backslash y) = (xu^i)(u^{-i}y)$.

Proof. By Lemma 2, $(Q, *_i)$ is isomorphic to Q. For any $x, y \in N$ and any $m, n \in \mathbb{Z}$

$$\begin{aligned} (xu^m)(yu^n) &= (xu^m)\big(u^n \cdot u^{-n}y \cdot u^n\big) \\ &= \big[(xu^m)u^n \cdot \big(u^{-n}y\big)\big]\, u^n \\ &= \big[\big(xu^{m+n}\big)\big(u^m \cdot u^{-m-n}yu^{-m} \cdot u^m\big)\big]\, u^n \\ &= \big[\big(xu^{m+n}\big)u^m \cdot \big(u^{-m-n}yu^{-m}\big)\big]\, u^m \cdot u^n \\ &= \big[\big(xu^{2m+n}\big)\big(u^{-2m-n}f^m(y)\big)\big]\, u^m \cdot u^n \\ &= (x *_{2m+n} f^m(y))\, u^{m+n}. \end{aligned}$$

□

If $2m+n \equiv 0 \pmod 3$ then, from Equation (1) of [4], the binary operation $*_{2m+n}$ is uniquely determined by $f : g \longmapsto ugu^{-1}$. But if $2m+n \not\equiv 0 \pmod 3$ then $x *_{2m+n} y$ depends on f along with either of the two operations $*_1$ or $*_{-1}$.

Lemma 3. *Let Q be a diassociative Bol loop with $u \in Q$. For any $x, y \in Q$ define $x *_i y = (xu^i)(u^{-i}y)$ and $f : Q \longrightarrow Q$ as $f(x) = uxu^{-1}$. If $2m+n \equiv 1 \pmod 3$, that is $2m+n = 3k+1$, then*

$$x *_{2m+n} y = f^k\big(f^{-k}(x) *_1 f^{-k}(y)\big)\,.$$

Likewise, if $2m+n \equiv 2 \pmod 3$ and $2m+n = 3k+2$ then

$$x *_{2m+n} y = f^{k+1}\big(f^{-k-1}(x) *_{-1} f^{-k-1}(y)\big)\,.$$

Proof. If $2m+n = 3k+1$ then, by using Equation (1) of [4],

$$\begin{aligned} x *_{2m+n} y &= \big(xu^{3k+1}\big)\big(u^{-3k-1}y\big) \\ &= \big(xuu^{3k}\big)\big(u^{-1}f^{-3k}(y)u^{-3k}\big) \\ &= f^k\big(f^{-k}(xu)f^{2k}(u^{-1}f^{-3k}(y))\big) \\ &= f^k\big(f^{-k}(x)u \cdot u^{-1}f^{-k}(y)\big) \\ &= f^k\big(f^{-k}(x) *_1 f^{-k}(y)\big)\,. \end{aligned}$$

Similarly, if $2m+n = 3k+2$ then $x *_{2m+n} y = f^{k+1}\big(f^{-k-1}(x) *_{-1} f^{-k-1}(y)\big)$. □

Note that for any integers i and k, $x *_i y = f^k\big(f^{-k}(x) *_{i-3k} f^{-k}(y)\big)$. In other words

$$f^k(x *_i y) = f^k(x) *_{i+3k} f^k(y). \tag{2}$$

From [4] it is known that if $Q = NH$ is a Moufang loop where $N \trianglelefteq Q$ and $H = \langle u \rangle = \langle u^3 \rangle$ then the binary operation of Q depends only on the binary operation of N, the intersection $N \cap H$ and how u permutes the elements in N. Thus without loss it can be assumed that $H = \langle u \rangle \neq \langle u^3 \rangle$ in which case the binary operation of Q also depends on the loops $(N, *_1)$ and $(N, *_{-1})$.

Theorem 2. *Let Q be a right Bol loop. Suppose $Q = NH$ where $N \trianglelefteq Q$ and $H = \langle u \rangle$ with $\langle u^3 \rangle \lneqq H$. If Q is diassociative then for any $x, y \in N$*

$$(xu^m)(yu^n) = \begin{cases} f^k\big(f^{-k}(x) *_1 f^{m-k}(y)\big)\,u^{m+n} & \text{if } 2m+n = 3k+1; \\ f^{k+1}\big(f^{-k-1}(x) *_{-1} f^{m-k-1}(y)\big)\,u^{m+n} & \text{if } 2m+n = 3k+2; \end{cases}$$

where

$$\begin{aligned} f : N &\longrightarrow N \\ g &\longmapsto ugu^{-1} \end{aligned}$$

and $(Q, *_i)$ is a right Bol loop isomorphic to Q with $x *_i y = (xu^i)(u^{-i}y)$.

Proof. By Theorem 1, $(xu^m)\,(yu^n) = (x *_{2m+n} f^m(y))u^{m+n}$ for any $x, y \in N$. If $2m + n = 3k + 1$ then, by Lemma 3,

$$\begin{aligned} x *_{2m+n} f^m(y) &= f^k\big(f^{-k}(x) *_1 f^{-k}(f^m(y))\big) \\ &= f^k\big(f^{-k}(x) *_1 f^{m-k}(y)\big)\,. \end{aligned}$$

Hence, $(xu^m)(yu^n) = f^k\big(f^{-k}(x) *_1 f^{m-k}(y)\big)\,u^{m+n}$. Similarly, if $2m+n = 3k+2$ then $(xu^m)(yu^n) = f^{k+1}\big(f^{-k-1}(x) *_{-1} f^{m-k-1}(y)\big)\,u^{m+n}$. □

From this we see that these extensions by cyclic groups with orders divisible by three depend on the permutation $f(x) = uxu^{-1}$ along with the binary operations $*_1$ and $*_{-1}$. In Section 4 it will be shown that such extensions depend on f along with just one of the binary operations $*_1$ or $*_{-1}$.

Proposition 1. *Suppose $Q = NH$ is a loop where $N \trianglelefteq Q$ and $H = \langle u \rangle$. For any $x, y \in N$ let*

$$\begin{aligned} f : N &\longrightarrow N \\ g &\longmapsto (ug)u^{-1} \end{aligned}$$

and $x *_i y = (xu^i)(u^{-i}y)$. If Q is a diassociative right Bol loop then

$$(x *_{t-s} y) *_t (z *_{t+s} f^s(x)) = x *_{2r-s} ((y *_t z) *_{2r} f^s(x)) \tag{3}$$

for any $r, s, t \in \mathbb{Z}$ and any $x, y, z \in N$. Furthermore, Q is a diassociative right Bol loop if and only if equations (1), (2) *and* (3) *hold.*

Proof. Let $x, y, z \in Q$ and $k, m, n \in \mathbb{Z}$. Using Equations (1) and (2) it follows that

$$\begin{aligned} &\Big((xu^k)\,(f^{-k}(y)u^m)\Big)\Big((f^{-k-m}(z)u^n)(xu^k)\Big) = \\ &\qquad = (x *_{2k+m} y)\,u^{k+m} \cdot \Big(f^{-k-m}(z) *_{2n+k} f^n(x)\Big)u^{n+k} \\ &\qquad = \Big((x *_{2k+m} y) *_{3k+2m+n} f^{k+m}(f^{-k-m}(z) *_{2n+k} f^n(x))\Big)u^{2k+m+n} \\ &\qquad = \Big((x *_{2k+m} y) *_{3k+2m+n} (z *_{4k+3m+2n} f^{k+m+n}(x))\Big)u^{2k+m+n} \end{aligned}$$

and

$$\begin{aligned} &(xu^k)\Big[(f^{-k}(y)u^m)(f^{-k-m}(z)u^n) \cdot (xu^k)\Big] = \\ &\quad = (xu^k)\,\Big[\Big(f^{-k}(y) *_{2m+n} f^{-k}(z)\Big)u^{m+n} \cdot (xu^k)\Big] \\ &\quad = (xu^k)\,\Big[\Big(f^{-k}(y) *_{2m+n} f^{-k}(z)\Big) *_{k+2m+2n} f^{m+n}(x) \cdot u^{k+m+n}\Big] \\ &\quad = \Big[x *_{3k+m+n} f^k\Big(\Big(f^{-k}(y) *_{2m+n} f^{-k}(z)\Big) *_{k+2m+2n} f^{m+n}(x)\Big)\Big]u^{2k+m+n} \\ &\quad = \Big[x *_{3k+m+n}\Big(f^k\Big(f^{-k}(y) *_{2m+n} f^{-k}(z)\Big) *_{4k+2m+2n} f^{k+m+n}(x)\Big)\Big]u^{2k+m+n} \\ &\quad = \Big[x *_{3k+m+n}\Big((y *_{3k+2m+n} z) *_{4k+2m+2n} f^{k+m+n}(x)\Big)\Big]u^{2k+m+n}. \end{aligned}$$

By letting $s = k + m + n$, $t = 3k + 2m + n$ and $r = 2k + m + n$ (i.e., $k = r - s$, $m = t + s - 2r$ and $n = s - t + r$)

$$\big((xu^k)(f^{-k}(y)u^m)\big)\big((f^{-k-m}(z)u^n)(xu^k)\big) = (x *_{t-s} y) *_t (z *_{t+s} f^s(x))$$

and

$$(xu^k)\big[(f^{-k}(y)u^m)(f^{-k-m}(z)u^n) \cdot (xu^k)\big] = x *_{2r-s} ((y *_t z) *_{2r} f^s(x)).$$

Hence, Q satisfies the Moufang identities if and only if Equations (1), (2) and (3) hold. □

Note that by letting $y = 1$, Equation (3) simplifies to

$$x *_t (z *_{t+s} f^s(x)) = x *_{2r-s} (z *_{2r} f^s(x)).$$

Since the right hand side of the equality is independent of t,

$$x *_{t_1} (z *_{t_1+s} f^s(x)) = x *_{t_2} (z *_{t_2+s} f^s(x))$$

for any $t_1, t_2 \in \mathbb{Z}$. Similarly, by letting $z = 1$ in Equation (3) and using a similar argument it follows that

$$(x *_{t_1} y) *_{t_1+s} f^s(x) = x *_{t_2} (y *_{t_2+s} f^s(x))$$

for any $t_1, t_2 \in \mathbb{Z}$. Therefore, from Equation (3) it follows that if Q is a diassociative right Bol loop then

$$\begin{aligned}(x *_{n-k} y) *_n (z *_{n+k} f^k(x)) &= x *_{m-k} ((y *_n z) *_m f^k(x)) \\ &= (x *_{\ell-k} (y *_n z)) *_\ell f^k(x)\end{aligned}$$

for any $x, y, z \in Q$ and $k, m, n, \ell \in \mathbb{Z}$.

4. The general case

Here Theorem 1 will be generalized for cyclic extensions resulting in arbitrary right Bol loops. The following is a useful lemma that will be used to prove the main result.

Lemma 4. *If Q is a right Bol loop with $u \in Q$ then $u \backslash x = \big(u^{-1}(xu)\big)\, u^{-1}$ for any $x \in Q$.*

Proof. For any $x \in Q$,

$$\begin{aligned} u\left[\big(u^{-1}(xu)\big)\, u^{-1}\right] &= \big((uu^{-1})(xu)\big)\, u^{-1} \\ &= (xu)u^{-1} \\ &= x. \end{aligned}$$

□

Theorem 3. *If $Q = NH$ is a right Bol loop with $N \trianglelefteq Q$ and $H = \langle u \rangle \leq Q$ then for any $x, y \in N$ and any $m, n \in \mathbb{Z}$*

$$(xu^m)\,(yu^n) = (x *_{2m+n} f_{m,n}(y))\,u^{m+n} \tag{4}$$

where

$$\begin{aligned} f_{m,n} : N &\longrightarrow N \\ g &\longmapsto (u^m\,(gu^n))\,u^{-m-n} \end{aligned}$$

and $(Q, *_i)$ is a right Bol loop isomorphic to Q with $x *_i y = (xu^i)(u^i \backslash y)$.

Proof. By Lemma 2, $(Q, *_i)$ is isomorphic to Q. Furthermore, for any $x, y \in N$ and any $m, n \in \mathbb{Z}$

$$\begin{aligned} (xu^m)\,(yu^n) &= \big((xu^{2m+n}u^{-m-n})(yu^n)\big)u^{-m-n}u^{m+n} \\ &= \big[(xu^{2m+n})\big[(u^{-m-n}(yu^n))u^{-m-n}\big]\big]u^{m+n} \\ &= \big[(xu^{2m+n})\big[(u^{-2m-n}u^m(yu^n))u^m \cdot u^{-2m-n}\big]\big]u^{m+n} \\ &= \big[(xu^{2m+n})\big[\big[u^{-2m-n}((u^m(yu^n))u^m)\big]u^{-2m-n}\big]\big]u^{m+n} \\ &= \big[(xu^{2m+n})\big[\big[u^{-2m-n}\big((u^m(yu^n))u^{-m-n} \cdot u^{2m+n}\big)\big]u^{-2m-n}\big]\big]u^{m+n} \\ &= \big[(xu^{2m+n})\big[\big[u^{-2m-n}\big(f_{m,n}(y)u^{2m+n}\big)\big]u^{-2m-n}\big]\big]u^{m+n} \\ &= \big[(xu^{2m+n})\big(u^{2m+n}\backslash f_{m,n}(y)\big)\big]u^{m+n} \\ &= (x *_{2m+n} f_{m,n}(y))u^{m+n}. \end{aligned}$$

□

Since right Bol loops are right power-alternative, it should be noted that $f_{m,n} : g \mapsto (u^m\,(gu^n))\,u^{-m-n}$ is the identity map whenever $m = 0$. Therefore, from Theorem 3, it follows that in any right Bol loop $x(yu^n) = (x *_n y)u^n$.

Proposition 2. *Suppose Q is a right Bol loop with $u \in Q$. Let*

$$\begin{aligned} f_{i,j} : Q &\longrightarrow Q \\ g &\longmapsto \big(u^i\,(gu^j)\big)\,u^{-i-j} \end{aligned}$$

and $(Q, *_i)$ be the right Bol loop isomorphic to Q with $x *_i y = (xu^i)(u^i \backslash y)$. Then by knowing the maps $f_{i,j}$ along with $(Q, *_n)$ and $(Q, *_{n+1})$ for some fixed integer n, the Bol loop $(Q, *_k)$ is uniquely determined for any integer k.

Proof. Since Q is a right Bol loop,

$$z\big((xu^{n-2m})u^{3m-n} \cdot (xu^{n-2m})\big) = \big((z(xu^{n-2m}))u^{3m-n}\big)(xu^{n-2m})$$

for any $z, x \in N$ and any $n, m \in \mathbb{Z}$. Therefore, by Theorem 3,

$$\begin{aligned}
& z\big((xu^{n-2m})u^{3m-n} \cdot (xu^{n-2m})\big) = \big((z(xu^{n-2m}))u^{3m-n}\big)(xu^{n-2m}) \\
\Longrightarrow \quad & z\big((xu^{m})(xu^{n-2m})\big) = \big(((z *_{n-2m} x)u^{n-2m})u^{3m-n}\big)(xu^{n-2m}) \\
\Longrightarrow \quad & z\big((x *_n f_{m,n-2m}(x))u^{n-m}\big) = ((z *_{n-2m} x)u^{m})(xu^{n-2m}) \\
\Longrightarrow \quad & (z *_{n-m} (x *_n f_{m,n-2m}(x)))u^{n-m} = ((z *_{n-2m} x) *_n f_{m,n-2m}(x))u^{n-m} \\
\Longrightarrow \quad & z *_{n-m} (x *_n f_{m,n-2m}(x)) = (z *_{n-2m} x) *_n f_{m,n-2m}(x). \qquad (5)
\end{aligned}$$

By letting $m = -1$, Equation (5) becomes

$$z *_{n+1} (x *_n f_{-1,n+2}(x)) = (z *_{n+2} x) *_n f_{-1,n+2}(x).$$

Whereas, by replacing n with $n+1$ and m with 1, Equation (5) becomes

$$z *_{n} (x *_{n+1} f_{1,n-1}(x)) = (z *_{n-1} x) *_{n+1} f_{1,n-1}(x).$$

Hence, with the operations $*_n$ and $*_{n+1}$, both $z *_{n+2} x$ and $z *_{n-1} x$ can be determined for any elements z and x. By induction, $*_k$ can then be obtained for any $k \in \mathbb{Z}$. □

Since $*_0$ is just the original binary operation of N, by letting n be either 0 or -1, it immediately follows that for any integer k the Bol loop $(Q, *_k)$ is uniquely determined by the maps $f_{i,j}$, the subloop N and either $(N, *_1)$ or $(N, *_{-1})$.

Corollary 1. *If $Q = NH$ is a right Bol loop with $N \trianglelefteq Q$ and $H = \langle u \rangle \leq Q$ then for any $x, y \in N$ and any $m, n \in \mathbb{Z}$ the product $(xu^m)(yu^n)$ is uniquely determined by the subloops N and $N \cap H$ along with the maps*

$$\begin{aligned}
f_{m,n} : N &\longrightarrow N \\
g &\longmapsto (u^m\,(gu^n))\,u^{-m-n}
\end{aligned}$$

and one of the two Bol loops $(N, *_1)$ or $(N, *_{-1})$ where $x *_i y = (xu^i)(u^i \backslash y)$.

But if $[Q, N] = 2$ then much of the Cayley table of $(N, *_1)$ may be determined by N and the maps $f_{i,j}$.

Proposition 3. *Suppose $Q = NH$ is a right Bol loop with $N \trianglelefteq Q$ and $H = \langle u \rangle \leq Q$ where $[Q : N] = 2$. Then for any $z \in N$ and*

$$y \in \{x *_2 f_{1,0}(x) \mid x \in N\} = \{(x(f_{1,0}(x)u^2))u^{-2} \mid x \in N\} \subseteq N,$$

$z *_1 y = (zu)(u \backslash y)$ is uniquely determined by the binary operation of N and

$$\begin{aligned}
f_{1,0} : N &\longrightarrow N \\
g &\longmapsto (ug)u^{-1}.
\end{aligned}$$

Proof. By Lemma 4, for any $a, x \in Q$,

$$\begin{aligned} a *_2 f_{1,0}(x) &= \big(au^2\big)\big(u^2\backslash f_{1,0}(x)\big) \\ &= \big(au^2\big)\big(u^{-2}\big(f_{1,0}(x)u^2\big)\cdot u^{-2}\big) \\ &= \big(au^2\cdot u^{-2}\big)\big(f_{1,0}(x)u^2\big)\cdot u^{-2} \\ &= a\big(f_{1,0}(x)u^2\big)\cdot u^{-2}. \end{aligned}$$

Since Q is a right Bol loop, for any $x, z \in N$, $z((xu)x) = ((zx)u)x$. Thus, by Theorem 3,

$$\begin{aligned} & & z((xu)x) &= ((zx)u)x \\ &\Longrightarrow & z((x *_2 f_{1,0}(x))u) &= ((zx) *_2 f_{1,0}(x))\, u \\ &\Longrightarrow & (z *_1 (x *_2 f_{1,0}(x)))\, u &= ((zx) *_2 f_{1,0}(x))\, u \\ &\Longrightarrow & z *_1 (x *_2 f_{1,0}(x)) &= (zx) *_2 f_{1,0}(x) \\ &\Longrightarrow & z *_1 \big(x\big(f_{1,0}(x)u^2\big)\cdot u^{-2}\big) &= (zx)\big(f_{1,0}(x)u^2\big)\cdot u^{-2}. \end{aligned}$$

Since $[Q : N] = 2$, $u^2 \in N$. Hence, for any elements $z \in N$ and

$$y \in \{x *_2 f_{1,0}(x) \mid x \in N\} = \{(x(f_{1,0}(x)u^2))u^{-2} \mid x \in N\} \subseteq N,$$

$z *_1 y$ is uniquely determined by $f_{1,0}$ and the binary operation of N. □

Acknowledgment. The author would like to thank Ales Drápal for the idea that certain loop extensions depend also on the binary operations $x * y = (x/u)(u^{-1}\backslash y)$.

References

[1] **O. Chein and E.G. Goodaire**, *A new construction of Bol loops of order 8k*, J. Algebra **287** (2005), 103–122.

[2] **O. Chein and E.G. Goodaire**, *A new construction of Bol loops: the "odd" case*, Quasigroups and Related Systems **13** (2005), 87–98.

[3] **T. Foguel, M.K. Kinyon and J.D. Phillips**, *On twisted subgroups and Bol loops of odd order*, Rocky Mountain J. Math. **36** (2006), 183–212.

[4] **S.M. Gagola III**, *Cyclic extensions of Moufang loops induced by semi-automorphisms*, J. Algebra Appl. **13** (2014), no. 4, 1350128, 7 p.

[5] **The GAP Group**, *GAP-Groups, Algorithms, and Programming*, Version 4.4.12, 2008, http://www.gap-system.org.

[6] **D.A. Robinson**, *Bol loops*, Trans. Amer. Math. Soc. **123** (1966), 341–354.

[7] **D.A. Robinson**, *A Bol loop isomorphic to all loop isotopes*, Proc. Amer. Math. Soc. **19** (1968), 671–672.

Received March 20, 2015

School of Mathematics, University of the Witwatersrand, 2050 Johannesburg. South Africa
E-mail: stephen.gagolaiii@wits.ac.za

Quasigroups and Related Systems **23** (2015), 41 − 90

Design of crypto primitives based on quasigroups

Smile Markovski

Abstract. Today, the security of the modern world is undoubtedly dependent on the cryptographic primitives built into the various protocols used for secure communication. Let us mention here the most important, like block ciphers, stream ciphers, digital signatures and encryption schemes, hash functions, pseudo random number generators, ... The design of these, and many other crypto primitives, uses different concepts from number theory, group and finite field theory, Boolean algebras, etc. In this survey article we will present how quasigroups can be used for construction of various crypto primitives. We will discuss especially what type of quasigroups are used and how they can be constructed. Some open research problem will be mentioned as well.

1. Introduction

It is well known that *One-time-pad* is the only information theoretically secure cryptographic product, i.e., there is a mathematical proof of its security. All other cryptographic primitives that are massively used for different purposes in communication, banking, commerce and many other today human activities, have security based on three facts: first one is the believing (that some mathematical problems are hard to be solved), the second one is the experience (some cryptographic primitives cannot be broken after several years, even decades, of attacking), and the third one is the adjusting (whenever a weakness of some used cryptographic system is found, it is immediately repaired or changed). Thus, in the last decades no catastrophic damage was made of breaking some cryptographic product (maybe ENIGMA was the last one, more than seventy years ago).

Having in mind the previous, we realized that designs of new cryptographic primitives, products, systems, algorithms, protocols etc. have as well theoretical as practical importance. Nowadays, crypto primitives are produced mainly by using results from number and group theory, finite field theory, Boolean algebras and functions, and all of them are associative structures. We think that broadening the set of used theories with non-associative mathematical structures, like quasigroup

2010 Mathematics Subject Classification: 20N05, 94A60, 68P25
Keywords: Quasigroups (left, right, n-ary, huge, orthogonal, MQQ, MQLQ), cryptographic primitives, quasigroup transformations, cryptographic S-boxes, block ciphers, stream ciphers, PRNGs, hush functions, signatures, public encryptions schemes.

theory, that can be used for making suitable cryptographic primitives, is also important. In such a way cryptographic primitives with different properties of the existing ones can be obtained, hence the domain of the crypto primitives will be enlarged.

In this paper we show how the quasigroups can be used for building different type of cryptographic primitives. For that aim we define some type of quasigroups that are suitable for that purpose (Section 2), we give the definitions of several kinds of quasigroup transformations (Section 3), and we explain the constructions of some types of cryptographic primitives obtained by quasigroup transformations (Section 4). The last section contains discussion and conclusion.

2. Quasigroups

We start by giving a brief overview of the quasigroup theory that we will use in the sequel.

Definition 1. *A quasigroup $(Q,*)$ is a groupoid, i.e., a set Q with binary operation $*: Q^2 \to Q$, satisfying the law*

$$(\forall u,v \in Q)(\exists!\ x,y \in Q) \quad u*x = v \ \&\ y*u = v. \tag{1}$$

The definition is equivalent to the statements that $*$ is a cancellative operation $(x*y = x*z \Rightarrow y = z,\ y*x = z*x \Rightarrow y = z)$ and the equations $a*x = b,\ y*a = b$ have solutions $x,\ y$ for each $a,b \in Q$.

In this paper we need only finite quasigroups, i.e., the order $|Q|$ of a quasigroup Q is a finite positive integer. Closely related combinatorial structures to finite quasigroups are the so called Latin squares:

Definition 2. *A Latin square L on a finite set Q of cardinality $|Q| = n$ is an $n \times n$-matrix with elements from Q such that each row and each column of the matrix is a permutation of Q.*

To any finite quasigroup $(Q,*)$, given by its multiplication table, there can be associated a Latin square L consisting of the matrix formed by the main body of the table, and each Latin square L on a set Q defines at most $|Q|!^2$ quasigroups $(Q,*)$ (obtained by all possible bordering).

A relation of *isotopism* and between two quasigroups are defined as follows.

Definition 3. *A quasigroup $(K,*)$ is said to be isotopic to a quasigroup $(Q,\bullet)$ if and only if there are bijections $\alpha,\ \beta,\ \gamma$ from K onto Q such that $\gamma(x*y) = \alpha(x)\bullet\beta(y)$ for each $x,y \in K$. Then the triple (α,β,γ) is called an isotopism from $(K,*)$ to $(Q,\bullet)$.*

Given a quasigroup $(Q,*)$ five new operations, so called parastrophes or adjoint operations, denoted by $\backslash,\ /,\ \bullet,\ \backslash\backslash,\ //$, can be derived from the operation $*$ as follows:

$$x*y = z \Leftrightarrow y = x\backslash z \Leftrightarrow\ x = z/y \Leftrightarrow y\bullet x = z \Leftrightarrow\ y = z\backslash\backslash x\ \Leftrightarrow\ x = y//z. \tag{2}$$

Then the algebras $(Q, *, \backslash, /)$ and $(Q, \bullet, \backslash\backslash, //)$ satisfy the identities

$$x \backslash (x * y) = y,\ x * (x \backslash y) = y,\ (x * y)/y = x,\ (x/y) * y = x \tag{3}$$

$$y = (x * y) \backslash\backslash x = (y \bullet x) \backslash\backslash x,\ x = y//(x * y) = y//(y \bullet x),$$
$$y = x * (y \backslash\backslash x) = (y \backslash\backslash x) \bullet x,\ x = (y//x) * y = y \bullet (y//x), \tag{4}$$

and $(Q, \backslash)$, $(Q, /)$, $(Q, \bullet)$ $(Q, \backslash\backslash)$, $(Q, //)$ are quasigroups too.

2.1. n-ary, left and right quasigroups

An n-ary quasigroup is a pair (Q, f) of a nonempty set Q and an n-ary operation f with the property that given any n of the elements $a_1, a_2, \dots, a_{n+1} \in Q$, the $n+1$-th is uniquely determined the equality $f(a_1, a_2, \dots, a_n) = a_{n+1}$ hold true. A quasigroup is a binary (2-ary) quasigroup. Given n-ary quasigroup (Q, f), we define n operations $f_1, f_2, \dots, f_n$ by

$$f(a_1, a_2, \dots, a_n) = a_{n+1} \Leftrightarrow f_i(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n) = a_i.$$

Then the following identities holds, for each $i = 1, 2, \dots, n$:

$$f(a_1, \dots, a_{i-1}, f_i(a_1, \dots, a_n), a_{i+1} \dots, a_n) = a_i,$$
$$f_i(a_1, \dots, a_{i-1}, f(a_1, a_2, \dots, a_n), a_{i+1}, \dots, a_n) = a_i. \tag{5}$$

Definition 4. *A left (right) quasigroup $(Q, *)$ is a groupoid satisfying the law*

$$(\forall u, v \in Q)(\exists !\ x \in Q) \quad u * x = v$$
$$((\forall u, v \in Q)(\exists !\ y \in Q) \quad y * u = v.)$$

It is clear that a groupoid is a quasigroup iff it is left and right quasigroup.

Given a left (right) quasigroup $(Q, *)$ the parastrophe $\backslash$ $(/)$ can be derived from the operation $*$ as following.

$$x * y = z \Leftrightarrow y = x \backslash z \quad (x * y = z \Leftrightarrow x = z/y)$$

and then the algebra $(Q, *, \backslash)$ $((Q, *, /))$ satisfies the identities

$$x \backslash (x * y) = y,\ x * (x \backslash y) = y, \quad ((x * y)/y = x,\ (x/y) * y = x).$$

2.2. Huge quasigroups

A quasigroup can be constructed by using a Latin square, that will be the main body of the multiplication table of the quasigroup, or analytically by some functions. A quasigroup of small order is easily representable by its multiplication table (as in Table 3). Clearly, it cannot be done for quasigroups of huge orders 2^{16}, 2^{64}, 2^{128}, 2^{256}, $2^{512}, \dots$ (we say huge quasigroups), that are used in the constructions of some crypto primitives. There are several known constructions of huge quasigroups, and we describe some of them.

2.2.1. Huge quasigroups obtained by Feistel networks

Extended Feistel networks $F_{A,B,C}$ are defined in [91] as follows.

Let $(G,+)$ be an abelian group, let $f : G \to G$ be a mapping and let $A, B, C \in G$ be constants. The extended Feistel network $F_{A,B,C} : G^2 \to G^2$ created by f is defined for every $(l,r) \in G^2$ as

$$F_{A,B,C}(l,r) = (r + A, l + B + f(r + C)).$$

When f is a bijection, $F_{A,B,C}$ is an orthomorphism of the group $(G^2,+)$ (i.e., $F_{A,B,C}$ and $F_{A,B,C} - I$ are permutations), so a quasigroup $(G^2, *_{F_{A,B,C}})$ can be produced by Sade's diagonal method [122] as

$$X *_{F_{A,B,C}} Y = F_{A,B,C}(X - Y) + Y.$$

This construction is suitable for many applications, since the parameters A, B, C of an extended Feistel network $F_{A,B,C}$ can be used for different purposes. By iterating, starting from a group of small order, we can construct a huge quasigroup. Namely, if f is bijection on G, then $f_1 = F_{A,B,C}$ is a bijection on G^2, so we can define suitable extended Feistel network F_{A_1,B_1,C_1} by choosing constants $A_1, B_1, C_1 \in G^2$. Again, by Sade's diagonal method we can construct a quasigroup $(G^4, *_{F_{A_1,B_1,C_1}})$ of order $|G|^4$. Hence, in such a way, after k steps, we have a quasigroup of order $|G|^{2^k}$. Thus, when $G = \mathbb{Z}_2$, after 8 steps wee have a huge quasigroup of order 2^{256}. Note that only the starting bijection f has to be kept in memory.

More constructions of quasigroups by different types of Feistel networks are given in [111].

2.2.2. Huge quasigroups obtained by T-functions

Huge quasigroups can be defined by so called $T-$functions [18] and one way how it can be done is the following [127].

Let $Q = \mathbb{Z}_{2^w}$ and let represent the element of Q binary, as bit strings of length w. (Thus, for $w = 4$, the integer 9 is represented as 1001.) Let $x_w, \dots, x_1$ be Boolean variables, and let $\mathbf{b}$ be a constant Boolean vector. Let $\mathbf{A_1} = [f_{ij}]_{w\times w}$ and $\mathbf{A_2} = [g_{ij}]_{w\times w}$ be upper triangular matrices of linear Boolean expressions with variables $x_w, \dots, x_1$, such that: 1) $f_{ii} = 1$, $g_{ii} = 1$ and f_{iw} are constants for every $i = 1, \dots, w$; 2) for all $i < j < w$, f_{ij} can depend only on the variables $x_{w-j}, \dots, x_1$ and 3) for all $i < j$, g_{ij} can depend only on the variables $x_w, \dots, x_1$. Let $\mathbf{x} = (x_w, \dots, x_1)$, $\mathbf{y} = (y_w, \dots, y_1)$ be binary presentation of the variables $\mathbf{x}, \mathbf{y}$ over Q. Then, $(Q, *)$ is a quasigroup of order 2^w, where $*$ is defined by

$$\mathbf{x} * \mathbf{y} = \mathbf{A_1} \cdot (x_w, \dots, x_1)^T + \mathbf{A_2} \cdot (y_w, \dots, y_1)^T + \mathbf{b}^T.$$

The parastrophe $(Q, \backslash)$ is defined by

$$\mathbf{x} \setminus \mathbf{y} = \mathbf{A_2^{-1}} \cdot ((y_w, \dots, y_1)^T - \mathbf{A_1} \cdot (x_w, \dots, x_1)^T - \mathbf{b}^T).$$

2.2.3. Huge quasigroups obtained by simple isotopies

The compression function of the hash function Edon-R [58] uses two huge quasigroups of order 2^{256} and 2^{512} and their operations are defined by isotopies of the Abelian group $((\mathbb{Z}_{2^w})^8, +_8)$, $w = 32$ and $w = 64$, respectfully. ($+_8$ is a componentwise addition on two 8-dimensional vectors in $(\mathbb{Z}_{2^w})^8$). The quasigroup operation $*$ is defined by

$$X * Y = \pi_1(\pi_2(X) +_8 \pi_3(Y))$$

where $X = (X_0, X_1, \ldots, X_7), Y = (Y_0, Y_1, \ldots, Y_7) \in (\mathbb{Z}_{2^w})^8$ and $\pi_i : \mathbb{Z}_{2^w} \to \mathbb{Z}_{2^w}$, $1 \leqslant i \leqslant 3$, are permutations obtained in a suitable simple (and efficient) way.

2.3. Quasigroups for symbolic computations

Designs of some crypto primitives (like digital signatures, public key encryptions) need symbolic computations. (For example, for producing a public key consisting of polynomials.) For that aim, quasigroups capable for symbolic computations are defined as well.

2.3.1. Multivariate quadratic quasigroups (MQQ)

As we already mentioned, the elements of a finite quasigroups $(Q, *)$ of order 2^d can be represented binary as bit strings of d bits. Now, the binary operation $*$ can be interpreted as a vector valued operation $*_{vv} : \{0,1\}^{2d} \to \{0,1\}^d$ defined as:

$$\mathbf{x} * \mathbf{y} = \mathbf{z} \Longleftrightarrow *_{vv}(x_1, \ldots, x_d, y_1, \ldots, y_d) = (z_1, \ldots, z_d),$$

where $x_1 \ldots x_d,\ y_1 \ldots y_d,\ z_1 \ldots z_d$ are binary representations of $\mathbf{x}, \mathbf{y}, \mathbf{z}$. Each z_i depends of the bits $x_1, x_2, \ldots, x_d, y_1, y_2, \ldots, y_d$ and is uniquely determined by them. So, each z_i can be seen as a $2d$-ary Boolean function $z_i = f_i(x_1, \ldots, x_d, y_1, \ldots, y_d)$, where $f_i : \{0,1\}^{2d} \to \{0,1\}$ strictly depends on, and is uniquely determined by, $*$.

A k-ary Boolean function $f(x_1, \ldots, x_k)$ can be represented in a unique way by its algebraic normal form (ANF) as a sum of products in the field $GF(2)$:

$$ANF(f) = \sum_{I \subseteq \{1,2,\ldots,k\}} \alpha_I \mathbf{x}^I,$$

where $\alpha_I \in \{0,1\}$ and $\mathbf{x}^I$ is the product of all variables x_i such that $i \in I$. The ANFs of the functions f_i give us information about the complexity of the quasigroup $(Q, *)$ via the degrees of the Boolean functions f_i. It can be observed that the degrees of the polynomials $ANF(f_i)$ rise with the order of the quasigroup. In general, for a randomly generated quasigroup of order 2^d, $d \geqslant 4$, the degrees are higher than 2.

The MQQ are defined in [51]. A quasigroup $(Q, *)$ of order 2^d is called Multivariate Quadratic Quasigroup (MQQ) of type $Quad_{d-k}Lin_k$ if exactly $d - k$ of its Boolean polynomials f_i are of degree 2 (i.e., they are quadratic) and k of them are of degree 1 (i.e., they are linear), where $0 \leqslant k < d$.

Theorem 1 below gives us sufficient conditions for a quasigroup $(Q, *)$ to be MQQ.

Theorem 1. *Let* $\mathbf{A_1} = [f_{ij}]_{d\times d}$ *and* $\mathbf{A_2} = [g_{ij}]_{d\times d}$ *be two* $d \times d$ *matrices of linear Boolean expressions, and let* $\mathbf{b_1} = [u_i]_{d\times 1}$ *and* $\mathbf{b_2} = [v_i]_{d\times 1}$ *be two* $d \times 1$ *vectors of linear or quadratic Boolean expressions. Let the functions* f_{ij} *and* u_i *depend only on variables* $x_1, \dots, x_d$*, and let the functions* g_{ij} *and* v_i *depend only on variables* $x_{d+1}, \dots, x_{2d}$*. If*

$$\mathbf{Det}(\mathbf{A_1}) = \mathbf{Det}(\mathbf{A_2}) = 1 \textit{ in } GF(2) \tag{6}$$

and if

$$\mathbf{A_1} \cdot (x_{d+1}, \dots, x_{2d})^T + \mathbf{b_1} \equiv \mathbf{A_2} \cdot (x_1, \dots, x_d)^T + \mathbf{b_2} \tag{7}$$

then the vector valued operation

$$*_{vv}(x_1, \dots, x_{2d}) = \mathbf{A_1} \cdot (x_{d+1}, \dots, x_{2d})^T + \mathbf{b_1}$$

defines a quasigroup $(Q, *)$ *of order* 2^d *that is MQQ.*

Similarly as in Theorem 1, a construction of so called Mutually Quadratic Left Quasigroups (MQLQ) is given in [124].

Theorem 2. *Let* $x_1, \dots, x_w, y_1, \dots, y_w$ *be Boolean variables,* $w > 1$*. Let* $\mathbf{A_1} = [f_{ij}]_{w\times w}$ *and* $\mathbf{A_2} = [g_{ij}]_{w\times w}$ *be two* $w \times w$ *nonsingular upper triangular matrices of random affine Boolean expressions, such that for every* $i = 1, \dots, w$*,* $f_{ii} = 1$ *and* $g_{ii} = 1$*, and for all* i, j*,* $i < j \leqslant w$*,* f_{ij} *and* g_{ij} *depend only on the variables* $x_1, \dots, x_w$*,* $y_{i+1}, \dots, y_w$*. Let* $\mathbf{D_1} = [d_{ij}]_{w\times w}$*,* $\mathbf{D_2} = [d_{ij}]_{w\times w}$ *and* $\mathbf{D} = [d_{ij}]_{w\times w}$ *be nonsingular Boolean matrices and let* $\mathbf{b} = [b_i]_{w\times 1}$*,* $\mathbf{c_1} = [c_i]_{w\times 1}$*,* $\mathbf{c_2} = [c_i]_{w\times 1}$ *and* $\mathbf{c} = [c_i]_{w\times 1}$ *be Boolean vectors.*

Then the vector valued operations

$$*_1(x_1, \dots, x_w, y_1, \dots, y_w) = \mathbf{A_1} \cdot (x_1, \dots, x_w) \oplus \mathbf{A_2} \cdot (y_1, \dots, y_w) \oplus \mathbf{b} \tag{8}$$

and

$$*_2(x_1, \dots, x_w, y_1, \dots, y_w) = \mathbf{D}(*_1(\mathbf{D}_1(x_1, \dots, x_w) \oplus \mathbf{c}_1, \mathbf{D}_2(y_1, \dots, y_w) \oplus \mathbf{c}_2)) \oplus \mathbf{c} \tag{9}$$

define left quasigroups $(Q, *_1)$ *and* $(Q, *_2)$ *of order* 2^w *that are MQLQ, where* $Q = \{0, 1, \dots \ \dots, 2^w - 1\}$.

The definition of the quasigroup $(Q, *)$ implies immediately that symbolic computations can be performed with linear polynomials on the field $GF(2)$.

More information for MQQ can be found in [125] and [17].

2.3.2. Matrix representation

All quasigroup operations on the set $Q = \{0, 1, 2, 3\}$ have so called matrix representations in the following form, given in the next theorem [137]:

Theorem 3. *Each quasigroup* $(Q, *)$ *of order* 4 *has a matrix representation of form*

$$\boldsymbol{x} * \boldsymbol{y} = \boldsymbol{m}^T + A\boldsymbol{x}^T + B\boldsymbol{y}^T + CA\boldsymbol{x}^T \circ CB\boldsymbol{y}^T, \tag{10}$$

where $\boldsymbol{x} = (x_1, x_2)$, $\boldsymbol{y} = (y_1, y_2) \in Q$ $(x_i, y_i$ *denotes bit variables*), $\boldsymbol{m} = (m_1, m_2)$ *is some constant from* Q, A *and* B *are nonsingular* 2*-dimensional matrices of bits,* C *is one of the matrices* $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, *and* $\circ$ *denotes the component-wise multiplication of vectors.* (Note: The addition and multiplication are in the field $GF(2)$.)

The matrix presentation of the parastrophe operation $\backslash$ of the quasigroup operation $*$ given by (10) is the following:

$$\begin{aligned} \mathbf{x} \backslash \mathbf{z} = B^{-1}\mathbf{m}^T + B^{-1}(I + C)A\mathbf{x}^T + B^{-1}(C\mathbf{m}^T \circ CA\mathbf{x}^T) + \\ + B^{-1}\mathbf{z}^T + B^{-1}(CA\mathbf{x}^T \circ C\mathbf{z}^T), \end{aligned} \tag{11}$$

where I denotes the identity matrix.

The variables $\mathbf{x}$ and $\mathbf{y}$ may vary over the polynomial ring $\mathbb{Z}[X]$, not only over Q.

Matrix representation for some types of quasigroups of order 8 are also investigated.

Here we note that for any order 2^n we have matrix representations of the so called linear quasigroups of order 2^n as follows. Let denote $\mathbf{x} = (x_1, \ldots, x_n)$, where x_i are bit variables.

Theorem 4. *Let* A *and* B *be nonsingular binary* $n \times n-$*matrices and* $\mathbf{m} \in Q = \{0, 1, 2, \ldots, 2^n - 1\}$ *be a constant. Then* $(Q, *)$ *is a quasigroup* (*called linear quasigroup*), *where*

$$\boldsymbol{x} * \boldsymbol{y} = \boldsymbol{m}^T + A\boldsymbol{x}^T + B\boldsymbol{y}^T. \tag{12}$$

By Theorem 4, we can take $\mathbf{m}$ to be $1 \times n$ matrix and A and B to be $n \times n-$matrices with entries that are Boolean expressions such that $det(A) \neq 0$, $det(B) \neq 0$, and then $\mathbf{x} * \mathbf{y}$ will be a Boolean expression too. So, we can use this matrix presentation for symbolic computations.

We can extended the previous result for k-ary case as well.

Theorem 5. *Let* A_i, $i = 1, 2, \ldots, k$, *be nonsingular binary* $n \times n-$*matrices and* $\mathbf{m} \in Q = \{0, 1, 2, \ldots, 2^n - 1\}$ *be a constant. Then* (Q, f) *is a* k*-ary quasigroup* (*called linear* $k-$*quasigroup*), *where*

$$f(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k) = \boldsymbol{m}^T + A_1\boldsymbol{x}_1^T + A_2\boldsymbol{x}_2^T + \cdots + A_k\boldsymbol{x}_k^T. \tag{13}$$

2.3.3. Polynomial quasigroups

Quasigroups of order 2^n can be defined by using bivariate polynomials $P(x,y)$ over the ring $(Z_{2^n},+,\cdot)$, $n \geqslant 2$ ([123], [121], [95]), when the polynomials satisfy the following condition: each of the functions $P(x,0), P(x,1), P(0,y)$ and $P(1,y)$ is a permutation on $\mathbb{Z}_{2^n}$. Then the quasigroup $(\mathbb{Z}_{2^n},*)$, called polynomial quasigroup, is defined by $x*y=P(x,y)$.

If only the univariate polynomials $P(x,0)$, $P(x,1)$ $(P(0,y), P(1,y))$ are permutations, $(\mathbb{Z}_{2^n},*)$ is right quasigroup (left quasigroup), and vice versa.

Polynomial quasigroups can be of huge order and, since defined by polynomials, they can be used for symbolic computations as well.

We note that there are effective algorithms for computing the parastrophic operations of the polynomial quasigroups.

3. Quasigroup string transformations

Quasigroup String Transformations were introduced in [84] and were investigated in several other papers ([85], [89], [90], [81], [80]).

Consider an alphabet (i.e., a finite set) Q, and denote by $Q^+ = \{a_1a_2\dots \dots a_n|\ a_i \in Q\}$ the set of all nonempty words (i.e., finite strings) formed by the elements of Q. (If there is no misunderstanding, we identify $a_1a_2\dots a_n$ and $(a_1,a_2,\dots,a_n)$.) Let $*$ be a quasigroup operation on the set Q, i.e., consider a quasigroup $(Q,*)$. For each $a \in Q$ we define two functions

$$e_{a,*},\ d_{a,*} : Q^+ \longrightarrow Q^+$$

as follows. Let $a_i \in Q,\ \alpha = a_1a_2\dots a_n$. Then

$$e_{a,*}(\alpha) = b_1b_2\dots b_n \Longleftrightarrow b_1 = a*a_1,\ b_2 = b_1*a_2, \dots,\ b_n = b_{n-1}*a_n$$

and

$$d_{a,*}(\alpha) = c_1c_2\dots c_n \Longleftrightarrow c_1 = a*a_1,\ c_2 = a_1*a_2, \dots,\ c_n = a_{n-1}*a_n.$$

The functions $e_{a,*},\ d_{a,*}$ are called e- and d-transformation of Q^+ based on the operation $*$ with leader a, and their graphical representation is shown on Fig. 1 and Fig. 2.

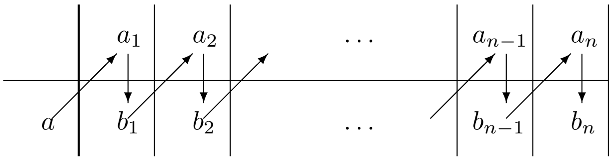


Figure 1: Graphical representation of $e_{a,*}$ function

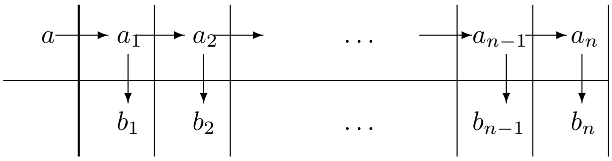


Figure 2: Graphical representation of $d_{a,*}$ function

$\bullet$	0	1	2	3
0	2	1	0	3
1	3	0	1	2
2	1	2	3	0
3	0	3	2	1

$\backslash$	0	1	2	3
0	2	1	0	3
1	1	2	3	0
2	3	0	1	2
3	0	3	2	1

/	0	1	2	3
0	3	1	0	2
1	2	0	1	3
2	0	2	3	1
3	1	3	2	0

Figure 3: A quasigroup $(Q, \bullet)$ and its parastrophes $(Q, \backslash)$ and $(Q, /)$

Example 1. Take $Q = \{0, 1, 2, 3\}$ and let the quasigroup $(Q, \bullet)$ and its parastrophes $(Q, \backslash)$ and $(Q, /)$ be given by the multiplication schemes in Figure 3.

Consider the string $\alpha = 1\ 0\ 2\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 2\ 1\ 0\ 2\ 2\ 0\ 1\ 0\ 1\ 0\ 3\ 0\ 0$ and choose the leader 0. Then by the transformations $e_{0,\bullet}$ and $d_{0,\bullet}$ we will obtain the following transformed strings $e_{0,\bullet}(\alpha)$ and $d_{0,\bullet}(\alpha)$:

$e_{0,\bullet}(\alpha) = 1\ 3\ 2\ 2\ 1\ 3\ 0\ 2\ 1\ 3\ 0\ 2\ 1\ 0\ 1\ 1\ 2\ 1\ 1\ 1\ 3\ 3\ 0\ 1\ 3\ 1\ 3\ 0$,

$d_{0,\bullet}(\alpha) = 1\ 3\ 0\ 2\ 3\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 1\ 0\ 1\ 2\ 3\ 0\ 3\ 1\ 1\ 3\ 1\ 3\ 3\ 0\ 2$.

We present four consecutive applications of the e-transformation on Table 1.

After that we apply four times the transformation $d_{0,\backslash}$ on the last obtained string $\beta = {e_{0,\bullet}}^4(\alpha)$ (see Table 1):

Notice that we have obtained

$$\alpha = {d_{0,\backslash}}^4(\beta) = {d_{0,\backslash}}^4({e_{0,\bullet}}^4(\alpha)) = ({d_{0,\backslash}}^4 \circ {e_{0,\bullet}}^4)(\alpha). \qquad \square$$

In fact, by (3), the following property is true([85]):

Theorem 6. *Let $(Q, *, \backslash, /)$ be a finite quasigroup. Then for each string $\alpha \in Q^+$ and for each leader $l \in Q$ we have that $e_{l,*}$ and $d_{l,\backslash}$ are mutually inverse permutations of Q^+, i.e., $d_{l,\backslash}(e_{l,*}(\alpha)) = \alpha = e_{l,*}(d_{l,\backslash}(\alpha))$.*

leader	$1\ 0\ 2\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 2\ 1\ 0\ 2\ 2\ 0\ 1\ 0\ 1\ 0\ 3\ 0\ 0 = \alpha$
0	$1\ 3\ 2\ 2\ 1\ 3\ 0\ 2\ 1\ 3\ 0\ 2\ 1\ 0\ 1\ 1\ 2\ 1\ 1\ 1\ 3\ 3\ 0\ 1\ 3\ 1\ 3\ 0 = e_{0,\bullet}(\alpha)$
0	$1\ 2\ 3\ 2\ 2\ 0\ 2\ 3\ 3\ 1\ 3\ 2\ 2\ 1\ 0\ 1\ 1\ 2\ 2\ 2\ 0\ 3\ 0\ 1\ 2\ 2\ 0\ 2 = {e_{0,\bullet}}^2(\alpha)$
0	$1\ 1\ 2\ 3\ 2\ 1\ 1\ 2\ 0\ 1\ 2\ 3\ 2\ 2\ 1\ 0\ 1\ 1\ 1\ 1\ 3\ 1\ 3\ 3\ 2\ 3\ 0\ 0 = {e_{0,\bullet}}^3(\alpha)$
0	$1\ 0\ 0\ 3\ 2\ 2\ 2\ 3\ 0\ 1\ 1\ 2\ 3\ 2\ 2\ 1\ 0\ 1\ 0\ 1\ 2\ 2\ 0\ 3\ 2\ 0\ 2\ 1 = {e_{0,\bullet}}^4(\alpha)$

Table 1: Consecutive e-transformations

leader	
0	1 0 0 3 2 2 2 3 0 1 1 2 3 2 2 1 0 1 0 1 2 2 0 3 2 0 2 1 $= \beta$
0	1 1 2 3 2 1 1 2 0 1 2 3 2 2 1 0 1 1 1 1 3 1 3 3 2 3 0 0 $= d_{0,\backslash}(\beta)$
0	1 2 3 2 2 0 2 3 3 1 3 2 2 1 0 1 1 2 2 2 0 3 0 1 2 2 0 2 $= {d_{0,\backslash}}^2(\beta)$
0	1 3 2 2 1 3 0 2 1 3 0 2 1 0 1 1 2 1 1 1 3 3 0 1 3 1 3 0 $= {d_{0,\backslash}}^3(\beta)$
	1 0 2 1 0 0 0 0 0 0 0 0 0 1 1 2 1 0 2 2 0 1 0 1 0 3 0 0 $= {d_{0,\backslash}}^4(\beta)$

Table 2: Consecutive d-transformations

By Theorem 6 we conclude that the transformations $e_{a,*}$ and $d_{a,\backslash}$ can be used for defining suitable functions for encryption and decryption. Much more, we can define in the similar way several pairs of quasigroup string transformations that can be used for defining suitable functions for encryption and decryption. Thus, let $a, a_1, a_2, \dots, a_n \in Q$ and let define the functions $e'_{a,*},\ d'_{a,*} : Q^+ \longrightarrow Q^+$ as follows:

$$e'_{a,*}(\alpha) = b_1 b_2 \dots b_n \Longleftrightarrow b_n = a_n * a,\ b_{n-1} = a_{n-1} * b_n, \dots,\ b_1 = a_1 * b_2,$$

$$d'_{a,*}(\alpha) = c_1 c_2 \dots c_n \Longleftrightarrow c_n = a_n * a\ c_{n-1} = a_{n-1} * a_n, \dots,\ c_1 = a_1 * a_2.$$

Then, by (4), Theorem 6 holds for the functions $e'_{a,*},\ d'_{a,\backslash}$ too. Also, for encryption/decryption purposes, in a suitable way transformations with the pair of functions $(e_{a,*},\ d_{a,/}), (e'_{a,*},\ d'_{a,/}), (e_{a,*},\ d_{a,\backslash}), (e'_{a,*},\ d'_{a,\backslash}), (e_{a,\bullet},\ d_{a,//}),\ (e'_{a,\bullet},\ d'_{a,//})$, $(e_{a,\bullet},\ d_{a,\backslash\backslash}), (e'_{a,\bullet},\ d'_{a,\backslash\backslash})$ can be defined in an obvious way.

Several quasigroup operations can be defined on the set Q and let $*_1,\ *_2,\ \dots,\ *_k$ be a sequence of (not necessarily distinct) such operations. We choose also leaders $l_1,\ l_2,\ \dots,\ l_k \in Q$ (not necessarily distinct either), and let $t^{(i)} \in \{e_{l_i,*},\ d_{l_i,/},\ e'_{l_i,*},\ d'_{l_i,/},\ d_{l_i,//},\ d'_{l_i,//},\ d_{a,\backslash\backslash},\ d'_{l_i,\backslash\backslash}, \dots\}$. Then, the transformation $T = t^{(1)} t^{(2)} \dots t^{(k)}$ of Q^+ is said to be a generalized T-transformation. It is a permutation of Q^+ with inverse $T^{-1} = (t^{(k)})^{-1} (t^{(k-1)})^{-1} \dots (t^{(1)})^{-1}$, where $(t^{(i)})^{-1} \in \{e_{l_i,*},\ e'_{l_i,*},\ e_{l_i,\bullet},\ e'_{l_i,\bullet},\ d_{l_i,/},\ d'_{l_i,/},\ d_{l_i,//},\ d'_{l_i,//},\ d_{a,\backslash\backslash},\ d'_{l_i,\backslash\backslash}, \dots\}$. The generalized transformations T, T^{-1} can be used as encryption/decryption functions.

3.1. Parastrophic quasigroup transformations

In order to exploit more completely one quasigroup, an idea for quasigroup string transformation that will be based on all isotopes of a quasigroup is given in [73]. Here we give a description of a slightly modification of this transformation, called parastrophic quasigroup transformation, as presented in [3]. For that aim we denote the parastrophic operation $\{*, \backslash, /, \bullet, //, \backslash\backslash\}$ of a quasigroup $(Q, *)$ respectively as $f_1, f_2, f_3, f_4, f_5, f_6$, and we write $f_1(x,y), f_2(x,y), \dots$ instead of $x * y, x\backslash y, \dots$ Note that some of the parastrophes f_i may coincides, depending of the quasigroup.

The parastrophic transformations PE is defined on finite quasigroups $(Q,*)$ of integers, i.e., $Q=\{1,2,\dots,t\}$. They are using the transformations e_{l,f_i} for transformations of block of letters, where l is a leader. Also, a positive integer p is used.

Let p be a positive integer and $x_1x_2\dots x_n$ be an input message. We define a parastrophic transformation $PE=PE_{l,p}:Q^+\to Q^+$ by using auxiliary parameters d_i,q_i and s_i as follows.

To start, let $d_1=p$, $q_1=d_1$, $s_1=(d_1 \bmod 6)+1$ and take a starting block $A_1=x_1x_2\dots x_{q_1}$. Denote by B_1 the block

$$B_1=y_1y_2\dots y_{q_1-1}y_{q_1}=e_{l,f_{s_1}}(x_1x_2\dots x_{q_1-1}x_{q_1}).$$

Further, we calculate the numbers $d_2=4y_{q_1-1}+y_{q_1}$ (that determines the length of the next block), $q_2=q_1+d_2$ and $s_2=(d_2 \bmod 6)+1$. We denote $A_2=x_{q_1+1}\dots x_{q_2-1}x_{q_2}$ and

$$B_2=y_{q_1+1}\dots y_{q_2-2}y_{q_2-1}y_{q_2}=E_{y_{q_1},f_{s_2}}(x_{q_1+1}\dots x_{q_2-2}x_{q_2-1}x_{q_2}).$$

Inductively, after getting the blocks $B_1,B_2,\dots,B_{i-1}$ where $B_{i-1}=y_{q_{i-2}+1}\dots$ $\dots y_{q_{i-1}-1}y_{q_{i-1}}$, we calculate $d_i=4y_{q_{i-1}-1}+y_{q_{i-1}}$, $q_i=q_{i-1}+d_i$, $s_i=(d_i \bmod 6)+1$, $A_i=x_{q_{i-1}+1}\dots x_{q_i-1}x_{q_i}$ and obtain the block

$$B_i=E_{y_{q_{i-1}},f_{s_i}}(x_{q_{i-1}+1}\dots x_{q_i}).$$

Now, the parastrophic transformation $PE_{l,p}$ is defined by concatenation of the obtained blocks as

$$PE_{l,p}(x_1x_2\dots x_n)=B_1||B_2||\dots||B_r. \tag{14}$$

(Note that the length of the last block A_r may be shorter than d_r, depending on the number of letters in input message).

3.2. Other types of transformations

For different purposes other types of quasigroups transformations are defined elsewhere. We will shortly mention some of them.

Special kind of E transformation is the quasigroup reverse string transformation R, introduced in [42], where the leaders are the elements of the string, taken in reverse order. Namely, a string of letters $\alpha=a_1a_2\dots a_n$ is transformed to $E(\alpha)$, where $E=e_{*,a_n}\circ e_{*,a_{n-1}}\circ\cdots\circ e_{*,a_1}$.

Let $(Q,*_1)$ and $(Q,*_2)$ be two orthogonal (finite) quasigroups, i.e., the equality $\{(x{*_1}y,x{*_2}y)|\,x,y\in Q\}=Q^2$ holds. Orthogonal quasigroup string transformation $OT:Q^+\to Q^+$ of a string $x_1x_2\dots x_r$ is defined in [110] by the following iterative procedure:

$$OT(x_1)=x_1, OT(x_1,x_2)=(x_1*_1x_2,x_1*_2x_2)$$

and if $OT(x_1, x_2, \dots, x_{t-1}) = (z_1, z_2, , \dots, z_{t-1})$ is defined for $t > 2$, then

$$OT(x1, x2, , \dots, x_{t-1}, x_t) = (z_1, z_2, , \dots, z_{t-2}, z_{t-1} *_1 x_t, z_{t-1} *_2 x_t).$$

OT is a permutation of Q.

Let $Q = \mathbb{Z}_{2^n}$, let $(Q, *)$ be a quasigroup and let $+$ denote addition modulo 2^n. Elementary quasigroup additive and reverse additive string transformations $A, RA : Q^+ \to Q^+$ with leader l are defined in [92] as follows:

$$A(x_1 x_2 \dots x_t) = (z_1 z_2, \dots z_t) \iff z_j = (z_{j-1} + x_j) * x_j,\ 1 \leqslant j \leqslant t,\quad z_0 = l,$$

$$RA(x_1 x_2 \dots x_t) = (z_1 z_2 \dots z_t) \iff z_j = x_j * (x_j + z_j + 1),\ 1 \leqslant j \leqslant t,\quad z_{t+1} = l.$$

These transformations are not bijective mappings. One can create composite quasigroup transformations M by composition of different A and/or RA transformations with different leaders.

Quasigroup string transformations $F_i, G_i,\ i = 1, 2, 3$, defined by 3-ary quasigroup (Q, f) are given in [117]. The operations F_1, F_2, F_3 are defined by f, while G_i are defined by f_i. By (5) all transformations are permutations and F_i has inverse G_i. Here we present the definitions of F_1 and G_1. Let take leaders $a_1, a_2, a_3, a_4 \in Q$, and define

$$F_1(x_1 x_2 \dots x_t) = (z_1 z_2 \dots z_t) \Leftrightarrow z_j = \begin{cases} f(x_1, a_1, a_2), & j = 1 \\ f(x_2, a_3, a_4), & j = 2 \\ f(x_j, z_{j-2}, z_{j-1}), & j > 2, \end{cases}$$

$$G_1(x_1 x_2 \dots x_t) = (z_1 z_2 \dots z_t) \Leftrightarrow z_j = \begin{cases} f_1(x_1, a_1, a_2), & j = 1 \\ f_1(x_2, a_3, a_4), & j = 2 \\ f_1(x_j, x_{j-2}, x_{j-1}), & j > 2. \end{cases}$$

4. Crypto primitives based on quasigroups

In this section we will consider several designs of cryptographic primitives based on quasigroups, i.e., on different kinds of quasigroup transformations. We emphasize that for getting suitable cryptographic properties of the designs, we have to choose the used quasigroups very carefully. One most desirable property of the quasigroup is its shapelessness [55]. This means that the quasigroup $(Q, *)$ should not be associative, commutative, idempotent, have (left,right) unit, it should not have proper subquasigroups and it should not satisfies identities of kind

$$(((y * \underbrace{x) * x) * \dots) * x}_{k} = y, \quad \underbrace{x * (x * \dots (x * (x}_{k} * y))) = y$$

for some $k < 2n$, where $n = |Q|$. More complete definition of a shapeless quasigroup is given in [82], and several construction of huge shapeless quasigroups are given in [111].

According to the properties satisfied by quasigroups, the set of quasigroups $\mathbf{Q}_n$ of fix order n is classified in several classes. Thus, $\mathbf{Q}_n$ may consists of two disjoint classes, the class of fractal and the class of non-fractal quasigroups ([34],[82]). By considering growing the periods of the strings $e_{l,*}{}^t(\alpha)$ of a periodic string α, $\mathbf{Q}_n$ can be classified again in two disjoint classes, the class of exponential and the class of linear quasigroups. A quasigroup is said to be exponential if the period of the string $e_{l,*}{}^t(\alpha)$ is down bounded by an exponential function $const \cdot 2^{at}$, where $const$ and a are positive constant ([33],[80],[87]). We note that for some quasigroups the constant a is enough big, so they can be used to produce suitable crypto primitives.

In the subsequent section we discus constructions based on quasigroups of several crypto primitives.

4.1. S-boxes defined by quaisgroups

The main point of security in symmetric cryptography in almost all modern block ciphers are the substitution boxes (S-boxes). S-boxes have to confuse the input data into the cipher. Since S-boxes contain a small amount of data, the construction of an S-box should be made very carefully in order the needed cryptographic properties to be satisfied. It is especially important when ultra-lightweight block cipher are designed, like PRESENT ([14]). PRESENT S-boxes are derived as a result of an exhaustive search of all 16! bijective 4-bit S-boxes. Then 16 different classes are obtained and all S-boxes in these classes are optimalwith respect to linear and differential properties.

Instead of an exhaustive search of all 16! bijections of 16 elements as it was done for the design of PRESENT, quasigroups of order 4 can be applied for construction of cryptographically strong S-boxes, called Q-S-boxes [103].

There is no formal definition for S-boxes, they are usually defined as lookup tables that are interpreted as vector valued Boolean functions or Boolean maps $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^q$, where $\mathbb{F}_2$ is a Galois field with two elements. Defined as mappings, for S-boxes so called linearity and differential potential can be computed and correspondingly resistance against linear and differential attacks can be measured.

We already mentioned that quasigroups of order 2^n have vector valued representation. For example, the next quasigroup of order 4

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

has representation with the following pair of Boolean functions

$$f(x_0, x_1, y_0, y_1) \;=\; (x_0 + y_0, \;\; x_1 + y_0 + y_1 + x_0 y_0).$$

The algebraic degree of this quasigroup is 2, since the Boolean function $f_2(x_0, x_1, y_0, y_1) = x_1 + y_0 + y_1 + x_0 y_0$ has degree 2. Generally, the quasigroups of order

4 can have algebraic degree 1 (144 of them, so called linear) and 2 (432 of them, so called nonlinear), [44]. Only nonlinear quasigroups are used for construction of suitable S-boxes, i.e., Q-S-boxes. Note that quasigroups of order 4 are 4 × 2-bit S-boxes.

We want to generate 4×4-bit cryptographically strong S-boxes by using quasigroups of order 4. One criterion for good S-box is to have highest possible algebraic degree, so we search for 4×4-bit S-boxes that have algebraic degree 3 for all output bits. For obtaining 4×4-bit S-boxes, e-transformations will be used to raise the algebraic degree of the produced final bijections. As it is shown in Figure 4, one non-linear quasigroup of order 4 and at least 4 e-transformations will be used to reach the desired degree of 3 for all the bits in final output block.

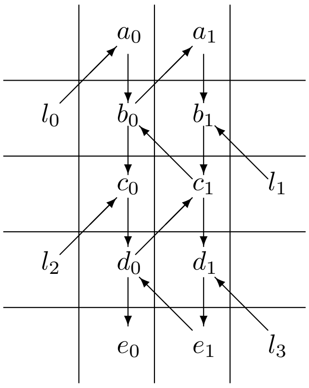


Figure 4: Four e-transformations that bijectively transforms 4 bits into 4 bits by a quasigroup of order 4.

So we can get a Q-S-box that satisfy one condition, to be of degree 3 for all output bits. If the other conditions are satisfied (linearity, differential potential, ...) we will put it in the set of optimal Q-S-boxes. The algorithm for this methodology is given in Table 3. We mention that the minimum number of rounds (iterations) is 4, and using the described methodology we can generate Q-S-boxes in different ways depending on the number of rounds and the number of leaders that we can choose. In our investigation we choose to work with 2, 4 and 8 different leaders and 4 and 8 rounds, respectively. We found all the Q-S-boxes that fulfill the predetermined criteria to be optimal.

Many experiments were made with 2, 4 and 8 different leaders and 4 and 8 rounds, respectively. The obtained results are given in the Table 4.

Some representative of optimal Q-S-boxes are given in Table 5.

An iterative method for construction of Q-S-boxes	
Step 1	Take one quasigroup of order 4 from the class of non-linear;
Step 2	Input the number of rounds;
Step 3	Input the leaders. Usually, their number is the same as the number of rounds;
Step 4	Generate all possible input blocks of 4 bits in the lexicographic ordering (they are 2^4);
Step 5	Take input blocks one by one, and for each of them:
Step 5.1	Apply e-transformation with leader l on the input block;
Step 5.2	Reverse the result from above and apply e-transformation with other leader l again;
Step 5.3	Continue this routine as many times as there is a number of rounds;
Step 5.4	Save the 4-bit result from the last round;
Step 6	At the end concatenate all saved results which generate permutation of order 16 or 4 × 4-bit Q-S-box;
Step 7	Investigate predetermined criteria;
Step 7.1	If the Q-S-box satisfies criteria, put it in the set of optimal S-boxes;
Step 7.2	If not, go to Step 3;
Step 8	Analyze the optimal set of newly obtained Q-S-boxes;

Table 3: Construction of one Q-S-box

Number of Leaders	Number of Rounds	Number of Optimal boxes
2	4	1 152
4	4	9 216
8	8	331 264

Table 4: The number of optimal Q-S-boxes under different parameters

4.2. Block ciphers

Block cipher is an enciphering method that encrypt a block M of plaintext of length n into a block C of ciphertext of length n, by using a secret key K. It uses an encryption function $E : \mathcal{P} \times \mathcal{K} \to \mathcal{C}$ and a decryption function $D : \mathcal{C} \times \mathcal{K} \to \mathcal{P}$, where $\mathcal{P}, \mathcal{C}$ and $\mathcal{K}$ are the spaces of plaintext, ciphertext and keys; usually $\mathcal{P} = \mathcal{C} = \{0,1\}^n$, $\mathcal{K} = \{0,1\}^k$. The functions $E(M,K)$ and $D(C,K)$ are permutation for fixed K and $D(E(M,K),K) = M$, and there are no different keys K_1, K_2 such that $E(M,K_1) = E(M,K_2)$. Note that when $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$, then E is a quasigroup operation with parastrophe D. Besides the last property, there are no many block ciphers based on quasigroup. Here we show the design of the block

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	C	1	2	E	F	9	3	4	8	0	A	B	7	D	6	5

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	D	9	F	C	B	5	7	6	3	8	E	2	0	1	4	A

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	D	9	F	C	B	5	7	6	3	8	E	2	0	1	4	A

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	5	E	6	D	7	4	2	A	8	C	0	9	1	B	F	3

Table 5: Examples of optimal Q-S-boxes given in its hexadecimal notation

cipher BCMPQ (Block Cipher Defined by Matrix Presentation of Quasigroups), [83].

The design of BCDMPQ uses matrix presentation of quasigroups of order 4. Thus, given a quasigroup $(Q,*)$ of order 4, for all $x,y \in Q, x = (x_1,x_2), y = (y_1,y_2)$, x_i, y_i are bits:

$$x * y = m^T + Ax^T + By^T + CAx^T \circ CBy^T \tag{15}$$

where $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$ are nonsingular Boolean matrices, $m = [m_1, m_2]$ is a Boolean vector and $C = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$. The operation "$\circ$" denotes the component wise product of two vectors.

There are 144 quasigroups of form (15). Out of them, a list of 128 is chosen and stored in memory as follows:

$$seq\_num \qquad m_1, m_2, a_{11}, a_{12}, a_{21}, a_{22}, b_{11}, b_{12}, b_{21}, b_{22} \tag{16}$$

where *seq_num* is a seven bit number (the number of the quasigroup in the list) while $m_1, m_2, a_{11}, a_{12}, a_{21}, a_{22}$, $b_{11}, b_{12}, b_{21}, b_{22}$ are the bits appearing in the matrix form (15) of the quasigroup operation. (Note that a quasigroup of order 4 is given by using only ten bits, while 32 bits are needed for its Latin square.)

The encryption and decryption algorithms use 16 quasigroups: $Q_1, Q_2, \ldots, Q_8$, $T_1, \ldots, T_8$ in different steps. These matrices are determined by using the round key *key*, which is generated out of the secret key K and consists of 128 bits.

The key length of 128 bits is distributed in the following way:

- 16 bits for the leaders $l_1, l_2, ..., l_8$ (two bits per each leader)

- 56 bits for the quasigroups $Q_1, Q_2, ..., Q_8$ (7 bits per each quasigroup, actually the value of *sequence_number*)

- 56 bits for the quasigroups $T_1, T_2, ..., T_8$ (7 bits per each quasigroup)

The design of this block cipher is based on three algorithms: round key generation, encryption and decryption.

Denote by K the secret symmetric key of 128 bits. In order to generate a round (working) key k out of the secret key, we first determine a fixed shapeless quasigroup Q and a fixed leader $l = 0 = [0, 0]$. The round key is obtained by e-transformations. The procedure for generation a round key is described in the RoundKeyGeneration Algorithm. (There, and in the next two algorithms, auxiliary variables are used, tmp is two bits variable and l_{tmp} is one bit variable.)

```
RoundKeyGeneration Algorithm

Input: The secret key $K = K_1K_2 \dots K_{128}$, $K_i$ are bits.
Output: The round key $key = k_1k_2 \dots k_{128}$, $k_i$ are bits.
Initialization: $(Q, *)$ is a fixed matrix quasigroup of order 4
such that $a * a \neq a$ for each $a \in Q$, $l = (0, 0)$ is a two bit leader.

for $i = 1$ to 128 do
$k_i \leftarrow K_i$;
for $i = 1$ to 4 do
    $l_{tmp} \leftarrow l$;
    for $j = 1$ to 127 step 2 do
        $tmp \leftarrow (k_j, k_{j+1})$;
        $(k_j, k_{j+1}) = m^T + Al_{tmp}^T + Btmp^T + CAl_{tmp}^T \circ CBtmp^T$;
        $l_{tmp} \leftarrow (k_j, k_{j+1})$;
    $l_{tmp} \leftarrow l$;
    for $j = 128$ to 2 step 2 do
        $tmp \leftarrow (k_{j-1}, k_j)$;
        $(k_{j-1}, k_j) = m^T + Al_{tmp}^T + Btmp^T + CAl_{tmp}^T \circ CBtmp^T$;
        $l_{tmp} \leftarrow (k_{j-1}, k_j)$;
```

The message block length of BCDMPQ can be $8n$ for any n, but we take that $n = 8$, i.e., we consider the light version of the cipher. So, the plaintext message should be split into blocks of 64 bits. Afterwards, the Encryption Algorithm should be applied on each block. (If the message length is not devided by 64, a suitable padding will be applied). The encryption algorithm consists of two steps. In the first step we use the matrices $Q_1, Q_2, ..., Q_8$ and in the second the matrices $T_1, T_2, ..., T_8$.

Briefly, in the first step we split the 64 bit block into 8 smaller blocks (mini-blocks) of 8 bits. We apply e-transformation on each of these mini-blocks with a different leader and a different quasigroup. Actually, we use the leader l_i and the quasigroup Q_i for the i-th mini-blocks. The resulting string is used as input in the next step.

In the second step, we apply e-transformations on each resulting string, repeating 8 times with alternately changing direction. In the i-th transformation we use the quasigroup T_i and the leader l_i. The detailed and formalized algorithm is presented in the Encryption Algorithm.

Encryption Algorithm

Input: The round key $key = k_1k_2\dots k_{128}$, k_i are bits,
the plaintext message $a = a_1a_2\dots a_{64}$, a_i are bits.
Output: The ciphertext message $c = c_1c_2\dots c_{64}$.
Initialization: Put $l_i = (k_{2i-1}, k_{2i})$ for $i = 1, 2, \dots, 8$.

Lookup the quasigroup Q_i using the sequence number binary presented as $(k_{7i-6}, k_{7i-5}, ..., k_{7i})$ where $i = 1, 2, ..., 8$. Initialize the matrices A_{Q_i} and B_{Q_i}, as well as the vector $m_{Q_i}$for $i = 1, 2, ..., 8$.

Lookup the quasigroup T_i using the sequence number binary presented as $(k_{7(i+8)-6}, k_{7(i+8)-5}, ..., k_{7(i+8)})$. Initialize the matrices A_{T_i} and B_{T_i}, as well as the vector m_{T_i} for $i = 1, 2, ..., 8$.

```
 **for** $i = 1$ **to** 8 **do**
    $l_{tmp} \leftarrow l_i$;
    **for** $j = 1$ **to** 7 **step** 2 **do**
        $tmp \leftarrow (a_j, a_{j+1})$;
        $(c_j, c_{j+1}) = m_{Q_i}^T + A_{Q_i} l_{tmp}^T + B_{Q_I} tmp^T$
                $+ CA_{Q_i} l_{tmp}^T \circ CB_{Q_i} tmp^T$;
        $l_{tmp} \leftarrow (c_j, c_{j+1})$;
**for** $i = 1$ **to** 4 **do**
    $l_{tmp} \leftarrow l_i$;
    **for** $j = 1$ **to** 63 **step** 2 **do**
        $tmp \leftarrow (c_j, c_{j+1})$;
        $(c_j, c_{j+1}) = m_{T_i}^T + A_{T_i} l_{tmp}^T + B_{T_i} tmp^T + CA_{T_i} l_{tmp}^T \circ CB_{T_i} tmp^T$;
        $l_{tmp} \leftarrow (c_j, c_{j+1})$;
    $l_{tmp} \leftarrow l_{i+4}$;
    **for** $j = 64$ **to** 2 **step** 2 **do**
        $tmp \leftarrow (c_{j-1}, c_j)$;
        $(c_{j-1}, c_j) = m_{T_{i+4}}^T + A_{T_{i+4}} l_{tmp}^T + B_{T_{i+4}} tmp^T +$
                        $CA_{T_{i+4}} l_{tmp}^T \circ CB_{T_{i+4}} tmp^T$;
        $l_{tmp} \leftarrow (c_{j-1}, c_j)$;
```

For decryption purposes we use parastrophe $(Q, \backslash)$ of quasigroup $(Q, *)$. If $x * y = z$, then recall that $y = x \backslash z$ has matrix representation

Decryption Algorithm

Input: The round key $key = k_1k_2 \dots k_{128},\ k_i$ are bits,
the ciphertext message $c = c_1c_2 \dots c_{64},\ c_i$ are bits.
Output: The plaintext message $a = a_1a_2 \dots a_{64}$.
Initialization: Put $l_i = (k_{2i-1}, k_{2i})$ for $i = 1, 2, \dots, 8$.

Lookup the quasigroup Q_i using the sequence number binary presented as $(k_{7i-6}, k_{7i-5}, ..., k_{7i})$ where $i = 1, 2, ..., 8$. Initialize the matrices A_{Q_i} and B_{Q_i}, as well as the vector m_{Q_i} for $i = 1, ..., 8$.

Lookup the quasigroup T_i using the sequence number binary presented as $(k_{7(i+8)-6}, k_{7(i+8)-5}, ..., k_{7(i+8)})$. Initialize the matrices A_{T_i} and B_{T_i}, as well as the vector m_{T_i} for $i = 1, 2, ..., 8$.

```
for $i = 1$ to 64 do  $a_i \leftarrow c_i$;
for $i = 1$ to 4 do
    $l_{tmp} \leftarrow l_{i+4}$;
    for $j = 64$ to 2 step 2 do
        $tmp \leftarrow (a_{j-1}, a_j)$;
        $(a_{j-1}, a_j) = B_{T_{i+4}}^{-1} m_{T_{i+4}}^T + B_{T_{i+4}}^{-1}(I + C)A_{T_{i+4}} l_{tmp}^T +$
        $B_{T_{i+4}}^{-1}(Cm_{T_{i+4}}^T \circ CA_{T_{i+4}} l_{tmp}^T) + B_{T_{i+4}}^{-1} tmp^T +$
        $B_{T_{i+4}}^{-1}(CA_{T_{i+4}} l_{tmp}^T \circ Ctmp^T)$;
        $l_{tmp} \leftarrow (a_{j-1}, a_j)$;
    $l_{tmp} \leftarrow l_i$;
    for $j = 1$ to 63 step 2 do
        $tmp \leftarrow (a_j, a_{j+1})$;
        $(a_{j-1}, a_j) = B_{T_i}^{-1} m_{T_i}^T + B_{T_i}^{-1}(I + C)A_{T_i} l_{tmp}^T +$
        $B_{T_i}^{-1}(Cm_{T_i}^T \circ CA_{T_i} l_{tmp}^T) + B_{T_i}^{-1} tmp^T +$
        $B_{T_i}^{-1}(CA_{T_i} l_{tmp}^T \circ Ctmp^T)$;
        $l_{tmp} \leftarrow (a_j, a_{j+1})$;
for $i = 1$ to 8 do
    $l_{tmp} \leftarrow l_i$;
    for $j = 1$ to 7 step 2 do
        $tmp \leftarrow (a_j, a_{j+1})$;
        $(a_{j-1}, a_j) = B_{Q_i}^{-1} m_{Q_i}^T + B_{Q_i}^{-1}(I + C)A_{Q_i} l_{tmp}^T +$
        $B_{Q_i}^{-1}(Cm_{Q_i}^T \circ CA_{Q_i} l_{tmp}^T) + B_{Q_i}^{-1} tmp^T + B_{Q_i}^{-1}(CA_{Q_i} l_{tmp}^T \circ Ctmp^T)$;
        $l_{tmp} \leftarrow (a_j, a_{j+1})$;
```

$$x \backslash z = B^{-1}m^T + B^{-1}(I+C)Ax^T + B^{-1}(Cm^T \circ CAx^T) + B^{-1}z^T + B^{-1}(CAx^T \circ Cz^T).$$

So, what we actually need to do to decrypt is to start from the ciphertext and reverse the e-transformation, using the quasigroups $T_8, T_7, ..., T_1$ sequentially at first, and then reverse the e-transformations of the mini-blocks (from the encryption algorithm) using the quasigroups $Q_8, Q_7, ..., Q_1$. This can be done using the inverse operation we mentioned shortly before. The decryption of a ciphertext $c_1c_2 \dots c_{64}$ is done by the Decryption Algoritam.

Period $q = 2.66$					Period $q = 2.48$					Period $q = 2.43$					Period $q = 2.37$				
$\bullet_0$	0	1	2	3	$\bullet_1$	0	1	2	3	$\bullet_2$	0	1	2	3	$\bullet_3$	0	1	2	3
0	0	2	1	3	0	1	3	0	2	0	2	1	0	3	0	3	2	1	0
1	2	1	3	0	1	0	1	2	3	1	1	2	3	0	1	1	0	3	2
2	1	3	0	2	2	2	0	3	1	2	3	0	2	1	2	0	3	2	1
3	3	0	2	1	3	3	2	1	0	3	0	3	1	2	3	2	1	0	3

Table 6: Quaigroups used in the design of Edon80

For the cipher BCDMPQ only preliminary security investigations were done. The avalanche effect and propagation of one bit and two bits changes were considered and satisfactory results were obtained. It is an open research problem to check the resistance on the other block cipher attacks.

4.3. Stream ciphers

Stream ciphers are classified mainly as synchronous (when the keystream is generated independently of plaintext and cyphertext) and asynchronous (when the keystream is generated by the key and a fixed number of previous ciphertext symbols). A synchronous stream cipher is binary additive when the alphabet consists of binary digits and the output function is the XORing of the keystream and the plaintext. Also, totally asynchronous stream cipher is defined (when the keystream is generated by the key and all previous ciphertext symbols). There are several designs of stream cipher based on quasigroups, and here we will consider two of them.

4.3.1. Edon80

Edon80 is a binary additive stream cipher that is an unbroken eSTREAM finalists [53]. Schematic and behavioral description of Edon80 is given on the Figure 5. Edon80 works in three possible modes:

1) *KeySetup*,
2) *IVSetup* and
3) *Keystream* mode.

For its proper work Edon80 beside the core (that will be described later) has the following additional resources:

1. One register *Key* of 80 bits to store the actual secret key,
2. One register *IV* of 80 bits to store padded initialization vector,
3. One internal 2-bit counter *Counter* as a feeder of Edon80 Core in Keystream mode,
4. One 7 bit SetupCounter that is used in IVSetup mode,
5. One $4 \times 4 = 16$ bytes ROM bank where 4 quasigroups (i.e., Latin squares) of order 4, indexed from $(Q, \bullet_0)$ to $(Q, \bullet_3)$, are stored.

Those 4 predefined quasigroups are described in Table 6.

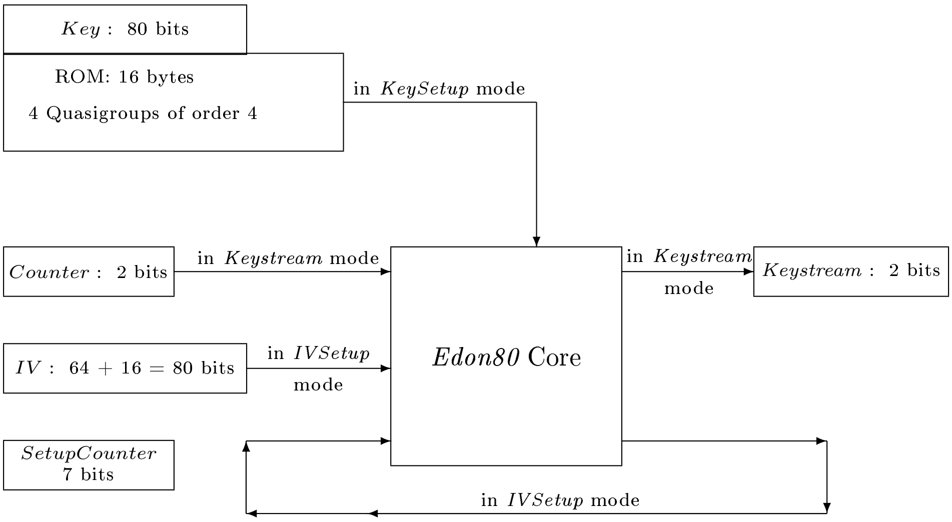


Figure 5: *Edon80* components and their relations.

The structure of the *Edon80* Core is described in the next two figures. The internal structure of *Edon80* can be seen as pipelined architecture of 80 simple 2-bit transformers called e-transformers. The schematic view of a single e-transformer is shown on Figure 6.

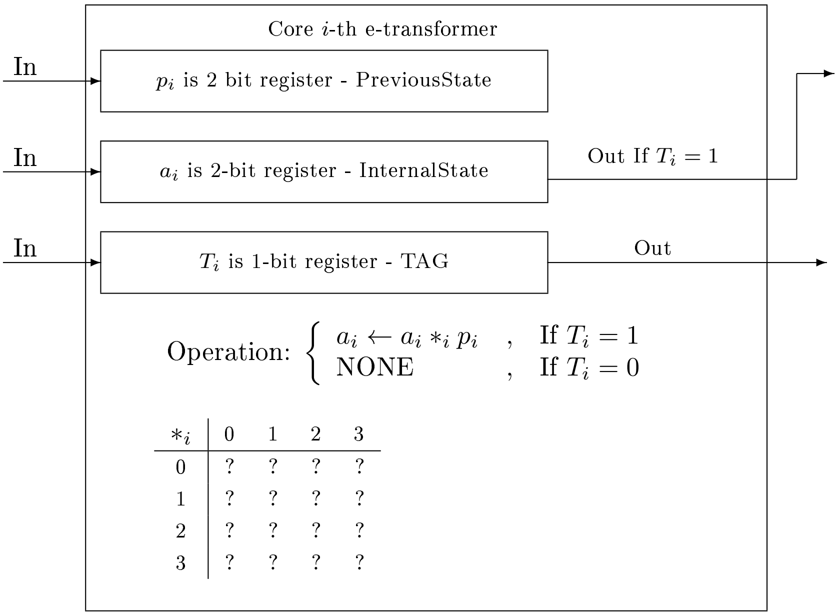
The structure that performs the operation $*_i$ in e-transformers is a quasigroup operation of order 4. We refer an e-transformer by its quasigroup operation $*_i$. So, in Edon80 we have 80 of this e-transformers, cascaded in a pipeline, one feeding another. The Figure 7 shows the pipelined core of *Edon80*.

We will not discuss in all details Edon80. What we want to emphasize is that the chosen quasigroups have enough big periods of growths. Thus, if any of the quasigroups is used k times in an e-transformations, the period of the obtained string will be correspondingly 2.66^k, 2.48^k, 2.43^k, 2.37^k. (Note that $2.48^{80} \approx 2^{104.8}$.) We have to state that 64 out of 576 quasigroups of order 4 have so big periods of growth, any 4 of them could be taken in the construction of Edon80.

Edon80 shows that, when adequately designed, the quasigroups of very small order can produce crypto primitives of high quality.

4.3.2. Edon X, Y, Z

Here we present a design of three different kinds of stream ciphers: the synchronous stream cipher EdonX, the asynchronous stream cipher EdonY and the totaly asynchronous stream cipher EdonZ.


Core i-th e-transformer
In
In
In
p_i is 2 bit register - PreviousState
a_i is 2-bit register - InternalState
T_i is 1-bit register - TAG
Out If $T_i = 1$
Out

$$\text{Operation: } \begin{cases} a_i \leftarrow a_i *_i p_i & , \text{ If } T_i = 1 \\ \text{NONE} & , \text{ If } T_i = 0 \end{cases}$$

$*_i$	0	1	2	3
0	?	?	?	?
1	?	?	?	?
2	?	?	?	?
3	?	?	?	?

Figure 6: Schematic representation of a single e-transformer of *Edon80*.

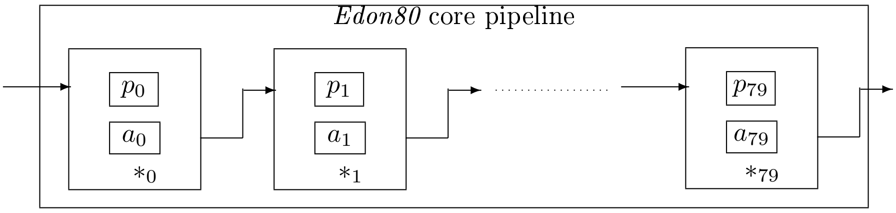


Figure 7: Edon80 core of 80 pipelined e-transformers.

All 3 ciphers EdonX,Y,Z have a same *Initialization phase*, and it is a very important phase of their designs. We denote by K_{in} secretly shared initial key an it is transformed in the initial phase to the working key K. The keys, as well as the messages, consist of s-bit words of any desired length $s \geqslant 4$. The used quasigroups are defined on the set of all s-bit words, and they have 2^s elements. The length n of the initial key (in s-bit words) can be any positive integer, larger n for higher security. This flexibility of the choice of the key length is one of the important performances of this Edon family.

The initialization phase of Edon family is described by following algorithm, where from the secret key K_{in} and the public quasigroup $(Q, \bullet)$ is obtained as output a secret working key K and a secret working quasigroup $(Q, *)$, that is an isotope of $(Q, \bullet)$.

```
Initialization of Edon X,Y,Z family of stream ciphers
Phase 1. Input of initial key
  1. Input: an integer $s$ – the length of the words, an integer $n$ – the initial length of the
     secret key, an integer $m$ – the length of the working key, a quasigroup $(Q, \bullet)$ of order $2^s$
     and the initial secret value of the key $K_{in} = K_0||K_1|| \cdots ||K_{n-1}$   ($K_i$ are s-bit words)
Phase 2. Padding the key
  2. Set $K := K_{in}||n_1||n_2$,        where $n_1$ is the most significant and $n_2$ is the least
     significant $s$-bit word of $n$.
Phase 3. Expanding the key to 512 s-bit words
  3. Set $K_{ex} := K||K|| \cdots ||K||K'$,        where $K'$ consists of the first $l$ s-bits words of $K$
     such that the total length of $K_{ex}$ is 512 s-bits words.
Phase 4. Transformation of $K_{ex}$ with the given quasigroup $(Q, \bullet)$ of order $2^s$
  4. For $i = 0$ to 511 do
       begin
         Set $leader := K[i \bmod (n+2)]$;
         $K_{ex} \leftarrow e_{leader,\bullet}(K_{ex})$;
         $K_{ex} \leftarrow RotateLeft(K_{ex})$;
       end;
Phase 5. Transformation $(Q, *) \leftarrow Isotope(Q, \bullet)$
  5. $(Q, *) \leftarrow (Q, \bullet)$;
     For $i = 0$ to 511 step 8 do
       begin
         Set $row_1 := K_{ex}[i]$; Set $row_2 = K_{ex}[i+1]$;
         $(Q, *) \leftarrow SwapRows(Q, row_1, row_2)$;
         Set $column_1 := K_{ex}[i+2]$; Set $column_2 = K_{ex}[i+3]$;
         $(Q, *) \leftarrow SwapColumns(Q, column_1, column_2)$;
         Set $\gamma := (K_{ex}[i+4], K_{ex}[i+6])$;
         $(Q, *) \leftarrow \gamma(Q, *)$;
       end;
Phase 6. Setting the working key $K = K_0|| \cdots ||K_{m-1}$ (the last $m$ s-bits words of $K_{ex}$)
  6. Set $K = K_0||K_1|| \cdots ||K_{m-1} := K_{ex}[512-m]|| \cdots ||K_{ex}[511]$
```

In the above algorithm K_{ex} means expanded key (it is an auxiliary variable) and the symbol $||$ means concatenation of s-bit words. The notation $K_{in}[j]$ ($K_{ex}[j]$, $K[j]$) means the j-th s-bit words of the K_{in} (K_{ex}, K). Thus, $K[j]$ and K_j have the same meaning. The function $RotateLeft(K_{ex})$ cyclicly rotates the values of the K_{ex} such that $K_{ex}[i] \leftarrow K_{ex}[i+1], i = 0, 1, 2, \ldots, 510$ and $K_{ex}[511] \leftarrow K_{ex}[0]$. The name of the functions *SwapRows* and *SwapColumns* speaks for themselves - they are functions by which the rows or columns of a quasigroup (i.e., the Latin square) are swapped.

EdonX

EdonX operates on nibbles, i.e., on 4-bit variables and consequently it uses quasigroups $Q = \{0, 1, \dots, 15\}$ of order 16 for doing quasigroup transformations on the streams of data. The working key K is stored in $m \geqslant 64$ internal variables K_i, i.e., $K = K_0 K_1 \dots K_{m-1}$ and $K_i \in Q$.

The secret key $K_{in} = K_{in}[0]K_{in}[1] \dots K_{in}[n-1]$, $K_{in}[j] \in Q$ of length n, $32 \leqslant n \leqslant 256$, and an initial public quasigroup $(Q, \bullet)$ of order 16. The decryption function of EdonX is the same as the encryption function. The encryption/decryption function of EdonX uses also two auxiliary 4-bit variables T and X, and one additional integer variable *Counter*. The operation $\oplus$ is the bitwise XOR operation on nibbles.

```
*EdonX* encryption and decryption function
Phase 1. Initialization
  From the secret initial key $K_{in}$ of length $n$
  and the initial quasigroup $(Q, \bullet)$ obtain
  new working key $K$ of length $m$ and new quasigroup
  $(Q, *) \leftarrow Isotope(Q, \bullet)$.
Phase 2. En(De)cryption
  1. $Counter \leftarrow 0$; $p = \lfloor \mathbb{F}racm2 \rfloor$;
  2. $X \leftarrow K[Counter \ \mathtt{mod}\ n]$;
  3. $T \leftarrow K[Counter + p \ \mathtt{mod}\ n]$;
  4. For $i = 0$ to $m - 1$ do
       begin
         $X \leftarrow K_i * X$;
         $T \leftarrow T \bullet X$;
         $K_i \leftarrow X$;
       end;
       $K_{m-1} \leftarrow T$;
  5. Output: $X \oplus Inputnibble$;
  6. $Counter \leftarrow Counter + 1$;
  7. Go to 2;
```

It is shown that EdonX is resistant to chosen plaintex/ciphertext attacks. In order to proof that theorems of this type are proved:

Theorem 7. *Any quasigroup* $(Q, *)$ *of order* 16*, where* $Q = \{0, 1, 2, \dots, 15\}$*, is a solution of the system of functional equations*

$$\begin{array}{l}
x_0 = y_0 * y_{i \ \mathtt{mod}\ m} \\
x_1 = y_1 * x_0 \\
x_2 = y_2 * x_1 \\
\cdots \\
x_{m-2} = y_{m-2} * x_{m-3} \\
a = y_{m-1} * x_{m-2} \\
z = ((\dots(y_{i+p \ \mathtt{mod}\ m} \bullet x_0) \bullet x_1) \bullet \cdots) \bullet x_{m-2}) \bullet a
\end{array} \tag{17}$$

with one unknown quasigroup operation $*$ *and unknown variables* $x_0,\ x_1,\ldots,$ $x_{m-2},\ y_0,\ y_1,\ldots,\ y_{m-1},\ z$ *over* Q*, where* $\bullet$ *is given quasigroup operation on* Q*,* $a\in Q$ *is fixed element,* i *is a nonnegative integer and* $p=\lfloor\frac{m}{2}\rfloor$*.*

EdonX can be used as secure pseudo-random number generator like any synchronous stream cipher. For that aim take the message $M = 000\ldots$ to consist of zeros only and let us analyze the output string $C = C_0C_1C_2\ldots$. Since $C_i = X_i \oplus 0 = X_i$ $(i = 0, 1, 2, \ldots)$, the output string C in this case consists of the values of the variable X.

From the encryption/decryption algorithm of EdonX the following system of iterative functions can be obtained:

$$\begin{array}{l}
K_{\lambda,0} = K_{\lambda-1,0} * K_{\lambda-1,i \texttt{ mod } m}\\
K_{\lambda,1} = K_{\lambda-1,1} * K_{\lambda,0}\\
\cdots\cdots\cdots\\
K_{\lambda,m-2} = K_{\lambda-1,m-2} * K_{\lambda,m-3}\\
X_{\lambda,m-1} = K_{\lambda-1,m-1} * K_{\lambda,m-2}\\
K_{\lambda,m-1} = ((\ldots(K_{\lambda-1,i+p \texttt{ mod } m} \bullet K_{\lambda,0}) \bullet K_{\lambda,1})\cdots \bullet K_{\lambda,m-2}) \bullet X_{\lambda,m-1}
\end{array} \tag{18}$$

What we are interested for are the values of $X_{\lambda,m-1}$ for $\lambda = 0, 1, \ldots,$ since the output string C is just the string $X_{0,m-1}X_{1,m-1}X_{2,m-1}X_{3,m-1}\ldots$. "What is the period and the nature of the string C"? The answer depends on the theory of discrete chaos systems, that is not developed yet! In several experiments with a reduced system (18) with initial keys of length 4 and $m = 16$ is obtained that either the ergodic part had length greater than 2^{32} or the periodic part had a period greater than 2^{32} (or both). It is resonable to to conjecture that in the standard version of EdonX (when $m = 64$ and the initial keys have length at least 32) either an ergodic part of length 2^{128} or a period 2^{128} (or both) will be obtained.

EdonY

The proof that EdonY is self-synchronized is a direct consequence of the following theorem.

Theorem 8. *Let* $E = e_{l_1,*_1}\circ\cdots\circ e_{l_n,*_n}$ *and* $D = d_{l_n,\backslash_n}\circ\cdots\circ d_{l_1,\backslash_1}$ *be transformations obtained with* n *quasigroup transformations* $*_1,\ldots,*_n$ *on* Q*, leaders* $l_1,\ldots,l_n$ *and corresponding parastrophes* $\backslash_1,\ldots,\backslash_n$*. Assume that* $E(b_1b_2\ldots b_k) = c_1c_2\ldots c_k$*,* $k > n$*, and* $d\neq c_i$ *for some fixed* i $(b_j, c_j, d \in Q)$*. Then, for some* $d_1,\ldots,d_{n+1}\in Q$*,*

$$D(c_1\ldots c_{i-1}dc_{i+1}\ldots c_k) = \left\{\begin{array}{ll} b_1\ldots b_{i-1}d_1\ldots d_{n+1}b_{i+n+1}\ldots b_k, & k > i+n\\ b_1\ldots b_{i-1}d_1\ldots d_{k-i+1}, & k\leqslant i+n\end{array}\right. .$$

In the construction of EdonY we use a public quasigroup $(Q,\bullet)$ of order 32 defined on 5-bits letters, $Q = \{0, 1, 2, \ldots, 31\}$ and a secret key K_{in} stored in n internal variables $K_i \in Q$, i.e., $K_{in} = K_0K_1\ldots K_{n-1}$ and $n \geqslant 32$.

The EdonY encryption algorithm and decryption algorithm are precisely defined by the following procedures, where $M = M_0M_1M_2M_3M_4\dots$ $(C = C_0C_1C_2C_3C_4\dots)$ is the input plaintext (output ciphertext) string. The variables X and Y in the decryption algorithm are auxiliary 5-bits variables.

```
EdonY encryption algorithm
Phase 1. Initialization
  From the secret initial key $K_{in}$ of length $n$
  and the initial quasigroup $(Q, \bullet)$ obtain
  new working key $K$ of length $m$ and new quasigroup
  $(Q, *) \leftarrow Isotope(Q, \bullet)$.
Phase 2. Encryption
  1. $Counter \leftarrow 0$; $p = \lfloor \mathbb{F}racn2 \rfloor$;
  2. $K_0 \leftarrow K_0 * (M_{Counter} * K_{Counter+p \bmod n})$
  3. For $i = 1$ to $n - 1$ do
        begin
          $K_i \leftarrow K_i * K_{i-1}$;
        end;
  4. Output: $C_{Counter} = K_{n-1}$;
  5. $Counter \leftarrow Counter + 1$;
  6. Go to 2;
```

```
EdonY decryption algorithm
Phase 1. Initialization
  From the secret initial key $K_{in}$ of length $n$
  and the initial quasigroup $(Q, \bullet)$ obtain
  new working key $K$ of length $m$ and new quasigroup
  $(Q, *) \leftarrow Isotope(Q, \bullet)$.
Phase 2. Decryption
  1. $Counter \leftarrow 0$; $p = \lfloor \mathbb{F}racn2 \rfloor$;
  2. $X \leftarrow K_{n-1}$
     $K_{n-1} \leftarrow C_{Counter}$;
  3. For $i = n - 2$ down to 0 do
        begin
          $Y \leftarrow K_i$
          $K_i \leftarrow X \setminus K_{i+1}$;
          $X \leftarrow Y$
        end;
  4. Output: $M_{Counter} = (X \setminus K_0)/K_{Counter+p \bmod n}$;
  5. $Counter \leftarrow Counter + 1$;
  6. Go to 2;
```

It follows from Theorem 8 that EdonY is self synchronized since one error in the cipher-text C will propagate $n + 1$ errors in the recovered plaintext M', i.e.,

<table>
<tr><td colspan="2"><b>Initialization</b>
From the secret initial key K_{in} of length n
and the initial quasigroup $(Q, \bullet)$ obtain
new working key K of length 64 and new quasigroup
$(Q, *) \leftarrow Isotope(Q, \bullet)$.</td></tr>
<tr><td><b>Encryption</b>.
<b>Input</b>: Key K of
length n and message M.
<b>Output</b>: Message C.</td><td><b>Decryption</b>.
<b>Input</b>: Key K of
length n and message C.
<b>Output</b>: Message M.</td></tr>
<tr><td>1) $X \leftarrow InputNibble$;
2) $T \leftarrow 0$;
3) For $i = 0$ to $n-1$ do
$X \leftarrow K_i * X]$;
$T \leftarrow T \oplus X$;
$K_i \leftarrow X$;
4) $K_{n-1} \leftarrow T$;
5) Output X;
6) Go to 1;</td><td>1) $X, T \leftarrow InputNibble$;
2) $temp \leftarrow K_{n-1}$;
3) For $i = n-1$ downto 0 do
$X \leftarrow temp \setminus X$;
$T \leftarrow T \oplus X$;
$temp \leftarrow K_{i-1}$;
$K_{i-1} \leftarrow X$;
4) $K_{n-1} \leftarrow T$;
5) Output X;
6) Go to 1;</td></tr>
</table>

Table 7: Totaly Asynchronous Stream Cipher

the original message M and M' will differ in $n+1$ consecutive letters. If there will be a string of errors in C of length r, then the recovered plaintext will have $r+n$ errors.

There are proofs that EdonY is resistent to dictionary and to chosen plaintext/ciphertext attacks. Considering only the known ciphertext attacks, the resistance follows from the next theorem.

Theorem 9. *Given a ciphertext C, for each quasigroup operation $*$ on $Q = \{0, 1, \ldots, 31\}$ and each key $K = K_0 K_1 \ldots K_{n-1}$ there is a plaintext M such that C is its ciphertext.*

EdonZ

EdonZ operates on nibbles, so it uses a quasigroup $(Q, \bullet)$, $Q = \{0, \ldots, 15\}$, of order 16. The secret key K_{in} is stored in $n = 64$ internal variables K_i, that have values in the range $Q = \{0, 1, \ldots, 15\}$.

EdonZ encryption and decryption algorithms use also temporal 4-bit variables T, X, and *temp*. EdonZ differs from the synchronous EdonX in the way how the initial value of the variables X and T are set and how the final computation of X is done. However, in decrypting algorithm EdonX does not use the left parastrophe of the $(Q, *)$ since it is binary additive stream cipher, but EdonZ needs $(Q, \setminus)$.

Next we will give an example that will work on the principles of EdonZ, but for the simplicity of the explanation, quasigroup of order 4 will be used and the working key will be of length 4. We take that the working key is $K = 2\ 3\ 2\ 3$, the message is $M = \{0, 0, 1, 0, 2, 3, 0, \dots\}$ and the quasigroup and its parastrophe are the following.

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

$\backslash$	0	1	2	3
0	1	3	2	0
1	2	0	1	3
2	0	2	3	1
3	3	1	0	2

Several steps of EdonZ encryption are as following.

		M_0			M_1			M_2			M_3		
	K	X	T	K	X	T	K	X	T	K	X	T	$\cdots$
i		0	0		0	0		1	0		0	0	$\cdots$
0	2	0	0	0	3	3	3	1	1	1	1	1	
1	3	2	2	2	2	1	2	3	2	3	1	0	
2	2	1	3	1	0	1	0	1	3	1	2	2	
3	3	1	2	2	0	1	1	2	1	1	0	2	
Output $C = X$		1			0			2			0		

We emphasize that EdonZ is used in the definition of the random error-correcting code RCBQ with cryptograpic properties ([55], [119]).

4.4. Pseudo random number generators

A truly random sequence can be obtained only by theory. Namely, if we take that a sequence is random only if it passes all of the statistical test for randomness, then we can never check if a sequence is random until all of the tests, infinitely many, are passed. So, sequences that look randomly are used in many applications were random sequences are needed. They are produced by some deterministic algorithms or physical phenomenas and are called Pseudo Random Sequences (PRS). PRS have to pass all known approved battery o statistical tests for randomness (like Diehard, NIST, ...) The algorithms for producing PRS are called Pseudo Random Sequence Generator (PRSG), i.e., PRNG when we have number sequences.

Many PRNG that are used for many purposes are biased, for example the next produced bit (or symbol) can be predictable with probability greater than 1/2. Then, the obtained sequence of such a generator should be unbiased. By using quasigroup transformations several type of PRNG can be designed. In fact, all of the previous stream ciphers can be used as PRNG, and they are cryptographically secure, since a key is used. What is a problem with those PRNG is their efficiency, since they are designed for other purposes.

Very simple PRNG can be obtained by the following procedure.

QPRNG can produce pseudo random sequences from very biased sequences, even from periodical sequences as well. We emphasize that in QPRNG the choice of the quasigroup is very important, it should be shapeless and exponential with

```
Quasigroup PRNG (QPRNG)

 Phase I. Initialization
 1. Choose a positive integer $s \geqslant 4$;
 2. Choose a quasigroup $(A, *)$ of order $s$;
 3. Set a positive integer $k$;
 4. Set a leader $l$, a fixed element of $A$ such that $l * l \neq l$;
 Phase II. Transformations of the random
           string $b_0 b_1 b_2 b_3 \ldots,\ \ b_j \in A$
 5. For $i = 1$ to $k$ do $L_i \leftarrow l$;
 6. $j \leftarrow 0$;
 7. do
        $b \leftarrow b_j$;
        $L_1 \leftarrow L_1 * b$;
        For $i = 2$ to $k$ do $L_i \leftarrow L_i * L_{i-1}$;
        Output: $L_k$;
        $j \leftarrow j + 1$;
    loop;
```

Table 8: Algorithm for simple QPRNG

as higher period of growth as possible. In fact, for quasigroups of order 4 one can compute the period of growth of all 576 quasigroups. The Table 9 shows that suitable quasigroups of order 16 can be find enough easily too.

As an example of the capacity of QPRNG we consider the PRNG used in GNU C v2.03 that do not passed all of the statistical tests in the Diehard Battery v0.2 beta [30], but after using QPRNG on the obtained sequence from GNU with a quasigroup of order 256 and for $k = 1$ (only one application of an e-transformation) all tests of Diehard were passed ([87]).

```
    ***** TEST SUMMARY FOR GNU C (v2.03) PRNG *****
    All p-values:
0.2929,0.8731,0.9113,0.8755,0.4637,0.5503,0.9435,0.7618,0.9990,0.0106,1.0000,0.0430,
1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,
1.0000,1.0000,1.0000,0.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,1.0000,
. . . . . . . . . . . .. . . . . . .
0.7921,0.4110,0.3050,0.8859,0.4783,0.3283,0.4073,0.2646,0.0929,0.6029,0.4634,0.8462,
0.2385,0.6137,0.1815,0.4001,0.1116,0.2328,0.0544,0.4320,0.0000,0.0000,0.0000,0.0000,
. . . . . . . . . . . .. . . . . . .
0.0003,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,
0.0753,0.0010,0.0000,0.0000,0.0000,0.0000,0.0000,0.0000,0.0233,0.0585,0.0000,0.0000,
0.0000,0.0000,0.0000,0.2195,0.0321,0.0000,0.0000,0.9948,0.0006,0.0000,0.0000,0.0688,
. . . . . . . . . . . .. . . . . . .
0.2303,0.1190,0.8802,0.0377,0.6887,0.4175,0.0803,0.3687,0.7010,0.7425,0.1003,0.0400,
0.9488,0.3209,0.5965,0.0676,0.0021,0.2337,0.5204,0.5343,0.0630,0.2008,0.6496,0.4157,
0.9746,0.1388,0.4657,0.5793,0.6455,0.8441,0.5248,0.7962,0.8870
```

Overall p-value after applying KStest on 269 p-values = 0.000000

Value of c	Number of quasigroups with period growth $2^{c\,k}$	Value of c	Number of quasigroups with period growth $2^{c\,k}$
$0.00 \leqslant c < 0.25$	4	$2.00 \leqslant c < 2.25$	79834
$0.25 \leqslant c < 0.50$	23	$2.25 \leqslant c < 2.50$	128836
$0.50 \leqslant c < 0.75$	194	$2.50 \leqslant c < 2.75$	174974
$0.75 \leqslant c < 1.00$	686	$2.75 \leqslant c < 3.00$	199040
$1.00 \leqslant c < 1.25$	2517	$3.00 \leqslant c < 3.25$	175848
$1.25 \leqslant c < 1.50$	7918	$3.25 \leqslant c < 3.50$	119279
$1.50 \leqslant c < 1.75$	18530	$3.50 \leqslant c < 3.75$	45103
$1.75 \leqslant c < 2.00$	42687	$3.75 \leqslant c \leqslant 4.00$	4527

Table 9: Period growth of 10^6 randomly chosen quasigroups of order 16 after 5 applications of e-transformations (k=5 in QPRNG)

```
    *** TEST SUMMARY FOR GNU C v2.03 + QUASIGROUP PRNG IMPROVER ***
    All p-values:
0.5804,0.3010,0.1509,0.5027,0.3103,0.5479,0.3730,0.9342,0.4373,0.5079,0.0089,0.3715
0.0584,0.1884,0.1148,0.0662,0.8664,0.5070,0.7752,0.1939,0.9568,0.4948,0.1114,0.2042,
0.4883,0.4537,0.0281,0.0503,0.0346,0.6085,0.1596,0.1545,0.0855,0.5665,0.0941,0.7693,
. . . . . . . . . . . . .. . . . . . .
0.6544,0.9673,0.8787,0.9520,0.8339,0.4397,0.3687,0.0044,0.7146,0.9782,0.7440,0.3042,
0.8465,0.7123,0.8752,0.8775,0.7552,0.5711,0.3768,0.1390,0.9870,0.9444,0.6101,0.1090,
. . . . . . . . . . . . .. . . . . . .
0.8538,0.6871,0.8785,0.9159,0.4128,0.4513,0.1512,0.8808,0.7079,0.2278,0.1400,0.6461,
0.3353,0.1064,0.6739,0.2066,0.5119,0.0558,0.5748,0.5064,0.8982,0.6422,0.7512,0.8633,
0.4625,0.0843,0.0903,0.7641,0.6253,0.8523,0.7768,0.8041,0.5360,0.0826,0.0378,0.8710,
. . . . . . . . . . . . .. . . . . . .
0.2115,0.8156,0.8468,0.9429,0.8382,0.1463,0.4212,0.6948,0.4816,0.3454,0.2114,0.3493,
0.3448,0.0413,0.2422,0.6363,0.2340,0.8404,0.0065,0.7319,0.8781,0.2751,0.5197,0.4105,
0.0832,0.1503,0.1148,0.3008,0.0121,0.0029,0.4423,0.6239,0.0651,0.3838,0.0165,0.2770,
0.2074,0.0004,0.7962,0.4750,0.4839,0.9152,0.1681,0.0822,0.0518
Overall p-value after applying KStest on 269 p-values = 0.018449
```

4.5. Hash functions

Hash functions on a set A are mappings $h : A^+ \to A^n$ that take a variable-size input messages and map them into fixed-size output, known as hash result, message digest, hash-code etc. They are used in checking data integrity, digital signature schemes, commitment schemes, password based identification systems, digital timestamping schemes, pseudo-random string generation, key derivation, one-time passwords etc.

The first attempts for using quasigroup transformations for creating cryptographic hash functions do not have actual implementations ([37], [38], [86], [47]). In [140] is proposed a hash function as one elementary e-transformation on the message $x_1x_2 \dots x_t$:

$H(x_1x_2 \dots x_t) = (((a \bullet x_1) \bullet x_2) \cdots \bullet x_t = e_{a,\bullet}(x_1x_2 \dots x_t)$.

The huge working quasigroup $(Q, \bullet)$ is obtained from the modular subtraction quasigroup $(Q, *)$ defined by $x * y = x + (r - y) \ mod \ r$, $|Q| = r$, and three secret permutations π, w, ρ as $x \bullet y = \pi^{-1}(w(x) + (r - \rho(y)) \ mod \ r)$. The leader a is used as initialization vector.

A generic hash function with quasigroup reverse string transformation R has been described in [54], with first implementation named Edon-R(256, 384, 512) given in [46]. Another interesting application of quasigroups is the quasigroup folding, a 2 time slower security fix of the MD4 family of hash functions [48], with shapeless randomly generated quasigroup of order 16. Similar technique has been used in [49] , where new hash function SHA-1Q2 has been constructed from SHA-1 by message expansion part with quasigroup folding and has only 8 internal iterative steps (and it is 3% faster than SHA-1).

Further on we will consider the candidate of NIST SHA-3 competition, Edon-$\mathcal{R}$ and NaSHA, whose designs were based on huge quasigroup transformations.

Edon-$\mathcal{R}$

Edon-$\mathcal{R}$ [58] is wide-pipe iterative hash function with standard MD-straitening. It was the fastest First round candidate of NIST SHA-3 competition.

The chaining value H_i and the message input M_i for the ith round are composed of two q-bits blocks, $q = 256, 512$, i.e., $H_i = (H_i^1, H_i^2)$ and $M_i = (M_i^1, M_i^2)$, and the new chaining value H_{i+1} is produced as follows

$H_{i+1} = (H_{i+1}^1, H_{i+1}^2) = R(H_i^1, H_i^2, M_i^1, M_i^2)$,

$\mathcal{R}$ is little bit modified reverse string transformation, in a sense that two parts from the message are taken reversed when are used like a leaders, and the order of leaders is $\bar{M}_i^2, H_i^1, H_i^2, \bar{M}_i^1$. The compression function $\mathcal{R}$ uses two huge quasigroups of order 2^{256} and 2^{512}. Algorithmic description of the quasigroup of order 2^{256} is given in the Table . There X_i, Y_i and Z_i are 32-bit variables, so $X = (X_0, X_1, \dots, X_7)$, $Y = (Y_0, Y_1, \dots, Y_7)$ and $Z = (Z_0, Z_1, \dots, Z_7)$ are 256-bits variables. (Note that the operation is $X * Y = Z$.) Operation "+" denotes addition modulo 2^{32} , operation $\oplus$ is the logical operation of bitwise exclusive or and the operation $ROTL^r(X_i)$ is the operation of bit rotation of the 32-bit X_i, to the left for r positions.

NaSHA

NaSHA [92] is another First round candidate to the NIST SHA-3 competition based on quasigroups . It is also wide-pipe iterative hash function with standard MD-straitening. NaSHA-(m, k, r) has three parameters m, k, r, where m denotes message length, k is the number of elementary quasigroup string transformations

Quasigroup operation of order 2^{256}

Input: $X = (X_0, X_1, \dots, X_7)$ and $Y = (Y_0, Y_1, \dots, Y_7)$,
where X_i and Y_i are 32-bit variables.
Output: $Z = (Z_0, Z_1, \dots, Z_7)$ where Z_i are 32-bit variables.
Temporary 32-bit variables: $T_0, \dots, T_{15}$.

```
   $T_0 \leftarrow ROTL^0(0xAAAAAAAA + X_0 + X_1 + X_2 + X_4 + X_7);$
   $T_1 \leftarrow ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);$
   $T_2 \leftarrow ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);$
1. $T_3 \leftarrow ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);$
   $T_4 \leftarrow ROTL_{17}(X_1 + X_2 + X_3 + X_5 + X_6);$
   $T_5 \leftarrow ROTL_{22}(X_0 + X_2 + X_3 + X_4 + X_5);$
   $T_6 \leftarrow ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);$
   $T_7 \leftarrow ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);$

   $T_8 \leftarrow T_3 \oplus T_5 \oplus T_6;$
   $T_9 \leftarrow T_2 \oplus T_5 \oplus T_6;$
   $T_{10} \leftarrow T_2 \oplus T_3 \oplus T_5;$
2. $T_{11} \leftarrow T_0 \oplus T_1 \oplus T_4;$
   $T_{12} \leftarrow T_0 \oplus T_4 \oplus T_7;$
   $T_{13} \leftarrow T_1 \oplus T_6 \oplus T_7;$
   $T_{14} \leftarrow T_2 \oplus T_3 \oplus T_4;$
   $T_{15} \leftarrow T_0 \oplus T_1 \oplus T_7;$

   $T_0 \leftarrow ROTL^0(0x55555555 + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);$
   $T_1 \leftarrow ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);$
   $T_2 \leftarrow ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);$
3. $T_3 \leftarrow ROTL_{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);$
   $T_4 \leftarrow ROTL_{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);$
   $T_5 \leftarrow ROTL_{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);$
   $T_6 \leftarrow ROTL_{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);$
   $T_7 \leftarrow ROTL_{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);$

   $Z_5 \leftarrow T_8 + (T_3 \oplus T_4 \oplus T_6);$
   $Z_6 \leftarrow T_9 + (T_2 \oplus T_5 \oplus T_7);$
   $Z_7 \leftarrow T_{10} + (T_4 \oplus T_6 \oplus T_7);$
4. $Z_0 \leftarrow T_{11} + (T_0 \oplus T_1 \oplus T_5);$
   $Z_1 \leftarrow T_{12} + (T_2 \oplus T_6 \oplus T_7);$
   $Z_2 \leftarrow T_{13} + (T_0 \oplus T_1 \oplus T_3);$
   $Z_3 \leftarrow T_{14} + (T_0 \oplus T_3 \oplus T_4);$
   $Z_4 \leftarrow T_{15} + (T_1 \oplus T_2 \oplus T_5);$
```

Table 10: An algorithmic description of a quasigroup of order 2^{256}.

of type A and RA, and r is from the order 2^{2^r} of used quasigroups. To the competition was sent NaSHA-$(m, 2, 6)$, $m = 224, 256, 384, 512$. Every round consists of one linear transformation obtained from an LFSR, followed by MT quasigroup string transformation, that is a composition of k alternate quasigroup string transformations A and RA. NaSHA uses novel design principle: the quasigroups used in every iteration in compression function are different, and depend on the processed message block. Even in one iteration, different quasigroups are used for two quasigroup transformations. Quasigroups in NaSHA are obtained by using Extended Feistel Networks as orthomorphisms and complete mappings on the groups $(\mathbb{Z}_{2^{16}}, \oplus)$, $(\mathbb{Z}_{2^{32}}, \oplus)$ and $(\mathbb{Z}_{2^{64}}, \oplus)$. NaSHA is of order 2^{64} and is produced from known starting bijection of order 2^8 by using xoring, addition modulo 2^{64} and table lookups.

The MQQ (Multivarite Quadratic Quasigroups) family of crytptosystems was first defined in 2007 [51]. Subsequently, a signature [57], and an improved encryption variant was proposed [59]. As the name suggests, the cryptosystems from this family are based on multivariate quadratic quasigroups – MQQs, defined over a finite field. It belongs to the broader family of multivariate public key cryptosystems ($\mathcal{MQ}$) whose security relies on the hardness of solving quadratic polynomial systems of equations over finite fields, known to be $\mathcal{NP}$-hard problem.

A typical ($\mathcal{MQ}$) public key cryptosystem relies on the knowledge of a trapdoor for a particular system of polynomials over a finite field $\mathbb{F}_q$. The public key of the cryptosystem is usually given by a multivariate quadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, i.e.,

$$\mathcal{P}(x_1, \dots, x_n) = \begin{pmatrix} p_1(x_1, \dots, x_n) = \sum\limits_{1 \leqslant i \leqslant j \leqslant n} \widetilde{\gamma}_{ij}^{(1)} x_i x_j + \sum\limits_{i=1}^{n} \widetilde{\beta}_i^{(1)} x_i + \widetilde{\alpha}^{(1)} \\ \vdots \\ p_m(x_1, \dots, x_n) = \sum\limits_{1 \leqslant i \leqslant j \leqslant n} \widetilde{\gamma}_{ij}^{(m)} x_i x_j + \sum\limits_{i=1}^{n} \widetilde{\beta}_i^{(m)} x_i + \widetilde{\alpha}^{(m)} \end{pmatrix}$$

for some coefficients $\widetilde{\gamma}_{ij}^{(s)}, \widetilde{\beta}_i^{(s)}, \widetilde{\alpha}^{(s)} \in \mathbb{F}_q$. It is obtained by obfuscating a structured central map

$$\mathcal{F} : (x_1, \dots, x_n) \in \mathbb{F}_q^n \to \big(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\big) \in \mathbb{F}_q^m,$$

using two bijective affine mappings $\mathcal{S}, \mathcal{T}$ over $\mathbb{F}_q^n$ that serve as a sort of mask to hide the structure of $\mathcal{F}$. The public key is defined as

$$\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}.$$

The mappings $\mathcal{S}$ and $\mathcal{T}$ are part of the private key s. Besides them, the private key may also contain other secret parameters that allow creation, but also easy inversion of the transformation $\mathcal{F}$. Without loss of generality, we can assume that the private key is $s = (\mathcal{F}, \mathcal{S}, \mathcal{T})$.

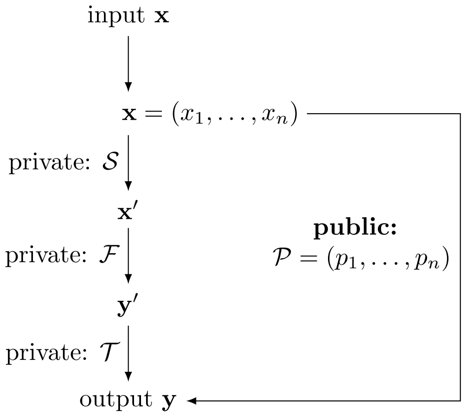


Figure 8: A general $\mathcal{MQ}$ trapdoor

Graphically, the trapdoor of an $\mathcal{MQ}$ scheme can be depicted as in Figure 8.

MQQ-SIG is a signature scheme that has excellent performance in signing. In particular, it is the fastest signature scheme in the ECRYPT benchmarking of cryptographic systems (eBACS) [13]. It is defined over $\mathbb{F}_2$ and has the minus modifier applied because of the possibility for direct algebraic attack and MinRank attack otherwise.

The length of the messages that can be signed is $n/2$, and the signing process is performed by prepending a random string of length $n/2$.

A high-level schematic presentation of the signing and verification process is given in Figure 9 and the corresponding algorithmic description in Algorithm 1.

The central mapping $\mathcal{F}$ of MQQ-SIG is a quasigroup string transformation using one quasigroup q. Both $\mathcal{F}$ and the inverse $\mathcal{F}^{-1}$ are depicted in Figure 10 and Figure 11. Algorithm 2 gives a detailed description of the construction of the central map $\mathcal{F}$.

The MQQs used are of relatively small order 2^8 that allows storing them in a lookup table, used for the signing process.

The algorithm used for construction of the MQQ is presented in Algorithm 3.

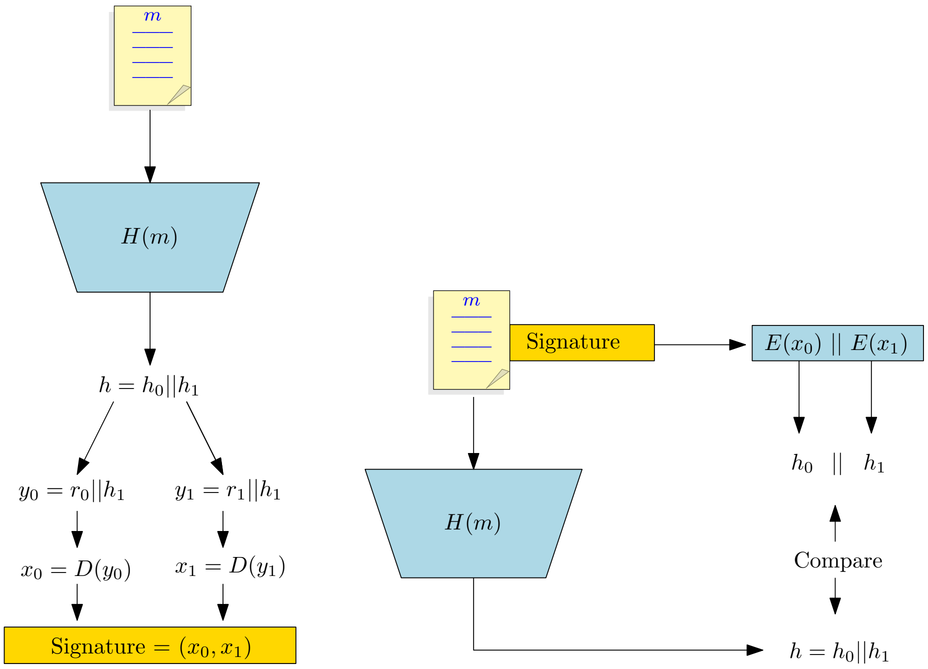


Figure 9: The signing and verification process of MQQ-SIG

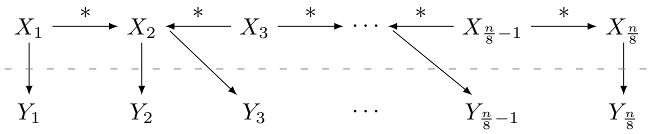


Figure 10: Graphical representation of the central map $\mathcal{F}$ in MQQ-SIG.

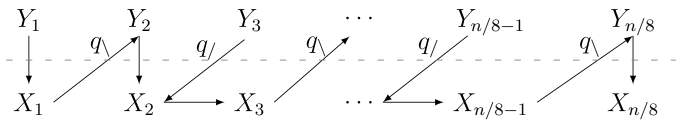


Figure 11: Graphical representation of the inverse map $\mathcal{F}^{-1}$ in MQQ-SIG, using the right and left parastrophes.

Algorithm 1 MQQ-SIG

Key Generation

1. Use Algorithm 2 to construct the central map $\mathcal{F}$.
2. Construct the affine mappings $\mathcal{S}$ and $\mathcal{S}'$ as defined in [57].
3. Pick a hash function $H : \{0,1\}^* \to \{0,1\}^n$.
4. Construct the mapping $\mathcal{P}' = \mathcal{S} \circ \mathcal{F} \circ \mathcal{S}'$ and define the public key $\mathcal{P}$ as the last $\frac{n}{2}$ coordinates of $\mathcal{P}'$. Denote by $\mathcal{P}'^{-1}$ the inverse of $\mathcal{P}'$. Algorithm 4 is used to compute $\mathcal{P}'^{-1}$.

Output: The public key $\mathcal{P}$ and the private key $(\mathcal{F}, \mathcal{S}, \mathcal{S}')$.

Signature Generation
Input: A message $m \in \{0,1\}^*$ to be signed.

1. Compute $h = h_0||h_1 \leftarrow H(m)$, where h_0 and h_1 are both $\frac{n}{2}$ bits long.
2. Generate two random $\frac{n}{2}$-bit values, r_0 and r_1, and set $\mathbf{y_0} = r_0||h_0$ and $\mathbf{y_1} = r_1||h_1$.
3. Compute $\mathbf{x_0} = \mathcal{P'}^{-1}(\mathbf{y_0})$ and $\mathbf{x_1} = \mathcal{P'}^{-1}(\mathbf{y_1})$.

Output: The digital signature $(\mathbf{x_0}, \mathbf{x_1})$.

Signature Verification
Input: A message-signature pair $(m, (\mathbf{x_0}, \mathbf{x_1}))$.

1. Compute $h = h_0||h_1 \leftarrow H(m)$.
2. Compute $\mathbf{z_0} \leftarrow \mathcal{P}(\mathbf{x_0})$ and $\mathbf{z_1} \leftarrow \mathcal{P}(\mathbf{x_1})$.

Accept the signature if $\mathbf{z_0} = h_0$ and $\mathbf{z_1} = h_1$, otherwise reject.

Algorithm 2 Construct$\mathcal{F}$

Input: A vector $\mathbf{x} = (x_1, \ldots, x_n)$, where n is a multiple of 8.

1. Represent the vector $\mathbf{x}$ as a string $X = X_1 X_2 \ldots X_k$, where $k = \frac{n}{8}$, and $X_i = (x_{8(i-1)+1}, \ldots, x_{8i})$ for every $i \in \{1, \ldots, k\}$.

2. Use Algorithm 3 to construct an MQQ $(\mathbb{F}_2^8, q)$.

3. Compute the string $Y = Y_1 Y_2 \ldots Y_k$, where

$$Y_i = \begin{cases} X_1 & \text{if } i = 1, \\ q(X_{i-1}, X_i) & \text{if } i = 2, 4, \ldots, k, \\ q(X_i, X_{i-1}) & \text{if } i = 3, 5, \ldots, k-1. \end{cases} \tag{19}$$

4. Represent Y as a vector $\mathbf{y} = (y_1, \ldots, y_n)$.

Output: The vector $\mathbf{y}$.

Algorithm 3 ConstructMQQ

Repeat

1. Construct $d \times d$ upper triangular Boolean matrices $\mathbf{U}_i$, $i \in \{1, \ldots d-1\}$ that have all elements 0 except the elements in the rows from $\{1, \ldots, i\}$ that are strictly above the main diagonal. Choose these elements uniformly at random from $\mathbb{F}_2$.

2. Choose randomly three nonsingular $d \times d$ matrices $\mathbf{A_1}$, $\mathbf{A_2}$ and $\mathbf{B}$ over $\mathbb{F}_2$ and a vector $\mathbf{c} \in \mathbb{F}_2^d$.

3. Form the $d \times d$ block matrix

$$\mathbf{U}(\mathbf{x}) = \mathbf{I}_d + \begin{bmatrix} \mathbf{0} & \mathbf{U}_1 \cdot \mathbf{A_1} \cdot \mathbf{x} & \mathbf{U}_2 \cdot \mathbf{A_1} \cdot \mathbf{x} & \ldots & \mathbf{U}_{d-1} \cdot \mathbf{A_1} \cdot \mathbf{x} \end{bmatrix}.$$

4. Construct the mapping $q(\mathbf{x}, \mathbf{y}) = \mathbf{B} \cdot \mathbf{U}(\mathbf{x}) \cdot \mathbf{A_2} \cdot \mathbf{y} + \mathbf{B} \cdot \mathbf{A_1} \cdot \mathbf{x} + \mathbf{c}$, that defines an MQQ of order 2^d.

Until the following conditions about the matrices $\mathfrak{Q}^{(i)}$ of the coordinates q_i are satisfied:

$$\forall i \in \{1, \ldots, d\}\,,\ \mathrm{Rank}(\mathfrak{Q}^{(i)}) \geqslant 2d - 4, \tag{20a}$$

$$\exists j \in \{1, \ldots, d\}\,,\ \mathrm{Rank}(\mathfrak{Q}^{(j)}) = 2d - 2, \tag{20b}$$

Output: The MQQ $q(\mathbf{x}, \mathbf{y})$.

An important feature of the MQQs used, as it can be seen from Algorithm 3, is their bilinear nature, *i.e.*, the variables from the two operands are only mixed with each other quadratically, and there is no quadratic mixing of variables from one operand. This property makes the private key smaller, in particular, the bilinear MQQs only require 81 bytes of memory. Further, it also enables fast signing even in constrained environments by solving systems of linear equations.

The Algorithm used for computing the inverse of $\mathcal{F}$ is given in Algorithm 4.

Algorithm 4 ComputeInverse$\mathcal{F}$

Input: A vector $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}_2^n$, where n is a multiple of 8.

1. Represent the vector $\mathbf{y}$ as a string $Y = Y_1 Y_2 \dots Y_k$, where $k = \frac{n}{8}$, and $Y_i \in \mathbb{F}_2^8$ for every $i \in \{1, \dots, k\}$.
2. Compute the string $X = X_1 X_2 \dots X_k$, where

$$X_i = \begin{cases} Y_1, & \text{if } i = 1 \\ \text{the solution of } Y_i = q(X_{i-1}, X_i), & \text{if } i = 2, 4, \dots, k \\ \text{the solution of } Y_i = q(X_i, X_{i-1}), & \text{if } i = 3, 5, \dots, k-1 \end{cases}$$

3. Represent X as a vector $\mathbf{x} \in \mathbb{F}_2^n$.

Output: The vector $\mathbf{x}$.

In [125], the authors propose a natural interpretation of the private key, in particular the secret quasigroup q. Instead of storing q, the holder of the private key can store the isotopic $q_0(\mathbf{x}, \mathbf{y}) = \mathbf{U}(\mathbf{A}_1^{-1} \cdot \mathbf{x}) \cdot \mathbf{y} + \mathbf{x} + \mathbf{c_0}$, and the invertible $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}$. In this case, the bilinear quasigroup can be stored in 50.5 bytes, rather than 81 bytes using the naive approach from the original paper.

In MQQ-SIG, as much as half of the public polynomials are removed in order to defend from Gröbner bases attacks. While this is not a problem for a signature scheme, an encryption scheme can not be build with such a heavy use of the minus modifier. Therefore, in the subsequent proposal MQQ-ENC for an encryption scheme [59], the authors propose to use left quasigroups instead.

Let (Q, q) be a left quasigroup of order p^{kd}. We say that (Q, q) is a Left Multivariate Quadratic Quasigroup (LMQQ) if q can be represented as a function $q = (q^{(1)}, q^{(2)}, \dots, q^{(d)}) : \mathbb{F}_{p^k}^{2d} \to \mathbb{F}_{p^k}^d$, where for every $s = 1, \dots, d$, $q^{(s)}$ is a quadratic polynomial over $\mathbb{F}_{p^k}$. For simplicity, we take that $Q = \mathbb{F}_{p^k}^d$.

The following theorem provides sufficient conditions for a multivariate mapping to define a quasigroup.

Theorem 10. *The function* $q_0 = (q^{(1)}, q^{(2)}, \dots, q^{(d)}) : \mathbb{F}_{p^k}^{2d} \to \mathbb{F}_{p^k}^{d}$ *such that for every* $s = 1, \dots, d$*, the component* $q_0^{(s)}$ *is of the form*

$$\begin{aligned} q_0^{(s)}(x_1, \dots, x_d, y_1, \dots, y_d) &= p^{(s)}(y_s) + \sum_{1 \leqslant i,j \leqslant d} \alpha_{i,j}^{(s)} x_i x_j + \sum_{s < i,j \leqslant d} \beta_{i,j}^{(s)} y_i y_j + \\ + \sum_{1 \leqslant i \leqslant d, s < j \leqslant d} \gamma_{i,j}^{(s)} x_i y_j &+ \sum_{1 \leqslant i \leqslant d} \delta_i^{(s)} x_i + \sum_{s < i \leqslant d} \epsilon_i^{(s)} y_i + \eta^{(s)}, \end{aligned} \tag{21}$$

where $p^{(s)}(x) = ax$*,* $a \neq 0$*, or* $p^{(s)}(x) = ax^2$*,* $a \neq 0$*,* $p = 2$*, defines an LMQQ* $(\mathbb{F}_{p^k}^{d}, q_0)$ *of order* p^{kd}*.*

For the purpose of MQQ-ENC, and using the form from Theorem 10 the LMQQs can be constructed using Algorithm 5.

Algorithm 5 CreateLMQQ(d, p, k)

Input $d, p, k \in \mathbb{N}$, where p is prime.

1. For all $s \in \{1, \dots, d\}$ generate at random from $\mathbb{F}_{p^k}$ the coefficients:
   - $\alpha_{i,j}^{(s)}$, $\delta_i^{(s)}$, for all i, j, $1 \leqslant i, j \leqslant d$, and $\beta_{i,j}^{(s)}$, $\epsilon_i^{(s)}$, for all i, j, $s < i, j \leqslant d$,
   - $\gamma_{i,j}^{(s)}$, for all i, j, $1 \leqslant i \leqslant d, s < j \leqslant d$, and the constant term $\eta^{(s)}$.
2. For all $s \in \{1, \dots, d\}$
   - If $p = 2$ generate at random a bit $r \in \mathbb{F}_2$, otherwise set $r = 0$.
   - Choose at random $a^{(s)} \in \mathbb{F}_{p^k} \setminus \{0\}$. If $r = 0$ set $p^{(s)} = a^{(s)} x_s$, otherwise set $p^{(s)} = a^{(s)} x_s^2$.
3. For all $s \in \{1, \dots, d\}$ construct $q_0^{(s)}(\mathbf{x}, \mathbf{y})$ given by (21), and the LMQQ $q_0 = (q_0^{(1)}, q_0^{(2)}, \dots, q_0^{(d)})$.
4. Generate at random over $\mathbb{F}_{p^k}$, $d \times d$ nonsingular matrices $\mathbf{D}, \mathbf{D_y}$, and vectors $\mathbf{c}, \mathbf{c_y}$ of dimension d.

Output the quintet $(q_0, \mathbf{D}^{-1}, \mathbf{D_y}^{-1}, \mathbf{c}, \mathbf{c_y})$ and the LMQQ of order p^{kd}:

$$q(\mathbf{x}, \mathbf{y}) = \mathbf{D} \cdot q_0(\mathbf{x}, \mathbf{D_y} \cdot \mathbf{y} + \mathbf{c_y}) + \mathbf{c}.$$

As in MQQ-SIG, an efficient algorithm for inverting the central mapping is based on efficiently computing the parastrophe $q_\backslash$ of q at a given point. In other words, the problem is reduced to to solving the system of d quadratic equations in d variables $y_1, y_2, \dots, y_d$ over $\mathbb{F}_{p^k}$

$$q(\mathbf{u}, \mathbf{y}) = \mathbf{v} \tag{22}$$

Even though this is a non trivial problem in general, the specific structure of the LMQQs in use, allows this system to be solved in polynomial time, very efficiently and fast.

The MQQ-ENC cryptosystem is defined as a triplet of probabilistic algorithms MQQ-ENC= $(\mathcal{G}^{MQQ}, \mathcal{E}^{MQQ}, \mathcal{D}^{MQQ})$, associated to a message space $\mathit{Mspace}(nk) = \{0,1\}^{nk/2}$, and random coins $\mathit{Coins}(nk) = \{0,1\}^{nk/4}$, given by Algorithms 6, 7 and 8 as follows.

Algorithm 6 Key-Generation algorithm $\mathcal{G}^{MQQ}$

Input: 1^{nk},

1. Run **CreateST**$(n, 2, k, r_1, r_2, rem)$ to obtain $(\sigma_1, \sigma_2, \mathbf{M}_0, (a_i^{(1)})_{r_1+1}, (a_i^{(2)})_{r_2+1})$ and the affine mappings $\mathcal{S}$ and $\mathcal{T}$.
2. Run **CreateLMQQ**$(8, 2, k)$ to obtain $(q_0, \mathbf{D}, \mathbf{D}_\mathbf{y}, \mathbf{c}, \mathbf{c}_\mathbf{y})$ and q.
3. Represent the vector $(x_1, x_2, \dots, x_n)$ of variables over $\mathbb{F}_{2^k}$ as a vector $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{n/8})$ of variables over $\mathbb{F}_{2^k}^8$, where $\mathbf{x}_i = (x_{8i-7}, x_{8i-6}, \dots, x_{8i})$.
4. Define a mapping $\mathcal{F} : \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$ (a quasigroup string transformation) by:
$$\begin{aligned} (y_1, \dots, y_n) &= \mathcal{F}(x_1, \dots, x_n) \Leftrightarrow \\ (\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_{n/8}) &= (q(11\dots1, \mathbf{x}_1), q(\mathbf{x}_1, \mathbf{x}_2), \dots, q(\mathbf{x}_{n/8-1}, \mathbf{x}_{n/8})) \end{aligned} \tag{23}$$
5. Construct the mapping $P_{full} : \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$ as $P_{full} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$. We use the notation $\mathcal{P}_{full} = (p_1, p_2, \dots, p_n)$, where $p_i(x_1, \dots, x_n)$, $1 \leqslant i \leqslant n$.
6. The vector of polynomials $\mathcal{P} : \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^{n-rem}$ is obtained by removing the last rem coordinates from $\mathcal{P}_{full}$, i.e., $\mathcal{P} = (p_1, p_2, \dots, p_{n-rem})$.
7. Choose a universal hash function $H : \{0,1\}^{3nk/4} \to \{0,1\}^{nk/4}$.
8. Set $\mathsf{pk} = (\mathcal{P}, H)$,
   and $\mathsf{sk} = (\sigma_1, \sigma_2, \mathbf{M}_0, (a_i^{(1)})_{r_1+1}, (a_i^{(2)})_{r_2+1}, q_0, \mathbf{D}^{-1}, \mathbf{D}_\mathbf{y}^{-1}, \mathbf{c}, \mathbf{c}_\mathbf{y})$.

Output: Public private key pair $(\mathsf{pk}, \mathsf{sk})$.

Algorithm 7 Encryption algorithm $\mathcal{E}^{MQQ}$

```
Input: Public key $\mathsf{pk} = (\mathcal{P}, H)$ and plaintext message $m = \{m_1, m_2, \ldots, m_{n/2}\} \in Mspace(nk)$,
    1. Generate a random string $r = \{r_1, r_2, \ldots, r_{n/4}\} \in Coins(nk)$.
    2. Evaluate $(h_1, \ldots, h_{n/4}) = H(m, r) = H(m_1, \ldots, m_{n/2}, r_1, \ldots, r_{n/4})$.
    3. Evaluate $\mathcal{P}(m, r, H(m, r)) = \mathcal{P}(m_1, \ldots, m_{n/2}, r_1, \ldots, r_{n/4}, h_1, \ldots, h_{n/4})$.
Output: Ciphertext $c = \mathcal{P}(m, r, H(m, r))$.
```

Algorithm 8 Decryption algorithm $\mathcal{D}^{MQQ}$

```
Input: Private key $\mathsf{sk}=(\sigma_1, \sigma_2, \mathbf{M}_0, (a_i^{(1)})_{r_1+1}, (a_i^{(2)})_{r_2+1}, q_0, \mathbf{D}^{-1}, \mathbf{D}_\mathbf{y}^{-1}, \mathbf{c}, \mathbf{c}_\mathbf{y})$
and cipher $c=(c_1, \ldots, c_{n-rem}) \in \mathbb{F}_{2^k}^{n-rem}$,
For all $(c_{n-rem+1}, c_{n-rem+2}, \ldots, c_n) \in \mathbb{F}_{2^k}^{rem}$ do
    1. Evaluate $(m'_1, m'_2, \ldots, m'_n) = \mathcal{S}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{T}^{-1}(c_1, c_2, \ldots, c_n)$, where $\mathcal{F}^{-1}$ is evaluated by:
           $(u_1, u_2, \ldots, u_n) = \mathcal{F}^{-1}(v_1, v_2, \ldots, v_n) \Leftrightarrow$
           $(\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{n/8}) = (q_\backslash(\mathbf{u}_0,\mathbf{v}_1), q_\backslash(\mathbf{u}_1,\mathbf{v}_2), q_\backslash(\mathbf{u}_2,\mathbf{v}_3), \ldots, q_\backslash(\mathbf{u}_{n/8-1}, \mathbf{v}_{n/8}))$ (24)
       Here, $\mathbf{u}_0 = (11\ldots1)$, and for every $i \in \{0, \ldots, n/8-1\}$, $\mathbf{u}_{i+1} = q_\backslash(\mathbf{u}_i, \mathbf{v}_{i+1})$ is evaluated by running Algorithm $\mathbf{Q}_\backslash(\mathbf{u}_i, \mathbf{v}_{i+1}, 8, 2, k, q_0, \mathbf{D}^{-1}, \mathbf{D}_\mathbf{y}^{-1}, \mathbf{c}, \mathbf{c}_\mathbf{y})$.
       The vector $(u_1, \ldots, u_n)$ over $\mathbb{F}_{2^k}$ is represented as a vector $(\mathbf{u}_1, \ldots, \mathbf{u}_{n/8})$ over $\mathbb{F}_{2^k}^8$, where $\mathbf{u}_i = (u_{8i-7}, u_{8i-6}, \ldots, u_{8i})$. Analogously, the same is done for the vector $(v_1, v_2, \ldots, v_n)$.
    2. If $H(m'_1, m'_2, \ldots, m'_{3n/4}) = (m'_{3n/4+1}, m'_{3n/4+2}, \ldots, m'_n)$ then break;
End for;
Output: Plaintext $m'$ or $\perp$ if the above test failed for all $(c_{n-rem+1}, \ldots, c_n) \in \mathbb{F}_{2^k}^{rem}$.
```

5. Conclusion

The aim of this article was to present how quasigroups can be exploit for building suitable cryptographic primitives. There were presented constructions of several types of quasigroups and several types of quasigroups string transformations. Designs with these types of quasigroups and transformations were illustrated in constructions of S-boxes, block cipher, stream ciphers, pseudo random number generators, hash functions and public key security and signatures. There are also other applications of quasigroups in cryptography (MAC, Identity encryption schemes, Authenticated encryption, ...) but we found that what we had presented is quite enough to conclude that, slowly but surely, quasigroups are taking there role in cryptography. We emphasize that there are several other survey papers where different applications of quasigroups in cryptography are discussed as well: [132], [60], [133], [134], [135], [108], etc.

We have to notice that cryptographic properties are not discussed in this paper. The efficiency and security of the crypto products based on quasigroup is an open research problem for cryptographers and cryptanalysts. There are many broken designs based on quasigroups, but also there are some with perfect crypto properties.

At the end, one can notice that the presented results were mostly from Macedonian quasigroupists and cryptographers; that was done intentionally.

Acknowledgment. The author is grateful to Aleksandra Mileva, Vesna Dimitrova, Simona Samardjiska, Aleksandra Popovska-Mitrovikj and Hristina Mihajloska for their support and help in writing of this article.

References

[1] **R. Ahlavat, K. Gupta and S.K. Pal**, *Fast generation of multivariate quadratic quasigroups for cryptographic applications*, IMA Conference on Mathematics in Defence, Farnborough, UK, 2009, http://www.ima.org.uk/_db_documents/defence09_ahlawat_v2.pdf.

[2] **V. Bakeva and V. Dimitrova**, *Some probabilistic properties of quasigroup processed strings useful for cryptanalysis*, Proc. of ICT Innovation 2010, Springer Berlin Heidelberg, 2010, pp. 61–70.

[3] **V. Bakeva, V. Dimitrova and A. Popovska-Mitrovikj**, *Parastrophic quasigrouop string processing*, Proc. of the 8^{th} Conf. Informatics and Information Technology, Bitola, Macedonia, 2011, 19–21.

[4] **V. Bakeva and N. Ilievska**, *A probabilistic model of error-detecting codes based on quasigroups*, Quasigroups and Related Systems **17** (2009), 151–164.

[5] **V. Bakeva, A. Popovska-Mitrovikj and V. Dimitrova**, *Resistance of statistical attacks of parastrophic quasigroup transformation*, arXiv: 1404.0781v1.

[6] **S. Bakhtiari, R. Safavi-Naini and J. Pieprzyk**, *A message authentication code based on Latin square*, Proc. of ACISP 97, LNCS **1270** (1997), 194–203.

[7] **M. Battey and A. Parakh**, *A quasigroup based random number generator for resource constrained environments*, IACR Cryptology ePrint Archive, Report 2012: 471.

[8] **V.D. Belousov**, *Foundations of the theory of quasigroups and loops*, (Russian), Nauka, Moscow, 1967.

[9] **V.D. Belousov**, *n-ary quasigroups*, (Russian), Ştiinţa, Kishinev, 1972.

[10] **G.B. Belyavskaya**, *Recursively r-differentiable quasigroups within S-systems and MDS-codes*, Quasigroups and Related Systems **20** (2012), 157–168.

[11] **G.B. Belyavskaya, V.I. Izbash and G.L. Mullen**, *Check character systems using quasigroups: II*, Designs, Codes and Cryptography **37** (2005), 405–419.

[12] **G.B. Belyavskaya, V.I. Izbash and V.A. Shcherbacov**, *Check character systems over quasigroups and loops*, Quasigroups and Related Systems **10** (2003), 1–28.

[13] **D.J. Bernstein and T. Lange (eds.)**, eBACS: ECRYPT Benchmarking of Cryptographic Systems, 2014.

[14] **A. Bogdanov, L.R. Knudsen, G. Le, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin and C. Vikkelsoe**, *PRESENT: An ultra-lightweight block cipher*, Proc. of CHES 2007, Springer-Verlag, pp. 450–466.

[15] **G. Carter, E. Dawson and L. Nielsen**, *DESV: A Latin square variation of DES*, Proc. of the Workshop on Selected Areas in Cryptography, Ottawa, Canada, 1995, pp. 144–158.

[16] **S. Chakrabarti, S.K. Pall and G. Gangopadhyay**, *An improved 3-quasigroup based encrytion scheme*, Proc. of ICT Innovations 2012, http://ictinnovations.org/2012/htmls/papers/WebProceedings2012.pdf, 2012, pp. 173–184.

[17] **Y. Chen, S.J. Knapskog and D. Gligoroski**, *Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity*, Inscrypt, 6th International Conference on Information Security and Cryptology. Science Press of China, 2010.

[18] **N. Courtois, A. Klimov, J. Patarin and A. Shamir**, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, LNCS **1807** (2000), 392–407.

[19] **P. Csőrgő and V. Shcherbacov**, *On some quasigroup cryptographical primitives*, arXiv: 1110.6591v1.

[20] **J. Daemen**, *Cipher and hash function design. Strategies based on linear and differential cryptanalysis*, Doctoral dissertation. Katholieke Universiteit Leuven, 1995.

[21] **H.M. Damm**, *Totally anti-symmetric quasigroups for all orders $n \neq 2, 6$*, Discrete Math. **307** (2007), 715–729.

[22] **H.M. Damm**, *Half quasigroups and generalized quasigroup orthogonality*, Discrete Math. **311** (2011), 145–153.

[23] **F. Dawson, D. Donowan and A. Offer**, *Quasigroups, isotopisms and authentication schemes*, Australasian J. Combin. **13** (1996), 75–88.

[24] **J. Dénes and A.D. Keedwell**, *Latin squares and their applications*, Akadémiai Kiado, Budapest, 1974.

[25] **J. Dénes and A.D. Keedwell (Eds.)**, *Latin squares: New developments in the theory and applications*, Annals Discr. Math. **46**, Elsevier, 1991.

[26] **J. Dénes and A.D. Keedwell**, *A new authentication scheme based on Latin squares*, Discrete Math. **106/107** (1992), 157–161.

[27] **J. Dénes and A.D. Keedwell**, *Some applications of non-associative algebraic systems in cryptology*, Pure Math. Appl. **12** (2001), 147–195.

[28] **M. Dichtl**, *Bad and good ways of post-processing biased physical random numbers*, LNCS **4593** (2007), 137–152.

[29] **M. Dichtl and P. Bőffgen**, *Breaking another quasigroup-based cryptographic scheme*, Cryptology ePrint Archive, Report 2012: 661.

[30] http://stat.fsu.edu/pub/diehard/, http://en.wikipedia.org/wiki/Diehard_tests

[31] **V. Dimitrova**, *Quasigroup processed strings, their Boolean presentation and application in cryptography and coding theory*, Doctoral dissertation. University Sts. Cyril and Methodius, Skopje, 2010.

[32] **V. Dimitrova, V. Bakeva, A. Popovska-Mitrovikj and A. Krapež**, *Cryptographic properties of parastrophic quasigroup transformation*, Advances in Intelligent Systems and Computing - ICT Innovations 2012, Springer, 2013, pp. 235–243.

[33] **V. Dimitrova and S. Markovski**, *On Quasigroup pseudo random sequence generators*, Proc. of the 1st Balkan Confer. in Informatics, Thessaloniki, Greece, 2004, pp. 235–243.

[34] **V. Dimitrova and S. Markovski**, *Classification of quasigroups by image patterns*, Proc. of the Fifth International Confer. for Informatics and Information Technology, Bitola, Macedonia, 2007, pp. 152–160.

[35] **H. Dobbertin**, *One-to-one highly nonlinear power functions on* $GF(2n)$, Applicable Algebra in Engineering, Communication and Computing **9** (1998), 139–152.

[36] **A. Drapal**, *Hamming distances of groups and quasigroups*, Discrete Math. **235** (2001), 189–197.

[37] **J. Dvorsky, E. Ochodkova and V. Snašel**, *Hash function based on quasigroups*, (Czech), Proc. of Mikulášska kryptobesídká, Praha, 2001, pp. 27–36.

[38] **J. Dvorsky, E. Ochodkova and V. Snašel**, *Hash function based on large quasigroups*, (Czech), Proc. of Velikonocní i kryptologie, Brno, 2002, pp. 1–8.

[39] **J. Dvorsky, E. Ochodkova and V. Snašel**, *Generation of large quasigroups: an application in cryptography*, Proc. of AAA (Arbeitstagung Allgemeine), 2002.

[40] **J.C. Faugère, R.S. Ødegård, L. Perret and D. Gligoroski**, *Analysis of the MQQ Public Key Cryptosystem*, LNCS **6467**, 169–183.

[41] **D. Gligoroski**, *Stream cipher based on quasigroup string transformations in* Z_p^*, Contributions, Sec. Math. Tech. Sci., MANU, 2004.

[42] **D. Gligoroski**, *Candidate one-way functions and one-way permutations based on quasigroup string transformations*, IACR Cryptology ePrint Archive, Report 2005: 352.

[43] **D. Gligoroski, S. Andova and S.J. Knapskog**, *On the importance of the key separation principle for different modes of operation*, LNCS **4991** (2008), 404–418.

[44] **D. Gligoroski, V. Dimitrova and S. Markovski**, *Quasigroups as Boolean functions, their equation systems and Groebner bases*, In M. Sala, T. Mora, L. Perret, S. Sakata, C. Traverso (Eds.) Groebner Bases, Coding, and Cryptography, Springer Berlin, 2009.

[45] **D. Gligoroski, S.J. Knapskog**, *Adding MAC functionality to Edon80*, International J. Computer Science and Network Security **7** (2007), 194–204.

[46] **D. Gligoroski, S.J. Knapskog**, *Edon-R*$(256, 384, 512)$*-an efficient implementation of Edon-R family of cryptographic hash functions*, Comment. Math. Univ. Carolin. **49** (2008), 219–239.

[47] **D. Gligoroski, S. Markovski and V. Bakeva**, *On infinite class of strongly collision resistant hash functions "Edon-F" with variable length of output*, Proc. of 1st International Confer. on Mathematics and Informatics for Industry, Thessaloniki, 2003, pp. 302–308.

[48] **D. Gligoroski, S. Markovski and S.J. Knapskog**, *A fix of the* $MD4$ *family of hash functions – quasigroup fold*, NIST Cryptographic Hash Workshop, Gaithersburg, Maryland, USA, http://csrc.nist.gov/groups/ST/hash/documents/Gligoroski_MD4Fix.pdf, 2005.

[49] **D. Gligoroski, S. Markovski and S.J. Knapskog**, *A secure hash algorithm with only* 8 *folded* $SHA-1$ *steps*, Intern. J. Computer Science and Network **6(10)** (2006), 194–205.

[50] **D. Gligoroski, S. Markovski and S.J. Knapskog**, *On periods of Edon-*$(2m, 2k)$ *family of stream ciphers*, SASC 2006 Conference.

[51] **D. Gligoroski, S. Markovski and S.J. Knapskog**, *Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups*, Proc. Amer. Confer. Appl. Math., Harvard, USA, 2008, pp. 44–49.

[52] **D. Gligoroski, S. Markovski and S.J. Knapskog**, *A pblic key block cipher based on multivariate quadratic quasigrops*, IACR Cryptology ePrint Archive, Report 2008: 320.

[53] **D. Gligoroski, S. Markovski and S.J. Knapskog**, *The stream cipher Edon80*, LNCS **4986** (2008), 152–169.

[54] **D. Gligoroski, S. Markovski and Lj. Kocarev**, *Edon-R, an infinite family of cryptographic hash functions*, International J. Network Security **8** (2006), 293–300.

[55] **D. Gligoroski, S. Markovski and Lj. Kocarev**, *Error-correcting codes based on quasigroups*, Proc. of 16th International Confer. on Computer Communications and Networks - ICCCN 2007, Honolulu, 2007, pp. 165–172.

[56] **D. Gligorovski and R.S. Ødegård**, *On the complexity of Khovratovich et. al. preimage attack on EDON-R*, IACR Cryptology ePrint Archive, Report 2009: 120.

[57] **D. Gligorovski, R.S. Ødegård, R.E. Jensen, L. Perret, J.C. Faugère, S.J. Knapskog and S. Markovski**, *MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme*, LNCS **7222** (2011), 184–203.

[58] **D. Gligorovski, R.S. Ødegård, M. Mihova, S.J. Knapskog, Lj. Kocarev, A. Drapal and V. Klima**, *Cryptographic hash function EDON-R*, from http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/Edon-RUpdate.zip, 2008.

[59] **D. Gligoroski and S. Samardjiska**, *The multivariate probabilistic encryption scheme MQQ-ENC.* IACR Cryptology ePrint Archive, Report 2012: 328.

[60] **M.M. Glukhov**, *On application of quasigroups in cryptology*, (Russian). Appl. Disc. Math. **2** (2008), 28–32.

[61] **S. Golomb, L. Welch and J. Dênes**, *Encryption system based on crossed inverse quasigroups*, US patent, WO0191368, 2001.

[62] **M. Hell and T. Johansson**, *A key recovery attack on Edon80*, LNCS **4833** (2007), 568–581.

[63] **Y. Hu**, *Security analysis of cryptosystem based on quasigroups*, Proc. of IEEE Intern. Conf. on Progress in Informatics and Computing, 2010, pp. 431–435.

[64] **L. Ji, X. Liangyu and G. Xu**, *Collision attack on NaSHA*-512, IACR Cryptology ePrint Archive, Report 2008: 519, 2008.

[65] **D.M. Johnson, A.L. Dulmage and N.S. Mendelsohn**, *Orthomorphisms of groups and orthogonal latin squares I*, Canadian J. Math. **13** (1961), 356–372.

[66] **A.D. Keedwell**, *Crossed inverse quasigroups with long inverse cycles and applications to cryptography*, Australasian J. Combin. **20** (1999), 241–250.

[67] **A.D. Keedwell and V.A. Shcherbacov**, *Construction and properties of* (r, s, t)*-inverse quasigroups. I*, Discrete Math. **266** (2003), 275–291.

[68] **D. Khovratovich, I. Nikolic and R.P. Weinmann**, *Cryptanalysis of Edon-R*, http://ehash.iaik.tugraz.at/uploads/7/74/Edon.pdf, 2008.

[69] **V. Klima**, *Multicollisions of EDON-R hash function and other observations*, http://cryptography.hyperlink.cz/BMW/EDONR_analysis_vk.pdf, 2008.

[70] **C. Kościelny**, *A method of constructing quasigroup-based stream-ciphers*, Appl. Math. Computer Sci. **6** (1996), 109–121.

[71] **C. Kościelny**, *Generating quasigroups for cryptographic applications*, Intern. J. Appl. Math. Computer Sci. **12** (2002), 559–569.

[72] **C. Kościelny and G.L. Mullen**, *A quasigroup-based public-key cryptosystem*, Intern. J. Appl. Math. Computer Sci. **9** (1999), 955–963.

[73] **A. Krapež**, *An application of quasigroup in cryptology*, Math. Macedonica **8** (2010), 47–52.

[74] **A. Krapež**, *Cryptographically suitable quasigroups via functional equations*, Advances in Intelligent Systems and Computing - ICT Innovations 2012, Springer Berlin Heidelberg, 2013, pp. 265–273.

[75] **C.F. Laywine, and G.L. Mullen**, *Discrete mathematics using Latin squares*, New York: John Wiley Sons, Inc., 1998.

[76] **G. Leander and V. Poschmann**, *On the classification of* 4 *bit S-boxes*, LNCS **4547** (2007), 159–176.

[77] **G. Leurent**, *Key recovery attack against secret-prefix Edon-R*, IACR Cryptology ePrint Archive, Report 2009: 135.

[78] **Z. Li and D. Li**, *Collision attack on NaSHA*-384/512, IACR Cryptology ePrint Archive, Report 2009: 026.

[79] **R.J.M. Maia, P.S.L. M. Barreto and B.T. de Oliveira**, *Implementation of multivariate quadratic quasigroup for Wireless Sensor Network*, LNCS **6480** (2010), 64–78.

[80] **S. Markovski**, *Quasigroup string processing and applications in cryptography*, Proc. 1-st Inter. Conf. Mathematics and Informatics for industry MII 2003, 14-16 April, Thessaloniki, 2003, pp. 278–290.

[81] **S. Markovski and V. Bakeva**, *Quasigroup string processing: Part* 4, Contributions, Sec. math. Tech.Sci., MANU, **22** (2001).

[82] **S. Markovski, V. Dimitrova and S. Samardziska**, *Identities sieves for quasigroups*, Quasigroups and Related Systems **18** (2010), 149–164.

[83] **S. Markovski, V. Dimitrova, Z. Trajcheska, M. Petkovska, M. Kostadinoski and D. Buhov**, *Block cipher defined by matrix presentation of quasigroups*, Proc. of the 11th Confer. on Informatics and Information Technology, CIIT 2014, Bitola (to appear).

[84] **S. Markovski, D. Gligoroski and S. Andova**, *Using quasigroups for one-one secure encoding*, Proc. of VIII Conf. Logic and Computer Science LIRA97, Novi Sad, Serbia, 1997, pp. 157–162.

[85] **S. Markovski, D. Gligoroski and V. Bakeva**, *Quasigroup string processing - Part* 1, Contributions, Sec. Math. Tech. Sci., MANU **20** (1999), 13–28.

[86] **S. Markovski, D. Gligoroski and V. Bakeva**, *Quasigroup and hash functions*, Proc. of the 6th ICDMA, Bansko, 2001, pp. 43–50.

[87] **S. Markovski, D. Gligoroski and Lj. Kocarev**, *Unbiased random sequences from quasigroup string transformations*, LNCS **3557** (2005), 163–180.

[88] **S. Markovski, D. Gligoroski and B. Stojčevska**, *Secure two-way on-line communication by using quasigroup enciphering with almost public key*, Novi Sad J. Math. **30(2)** (2000), 43–49.

[89] **S. Markovski and V. Kusakatov**, *Quasigroup string processing - Part* 2, Contributions, Sec. Math. Tech. Sci., MANU **21** (2000), 15–32.

[90] **S. Markovski and V. Kusakatov**, *Quasigroup string processing - Part* 3, Contributions, Sec. Math. Tech. Sci., MANU **23-24** (2002-2003), 7–27.

[91] **S. Markovski and A. Mileva**, *Generating huge quasigroups from small nonlinear bijections via extended Feistel function*, Quasigroups and Related Systems **17** (2009), 91–106.

[92] **S. Markovski and A. Mileva**, *NaSHA*, Submission to NIST, First Round SHA-3 Candidate, http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/NaSHAUpdate.zip, 2008.

[93] **S. Markovski, A. Mileva, V. Dimitrova and D. Gligoroski**, *On a conditional collision attack on NaSHA*-512, IACR Cryptology ePrint Archive, Report 2009: 034.

[94] **S. Markovski, S. Samardziska, D. Gligoroski and S.J. Knapskog**, *Multivariate Trapdoor functions based on multivariate left quasigroups and left polynomial quasigroups*, Proc. of the Second Intern. Confer. on Symbolic Computation and Cryptography, Royal Holloway, University of London, Egham, UK, 2010, pp. 237–251.

[95] **S. Markovski, Z. Šunić and D. Gligoroski**, *Polynomial functions on the units of* $\mathbb{Z}_{2^n}$, Quasigroups and Related System **18** (2010), 11–34.

[96] **S.I. Marnas, L. Angelis and G.L. Bleris**, *All-Or-Nothing Transform using quasigroups*, Proc. 1st Balkan Conference in Informatics, Thessaloniki, 2004, pp. 183–191.

[97] **M. Matsumoto, M. Saito, T. Nishimura and M. Hagita**, *A fast stream cipher with huge state space and quasigroup filter for software*, LNCS **4876** (2007), 246–263.

[98] **M. Matsumoto, M. Saito, T. Nishimura and M. Hagita**, *CryptMT*3 *stream cipher*, LNCS **4986** (2007), 7–19.

[99] **T. Matsumoto and H. Imai**, *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, LNCS **330** (1988), 419–453.

[100] **B.D. McKay, A. Meynert and W. Myrvold**, *Small Latin squares, quasigroups and loops*, J. Combinatorial Designs **15** (2007), 98–119.

[101] **A.J. Menezes, P.C. van Oorschot and S.A. Vanstone**, *Handbook of Applied Cryptography*, CRC Press, 2001.

[102] **K.A. Meyer**, *A new message authentication code based on the non-associativity of quasigroups*, Doctoral dissertation, Iowa State University, 2006.

[103] **H. Mihajloska and D. Gligoroski**, *Construction of optimal* 4*-bit S-boxes by quasigroups of order* 4, Proc. of SECURWARE 2012, Rome, Italy, 2012, pp. 163–168.

[104] **H. Mihajloska, T. Yalcin and D. Gligoroski**, *How lightweight is the hardware implementation of quasigroup S-boxes*, Advances in Intelligent Systems and Computing - ICT Innovations 2012 207 , Springer Berlin Heidelberg, 2013, pp. 121–127.

[105] **M. Mihova, M. Siljanoska and S. Markovski**, *Tracing bit differences in strings transformed by linear quasigroups of order* 4, Proc. of the 9th Confer. for Informatics and Information Technology, Bitola, Macedonia, 2012, pp. 229–233.

[106] **A. Mileva**, *Cryptographic primitives with quasigroup transformations*, Doctoral dissertation, University Sts. Cyril and Methodius, Skopje, 2010.

[107] **A. Mileva**, *Analysis of some quasigroup transformations as Boolean functions*, Mathematica Balkanica **3-4** (2012).

[108] **A. Mileva**, *New developments in quasigroup-based cryptography*, Multidisciplinary Perspectives in Cryptology and Information Security. IGI-Global, 2014, pp. 286–317.

[109] **A. Mileva and S. Markovski**, *Correlation matrices and prop ratio tables for quasigroups of order* 4, Proc. of the 6th Intern. Confer. for Informatics and Information Technology, Ohrid, Macedonia, 2008, pp. 17–22.

[110] **A. Mileva and S. Markovski**, *Quasigroups string transformations and hash function design*, ICT Innovations 2009, Springer Berlin Heidelberg, 2010, pp. 367–376.

[111] **A. Mileva and S. Markovski**, *Shapeless quasigroups derived by Feistel orthomorphisms*, Glasnik Matematicki **47** (2012), 333–349.

[112] **A. Mileva and S. Markovski**, *Quasigroup representation of some Feistel and Generalized Feistel Ciphers*, Advances in Intelligent Systems and Computing - ICT Innovations 2012, 207, Springer, 2013, pp. 161–171.

[113] **M.S. Mohamed, J. Ding, J. Buchmann and F. Werner**, *Algebraic attack on the MQQ public key cryptosystem*, Proc. of 8th Intern. Confer. on Cryptology and Network Security, Springer Berlin Heidelberg, 2009, pp. 391–401.

[114] **I. Nikolić and D. Khovratovich**, *Free-start attacks on NaSHA*, http://ehash.iaik.tugraz.at/uploads/3/33/Free-start_attacks_on_Nasha.pdf, 2008.

[115] **P. Novotney and N. Ferguson**, *Detectable correlation in Edon-R.* IACR Cryptology ePrint Archive 2009: 378.

[116] **J. Patarin**, *Hidden fields equations* (HFE) *and isomorphisms of polynomials* (IP)*: two new families of asymmetric algorithms*, LNCS **1440** (1996), 33–48.

[117] **A. Petrescu**, *n-quasigroup cryptographic primitives: stream ciphers*, Studia Univ. Babes Bolyai, Informatica **55(2)** (2010), 27–34.

[118] **H.O. Pflugfelder**, *Quasigroups and Loops: Introduction.* Heldermann Verlag, Berlin, 1991.

[119] **A. Popovska-Mitrovikj, V. Bakeva and S. Markovski**, *On random error correcting codes based on quasigroups*, Quasigroups and Related Systems **19** (2011), 301–316.

[120] **R.L. Rivest**, *All-or-nothing encryption and the package transform*, LNCS **1267** (1997), 210–218.

[121] **R.L. Rivest**, *Permutation polynomials modulo* $2w$, Finite Fields and Their Appl. **7** (2001), 287–292

[122] **A. Sade**, *Quasigroups automorphes par le groupe cyclique*, Canadian J. Math. **9** (1957), 321–335.

[123] **S. Samardziska**, *Polynomial n-ary quasigroups of order w*, Master thesis, University Ss. Cyril and Methodius, Skopje, 2009.

[124] **S. Samardziska**, *ID based identification schemes using multivariate left quasigroups*, (submitted).

[125] **S. Samardziska, Y. Chen and D. Gligoroski**, *Algorithms for construction of multivariate quadratic quasigroups* ($MQQs$) *and their parastrophe operations in arbitrary Galois Fields*, J. Inform. Assurance and Security **7(3)** (2012), 164–172.

[126] **S. Samardziska and D. Gligoroski**, *Identity-based identification schemes using left multivariate quasigroups*, NIK-2011, Tapir Akad, Forlag, 2011, pp. 19–30.

[127] **S. Samardziska, S. Markovski and D. Gligoroski**, *Multivariate quasigroups defined by T-functions*, Proc. of the Second Intern. Confer. on Symbolic Computation and Cryptography, University of London, 2010, pp. 117–127.

[128] **D.G. Sarvate and J. Seberry**, *Encryption methods based on combinatorial designs*, Ars Combinatoria **21A** (1986), 237–246.

[129] **M.V.K. Satti**, *Quasi-group based crypto-system*, Master thesis, Louisiana State University, 2007.

[130] **M. Satti and S. Kak**, *Multilevel indexed quasigroup encryption for data and speech*, IEEE Transactions on Broadcasting **55(2)** (2009), 270–281.

[131] **R.H. Schulz**, *A note on check character systems using latin squares*, Discrete Math. **97** (1991), 371–375.

[132] **V.A. Shcherbacov**, *On some known possible applications of quasigroups in cryptology*, http://www.karlin.mff.cuni.cz/ drapal/krypto.pdf, 2003.

[133] **V.A. Shcherbacov**, *Quasigroups in cryptology*, Computer Sci. J. Moldova **17(2)** (2009), 193–228.

[134] **V.A. Shcherbacov**, *Quasigroups in cryptology*, arXiv:1007.3572.

[135] **V.A. Shcherbacov**, *Quasigroup based crypto-algorithms*, arXiv:1201.3016v1.

[136] **V.A. Shcherbacov**, *Quasigroup based hybrid of a code and a cipher*, http://ictinnovations.org/2012/htmls/papers/WebProceedings2012.pdf, p.411–417.

[137] **M. Simjanovska, M. Mihova and S. Markovski**, *Matrix presentation of quasigroups of order* 4, Proc. of the Tenth International Conference CIIT 2013, Bitola, 2013, pp. 192–196.

[138] **I. Slaminková and M. Vojvoda**, *Cryptanalysis of a hash function based on isotopy of quasigroups*, Tatra Mountains Math. Publ. **45** (2010), 137–149.

[139] **J.D.H. Smith**, *An introduction to quasigroups and their representations*, Chapman and Hall/ CRC, 2006.

[140] **V. Snášel, A. Abraham, J. Dvorsky, P. Krőmer and J. Platoš**, *Hash function based on large quasigroups*, LNCS **5544** (2009), 521–529.

[141] **V. Snášel, J. Dvorsky, E. Ochodkova, P. Krőmer, J. Platoš and A. Abraham**, *Evolving quasigroups by genetic algorithms*, Proc. of DATESO 2010, 2010, pp. 108–117.

[142] **D.R. Stinson**, *Cryptography: Theory and practice*, Second edition. Chapman and Hall / CRC, 2002.

[143] **S. Vaudenay**, *On the need for multipermutations: Cryptanalysis of $MD4$ and $SAFER$*, LNCS **1008** (1995), 286–297.

[144] **M. Vojvoda**, *Cryptanalysis of one hash function based on quasigroup*, Tatra Mountains Math. Publ. **29** (2004), 173–181.

[145] **M. Vojvoda, M. Sýs and M. Jókay**, *A note on algebraic properties of quasigroups in Edon80*, SASC 2007, Bochum, Germany, 2007.

[146] **C. Wolf and B. Preneel**, *Taxonomy of public key schemes based on the problem of multivariate quadratic equations*, IACR Cryptology ePrint Archive, Report 2005/077.

[147] **C. Wolf and B. Preneel**, *MQ*-IP: An identity-based identification scheme without number-theoretic assumptions*, ICAR Cryptology ePrint Archive, Report 2010/087.

[148] **Y. Xu**, *A cryptography application of conjugate quasigroups*, Proc. of the Intern. Confer. on Web Information Systems and Mining 2010, vol. II, Sanya, China, 2010, pp. 63–65.

Received May 5, 2015

Faculty of Computer Science and Engineering, Ss “Cyril and Methodius” University, Skopje, Macedonia
E-mail: smile.markovski@gmail.com

Quasigroups and Related Systems **23** (2015), 91 – 128

A guide to self-distributive quasigroups, or latin quandles

David Stanovský

Abstract. We present an overview of the theory of self-distributive quasigroups, both in the two-sided and one-sided cases, and relate the older results to the modern theory of quandles, to which self-distributive quasigroups are a special case. Most attention is paid to the representation results (loop isotopy, linear representation, homogeneous representation), as the main tool to investigate self-distributive quasigroups.

1. Introduction

1.1. The origins of self-distributivity. *Self-distributivity* is such a natural concept: given a binary operation $*$ on a set A, fix one parameter, say the left one, and consider the mappings $L_a(x) = a * x$, called *left translations.* If all such mappings are endomorphisms of the algebraic structure $(A, *)$, the operation is called *left self-distributive* (the prefix self- is usually omitted). Equationally, the property says

$$a * (x * y) = (a * x) * (a * y)$$

for every $a, x, y \in A$, and we see that $*$ distributes over itself.

Self-distributivity was pinpointed already in the late 19th century works of logicians Peirce and Schröder [69, 76], and ever since, it keeps appearing in a natural way throughout mathematics, perhaps most notably in low dimensional topology (knot and braid invariants) [12, 15, 63], in the theory of symmetric spaces [57] and in set theory (Laver's groupoids of elementary embeddings) [15]. Recently, Moskovich expressed an interesting statement on his blog [60] that while associativity caters to the classical world of space and time, distributivity is, perhaps, the setting for the emerging world of information.

Latin squares are one of the classical topics in combinatorics. Algebraically, a latin square is represented by a binary operation, and such algebraic structures are called *quasigroups.* Formally, a binary algebraic structure $(A, *)$ is called a *quasigroup*, if the equations $a * x = b$ and $y * a = b$ have unique solutions x, y, for every $a, b \in A$.

2010 Mathematics Subject Classification: 20N05, 57M27
Keywords: Distributive quasigroup, left distributive quasigroup, latin quandle, commutative Moufang loop, Bruck loop, B-loop, affine representation.
The author was partially supported by the GAČR grant 13-01832S.

It is therefore no surprise that one of the very first algebraic works fully devoted to non-associative algebraic strucures was Burstin and Mayer's 1929 paper *Distributive Gruppen von endlicher Ordnung* [11] about quasigroups that are both left and right distributive. Another earliest treatise on non-associative algebraic structures was [86] by Sushkevich who observed that the proof of Lagrange's theorem (the one in elementary group theory) does not use associativity in full strength and discussed weaker conditions, some related to self-distributivity, that make the proof work. These pioneering works were quickly followed by others, with various motivations. For example, Frink [22] argued that the abstract properties of the mean value are precisely those of medial idempotent quasigroups, and self-distributivity pops up again.

The foundations of the general theory of quasigroups were laid in the 1950s and carved in stone in Bruck's book *A survey of binary systems* [10] (despite the general title, the book leans strongly towards a particular class of *Moufang loops*). Ever since, self-distributive quasigroups and their generalizations played a prominent role in the theory of quasigroups, both in the Western and the Soviet schools [3, 30, 71]. More in the Soviet one, where the dominant driving force was Belousov's program to investigate loop isotopes of various types of quasigroups (see the list of problems at the end of the book [3]). We refer to [72] for a more detailed historical account.

Reflection in euclidean geometry (and elsewhere) is another example of a self-distributive operation: for two points a, b, consider $a * b$ to be the reflection of b over a. The equation $a * x = b$ always has a unique solution, namely, $x = a * b$, but in many cases, reflections do not yield a quasigroup operation (e.g. on a sphere). These observations, and the resulting abstraction of the notion of a reflection, can be attributed to Takasaki and his remote 1942 work [87], but the real advances have been made by Loos and others two decades later [57]. The resulting notions of *kei* (Takasaki), *symmetric spaces* (Loos), or *involutory quandles* in the modern terminology, are axiomatized by three simple algebraic properties: left distributivity, *idempotence* ($a * a = a$ for every a), and the *left involutory law* (the unique solution to $a * x = b$ is $x = a * b$; the property is also called *left symmetry*). The background is described e.g. in [54].

Group conjugation, $a * b = aba^{-1}$ on any subset of a group closed with respect to conjugation, is another prototypical self-distributive operation. This observation is often attributed to Conway and Wraithe [60], who also coined the the term *wrack of a group*, although the idea to represent self-distributive quasigroups by conjugation appeared earlier in [84] by Stein. The conjugation operation is idempotent, left distributive, but again, rarely a quasigroup: only solutions to the equation $a * x = b$ are guaranteed to exist uniquely. Algebraic structures satisfying the three conditions are called *quandles* nowadays. (The word *quandle* has no meaning in English and was entirely made up by Joyce [40]. Many other names have been introduced for quandles, such as *automorphic sets*, *pseudo-symmetric sets*, *left distributive left quasigroups*, etc.)

In early 1980s, Joyce [40] and Matveev [58], independently, picked up the idea of "wracking a group" to extract the essential part of the fundamental group of a knot complement. Unlike the fundamental group, the resulting structure, called the *fundamental quandle* of a knot, is a full invariant of (tame, oriented) knots (up to reverse mirroring) with respect to ambient isotopy. Ever sicne, quandles were successfully used in knot theory to design efficiently computable invariants, see e.g. [12, 21].

The works of Joyce and Matveev put the foundations for the modern theory of quandles, which covers, to some extent, many traditional aspects of self-distributivity as a special case (self-distributive quasigroups, or *latin quandles*, in particular). It is the main purpose of the present paper to overview the classical results on self-distributive quasigroups, and relate them to the results in modern quandle theory.

1.1. Contents of the paper. The paper is organized as a guide to the literature on self-distributive quasigroups, or latin quandles, trying to relate the results of various mathematical schools, which are often fairly hard to find and navigate (at least to me, due to a combination of writing style, terminology mess, and, to most mathematicians, language barrier).

As in most survey tasks, I had to narrow down my focus. The main subject of the paper are representation theorems, serving as the main tool to investigate self-distributive algebraic structures, such as quandles and quasigroups. To see the tools in action, my subjective choice are enumeration results. Other interesting results are cited and commented. I do not claim completeness of my survey, and apologize in advance for eventual ignorance.

In Section 2, we overview the background from the theory of quasigroups, loops and from universal algebra. First, we recall various equational properties of quasigroups and quandles, and define the multiplication groups. Then, various weakenings of the associative and commutative laws are introduced, with a focus towards the classes of commutative Moufang loops and Bruck loops, which are used in the representation theorems. Finally, we talk about isotopy, linear and affine representation, and polynomial equivalence between quasigroups and loops.

Section 3 addresses distributive and trimedial quasigroups. In the first part, we prove the classical affine representation of medial quasigroups (Theorem 3.1), outline Kepka's affine representation of trimedial quasigroups over commutative Moufang loops (Theorem 3.2), and comment upon some special cases and generalizations. Then, in the second part, we present a few consequences of the representation theorem, namely, a classification theorem (Theorem 3.5), enumeration results (Table 1), and we also mention the property called symmetry-by-mediality.

In a short intermezzo, Section 4, we briefly comment on the Cayley-like representation of quandles using conjugation in symmetric groups, and on the construction called the core of a loop. These were some of the first families of examples of left distributive quasigroups which are not right distributive.

In Section 5, we investigate loop isotopes of left distributive quasigroups, so called Belousov-Onoi loops. First, we prove a representation theorem (Theo-

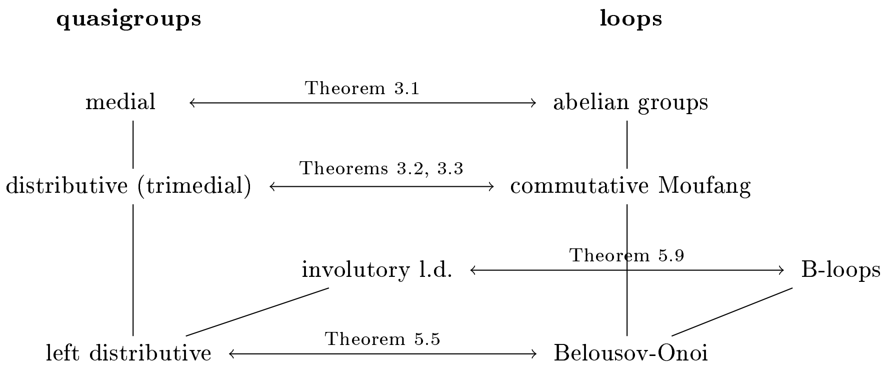


Figure 1: Correspondence between certain classes of quasigroups and loops.

rem 5.5, based on more detailed Propositions 5.2 and 5.4), and then continue with the properties of Belousov-Onoi loops (among others, Propositions 5.8, 5.7, 5.10 and Theorem 5.11). We explain why, at the moment, the correspondence is of limited value for the general theory of left distributive quasigroups. Nevertheless, one special case is important: involutory left distributive quasigroups correspond to the well established class of B-loops (Theorem 5.9). The representation theorems are outlined in Figure 1.

In Section 6, we introduce the homogeneous representation of connected quandles, which is perhaps the strongest tool to study self-distributive quasigroups developed so far. We present several applications to the structure theory, with most attention paid to enumeration results.

Many proofs in our paper are only sketched. In the case of trimedial and distributive quasigroups (Theorems 3.2 and 3.3), we believe that new, shorter, and conceptually cleaner proofs are possible, using modern methods of universal algebra, but we did not succeed to make a substantial progress yet. The only minor contribution in this part is yet another proof of the Toyoda-Murdoch-Bruck theorem on medial quasigroups (Theorem 3.1). Neither we go into details in Section 6 on homogeneous representation, since it has been presented in our recent paper [35]. On the other hand, many details are given in Section 5, the Belousov-Onoi theory is presented in a substantially different way. In particular, we provide a new and cleaner proof of the representation theorem for left distributive quasigroups (Theorem 5.5), which contains as a special case the classical results of Belousov on distributive quasigroups (a part of Theorem 3.3), and the Kikkawa-Robinson theorem on involutory left distributive quasigroups (Theorem 5.9).

1.3. A remark on automated theorem proving. Many theorems discussed in the present paper admit a short first order theory formulation, and subsequently could be attempted by automated theorem proving (ATP). Most of them are beyond the capabilites of current provers, but a few can be proved by any state-of-the art theorem prover within a few seconds. In those cases, we do not always bother to provide a reference or a proof, considering such problems "easy symbolic manipulation", although it may be rather intricate to find a proof without the aid of a computer. We refer to [73] for more information about automated theorem proving in algebra.

2. Background

2.1. Quasigroups and quandles. Let $(A, *)$ be an algebraic structure with a single binary operation, or, shortly, a *binary algebra* (also referred to as *magma* or *groupoid* elsewhere). We say it possesses *unique left division*, if for every $a, b \in A$, there is a unique $x \in A$ such that $a * x = b$; such an x is often denoted $x = a\backslash b$. *Unique right division* is defined dually: for every $a, b \in A$, there is a unique $y \in A$ such that $y * a = b$; such a y is often denoted $y = b/a$. Binary algebras with unique left and right division are called *quasigroups*.

We list a few identities which are met frequently (all identities are assumed to be universally quantified, unless stated otherwise). A binary algebra $(A, *)$ is called

- *left distributive* if $x * (y * z) = (x * y) * (x * z)$,
- *right distributive* if $(z * y) * x = (z * x) * (y * x)$,
- *distributive* if it is both left and right distributive,
- *medial* if $(x * y) * (u * v) = (x * u) * (y * v)$,
- *trimedial* if every 3-generated subquasigroup is medial,
- *idempotent* if $x * x = x$,
- *left involutory* (or *left symmetric*) if $x * (x * y) = y$ (hence we have unique left division with $x\backslash y = x * y$).

Observe that left distributive quasigroups are idempotent: $x*(x*x) = (x*x)*(x*x)$ by left distributivity and we can cancel from the right. Non-idempotent medial quasigroups exist, indeed, abelian groups are examples. Also observe that idempotent trimedial binary algebras are distributive: given $a, b, c \in A$, the subalgebra $\langle a, b, c\rangle$ is medial, hence $(a * b) * (a * c) = (a * a) * (b * c) = a * (b * c)$, and dually for right distributivity; it requires quite an effort to prove the converse for quasigroups, see Theorem 3.3.

A binary algebra is called a (left) *quandle*, if it is idempotent, left distributive and has unique left division (remarkably, the three conditions correspond neatly to the three Reidemeister moves in knot theory, see [12, 63]). Quandles that also have unique right division are called *latin quandles.* Indeed, latin quandles and left distributive quasigroups are the very same things.

For universal algebraic considerations, it is often necessary to consider quandles as algebraic structures with two binary operations, $(A, *, \backslash)$, and quasigroups as structures with three binary operations, $(A, *, /, \backslash)$. Then, subalgebras are really quandles (quasigroups, respectively), etc. We will implicitly assume the division operations to be part of the algebraic structure whenever needed (e.g. when considering term operations in Section).

Given a binary algebra $(A, *)$, it is natural to consider *left translations* $L_a(x) = a * x$, and *right translations* $R_a(x) = x * a$, and the semigroups they generate, the *left multiplication semigroup* $\mathrm{LMlt}(A, *) = \langle L_a : a \in A\rangle$, the *right multiplication semigroup* $\mathrm{RMlt}(A, *) = \langle R_a : a \in A\rangle$, and the *multiplication semigroup* $\mathrm{Mlt}(A, *) = \langle L_a, R_a : a \in A\rangle$. Unique left division turns left translations into permutations, and thus the left multiplication semigroup into a group (and dually for right translations). Observe that $L_a^{-1}(x) = a\backslash x$ and $R_a^{-1}(x) = x/a$. Also note that $(A, *)$ is left distributive if and only if L_a is an endomorphism for every $a \in A$. Hence, in quandles, $\mathrm{LMlt}(A, *)$ is a subgroup of the automorphism group.

A binary algebra $(A, *)$ is called *homogeneous* if $\mathrm{Aut}(A, *)$ acts transitively on A. It is called *left connected* if $\mathrm{LMlt}(A, *)$ acts transitively on A (we will omit the adjective "left" for quandles). A finite quandle is therefore connected if, for every $a, b \in A$, there exist $x_1, \dots, x_n \in A$ such that $b = x_1 * (x_2 * (\dots (x_n * a)))$ (compare to unique right division!). Connected quandles are arguably the most important class of quandles, both from the algebraic and topological points of view. Indeed, latin quandles are connected, and the class of connected quandles is a very natural generalization of left distributive quasigroups: many structural properties of left distributive quasigroups extend to connected quandles, as we shall see throughout Section 6.

To illustrate the power of connectedness, let us prove the following implication for quandles that are (both left and right) distributive.

Proposition 2.1 ([13, Theorem 5.10]). *Finite connected distributive quandles are quasigroups.*

Proof. Assume the contrary, and let $(Q, *)$ be the smallest counterexample. Right distributivity says that every right translation R_a is a homomorphism, hence, its image, $R_a(Q)$, forms a subquandle that is also connected and distributive (both properties project to homomorphic images). For every $a, b \in Q$, the subquandles $R_a(Q)$ and $R_b(Q)$ are isomorphic: connectedness of $(Q, *)$ provides an automorphism $\alpha \in \mathrm{LMlt}(Q, *)$ such that $\alpha(a) = b$, and it follows from $\alpha(x * a) = \alpha(x)*\alpha(a) = \alpha(x)*b$ that α restricts to an isomorphism between $R_a(Q)$ and $R_b(Q)$. Therefore, by minimality, all subquandles $R_a(Q)$ are proper subquasigroups. Now we prove that $R_a(Q) \subseteq R_{x*a}(Q)$ for every $x, a \in Q$. Let $y * a \in R_a(Q)$. Since $R_a(Q)$ is a quasigroup, there is $z * a \in R_a(Q)$ such that $y * a = (z * a) * (x * a)$. Hence $y * a \in R_{x*a}(Q)$. By induction, $R_a(Q) \subseteq R_{x_1*a}(Q) \subseteq R_{x_2*(x_1*a)}(Q) \subseteq \dots$, and thus, from connectedness, $R_a(Q) \subseteq R_b(Q)$ for every $a, b \in Q$. Hence all subquasigroups $R_a(Q)$ are equal, and since $x \in R_x(Q)$ for every $x \in Q$, all of them are equal to Q, a contradiction. □

2.2. Loops. A *loop* is a quasigroup $(Q, \cdot)$ with a *unit* element 1, i.e., $1 \cdot a = a \cdot 1 = a$ for every $a \in A$. In the present paper, loops will be denoted multiplicatively. To avoid parenthesizing, we shortcut $x \cdot yz = x \cdot (y \cdot z)$ etc., and we remove parentheses whenever the elements associate, i.e. write xyz whenever we know that $x \cdot yz = xy \cdot z$. For all unproved statements, we refer to any introductory book on loops, such as [10, 71].

Let $(Q, \cdot)$ be a loop. *Inner mappings* are those elements of the multiplication group $\mathrm{Mlt}(Q, \cdot)$ that fix the unit element. For example, the conjugation mappings $T_x(z) = xz/x$ are inner and, in a way, measure the non-commutativity in the loop. The *left inner mappings* are defined by $L_{x,y}(z) = (xy)\backslash(x \cdot yz)$ and measure the non-associativity from the left.

The most common example of loops are groups (i.e. associative loops), and most classes of loops studied in literature are those satisfying a weak version of associativity or commutativity. We list a few weak associative laws (note that all the conditions hold in groups): a loop is called

- *diassociative* if all 2-generated subloops are associative;
- *left alternative* if $x \cdot xy = x^2y$;
- *power-associative* if all 1-generated subloops are associative;
- *Moufang* if $(xy \cdot x)z = x(y \cdot xz)$ (the dual law is equivalent in loops);
- *left Bol* if $(x \cdot yx)z = x(y \cdot xz)$;
- *automorphic* if all inner mappings are automorphisms.
- *left automorphic* if all left inner mappings $L_{x,y}$ are automorphisms.

Moufang's theorem [18] says that in a Moufang loop, every subloop generated by three elements that associate, is associative. In particular, Moufang loops are diassociative, since $a(ba) = (ab)a$ for every a, b, as directly follows from the Moufang law. Bol loops are power-associative.

The *nucleus* of a loop $(Q, \cdot)$ is the set of all elements $a \in Q$ that associate with all other elements, i.e.,

$$N = \{a \in Q : \ a \cdot xy = ax \cdot y, \ x \cdot ay = xa \cdot y, \ x \cdot ya = xy \cdot a \text{ for all } x, y \in Q\}.$$

An element of a loop is called *nuclear* if it belongs to the nucleus. A mapping $f : Q \to Q$ is called k-*nuclear* if $x^k f(x) \in N$ for every $x \in Q$.

Commutative Moufang loops were a central topic in the Bruck's book [10], and newer results are surveyed in [7, 78]. The following characterization shows how natural the class is.

Theorem 2.2 ([10, 70]). *The following are equivalent for a commutative loop* $(Q,\cdot)$*:*

(1) *it is diassociative and automorphic;*

(2) *it is Moufang;*

(2′) *the identity* $xx\cdot yz=xy\cdot xz$ *holds.*

(3) *the identity* $f(x)x\cdot yz=f(x)y\cdot xz$ *holds for some* $f:Q\to Q$*.*

Moreover, if $(Q,\cdot)$ *is a commutative Moufang loop, than the identity of* (3) *holds if and only if* f *is a* (-1)*-nuclear mapping.*

The equivalence of (1), (2), (2') is well-known [10]. The rest is a special case of a lesser known, but intriguing characterization of Moufang loops by Pflugfelder [70]. It is one of the crucial ingrediences in Kepka's proof of Theorem 3.2, and also in our new proof of Proposition 5.7.

Example 2.3. According to Kepka and Němec [49, Theorem 9.2], the smallest non-associative commutative Moufang loops have order 81, there are two of them (up to isomorphism), and can be constructed as follows. Consider the groups $G_1=(\mathbb{Z}_3)^4$ and $G_2=(\mathbb{Z}_3)^2\times\mathbb{Z}_9$. Let $e_1,e_2,e_3(,e_4)$ be the canonical generators. Let t_1 be the triaditive mapping over G_1 satisfying

$$t_1(e_2,e_3,e_4)=e_1,\ t_1(e_3,e_2,e_4)=-e_1,\ t_1(e_i,e_j,e_k)=0 \text{ otherwise.}$$

Let t_2 be the triaditive mapping over G_2 satisfying

$$t_2(e_1,e_2,e_3)=3e_3,\ t_2(e_2,e_1,e_3)=-3e_3,\ t_2(e_i,e_j,e_k)=0 \text{ otherwise.}$$

The loops $Q_i=(G_i,\cdot)$, $i=1,2$, with

$$x\cdot y=x+y+t_i(x,y,x-y),$$

are non-isomorphic commutative Moufang loops, and every commutative Moufang loop of order 81 is isomorphic to one of them. □

In an arbitrary loop $(Q,\cdot)$, we can define the left inverse as $x^{-1}=x\backslash 1$ (in general, $x\backslash 1\neq 1/x$). Then, the *left inverse property* (LIP) requests that $a\backslash b=a^{-1}b$ for every $a,b\in Q$, and the *left automorphic inverse property* (LAIP) requests that $(ab)^{-1}=a^{-1}b^{-1}$ for every $a,b\in Q$. The RIP and RAIP are defined dually; if left and right inverses coincide, we talk about IP and AIP.

Diassociative loops have the IP, and then, commutativity is indeed equivalent to the AIP. Bol loops have the LIP, and are power associative, hence the left and right inverses coincide. Occasionally, we will need the following technical lemma.

Lemma 2.4 ([51] or ATP). *The following properties are equivalent for a left Bol loop* $(Q,\cdot)$*:*

(1) *the AIP;*

(2) *the identity* $(xy)^2 = x \cdot y^2x$*;*

(3) $L_{ab}^2 = L_a L_b^2 L_a$ *for every* $a, b \in Q$.

It seems that the AIP is the appropriate generalization of commutativity into the Bol setting (commutativity is no good, as it implies the Moufang law). We have the following "left version" of Theorem 2.2, under the additional assumption of *unique 2-divisibility*, which states that the mapping $x \mapsto x^2$ is a permutation.

Theorem 2.5 ([53] and ATP). *The following are equivalent for a uniquely 2-divisible loop* $(Q, \cdot)$ *with the LAIP:*

(1) *it has the LIP, is left alternative and left automorphic;*

(1′) *the identities* $x^2 \cdot x^{-1}y = xy$ *and* $L_{x,y}(z^{-1}) = L_{x,y}(z)^{-1}$ *hold;*

(2) *it is left Bol;*

(2′) *the identity* $(xy)^2 \cdot (x^{-1}z) = x \cdot y^2z$ *holds.*

Proof sketch. (1') is an immediate consequence of (1), and (2') easily follows from (2) by Lemma 2.4, but the converse implications are trickier; we could not find them anywhere in literature, but they can be verified by an automated theorem prover.

To prove that the equivalent conditions (1),(1') are in turn equivalent to the equivalent conditions (2),(2'), we can use [53, Theorem 3], which states that, for left alternative uniquely 2-divisible loops with the LIP and LAIP, the identity (2') is equivalent to being left automorphic. □

Left Bol loops with the AIP are called *Bruck loops* (or *K-loops* or *gyrocommutative gyrogroups*). A lot of structure theory is collected in Kiechle's book [51]. Uniquely 2-divisible Bruck loops were called *B-loops* (we will use the shortcut, too) and studied in detail by Glauberman [31]. A finite Bruck loop is uniquely 2-divisible if and only if it has odd order [31, Proposition 1]. Every B-loop can be realized as a subset Q of a group $(G, \circ)$ such that the mapping $x \mapsto x \circ x$ is a permutation on Q and the loop operation is $a \cdot b = \sqrt{a} \circ b \circ \sqrt{a}$ [31, Theorem 2].

Example 2.6. The smallest non-associative B-loop has order 15 and can be constructed as follows. Consider the loop $(\mathbb{Z}_5 \times \mathbb{Z}_3, \cdot)$ with

$$(a, x) \cdot (b, y) = (\varphi_{x,y}a + b, x + y)$$

where $\varphi_{x,y} \in \mathbb{Z}_5^*$ are given by the following table:

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

It is straightforward to check that this is a B-loop. It is an abelian extension of $\mathbb{Z}_5$ by $\mathbb{Z}_3$ in the sense of [82]. □

2.3. Linear and affine representation. A great portion of the present paper is about establishing that "two algebraic structures are essentially the same". To formalize the statement, we borrow a formal definition from universal algebra. Let $(A, f_1, f_2, \dots)$ be an arbitrary algebraic structure (shortly, algebra), with basic operations $f_1, f_2, \dots$ A *term operation* is any operation that results as a composition of the basic operations. *Polynomial operations* result from term operations by substituting constants for some of the variables. Two algebras with the same underlying set are called *term equivalent* (or *polynomially equivalent*, respectively), if they have the same term operations (or polynomial operations). For example, a group can be presented in the standard way, as $(G, \cdot, ^{-1}, 1)$, or in the loop theoretical way, as an associative loop $(G, \cdot, /, \backslash, 1)$; the two algebraic structures are formally different, but they are term equivalent, since the basic operations in any one of them are term operations in the other one. Term equivalent algebras have identical subalgebras, polynomially equivalent algebras have identical congruences, and share all properties that only depend on terms or polynomials (for example, the Lagrange property, see Section 6.3). To learn more, consult [8, Section 4.8].

One of the fundamental tools to study a quasigroup is, to determine its loop isotopes, and use the properties of the loops to obtain an information about the original quasigroup. An *isotopy* between two quasigroups $(Q_1, *)$ and $(Q_2, \cdot)$ is a triple of bijective mappings $\alpha, \beta, \gamma : Q_1 \to Q_2$ such that

$$\alpha(a) \cdot \beta(b) = \gamma(a * b)$$

for every $a, b \in Q_1$. Then, $(Q_2, \cdot)$ is called an *isotope* of $(Q_1, *)$. The combinatorial interpretation is that $(Q_2, \cdot)$ is obtained from $(Q_1, *)$ by permuting rows, columns and renaming entries in the multiplication table. Up to isomorphism, we can only consider isotopes with $Q_1 = Q_2$ and $\gamma = id$, so called *principal isotopes*.

Every quasigroup admits many principal loop isotopes, often falling into more isomorphism classes, yet all of them have a particularly nice form.

Proposition 2.7 ([10, Section III]). *Let $(Q, *)$ be a quasigroup and α, β permutations on Q. The following are equivalent:*

- *the isotope $a \cdot b = \alpha(a) * \beta(b)$ is a loop;*
- *$\alpha = R_{e_1}$ and $\beta = L_{e_2}$ for some $e_1, e_2 \in Q$.*

Rephrased, given a quasigroup $(Q, *)$, the only loop isotopes, up to isomorphism, are $(Q, \cdot)$ with

$$a \cdot b = (a/e_1) * (e_2 \backslash b),$$

where $e_1, e_2 \in Q$ can be chosen arbitrarily. Then the unit element is $1 = e_2 * e_1$. For the division operations, we will use the symbols $\backslash^{\cdot}$ and $/^{\cdot}$, to distinguish them from the quasigroup division.

Notice that the new operation $\cdot$ is a polynomial operation over the original quasigroup, and so are the division operations. We can recover the quasigroup operation as

$$a * b = R_{e_1}(a) \cdot L_{e_2}(b),$$

but this is rarely a polynomial operation over $(Q, \cdot)$. The most satisfactory loop isotopes are those where R_{e_1} and L_{e_2} are affine mappings over $(Q, \cdot)$.

A permutation φ of Q is called *affine* over $(Q, \cdot)$, if

$$\varphi(x) = \tilde{\varphi}(x) \cdot u \quad \text{or} \quad \varphi(x) = u \cdot \tilde{\varphi}(x)$$

where $\tilde{\varphi}$ is an automorphism of $(Q, \cdot)$ and $u \in Q$. In other terms, if $\varphi = R_u\tilde{\varphi}$ or $\varphi = L_u\tilde{\varphi}$. A quasigroup $(Q, *)$ is called *affine* over a loop $(Q, \cdot)$ if, for every $a, b \in Q$,

$$a * b = \varphi(a) \cdot \psi(b),$$

where φ, ψ are affine mappings over $(Q, \cdot)$ such that $\tilde{\varphi}\tilde{\psi} = \tilde{\psi}\tilde{\varphi}$. If both φ, ψ are automorphisms, we call $(Q, *)$ *linear* over $(Q, \cdot)$. (Note that the affine mappings φ, ψ do not necessarily commute.)

Example 2.8. To illustrate the concept of affine representation, consider a quasigroup $(Q, *)$ affine over an abelian group $(Q, \cdot)$. We prove that it is medial. With $\varphi = R_u\tilde{\varphi}$, $\psi = R_v\tilde{\psi}$ (left or right makes no difference here), we have

$$\begin{aligned}(a * b) * (c * d) &= \varphi\left(\varphi(a) \cdot \psi(b)\right) \cdot \psi\left(\varphi(c) \cdot \psi(d)\right)\\ &= \tilde{\varphi}\left(\tilde{\varphi}(a)u \cdot \tilde{\psi}(b)v\right) u \cdot \tilde{\psi}\left(\tilde{\varphi}(c)u \cdot \tilde{\psi}(d)v\right) v\\ &= \tilde{\varphi}^2(a) \cdot \tilde{\varphi}\tilde{\psi}(b) \cdot \tilde{\psi}\tilde{\varphi}(c) \cdot \tilde{\psi}^2(d) \cdot \tilde{\varphi}(uv) \cdot \tilde{\psi}(uv) \cdot uv.\end{aligned}$$

Since $\tilde{\varphi}\tilde{\psi} = \tilde{\psi}\tilde{\varphi}$, the expression is invariant with respect to interchange of b and c. As we shall see, Theorem 3.1 states also the converse: every medial quasigroup is affine over an abelian group. □

Any adjective to the words "affine" or "linear" will refer to the properties of the mappings φ and ψ. In Section 3, we will consider 1-nuclear affine representations over commutative Moufang loops, i.e. we will assume that φ, ψ are 1-nuclear affine mappings. Notice that if $\varphi = F_u\tilde{\varphi}$, with $F \in \{L, R\}$, is 1-nuclear, then u is nuclear (substitute 1), and if the nucleus is a normal subloop, then $\tilde{\varphi}$ is also 1-nuclear.

How to turn an affine representation into a polynomial equivalence? Consider affine mappings $\varphi = F_u\tilde{\varphi}$, $\psi = G_v\tilde{\psi}$ where $F, G \in \{L, R\}$ and $\tilde{\varphi}, \tilde{\psi}$ are automorphisms of $(Q, \cdot)$. Then $x*y = \varphi(x)\cdot\psi(y)$ is a polynomial operation over the algebra $(Q, \cdot, \tilde{\varphi}, \tilde{\psi})$, and a similar statement applies to the division operations, too (one also needs to use the inverse automorphisms $\tilde{\varphi}^{-1}, \tilde{\psi}^{-1}$). Conversely, if $(Q, \cdot)$ is a loop isotope of a quasigroup $(Q, *)$, then $x \cdot y = (x/e_1) * (e_2\backslash y)$, $x\backslash^{\cdot} y = e_2 * ((x/e_1)\backslash y)$, and $x/^{\cdot} y = (x/(e_2\backslash y)) * e_1$ are all polynomial operations over the quasigroup. If the translations R_{e_1}, L_{e_2} are affine over $(Q, \cdot)$, then $\tilde{R}_{e_1}(x) = (x * e_1)/^{\cdot}(1 * e_1)$,

$\tilde{L}_{e_2}(x) = (e_2 * x)/^{\cdot}(e_2 * 1)$ are polynomial operations, too, hence the quasigroup $(Q, *, \backslash, /)$ and the algebra $(Q, \cdot, \backslash^{\cdot}, /^{\cdot}, \tilde{R}_{e_1}, \tilde{R}_{e_1}^{-1}, \tilde{L}_{e_2}, \tilde{L}_{e_2}^{-1})$ are polynomially equivalent, i.e. essentially the same object. It is convenient to perceive the loop expanded by two automorphisms in a module-theoretic way, as we shall explain now.

The classical case first: assume the loop is an abelian group and let us denote it additively, $(Q,+)$. Let φ, ψ be two commuting automorphisms of $(Q,+)$. Then the algebra $(Q, +, -, 0, \varphi, \varphi^{-1}, \psi, \psi^{-1})$ is term equivalent to the module over the ring of Laurent polynomials $\mathbb{Z}[s, s^{-1}, t, t^{-1}]$ whose underlying additive structure is $(Q,+)$ and the action of s, t is that of φ, ψ, respectively. The corresponding quasigroup operation can be written as the affine form

$$x * y = sx + ty + c,$$

where $c \in Q$ is a constant.

For general loops, one can consider "generalized modules" over commutative "generalized rings", where the underlying additive structures are not necessarily associative. No general theory has been developed yet, but there are indications that this approach could provide a powerful tool. For example, commutative diassociative loops share a lot of module-theoretic properties of abelian groups, such as the primary decomposition [56]. The idea of "generalized modules" and the corresponding homological methods have been exploited several times to prove interesting theorems about quasigroups [33, 34, 48].

Finally, let us note that our definition of affine quasigroup is too strong in one sense, and possibly weak in another sense.

The condition that the two automorphisms $\tilde{\varphi}, \tilde{\psi}$ commute is strongly tied to mediality and its weaker forms, and we included it only for brevity. Omitting the condition makes a very good sense from the universal algebra point of view. Quasigroups that admit a "non-commuting" affine representation over an abelian group (and thus polynomially equivalent to a module over the ring of Laurent polynomials of two non-commuting variables) have been studied since the 1970s, see [79, Chapter 3] or [17] for recent developments (the original name *T-quasigroups* is slowly fading away, being replaced by the adjective *central*; in universal algebra, they would be called *abelian* or *affine*, as the two concepts are equivalent for quasigroups).

In Section 3, all affine representations will be 1-nuclear. However, we resist to enforce nuclearity in the definition of affineness, since we do not understand its role properly (in particular, we do not know whether the representation of Theorem 5.5 admits any sort of nuclearity). We are not yet certain what is the appropriate generalization of the notion of an affine form into the non-associative setting.

3. Distributive quasigroups

3.1. Affine representation. The first ever affine representation theorem was the one for medial quasigroups, proved independently by Toyoda [88], Murdoch

[61] and Bruck [9] in the 1940s.

Theorem 3.1 ([9, 61, 88]). *The following are equivalent for a quasigroup $(Q,*)$:*

(1) *it is medial;*

(2) *it is affine over an abelian group.*

Proof. (2) ⇒ (1) was calculated in Example 2.8.

(1) ⇒ (2). Pick arbitrary $e_1, e_2 \in Q$ and define a loop operation on Q by $a \cdot b = (a/e_1) * (e_2\backslash b)$. We can recover the quasigroup operation as $a * b = R_{e_1}(a) \cdot L_{e_2}(b)$, where R_{e_1}, L_{e_2} are translations in $(Q,*)$. We show that $(Q,\cdot)$ is an abelian group, and that R_{e_1}, L_{e_2} are affine mappings over $(Q,\cdot)$.

First, consider the quasigroup $(Q,\circ)$ with $a \circ b = (a/e_1) * b$. We prove that it is also medial. Observe that, for every $x, y, u, v \in Q$,

$$(x/y) * (u/v) = (x * u)/(y * v), \tag{†}$$

since $((x/y) * (u/v)) * (y * v) = ((x/y) * y) * ((u/v) * v) = x * u$, and we obtain the identity by division from the right. Now we expand

$$\begin{aligned}(a \circ b) \circ (c \circ d) &= (((a/e_1) * b)/e_1) * ((c/e_1) * d)\\ &= (((a/e_1) * b)/((e_1/e_1) * e_1)) * ((c/e_1) * d)\\ &= (((a/e_1)/(e_1/e_1)) * (b/e_1)) * ((c/e_1) * d),\end{aligned}$$

and using mediality, we can interchange b/e_1 and c/e_1, and by an analogous calculation obtain $(a \circ b) \circ (c \circ d) = (a \circ c) \circ (b \circ d)$. Now notice that $a \cdot b = a \circ (e_2\backslash b) = a \circ ((e_2 * e_1)\backslash^\circ b)$, hence a dual argument, with $*$ replaced for $\circ$ and e_1 replaced for $e_2 * e_1$, shows that the loop $(Q,\cdot)$ is also medial. But medial loops are abelian groups.

It remains to prove that the mappings R_{e_1}, L_{e_2} are affine over $(Q,\cdot)$ and that the corresponding automorphisms $\tilde{R}_{e_1}, \tilde{L}_{e_2}$ commute. Let 1 denote the unit and $^{-1}$ the inverse element in the group $(Q,\cdot)$. Consider $a, b \in Q$. By mediality,

$$(R_{e_1}^{-1}(a) * L_{e_2}^{-1}(b)) * (L_{e_2}^{-1}(1) * L_{e_2}^{-1}(1)) = (R_{e_1}^{-1}(a) * L_{e_2}^{-1}(1)) * (L_{e_2}^{-1}(b) * L_{e_2}^{-1}(1)).$$

Rewriting $x * y = R_{e_1}(x) \cdot L_{e_2}(y)$, we obtain

$$R_{e_1}(a \cdot b) \cdot L_{e_2} R_{e_1} L_{e_2}^{-1}(1) = R_{e_1}(a) \cdot L_{e_2} R_{e_1} L_{e_2}^{-1}(b).$$

With $a = 1$, we obtain $L_{e_2} R_{e_1} L_{e_2}^{-1}(b) = R_{e_1}(b) \cdot L_{e_2} R_{e_1} L_{e_2}^{-1}(1) \cdot R_{e_1}(1)^{-1}$, and after replacement of the last term in the previous identity, and after cancelling the term $L_{e_2} R_{e_1} L_{e_2}^{-1}(1)$, we obtain

$$R_{e_1}(a \cdot b) = R_{e_1}(a) \cdot R_{e_1}(b) \cdot R_{e_1}(1)^{-1}.$$

This shows that R_{e_1} is an affine mapping, with the underlying automorphism $\tilde{R}_{e_1}(x) = R_{e_1}(x)R_{e_1}(1)^{-1}$. Dually, we obtain that L_{e_2} is an affine mapping, with the underlying automorphism $\tilde{L}_{e_2}(x) = L_{e_2}(x)L_{e_2}(1)^{-1}$.

Finally we show that the two automorphisms commute. With $\varphi = R_{e_1}$, $\psi = L_{e_2}$, $u = R_{e_1}(1)^{-1}$ and $v = L_{e_2}(1)^{-1}$, we can calculate as in Example 2.8 that, for every $x \in Q$,

$$\tilde{\varphi}\tilde{\psi}(x)\cdot\tilde{\varphi}(uv)\cdot\tilde{\psi}(uv)\cdot uv = (1*x)*(1*1) = (1*1)*(x*1) = \tilde{\psi}\tilde{\varphi}(x)\cdot\tilde{\varphi}(uv)\cdot\tilde{\psi}(uv)\cdot uv.$$

After cancellation, we see that $\tilde{\varphi}\tilde{\psi} = \tilde{\psi}\tilde{\varphi}$. □

Note that we proved a stronger statement: *any* loop isotope of a medial quasigroup is an abelian group that provides an affine representation. For other classes, in order to obtain an affine representation over a nice class of loops, one often has to choose the parameters e_1, e_2 in a special way. For instance, for trimedial quasigroups, one has to take $e_1 = e_2$ which is a square, as we shall see.

Perhaps the best way to perceive distributive quasigroups is through *trimediality.* As we shall see, a quasigroup is distributive if and only if it is idempotent and trimedial. This was first realized by Belousov in [2], and his proof was based on finding an isotopy of a distributive quasigroup to a commutative Moufang loop, and subsequently using Moufang's theorem (see also his book [3, Theorems 8.1 and 8.6]). Belousov's method actually provides a linear representation, but this fact was recognized and explicitly formulated only later by Soublin [80, Section II.7, Theorem 1]. An analogous theorem for general (not necessarily idempotent) trimedial quasigroups was proved by Kepka [43] a few years later (Theorem 3.2). We will now outline Kepka's proof, and show how the Belousov-Soublin theorem follows as a special case (Theorem 3.3).

Many equivalent conditions charecterizing trimediality are formulated in [43], we only pick the most important ones here: (1) trimediality, (2) a stronger fact stating that mediating elements generate a medial subquasigroup, (3) a finite equational base for trimediality, and (4) the affine representation. In fact, Kepka lists several finite bases, but not the one we state here: our condition (3) is a *minimal* base, found in [55], and subsumes most of Kepka's bases.

Theorem 3.2 ([43]). *The following are equivalent for a quasigroup $(Q, *)$:*

(1) *it is trimedial;*

(2) *for every $a, b, c, d \in Q$, if $(a*b)*(c*d) = (a*c)*(b*d)$ then the subquasigroup $\langle a, b, c, d\rangle$ is medial;*

(3) *it satisfies, for every $a, b, c \in Q$, the identities*

$$(c * b) * (a * a) = (c * a) * (b * a),$$
$$(a * (a * a)) * (b * c) = (a * b) * ((a * a) * c);$$

(4) *it is 1-nuclear affine over a commutative Moufang loop.*

Proof sketch. (2) ⇒ (1). For any $a, b, c \in Q$, we have $(b*a)*(a*c) = (b*a)*(a*c)$. Hence, by (2), $\langle a, b, c\rangle$ is medial.

(1) ⇒ (3). Given $a, b, c \in Q$, consider the subquasigroup $\langle a, b, c\rangle$. It is medial, hence the two identities hold for a, b, c.

(3) ⇒ (4). First of all, we need to prove the following two additional identities: $(a * a) * (b * c) = (a * b) * (a * c)$ and $(a * b) * (c * a) = (a * c) * (b * a)$ (in Kepka's terminology, to prove that $(Q, *)$ is a WAD-quasigroup). A proof can be found quickly by an automated theorem prover, or read in [55]. Now we can follow Kepka's proof from [43], whose structure is similar to our proof of Theorem 3.1.

Pick an arbitrary square $e \in Q$ (i.e. $e = e' * e'$ for some e') and define the loop operation on Q by $a \cdot b = (a/e) * (e\backslash b)$. We can recover the quasigroup operation as $a*b = R_e(a) \cdot L_e(b)$, where L_e, R_e are translations in $(Q, *)$. To show that $(Q, \cdot)$ is a commutative Moufang loop, it is sufficient to verify condition (3) of Theorem 2.2 with $f = R_e L_e^{-1}$. The proof is rather technical, see [42, Proposition 4.8(iii)]. It also follows that the mapping f is (-1)-nuclear, and another technical calculation, see [43, Lemma 3(iii)], shows that the mappings L_e, R_e are 1-nuclear. Finally, we can reuse the second part of our proof of Theorem 3.1 to show that the two mappings are affine and that the underlying automorphisms commute, since we only used the identity $(a*a)*(b*c) = (a*b)*(a*c)$ and its dual in the proof. We have to be careful about non-associativity of the multiplication, but fortunately, all calculations are correct thanks to the fact that the mappings L_e, R_e are 1-nuclear, hence preserve the nucleus (in particular, all elements resulting by application of L_e, R_e on 1 are nuclear).

(4) ⇒ (2). The idea is, find a subloop Q' of $(Q, \cdot)$ that contains all four elements a, b, c, d and is generated by three elements u, v, w that associate. Then, by Moufang's theorem [18], Q' is an abelian group, and thus the subquasigroup $\langle a, b, c, d\rangle$ is medial by Theorem 3.1. The construction is described in [43, Theorem 2 (vi)⇒(vii)]. □

As a corollary to Theorem 3.2, we settle the case of distributive quasigroups.

Theorem 3.3 ([80]). *The following are equivalent for an idempotent quasigroup $(Q, *)$:*

(1) *it is trimedial;*

(2) *for every $a, b, c, d \in Q$, if $(a*b)*(c*d) = (a*c)*(b*d)$ then the subquasigroup $\langle a, b, c, d\rangle$ is medial;*

(3) *it is distributive;*

(4) *it is 1-nuclear linear over a commutative Moufang loop.*

Proof. Look at Theorem 3.2. Conditions (1) and (2) are identical. Under the assumption of idempotence, condition (3) of Theorem 3.2 is equivalent to distributivity. To obtain the equivalence of the fourth conditions, we observe that an idempotent quasigroup which is 1-nuclear affine over a commutative Moufang loop $(Q,\cdot)$ is actually linear over $(Q,\cdot)$: with $\varphi = R_u\tilde{\varphi}$ and $\psi = R_v\tilde{\psi}$, thanks to nuclearity and commutativity, we have $a*b = \tilde{\varphi}(a)\tilde{\psi}(a)uv$, and since $1 = 1*1 = \tilde{\varphi}(1)\tilde{\psi}(1)uv = uv$ we see that $a*b = \tilde{\varphi}(a)\tilde{\psi}(a)$ is a linear representation. □

For idempotent quasigroups, the linear representation $a*b = \varphi(a)\cdot\psi(b)$ is determined by either one of the automorphisms φ or ψ, since $a = a*a = \varphi(a)\cdot\psi(a)$, hence $\varphi(a) = a/^{\cdot}\psi(a)$ or $\psi(a) = \varphi(a)\backslash^{\cdot} a$. Mappings φ, ψ satisfying $\varphi(a)\cdot\psi(a) = a$ will be called *companions*. Note that the companion of an automorphism is not necessarily a permutation or an endomorphism! However, if it is an endomorphism, then the two mappings commute.

Example 3.4. Combining Theorem 3.3 and Example 2.3, one can determine the smallest non-medial distributive quasigroups. They have order 81 and there are six of them (up to isomorphism) [49, Theorem 12.4]. A careful analysis of the automorphisms of the loops $(G_1,\cdot)$ and $(G_2,\cdot)$ of Example 2.3 (see [49, Sections 5 and 6], respectively) leads to the following classification:

1. $(G_1,*)$ with $x*y = x^{-1}\cdot y^{-1}$.
2. $(G_1,*)$ with $x*y = \varphi(x)\cdot\psi(y)$ where $\varphi(x) = (x_2-x_1)e_1 - x_2e_2 - x_3e_3 - x_4e_4$ and ψ is its companion.
3. $(G_2,*)$ with $x*y = \sqrt{x}\cdot\sqrt{y}$. In $(G_2,\cdot)$, the mapping $x \mapsto x^2$ is a 1-nuclear automorphism, and so is its inverse $x \mapsto \sqrt{x}$.
4. $(G_2,*)$ with $x*y = x^{-1}\cdot y^2$.
5. $(G_2,*)$ with $x*y = x^2\cdot y^{-1}$.
6. $(G_2,*)$ with $x*y = \varphi(x)\cdot\psi(y)$ where $\varphi(x) = -x_1e_1 - x_2e_2 - (3x_1+x_3)e_3$ and ψ is its companion. □

Theorem 3.3 has an interesting connection to design theory. It is well known that *Steiner triple systems* correspond to a certain class of (finite) idempotent quasigroups, called *Steiner quasigroups*. Affine Steiner triple systems, constructed over the affine spaces $(\mathbb{F}_3)^k$, correspond to medial Steiner quasigroups, $((\mathbb{F}_3)^k,*)$ with $a*b = -a-b$. *Hall triple systems* can be defined by the property that every subsystem generated by three points is affine. Theorem 3.3 implies that the corresponding quasigroups are precisely the distributive Steiner quasigroups. As a consequence, one can obtain, for instance, the enumeration of Hall triple systems, see the numbers $DQ(n)$ in Table 1 (the one of order 81 is item 1. of Example 3.4). We refer to [6, 16] for details and other relations between distributive quasigroups, finite geometries and combinatorial designs.

Theorems 3.2 and 3.3 can be further generalized in several directions. For example, it was proved by Kepka, Kinyon and Phillips [47, Theorem 1.2] that the class of *F-quasigroups*, properly containing the trimedial quasigroups, admits a 1-nuclear (-1)-Moufang-central affine representation over *NK-loops*, a class of Moufang loops that are sums of their nucleus and Moufang center. Another direction is weakening the unique divisibility condition, see the comprehensive studies by Ježek, Kepka and Němec [36, 38, 39, 45, 49]. In all of these papers, a self-dual condition (such as trimediality or both-sided distributivity) is essential for linearization. The one-sided case is quite different and will be studied in Section 5. Nevertheless, we will be able to obtain the representation from Theorem 3.3 as a consequence of the one-sided theory.

3.2. Structure and enumeration. Theorem 3.3 allows to use the well developed theory of commutative Moufang loops to build the structure theory of distributive quasigroups. We will describe a few examples. Further results can be found in the comprehensive survey [7].

We start with Galkin's interpretation of the Fischer-Smith theorem [23, 77].

Theorem 3.5 ([23]). *Let Q be a finite distributive quasigroup of order $p_1^{n_1}\cdot\ldots\cdot p_k^{n_k}$ where $p_1,\ldots,p_k$ are pairwise different primes. Then*

$$Q \simeq Q_1 \times \ldots \times Q_k$$

where $|Q_i| = p_i^{n_i}$. Moreover, if Q_i is not medial, then $p_i = 3$ and $n_i \geq 4$.

The story of the proof goes as follows. Let Q be a finite distributive quasigroup. The first step was Fischer's proof [20] that $\mathrm{LMlt}(Q)$ is solvable, using substantial results from group theory, including the Feit-Thompson theorem and the Brauer-Suzuki theorem. Then Smith [77] was able to strengthen Fischer's theorem, while avoiding the heavy finite group machinery, by combining Theorem 3.3 and the Bruck-Slaby theorem [10, Chapter VIII] stating that finite commutative Moufang loops are centrally nilpotent. Smith's result says that the derived subgroup $\mathrm{LMlt}(Q)'$ is the direct product of a 3-group and an abelian group of order coprime to 3 (hence $\mathrm{LMlt}(Q)'$ is nilpotent and $\mathrm{LMlt}(Q)$ is solvable, as proved by Fischer). Finally, Galkin [23] observed that his idea of minimal representation (explained in our Section 6) implies that the quasigroup Q decomposes in a way analogous to the decomposition of $\mathrm{LMlt}(Q)'$. Using the fact that every 3-generated subquasigroup is medial (see Theorem 3.3), one concludes that a non-medial distributive quasigroup has at least $3^4 = 81$ elements.

A somewhat different approach to the Fischer-Smith theorem, based on the homogeneous representation of Section 6, is presented in [29].

An interesting story is the *enumeration* of distributive quasigroups. Again, Theorem 3.3 is crucial here, as it allows to focus on the enumeration of commutative Moufang loops and their automorphism groups. It is not difficult to prove (see e.g. [49, Lemma 12.3]) that two commutative Moufang loops, Q_1 and Q_2, and their nuclear automorphisms, ψ_1 and ψ_2, respectively, provide isomorphic distributive quasigroups if and only if there is a loop isomorphism $\varphi : Q_1 \to Q_2$ such that $\psi_2 = \varphi\psi_1\varphi^{-1}$.

In particular, the lemma applies to abelian groups, hence the number $MI(n)$ of medial idempotent quasigroups of order n up to isomorphism can be determined using the classification of finite abelian groups and the corresponding linear algebra. The function $MI(n)$ is indeed multiplicative (i.e. $MI(mn) = MI(m)MI(n)$ for every m, n coprime) and explicit formulas for $MI(p^k)$, p prime and $k \leq 4$, were found by Hou [34] (in his paper, (finite) medial idempotent quasigroups are referred to as connected Alexander quandles; the formulas are given in [34, equation (4.2)] and the complete list of quasigroups is displayed in [34, Table 1]). See our Table 3 for the first 47 values of $MI(n)$.

Theorem 3.5 says that the interesting (i.e. directly indecomposable) non-medial distributive quasigroups have orders $n = 3^k$, $k \geq 4$. Table 1 summarizes some of the enumeration results found in literature. $CML(n)$ denotes the number of non-associative commutative Moufang loops of order n up to isomorphism, as calculated in [49]; the next four rows describe the numbers of non-medial quasigroups of order n up to isomorphism in the following classes: $3M(n)$ refers to trimedial quasigroups [46], $D(n)$ to distributive quasigroups [49], $DM(n)$ to distributive Mendelsohn quasigroups [16], and $DS(n)$ to distributive Steiner quasigroups [6, 44]; the last row displays the medial case.

n	3	3^2	3^3	3^4	3^5	3^6
$CML(n)$	0	0	0	2	6	≥ 8
$3M(n)$	0	0	0	35		
$D(n)$	0	0	0	6		
$DM(n)$	0	0	0	2	≥ 3	
$DS(n)$	0	0	0	1	1	3
$MI(n)$	1	8	30	166		

Table 1: Enumeration of commutative Moufang loops and of various classes of distributive quasigroups.

Another interesting enumeration result says that the smallest non-medial *hamiltonian* distributive quasigroup has order 3^6, and that there are two of them [33]. This is perhaps the deepest application of the module-theoretical approach to distributive quasigroups.

Finally, let us mention the property called *symmetry-by-mediality*. An idempotent binary algebra is called symmetric-by-medial, if it has a congruence α such that its blocks are *symmetric* (i.e. both left and right involutory), and the factor over α is medial. (In idempotent algebras, congruence blocks are always subalgebras.) Symmetric distributive quasigroups are commutative, and they are precisely the distributive Steiner quasigroups. Using Bruck's associator calculus for Moufang loops, Belousov proved that distributive quasigroups are symmetric-by-medial [3, Theorem 8.7]. Again, the theorem generalizes to a non-quasigroup setting [37, 81].

4. Conjugation and cores

Let $(G,\cdot)$ be a group and Q a subset of G closed with respect to conjugation. Then the binary algebra $(Q,*)$ with

$$a*b=aba^{-1}$$

is a quandle, called a *conjugation quandle* over the group $(G,\cdot)$. It is easy to verify that every quandle admits a *Cayley-like representation* over a conjugation quandle.

Proposition 4.1. *Let $(Q,*)$ be a quandle. Then $a\mapsto L_a$ is a quandle homomorphism of $(Q,*)$ onto a conjugation quandle over the group* $\mathrm{LMlt}(Q,*)$.

Proof. Left distributivity implies $a*(b*(a\backslash x))=(a*b)*x$, hence $L_a*L_b=L_aL_bL_a^{-1}=L_{a*b}$. □

This homomorphism is rarely an embedding, even for connected quandles. However, it is an embedding for every latin quandle, because, in a latin quandle, $L_a(x)=a*x\neq b*x=L_b(x)$ for every $a\neq b$ and every x. Hence, every latin quandle *is* a conjugation quandle, up to isomorphism. This observation can probably be attributed to Stein [84]. He also found the following criterion.

Proposition 4.2 ([84]). *Let $(G,\cdot)$ be a group, Q a subset of G closed with respect to conjugation, and assume that for every $a,b,c\in Q$, $aN_G(c)=bN_G(c)$ iff $a=b$. Then the conjugation quandle $(Q,*)$ is latin.*

A few structural results on quandles have been proved using the Cayley representation. For instance, Kano, Nagao and Nobusawa [41] used it for involutory quandles (in this case, the quandle is represented by involutions), and proved the following characterization of involutory quandles that are latin.

Theorem 4.3 ([41]). *A finite involutory quandle $(Q,*)$ is a quasigroup if and only if the derived subgroup* $\mathrm{LMlt}(Q,*)'$ *has odd order.*

The proof is not easy and uses Glauberman's Z^*-theorem. They conclude that involutory left distributive quasigroups are solvable, and possess the Lagrange and Sylow properties (see Section 6.3 for a more comprehensive discussion).

The Cayley representation is fundamental in Pierce's work on involutory quandles [74], and McCarron [59] used conjugation to represent simple quandles and to argue that there were no connected quandles with $2p$ elements, for any prime $p>5$ (see also Section 6.2).

Let $(G,\cdot)$ be a group, or, more generally, a Bol loop. The binary algebra $(G,*)$ with

$$a * b = a \cdot b^{-1}a$$

is an involutory quandle, called the *core* of $(G,\cdot)$. The core is a quasigroup if and only if the loop is uniquely 2-divisible [3, Theorem 9.4]. The core operation was introduced by Bruck who proved that isotopic Moufang loops have isomorphic cores [10]. It was later picked up by Belousov and others to construct some of the first examples of involutory left distributive quasigroups, see e.g. [3, Chapter IX] or [89].

Example 4.4. The smallest non-medial involutory left distributive quasigroup has order 15 and it is the core of the B-loop constructed in Example 2.6. Explicitly, it is the quasigroup $(\mathbb{Z}_5 \times \mathbb{Z}_3, *)$ with

$$(a,x) * (b,y) = (\mu_{x,y}a - b, -x - y)$$

where $\mu_{x,y} \in \mathbb{Z}_5^*$ are given by the following table:

	0	1	2
0	2	−1	−1
1	−1	2	−1
2	−1	−1	2

5. Left distributive quasigroups: Isotopy

5.1. Right linear representation. Restricting self-distributivity to only one side, it is natural to expect that the loop counterpart will admit one of the weaker one-sided loop conditions mentioned in Section 2.2. There are good news and bad news. Left distributive quasigroups are polynomially equivalent to a certain class of "non-associative modules", satisfying a (very) weak associative law. However, the connection is non-linear (only one of the defining mappings is an automorphism), and the corresponding class of loops, called *Belousov-Onoi loops* here, extends beyond the well-established theories (except for some special cases). The correspondence is therefore of limited utility at the moment. Nevertheless, it is interesting to look at details. Most of the ideas of the present section were discovered by Belousov and Onoi [5], but our presentation is substantially different.

Let $(Q,\cdot)$ be a loop and ψ its automorphism. We will call $(Q,\cdot,\psi)$ a *Belousov-Onoi module* (shortly, *BO-module*) if

$$\varphi(ab) \cdot \psi(ac) = a \cdot \varphi(b)\psi(c) \tag{BO}$$

holds for every $a,b,c \in Q$, where $\varphi(x) = x/^{\cdot}\psi(x)$ is the *companion mapping* for ψ. (The explanation why is it reasonable to consider such structures as "non-associative modules" has been explained at the end of Section 2.3.) To match the identity (BO) to the Bol identity, substitute $\psi^{-1}(ac)$ for c and obtain an equivalent identity

$$\varphi(ab)\cdot(\psi(a)\cdot ac) = a\cdot(\varphi(b)\cdot ac). \tag{BO'}$$

Example 5.1. We state a few examples of Belousov-Onoi modules.

1. Every loop $(Q,\cdot)$ turns into the BO-module $(Q,\cdot,id)$. If $\psi(x)=x$, then $\varphi(x)=1$ and thus the identity (BO) holds.
2. Every group $(Q,\cdot)$ with any automorphism ψ turns into the BO-module $(Q,\cdot,\psi)$. Condition (BO) is easily verified.
3. Every Bruck loop $(Q,\cdot)$ turns into the BO-module $(Q,\cdot,^{-1})$. If $\psi(x)=x^{-1}$, then $\varphi(x)=x^2$ by power-associativity, and we verify (BO') by $(ab)^2\cdot(a^{-1}\cdot ac)=(ab)^2\cdot c = a\cdot(b^2\cdot ac)$ using Lemma 2.4 in the second step. □

Call a BO-module *non-trivial* if $\psi\neq id$. There are relatively few loops that turn into a non-trivial BO-module, see the values of $BOM(n)$ in Table 2. Nevertheless, nearly all groups and all Bruck loops (except possibly those where $x^{-1}=x$) have the property.

A BO-module turns naturally into a quandle. The proof illustrates very well the conditions imposed by the definition.

Proposition 5.2. *Let $(Q,\cdot,\psi)$ be a Belousov-Onoi module, φ the companion mapping, and define for every $a,b\in Q$*

$$a*b=\varphi(a)\cdot\psi(b).$$

Then $(Q,*)$ is a quandle. The quandle is a quasigroup if and only if φ is a permutation.

Proof. Idempotence explains the definition of the companion mapping: we have $a*a=a$ iff $\varphi(a)\cdot\psi(a)=a$ iff $\varphi(a)=a/^{\cdot}\psi(a)$.

Unique left division follows from the fact that ψ is a permutation: we have $a*x=\varphi(a)\cdot\psi(x)=b$ iff $\psi(x)=\varphi(a)\backslash^{\cdot}b$ iff $x=\psi^{-1}(\varphi(a)\backslash^{\cdot}b)$.

Left distributivity is verified as follows: expanding the definition of $*$ and using the identity (BO), we obtain

$$(a*b)*(a*c)=\varphi(\varphi(a)\psi(b))\cdot\psi(\varphi(a)\psi(c))=\varphi(a)\cdot(\varphi\psi(b)\cdot\psi^2(c)),$$

and since ψ is an automorphism and φ a term operation, we have $\varphi\psi=\psi\varphi$, and thus the right hand side equals

$$\varphi(a)\cdot(\psi\varphi(b)\cdot\psi^2(c))=\varphi(a)\cdot\psi(\varphi(b)\psi(c))=a*(b*c).$$

Unique right division is dual to the left case: it happens if and only if φ is a permutation. □

Example 5.3. Consider the three items from Example 5.1.

1. Any trivial BO-module $(Q,\cdot,id)$ results in a projection quandle $(Q,*)$ with $a*b=b$.

2. The BO-module $(Q,\cdot,\psi)$, constructed over a group with an automorphism, results in a homogeneous quandle $(Q,*)$ with
$$a*b=a\psi(a^{-1}b).$$
If Q is finite, then $(Q,*)$ is a quasigroup if and only if ψ is a regular automorphism (i.e. the unit is the only fixed point of ψ). Belousov [3, Theorem 9.2] proves that all left distributive quasigroups isotopic to a group result in this particular way, and Galkin [24, Section 5] shows a number of interesting properties of such quasigroups. See Construction 6.1 for a generalization of this idea which covers all left distributive quasigroups.

3. The BO-module $(Q,\cdot,^{-1})$, constructed over a Bruck loop, results in an involutory quandle $(Q,*)$ with $a*b=a^2b^{-1}$. It follows from Lemma 2.4(2) that $x\mapsto x^2$ is a homomorphism from $(Q,*)$ to the core of $(Q,\cdot)$; hence, if $(Q,\cdot)$ is a B-loop, then the two constructions result in isomorphic quasigroups. In Theorem 5.9, we shall see that all involutory left distributive quasigroups result this way. □

Relatively few quandles admit a *Belousov-Onoi representation* as in Proposition 5.2, see the values of $BOQ(n)$ in Table 2. Even connected quandles do not always result from a BO-module: for example, a quick computer search reveals that none of the quandles constructed over a BO-module of order 6 is connected (compare to [35, Table 2]). In the latin case, however, the situation is different. The setting of BO-modules was designed by Belousov and Onoi in order to prove that all left distributive quasigroups (latin quandles) admit a representation as in Proposition 5.2.

A loop $(Q,\cdot)$ possesing an automorphism ψ such that $(B,\cdot,\psi)$ is a BO-module and the companion mapping for ψ is a permutation, will be called a *Belousov-Onoi loop* (shortly, *BO-loop*) with respect to ψ. (The original name was *S-loops*, for no apparent reason. Our definition uses the characterizing condition of [5, Theorem 4].)

Proposition 5.4 ([5]). *Let $(Q,*)$ be a left distributive quasigroup, $e\in Q$ and let*
$$a\cdot b=(a/e)*(e\backslash b).$$
Then $(Q,\cdot)$ is a Belousov-Onoi loop with respect to $\psi=L_e$, the companion mapping is $\varphi=R_e$ and
$$a*b=\varphi(a)\cdot\psi(b).$$
Moreover, different choices of e result in isomorphic loops.

Proof. First notice that $a*b=(a*e)\cdot(e*b)=\varphi(a)\cdot\psi(b)$. Indeed, both φ,ψ are permutations and φ is the companion for ψ, since $\varphi(a)\cdot\psi(a)=a$. To prove that ψ is an automorphism of $(Q,\cdot)$, we calculate for every $a,b\in Q$

$$\begin{aligned}\psi(ab)=e*ab&=e*((a/e)*(e\backslash b))\\&=(e*(a/e))*(e*(e\backslash b))\\&=((e*a)/e)*(e\backslash(e*b)=(e*a)\cdot(e*b)=\psi(a)\psi(b).\end{aligned}$$

In the third and fourth steps, we used left distributivity: in the latter case, since L_e is an automorphism of $(Q,*)$, we also have $L_e(x/y)=L_e(x)/L_e(y)$ for every x,y. To prove the condition (BO), we calculate for every $a,b\in Q$

$$\begin{aligned}\varphi(ab)\cdot\psi(ac)&=(ab*e)\cdot(e*ac)=ab*ac\\&=((a/e)*(e\backslash b))*((a/e)*(e\backslash c))\\&=(a/e)*((e\backslash b)*(e\backslash c))\\&=(a/e)*(e\backslash(b*c))=a\cdot(b*c)=a\cdot\varphi(b)\psi(c).\end{aligned}$$

In the fourth and fifth steps, we used left distributivity: in the latter case, using the fact that L_e^{-1} is also an automorphism of $(Q,*)$.

Let $e_1,e_2\in Q$ and consider an automorphism ρ of $(Q,*)$ such that $\rho(e_1)=e_2$ (for example, we can take $\rho=L_{e_2/e_1}$). Then ρ is an isomorphism of the corresponding loops $(Q,\cdot_1)$ and $(Q,\cdot_2)$, since

$$\rho(a\cdot_1 b)=\rho((a/e_1)*(e_1\backslash b))=(\rho(a)/\rho(e_1))*(\rho(e_1)\backslash\rho(b))=\rho(a)\cdot_2\rho(b)$$

for every $a,b\in Q$. □

If $(Q,\cdot)$ is a Belousov-Onoi loop with respect to ψ, the companion mapping φ is usually not an automorphism. In such a case, the representation of $(Q,*)$ over $(Q,\cdot)$ will be called *right linear*. In Proposition 5.7, we shall prove that φ is an automorphism if and only if the loop is commutative Moufang. Therefore, according to Theorem 3.3, we do not have a linear representation, unless we handle a (both-side) distributive quasigroup.

Still, the left distributive quasigroup $(Q,*)$ (formally, the algebra $(Q,*,\backslash,/)$) is *polynomially equivalent* to the Belousov-Onoi module $(Q,\cdot,\psi)$ (formally, the algebra $(Q,\cdot,\backslash^{\cdot},/^{\cdot},\psi,\psi^{-1})$): all operations in Proposition 5.4 were defined polynomially, the same can be shown about the division operations, and $\varphi(x)=x/^{\cdot}\psi(x)$ is a polynomial, too. In fact, we can think of the mapping φ as *quadratic* over the BO-module $(Q,\cdot,\psi)$, as the variable x appears only twice in its definition.

Combining Propositions 5.2 and 5.4, we can formulate the following representation theorem.

Theorem 5.5 ([5]). *The following are equivalent for a quasigroup $(Q,*)$:*

(1) *it is left distributive;*

(2) *it is right linear over a Belousov-Onoi loop (with respect to the automorphism used in the right linear representation).*

Example 5.6. The smallest non-associative Belousov-Onoi loops have order 15, and there are two of them (up to isomorphism). One is a B-loop, see Example 2.6. The other one can be constructed by a modification of the previous construction. Consider the loop $(\mathbb{Z}_5 \times \mathbb{Z}_3, \cdot)$ with

$$(a, x) \cdot (b, y) = (\varphi_{x,y} a + b + \theta_{x,y}, x + y)$$

where $\varphi_{x,y} \in \mathbb{Z}_5^*$ are as before, and $\theta_{x,y} \in \mathbb{Z}_5$ are given by the following table:

	0	1	2
0	0	0	0
1	0	-1	1
2	0	-2	2

It is straightforward to check that this is a BO-loop with respect to the automorphism $(a, x) \mapsto (-a + \delta_{x,2}, -x)$ where $\delta_{x,y} = 1$ if $x = y$ and $\delta_{x,y} = 0$ otherwise. It is not a B-loop, it does not even have the LIP. It is also an abelian extension of $\mathbb{Z}_5$ by $\mathbb{Z}_3$. If we set $\theta_{x,y} = 0$ for every x, y, we would have obtained the B-loop of Example 2.6.

Correspondingly, the smallest non-medial left distributive quasigroups have order 15, and there are two of them (up to isomorphism). One is involutory, see Example 4.4. The other one can be constructed as $(\mathbb{Z}_5 \times \mathbb{Z}_3, *)$ with

$$(a, x) * (b, y) = (\mu_{x,y} a - b + \tau_{x,y}, -x - y)$$

where $\mu_{x,y} \in \mathbb{Z}_5^*$ is as before, and $\tau_{x,y} = \delta_{x-y,1}$ for every x, y. (See [13, 14] for a generalization of this construction, originally suggested by Galkin [26].) □

5.2. Belousov-Onoi loops. Given the correspondence of Theorem 5.5, a natural question arises. What are these Belousov-Onoi loops? Can we use an established part of loop theory to investigate left distributive quasigroups? The current state of knowledge is unsatisfactory in this respect. In the rest of the section, we summarize most of the known results on BO-loops.

First of all, it is not even clear how to construct Belousov-Onoi loops which are not B-loops. All BO-loops of order less than 15 are abelian groups, and there are two non-associative BO-loops of order 15, see Example 5.6. Nowadays, these facts are easy to check on a computer, but back in the 1970s, this was realized only indirectly, via Theorem 5.5, using the theory of left distributive quasigroups. The first example of a left distributive quasigroup not isotopic to any Bol loop was constructed by Onoi in [67]. The construction is quite intricate, and occupies a major part of the paper: Onoi starts with 2×2 matrices over a certain non-associative ring with four elements, takes a quadratic operation on pairs of the matrices, and then creates a left distributive isotope; thus, the quasigroup has order 2^{16}. The smallest example, of order 15, was found later by Galkin in [26]. We see the situation twisted: it is not the loops that reveal properties of the quasigroups, it is the other way around!

Table 2 shows some enumeration results related to Belousov-Onoi loops. The upper part compares the numbers $L(n)$ of all loops, $BOM(n)$ of loops that turn into a non-trivial BO-module, and $BOL(n)$ of BO-loops, of order n up to isomorphism. The lower part compares the numbers $Q(n)$ of all quandles, $BOQ(n)$ of quandles that admit a Belousov-Onoi representation as in Proposition 5.2, and $LQ(n)$ of latin quandles (left distributive quasigroups), of order n up to isomorphism. The sequences $L(n)$, $Q(n)$ are well known [66], the other numbers were calculated using an exhaustive computer search.

n	1	2	3	4	5	6	7	8
$L(n)$	1	1	1	2	6	109	23746	106228849
$BOM(n)$	0	0	1	1	1	3	1	144
$BOL(n)$	1	0	1	1	1	0	1	3
$Q(n)$	1	1	3	7	22	73	298	1581
$BOQ(n)$	1	1	2	3	4	3	6	9
$LQ(n)$	1	0	1	1	3	0	5	2

Table 2: Enumeration of small loops and quandles related to the Belousov-Onoi representation.

In the rest of the section, we present a few results that relate the Belousov-Onoi loops to more established classes of loops, and specialize the correspondence between left distributive quasigroups and Belousov-Onoi loops, proved in Theorem 5.5, on two important subclasses: the distributive quasigroups, and the involutory left distributive quasigroups.

We start with a variation on [68, Theorem 2]. Our proof, based on Theorem 2.2 (the Pflugfelder's part), is much simpler.

Proposition 5.7. *Let $(Q,\cdot)$ be a loop, ψ an automorphism of $(Q,\cdot)$ and assume its companion mapping φ is a permutation. Then any two of the following properties imply the third:*

- *$(Q,\cdot)$ is a Belousov-Onoi loop with respect to ψ;*
- *$(Q,\cdot)$ is a commutative Moufang loop;*
- *φ is an automorphism.*

Proof. According to Theorem 2.2, $(Q,\cdot)$ is a commutative Moufang loop if and only if, for some mapping f on Q, the identity $f(x)y\cdot xz = f(x)x\cdot yz$ holds. Let $f=\varphi\psi^{-1}$ and substitute $x=\psi(a)$, $y=\varphi(b)$, $z=\psi(c)$. We obtain that $(Q,\cdot)$ is a commutative Moufang loop if and only if $\varphi(a)\varphi(b)\cdot\psi(a)\psi(c) = \varphi(a)\psi(a)\cdot\varphi(b)\psi(c) = a\cdot\varphi(b)\psi(c)$ for every $a,b,c\in Q$. Consider the following three expressions:

$$\begin{aligned} X &= \varphi(a)\varphi(b)\cdot\psi(a)\psi(c)\\ Y &= a\cdot\varphi(b)\psi(c)\\ Z &= \varphi(ab)\cdot\psi(a)\psi(c)\end{aligned}$$

We just proved that $X=Y$ for every $a,b,c\in Q$ iff $(Q,\cdot)$ is commutative Moufang. According to condition (BO), $Y=Z$ for every $a,b,c\in Q$ iff $(Q,\cdot)$ is a BO-loop with respect to ψ. And, obviously, $X=Z$ for every $a,b,c\in Q$ iff φ is an automorphism of $(Q,\cdot)$. □

Now we can reprove Belousov's result that every distributive quasigroup is linear over a commutative Moufang loop (a similar argument is presented in [68, Theorem 3]).

Proof of Theorem 3.3, (3) ⇒ (4). Let $(Q,*)$ be a distributive quasigroup, pick $e\in Q$ a let $a\cdot b=(a/e)*(e\backslash b)$. Since $(Q,*)$ is left distributive, $(Q,\cdot)$ is a BO-loop with respect to L_e, which in turn is an automorphism of $(Q,\cdot)$. Since $(Q,*)$ is right distributive, $(Q,\cdot)$ is also a right(!) BO-loop (this is irrelevant for us) with respect to R_e, which in turn is an automorphism of $(Q,\cdot)$. We showed that the companion of L_e is an automorphism, hence $(Q,\cdot)$ is a commutative Moufang loop by Proposition 5.7. □

Next we show that B-loops are precisely the BO-loops with respect to the left inverse mapping.

Proposition 5.8 ([5, Theorem 8]). *Let $(Q,\cdot)$ be a loop and $\psi(x)=x\backslash^{\cdot}1$. Then $(Q,\cdot)$ is a Belousov-Onoi loop with respect to ψ if and only if it is a B-loop.*

Proof. The backward implication was proved in Example 5.1, item 3. In the forward direction, condition (BO) with $b=1$ and $c=a$ says that $\varphi(a)\psi(a^2)=a\psi(a)=1$, and thus

$$\varphi(a)=1/^{\cdot}\psi(a^2)=1/^{\cdot}(a^2\backslash^{\cdot}1)=a^2$$

for every $a\in Q$. Hence, $(Q,\cdot)$ is a uniquely 2-divisible loop with the LAIP. Now, condition (BO), upon substitution of $\psi^{-1}(c)$ for c, says that $(ab)^2\cdot((a\backslash^{\cdot}1)\cdot c)=a\cdot b^2c$, and we can use Theorem 2.5 to conclude that $(Q,\cdot)$ is a Bol loop. □

With the aid of Proposition 5.8, we establish the correspondence between involutory left distributive quasigroups and B-loops. This connection has a rich history: it was first realized by Robinson in his 1964 PhD thesis, but published only 15 years later in [75]. Independently, Belousov and Florya [4, Theorem 3] noticed that involutory left distributive quasigroups are isotopic to Bol loops, but they did not formulate the full correspondence. Independently, the theorem was formulated by Kikkawa [52] (at the first glance, it is not obvious that his loop axioms are equivalent to those of B-loops, as he uses condition (2') of Theorem 2.5 instead of the Bol identity). The theorem was rediscovered once more in [62, Theorems 2.5 and 2.7]. Unlike all of the other representation theorems in the present paper, Theorem 5.9 has a fairly straightforward direct proof, and contemporary ATP systems can prove it within a second.

Theorem 5.9 ([52, 62, 75])**.** *The following are equivalent for a quasigroup $(Q,*)$:*

(1) *it is involutory left distributive;*

(2) *there is a B-loop $(Q,\cdot)$ such that $a*b = a^2\cdot b^{-1}$.*

Proof. (1) ⇒ (2) Consider the quasigroup operation $a\cdot b = (a/e)*(e\backslash b)$. According to Theorem 5.5, $(Q,\cdot)$ is a BO-loop with respect to L_e. If we prove that $L_e(x) = x\backslash^{\cdot}1$, Proposition 5.8 applies and $(Q,\cdot)$ is a B-loop. Then, clearly, the companion mapping is $\varphi(x) = x^2$, and thus $a*b = a^2\cdot b^{-1}$.

We need to check that $L_e(a) = e*a$ equals $a\backslash^{\cdot}1 = a\backslash^{\cdot}e$ for every $a\in Q$. We have $e*a = a\backslash^{\cdot}e$ iff $a\cdot(e*a) = e$ iff $(a/e)*a = e$ (we expanded the definition of $\cdot$). Now multiply the last identity by a/e from the left, and obtain $(a/e)*((a/e)*a) = (a/e)*e = a$, which is always true thanks to the involutory law.

(2) ⇒ (1) Left distributivity was verified in Proposition 5.2 through Example 5.1. It is involutory, as $a*(a*b) = a^2(a^2b^{-1})^{-1} = a^2(a^{-2}b) = b$ thanks to the AIP and LIP in Bruck loops. □

As far as we know, only two papers, [5, 68], are devoted to Belousov-Onoi loops. We state two more results here. The first one identifies some important subclasses of BO-loops, see [5, Theorem 2], [68, Theorem 1] and [5, Theorem 3], respectively.

Proposition 5.10 ([5, 68])**.** *Let $(Q,\cdot)$ be a Belousov-Onoi loop.*

(1) *It is Bol if and only if it is left alternative.*

(2) *It is Moufang iff it is right alternative, iff it has the RIP, iff the identity $(xy)^{-1} = y^{-1}x^{-1}$ holds, iff the identity $x\cdot yx = xy\cdot x$ holds.*

(3) *It is a group if and only if it is left alternative and every square is nuclear.*

The second is a characterization of Belousov-Onoi loops that matches well with Theorem 2.5 on B-loops.

Theorem 5.11 ([5])**.** *The following are equivalent for a loop $(Q,\cdot)$ with an automorphism ψ such that its companion mapping φ is a permutation:*

(1) *it satisfies the identity $\varphi(x)\cdot\psi(x)y = xy$ and it is left automorphic as a BO-module (i.e. the left inner mappings are automorphisms of $(Q,\cdot,\psi)$);*

(1′) *the identities* $\varphi(x) \cdot \psi(x)y = xy$ *and* $L_{x,y}\psi = \psi L_{x,y}$ *hold;*

(2) *it satisfies condition (BO).*

Proof sketch. The equivalence of (1') and (2) is proved in [5, Theorem 4]. Condition (1') is a special case of (1). It remains to prove that in any BO-loop $(Q,\cdot)$, every inner mapping $L_{x,y}$ is an automorphism of $(Q,\cdot,\psi)$. It respects ψ as postulated in (1'). According to Theorem 5.5, $(Q,\cdot)$ is isotopic to a left distributive quasigroup, and Belousov and Florya prove in [4, Theorem 2] that every loop isotope of a left distributive quasigroup (actually, more generally, of any F-quasigroup) is left automorphic. □

We are not aware of any general structural results on left distributive quasigroups proved using the correspondence of Theorem 5.5. Actually, with the efficient methods we will describe in Section 6, the correspondence could be used in the other direction, to investigate properties of Belousov-Onoi loops via left distributive quasigroups.

Nevertheless, in the involutory case, loop theory helps considerably, as the theory of Bruck loops is well developed. One example for all: Glauberman proved that finite B-loops are solvable, and that analogies of the Lagrange and Sylow theorems hold (see [31, Section 8] for precise statements). Since a B-loop $(Q,\cdot)$ and its corresponding involutory left distributive quasigroup $(Q,*)$ are polynomially equivalent, they share all the properties defined by polynomial operations. For instance, congruences and solvability. The polynomial correspondence uses a single constant, e, therefore, the subloops of $(Q,\cdot)$ are exactly the subquasigroups of $(Q,*)$ containing e. Since e can be chosen arbitrarily, the Lagrange and Sylow properties are shared by $(Q,*)$ as well. In Section 6.3, we put these results into a broader context.

6. Left distributive quasigroups: Homogeneous representation

6.1. Homogeneous representation. Our exposition in this section follows our recent paper [35] where many older ideas are collected and adjusted to the modern quandle setting. A reader interested in more details (proofs in particular), is recommended to consult [35]. Here we try to reference the original sources.

Recall that a quandle Q is *homogeneous*, if $\mathrm{Aut}(Q)$ acts transitively on Q. Since $\mathrm{LMlt}(Q)$ is a subgroup of $\mathrm{Aut}(Q)$, all connected quandles (and thus all left distributive quasigroups) are homogeneous.

It is not clear who came up with Construction 6.1. But it was certainly Galkin [24] who recognized its importance for representing self-distributive algebraic structures, followed independently by Joyce and others (perhaps a partial credit could be paid to Loos [57], too).

Construction 6.1 ([24, 40])**.** Let $(G,\cdot)$ be a group, H its subgroup, and ψ an automorphism of $(G,\cdot)$ such that $\psi(a)=a$ for every $a\in H$. Such a triple (G,H,ψ) will be called *admissible*. Denote G/H the set of left cosets $\{aH : a\in G\}$, and consider the binary algebra $\mathcal{Q}(G,H,\psi)=(G/H,*)$ with

$$aH * bH = a\psi(a^{-1}b)H.$$

It is straightforward to verify that $\mathcal{Q}(G,H,\psi)$ is a homogeneous quandle. If G is finite, then $\mathcal{Q}(G,H,\psi)$ is a quasigroup if and only if, for every $a,u\in G$, $a\psi(a^{-1})\in H^u$ implies $a\in H$. □

Note that the operation can be written as $aH*bH=\varphi(a)\psi(b)H$, where φ is the companion mapping to ψ, so this really is, in a way, a variation on the isotopy method. Also note that the special case $\mathcal{Q}(G,1,\psi)$, with the trivial subgroup $H=1$, is the same construction as in Example 5.3, item 2.

Example 6.2. According to Theorem 3.1, medial idempotent quasigroups are precisely the quasigroups $\mathcal{Q}(G,1,\psi)$ where G is an abelian group and ψ is an automorphism such that its companion is a permutation (and therefore an automorphism, too). □

In the present section, we will denote conjugation as $a^b=bab^{-1}$ (unlike most texts on group theory, we use the right-left composition of mappings, hence it is natural to use the dual notation for conjugation). Similarly, we will denote $a^G=\{a^g : g\in G\}$ the conjugacy class of a in G, $H^b=\{h^b : h\in H\}$, and $-^b$ the mapping $x\mapsto x^b$. If G is a group acting on a set X and $e\in X$, we will denote e^G the orbit containing e, and G_e the stabilizer of e.

The following observation appeared in many sources in various forms, its complete proof can be found e.g. in [35, Section 3].

Proposition 6.3. *Let $(Q,*)$ be a quandle and $e\in Q$. Let G be a normal subgroup of $\mathrm{Aut}(Q,*)$. Then $(G,G_e,-^{L_e})$ is an admissible triple and the orbit subquandle $(e^G,*)$ is isomorphic to the quandle $\mathcal{Q}(G,G_e,-^{L_e})$.*

Proof sketch. Since $-^{L_e}$ is a restriction of an inner automorphism to a normal subgroup, it is an automorphism of G. It is straightforward to check that it fixes the stabilizer pointwise. Consider the bijective mapping $f: G/G_e\to e^G$, $\alpha G_e\mapsto \alpha(e)$. Again, it is straightforward to check that this is a quandle isomorphism $\mathcal{Q}(G,G_e,-^{L_e})\simeq(e^G,*)$. □

Consider three particular choices of the normal subgroup: $G=\mathrm{Aut}(Q,*)$, $G=\mathrm{LMlt}(Q,*)$ and $G=\mathrm{LMlt}(Q,*)'$, respectively. If G acts transitively on Q, Proposition 6.3 claims the following:

(1) Every homogeneous quandle $(Q,*)$ is isomorphic to $\mathcal{Q}(G,G_e,-^{L_e})$ with $G=\mathrm{Aut}(Q,*)$.

(2) Every connected quandle $(Q,*)$ is isomorphic to $\mathcal{Q}(G,G_e,-^{L_e})$ with $G = \mathrm{LMlt}(Q,*)$. This will be called the *canonical representation* of $(Q,*)$.

(3) Every connected quandle $(Q,*)$ is isomorphic to $\mathcal{Q}(G,G_e,-^{L_e})$ with $G = \mathrm{LMlt}(Q,*)'$. This will be called the *minimal representation* of $(Q,*)$. (To make it work, one has to show that the actions of $\mathrm{LMlt}(Q,*)$ and $\mathrm{LMlt}(Q,*)'$ have identical orbits [24, 40].)

Corollary 6.4 ([40, Theorem 7.1]). *A quandle is isomorphic to $\mathcal{Q}(G,H,\psi)$ for some admissible triple (G,H,ψ) if and only if it is homogeneous.*

Why minimal representation? Galkin [24, Theorem 4.4] proved the following fact: if a connected quandle $(Q,*)$ is isomorphic to $\mathcal{Q}(G,H,\psi)$ for some admissible triple (G,H,ψ), then $\mathrm{LMlt}(Q)'$ embeds into a quotient of G. Hence, if Q is finite, the minimal representation is the one with the smallest group G.

Why canonical representation? Fix a set Q and an element e. We have a 1-1 correspondence between connected quandles $(Q,*)$ on one side, and certain configurations in transitive groups acting on Q on the other side. A *quandle envelope* is a pair (G,ζ) where G is a transitive group on Q and $\zeta \in Z(G_e)$ (here Z denotes the center) such that $\langle \zeta^G \rangle = G$. The correspondence is given by the following two mutually inverse mappings:

$$\begin{array}{rcl} \text{connected quandle} & \leftrightarrow & \text{quandle envelope} \\ (Q,*) & \rightarrow & (\mathrm{LMlt}(Q,*), L_e) \\ \mathcal{Q}(G,G_e,-^{\zeta}) & \leftarrow & (G,\zeta) \end{array}$$

If Q is finite, then an envelope (G,ζ) corresponds to a latin quandle if and only if $\zeta^{-1}\zeta^{\alpha}$ has no fixed point for every $\alpha \in G \smallsetminus G_e$. Moreover, two envelopes (G_1,ζ_1) and (G_2,ζ_2) yield isomorphic quandles if and only if there is a permutation f of Q such that $f(e)=e$, $\zeta_1^f = \zeta_2$ and $G_1^f = G_2$ (in particular, the two groups are isomorphic). See [35, Section 5] for details, and [35, Section 7] for a plenty of illustrative examples (the correspondence seems to be an original contribution of the paper).

Canonical representation is arguably the most powerful tool currently available to study connected quandles, and left distributive quasigroups in particular, as we shall see in the remaining part of the section.

6.2. Enumeration. Canonical representation allows to enumerate connected quandles (left distributive quasigroups in particular) with n elements, provided a classification of transitive groups of degree n. Currently, such a library is available for $n \le 47$. The enumeration of small connected quandles was carried out in [35, 90]. Here, in Table 3, we present the numbers of quasigroups, where $LD(n)$ refers to non-medial left distributive ones, and $ILD(n)$ to non-medial involutory left distributive ones, of order n up to isomorphism. We recall from Section 3.2 that $MI(n)$ denotes the number of medial idempotent quasigroups and can be determined by Hou's formulas [34].

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	**15**	16
$LD(n)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**2**	0
$ILD(n)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0
$MI(n)$	1	0	1	1	3	0	5	2	8	0	9	1	11	0	3	9

n	17	18	19	20	**21**	22	23	24	25	26	**27**	**28**	29	30	31	32
$LD(n)$	0	0	0	0	**2**	0	0	0	0	0	**32**	**2**	0	0	0	0
$ILD(n)$	0	0	0	0	**1**	0	0	0	0	0	**4**	**0**	0	0	0	0
$MI(n)$	15	0	17	3	5	0	21	2	34	0	30	5	27	0	29	8

n	**33**	34	35	**36**	37	38	**39**	40	41	42	43	44	**45**	46	47
$LD(n)$	**2**	0	0	**1**	0	0	**2**	0	0	0	0	0	**12**	0	0
$ILD(n)$	**1**	0	0	**0**	0	0	**1**	0	0	0	0	0	**3**	0	0
$MI(n)$	9	0	15	8	35	0	11	6	39	0	41	9	24	0	45

Table 3: Enumeration of small left distributive quasigroups.

From the historical perspective, the first serious attempt on enumeration was carried out by Galkin [26] who calculated (without a computer!) the numbers $LD(n)$ for $n < 27$, and found that $LD(27) \geq 3$. A few results in the involutory case can be found in an earlier paper by Nobusawa [64]. In [90], Vendramin enumerated connected quandles of size $n \leq 35$, which was the state-of-the-art in the classification of transitive groups at the time, but his algorithm works for larger orders as well.

One can make a few observations about Table 3. Most obviously, we do not see any left distributive quasigroups (medial or not) with $4k+2$ elements. This is true for every k, as proved by Stein already in the 1950s [83, Theorem 9.9].

Theorem 6.5 ([83]). *There are no left distributive quasigroups of order $4k+2$, for any $k \geq 0$.*

The fact is easy to observe in the medial case: any medial idempotent quasigroup of order $4k+2$ is linear over an abelian group which is the direct product of $\mathbb{Z}_2$ and a group of odd order; however, there is no idempotent quasigroup of order 2. Stein's remarkable argument uses a topological reasoning, constructing a triangulated polyhedron from the graph of the quasigroup and discussing parity of its Euler characteristic (for details, see [83] or [30, Section 6]). In [85], Stein observed that the result extends to all homogeneous quasigroups, since each of them is isotopic to an idempotent quasigroup and the same method as in the self-distributive case proves non-existence. In [24, Theorem 6.1], Galkin proved Stein's theorem using a short group theoretical argument about the minimal representation.

Let us note that connected quandles of order $4k+2$ do exist, although there are no connected quandles with $2p$ elements for any prime $p > 5$ [35, 59].

Our second observation about Table 3 is that there are severe restrictions on the admissible orders of non-medial left distributive quasigroups. Many gaps are justified by the following theorem.

Theorem 6.6 ([19, 32]). *Every connected quandle with p or p^2 elements, p prime, is medial.*

The prime case was proved by Galkin [24] for quasigroups, and by Etingof, Soloviev and Guralnick [19] for connected quandles. A conceptually simpler proof using canonical representation can be found in [35, Section 8], here is an outline. First, use a group-theoretical result by Kazarin: in a finite group G, if $|a^G|$ is a prime power, then $\langle a^G\rangle$ is solvable; with little work, it follows that if Q is a connected quandle of prime power size, then $\mathrm{LMlt}(Q)$ is solvable. Now recall that a transitive group (here: $\mathrm{LMlt}(Q)$) acting on a set of prime size (here: Q) is primitive, and apply a theorem of Galois stating that any finite solvable primitive group acts as a subgroup of the affine group over a finite field.

The prime square case for quasigroups is claimed by Galkin in [30] but never appeared in print; for connected quandles, it was solved by Graña [32]. For involutory left distributive quasigroups, the proof is substantially easier, see [64]. The prime cubed case is discussed in [1], but the classification is not easy to state.

We can also observe that there are no non-medial left distributive quasigroups of order 2^k for $k = 1, 2, 3, 4, 5$. However, this is not a general property: in fact, the first ever example of a left distributive quasigroup not isotopic to a Bol loop, constructed by Onoi [67], has 2^{16} elements. The smallest non-medial connected quandle with 2^k elements exists for $k = 5$, but we do not know the smallest k in the quasigroup case.

Our final observation is that there are precisely two non-medial left distributive quasigroups of order $3p$ for $p = 5, 7, 11, 13$. Two such examples were constructed for every prime $p \geq 5$ by Galkin in [26] (the construction was studied recently in a great detail in [13, 14], see also Example 5.6). It is an open problem whether there exist any other connected quandles with $3p$ elements.

6.3. Structural properties. We will mention a few subalgebra and congruence properties here. A finite quasigroup of order n has the *Lagrange property*, if the order of every subquasigroup divides n. It has the *Sylow property*, if, for every maximal prime power divisor p^k of n, there is a subquasigroup of order p^k (stronger versions of the Sylow property exist, and we refer to each particular paper for its own precise definition). Informally, a left distributive quasigroup is called *solvable*, if it can be constructed by a chain of extensions by medial quasigroups; formal definitions differ [25, 41, 65], but they seem to share the following property: a left distributive quasigroup is solvable if and only if its left multiplication group is solvable. (We note that it is not at all clear what is the "correct" notion of solvability for quasigroups and loops, see [82] for a thorough discussion; the particular choice made by Glauberman, following Bruck, is only one of the reasonable options.)

Finite involutory left distributive quasigroups are solvable and have the Lagrange and Sylow properties. This has been proved independently several times, using each of the three methods we have discussed: through the conjugation representation in [41], through the isotopy to B-loops (combining Theorem 5.9 and the results of Glauberman on B-loops [31]), and through the homogeneous representation in [28]. In each case, the underlying group theoretical result is Glauberman's Z*-theorem, which is used to show that the left multiplication group is solvable. An infinite counterexample to solvability is presented in [28].

Later, Galkin generalized the results into the non-involutory setting. In [25], he proves that every finite solvable left distributive quasigroup has the Lagrange property, but not necessarily the Sylow property (a counterexample of order 15 exists). In [27], he proves the Sylow property under the additional assumption that the order of the quasigroup, and the order of its translations, are coprime (this is always true in the involutory case).

Recall that all left distributive quasigroups isotopic to a group admit a homogeneous representation of the form $\mathcal{Q}(G,1,\psi)$, cf. Example 5.3. They also satisfy the Lagrange and Sylow properties [24, Theorem 5.3]. This fact is used to show an important structural feature: a finite left distributive quasigroup with no non-trivial subquasigroups is medial [24, Theorems 5.5 and 7.2].

More information about Galkin's results on left distributive quasigroups can be found in his survey paper [30, Section 6]. A part of Galkin's theory was translated to English and clarified in [91].

7. Open problems

Several interesting problems appeared to us while writing the paper.

7.1. Commutator theory over "non-associative modules". Universal algebra develops a commutator theory based on the notion of *abelianess*, related to affine representation over classical modules (see [82] for the commutator theory adapted to loops, and the references thereof). For instance, Theorem 3.1 can be explained in this manner. Is there a meaningful weakening of the principle of abelianess, related to affine representation over some sort of "non-associative modules"? A one that would, for instance, explain Theorem 3.2? To what extent the module theoretic methods can be adapted to the non-associative setting?

7.2. Non-idempotent generalization of left distributive quasigroups. Find a "non-idempotent generalization" of Theorem 5.5: describe the class of quasigroups (whose idempotent members are precisely the left distributive quasigroups) that are right affine over Belousov-Onoi loops; perhaps, impose an additional condition on the representation in order to obtain an elegant description of the class. Theorem 3.2 shall follow as an easy consequence of this generalization, just as it happens in the idempotent case (see Section 5.2). We are not aware of any results even in the involutory case (generalizing Theorem 5.9).

7.3. Enumeration. The generic problem is, to extend all enumeration results presented in this paper. Perhaps the most interesting questions are:

1. distributive and trimedial quasigroups of order 3^5;
2. commutative Moufang loops of order 3^6 and the corresponding enumeration of distributive and trimedial quasigroups of order 3^6;
3. connected quandles and left distributive quasigroups of order $3p$, p prime, or more generally, pq, p, q primes;
4. left distributive quasigroups of order 2^k, $k > 5$ (cf. [67]).

Acknowledgement. I am indebted to my former student Jan Vlachý for a thorough research on Galkin's papers and for explaining me their contents and significance. His remarkable student project [91] on enumeration of small left distributive quasigroups convinced me that this is the right approach to left distributive quasigroups in particular, and connected quandles in general.

References

[1] **G. Bianco**, PhD Thesis, University of Ferrara (2015).

[2] **V.D. Belousov**, *On structure of distributive quasigroups*, (Russian), Mat. Sb. (N.S.) **50(92)** (1960), 267–298.

[3] **V.D. Belousov**, *Fundametals of the theory of quasigroups and loops*, (Russian), Nauka, Moskva (1967).

[4] **V.D. Belousov and I.A. Florya**, *On left-distributive quasigroups*, (Russian), Bul. Akad. Ştiinţe RSS Moldoven. **7** (1965), 3–13.

[5] **V.D. Belousov and V.I. Onoi**, *On loops isotopic to left distributive quasigroups*, (Russian), Mat. Issled. **25** (1972), 135–152.

[6] **L. Bénéteau**, *The geometry of distributive quasigroups*, Rend. Semin. Math. Brescia **7** (1984), 57–65.

[7] **L. Bénéteau**, *Commutative Moufang loops and related groupoids*, in: O. Chein, H. O. Pflugfelder, J.D.H. Smith (eds.), *Quasigroups and Loops: Theory and Applications*, Sigma Series in Pure Math. **9**, Heldermann Verlag (1990), 115–142.

[8] **C. Bergman**, *Universal algebra: Fundamentals and selected topics*, Chapman & Hall/CRC Press (2011).

[9] **R.H. Bruck**, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. **55** (1944), 19–52.

[10] **R.H. Bruck**, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer Verlag, Berlin-Göttingen-Heidelberg (1958).

[11] **C. Burstin and W. Mayer**, *Distributive Gruppen von endlicher Ordnung*, J. reine und angew. Math. **160** (1929), 111–130.

[12] **J.S. Carter**, *A survey of quandle ideas*, in: L.H. Kauffman (ed.) et al., *Introductory lectures on knot theory,* Series on Knots and Everything **46**, World Scientific (2012), 22–53.

[13] **W.E. Clark, M. Elhamdadi, X. Hou, M. Saito and T. Yeatman**, *Connected quandles associated with pointed abelian groups*, Pac. J. Math. **264** (2013), 31–60.

[14] **W.E. Clark and X. Hou**, *Galkin quandles, pointed abelian groups, and sequence* $A000712$, Electron. J. Comb. **20** (2013), no. 1, P45, 8 pp.

[15] **P. Dehornoy**, *Braids and self-distributivity*, Progress in Math. **192**, Birkhäuser, Basel (2000).

[16] **D. Donovan, T. Griggs, T. McCourt, J. Opršal and D. Stanovský**, *Distributive and anti-distributive Mendelsohn triple systems*, `http://arxiv.org/abs/1411.5194`.

[17] **A. Drápal**, *Group isotopes and a holomorphic action*, Results in Math. **54** (2009), 253–272.

[18] **A. Drápal**, *A simplified proof of Moufang's theorem*, Proc. Amer. Math. Soc. **139** (2011), 93–98.

[19] **P. Etingof, A. Soloviev and R. Guralnick**, *Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements*, J. Algebra **242** (2001), 709–719.

[20] **B. Fischer**, *Distributive Quasigruppen endlicher Ordnung*, Math. Z. **83** (1964), 267–303.

[21] **A. Fish, A. Lisitsa and D. Stanovský**, *Combinatorial approach to knot recognition*, in: R. Horn (ed.), *Embracing global computing in emerging economies*, Commun. in Computer and Information Science, Springer (to appear).

[22] **O. Frink**, *Symmetric and self-distributive systems*, Am. Math. Monthly **62** (1955), 697–707.

[23] **V.M. Galkin**, *Finite distributive quasigroups*, (Russian), Mat. Zametki **24** (1978), 39–41.

[24] **V.M. Galkin**, *Left distributive finite order quasigroups*, (Russian), Mat. Issled. **51** (1979), 43–54.

[25] **V.M. Galkin**, *φ-groups and left distributive quasigroups*, (Russian) Preprint VINITI No. 4406-81, Gor'kovskiy politechnicheskiy tekhnicheskiy institut, Gorkiy (1981).

[26] **V.M. Galkin**, *Left distributive quasigroups of small orders*, (Russian), Preprint VINITI No. 6510-84, Gor'kovskiy politechnicheskiy tekhnicheskiy institut, Gorkiy (1984).

[27] **V.M. Galkin**, *Sylow properties in a class of quasigroups*, (Russian), Mat. Zametki **36** (1984), 617–620.

[28] **V.M. Galkin**, *On symmetric quasigroups*, (Russian), Uspekhi mat. nauk **39** (1984), no. 6, 191–192.

[29] **V.M. Galkin**, *On the Fischer-Smith theorem*, J. Soviet Math. **32** (1988), no. 11, 23–30.

[30] **V.M. Galkin**, *Quasigroups*, J. Soviet Math. **49** (1990), 941–967 (translation from Itogi nauki i tekhniki **26** (1988), 3–44).

[31] **G. Glauberman**, *On loops of odd order*, J. Algebra **1** (1964), 374–396.

[32] **M. Graña**, *Indecomposable racks of order p^2*, Beiträge Algebra Geom. **45** (2004), 665–676.

[33] **D. Herbera, T. Kepka and P. Němec**, *Hamiltonian selfdistributive quasigroups*, J. Algebra **289** (2005), 70–104.

[34] **X. Hou**, *Finite modules over $\mathbb{Z}[t, t^{-1}]$*, J. Knot Theory Ramifications **21** (2012), no. 8, 1250079, 28 pp.

[35] **A. Hulpke, D. Stanovský and P. Vojtěchovský**, *Connected quandles and transitive groups*, `http://arxiv.org/abs/1409.2249`.

[36] **J. Ježek and T. Kepka**, *Notes on distributive groupoids*, Comment. Math. Univ. Carolin. **24** (1983), 237–249.

[37] **J. Ježek and T. Kepka**, *Distributive groupoids and symmetry-by-mediality*, Algebra Universalis **19** (1984), 208–216.

[38] **J. Ježek and T. Kepka**, *Selfdistributive groupoids of small orders*, Czech. Math. J. **47** (1997), 463–468.

[39] **J. Ježek, T. Kepka and P. Němec**, *Distributive groupoids*, Rozpravy ČSAV **91** (1981).

[40] **D. Joyce**, *Classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra **23** (1982), 37–65.

[41] **M. Kano, H. Nagao and N. Nobusawa**, *On finite homogeneous symmetric sets*, Osaka J. Math. **13** (1976), 399–406.

[42] **T. Kepka**, *Quasigroups which satisfy certain generalized forms of the Abelian identity*, Čas. pěst. mat. **100** (1975), 46–60.

[43] **T. Kepka**, *Structure of triabelian quasigroups*, Comment. Math. Univ. Carolin. **17** (1976), 229–240.

[44] **T. Kepka**, *Distributive Steiner quasigroups of order 3^5*, Comment. Math. Univ. Carolin. **19** (1978), 389–401.

[45] **T. Kepka**, *Distributive division groupoids*, Math. Nachr. **87** (1979), 103–107.

[46] **T. Kepka, L. Bénéteau and J. Lacaze**, *Small finite trimedial quasigroups*, Commun. Algebra **14** (1986), 1067–1090.

[47] **T. Kepka, M. Kinyon and J.D. Phillips**, *The structure of F-quasigroups*, J. Algebra **317** (2007), 435–461.

[48] **T. Kepka, M. Kinyon and J.D. Phillips**, *F-quasigroups and generalized modules*, Comment. Math. Univ. Carolin. **49** (2008), 249–257.

[49] **T. Kepka and P. Němec**, *Commutative Moufang loops and distributive groupoids of small orders*, Czech. Math. J. **31(106)** (1981), 633–669.

[50] **T. Kepka and P. Němec**, *T-quasigroups. I, II*, Acta Univ. Carolin. Math. Phys. **12** (1972), no. 1, 39–49; no. 2, 31–49.

[51] **H. Kiechle**, *Theory of K-loops*, Lecture Notes in Math. **1778** (2002).

[52] **M. Kikkawa**, *On some quasigroups of algebraic models of symmetric spaces*, Mem. Fac. Lit. Sci., Shimane Univ. (Natur. Sci.) **6** (1973), 9–13.

[53] **M. Kikkawa**, *On some quasigroups of algebraic models of symmetric spaces II*, Mem. Fac. Lit. Sci., Shimane Univ. (Natur. Sci.) **7** (1974), 29–35.

[54] **M. Kikkawa**, *Kikkawa loops and homogeneous loops*, Comment. Math. Univ. Carolin. **45** (2004), 279–285.

[55] **M. Kinyon and J.D. Phillips**, *A note on trimedial quasigroups*, Quasigroups and Related Systems **9** (2002), 65–66.

[56] **M. Kinyon and P. Vojtěchovský**, *Primary decompositions in varieties of commutative diassociative loops*, Commun. Algebra **37** (2009), 1428–1444.

[57] **O. Loos**, *Symmetric spaces*, J. Benjamin, New York (1969).

[58] **S.V. Matveev**, *Distributive groupoids in knot theory*, Math. USSR - Sbornik **47** (1984), 73–83.

[59] **J. McCarron**, *Connected quandles with order equal to twice an odd prime*, `http://arxiv.org/abs/1210.2150`.

[60] **D. Moskovich**, *Associativity vs. Distributivity*, Low Dimensional Topology Blog, July 21, 2014, `https://ldtopology.wordpress.com/2014/07/21/associativity-vs-distributivity`.

[61] **D C. Murdoch**, *Structure of abelian quasi-groups*, Trans. Amer. Math. Soc. **49** (1941), 392–409.

[62] **P. Nagy and K. Strambach**, *Loops, their cores and symmetric spaces*, Israel J. Math. **105** (1998), 285–322.

[63] **S. Nelson**, *The combinatorial revolution in knot theory*, Notices Amer. Math. Soc. **58** (2011), 1553–1561.

[64] **N. Nobusawa**, *On symmetric structures of a finite set*, Osaka J. Math. **11** (1974), 569–575.

[65] **N. Nobusawa**, *Some structure theorems on pseudo-symmetric sets*, Osaka J. Math. **20** (1983), 727–734.

[66] **OEIS Foundation Inc.**, *The on-line encyclopedia of integer sequences*, `http://oeis.org`.

[67] **V.I. Onoi**, *Left distributive quasigroups that are left homogeneous over a quasigroup*, (Russian), Bul. Akad. Ştiinţe RSS Moldoven. **2** (1970), 24–31.

[68] **V.I. Onoi**, *A connection between S-loops and Moufang loops*, (Russian), Mat. Issled. **7** (1972), 197–212.

[69] **C.S. Peirce**, *On the algebra of logic*, Amer. J. Math. **3** (1880), 15–57.

[70] **H.O. Pflugfelder**, *A special class of Moufang loops*, Proc. Amer. Math. Soc. **26** (1970), 583–586.

[71] **H.O. Pflugfelder**, *Quasigroups and loops: introduction*, Sigma Series in Pure Mathematics **7**, Heldermann Verlag (1990).

[72] **H.O. Pflugfelder**, *Historical notes on loop theory*, Comment. Math. Univ. Carolin. **41** (2000), 359–370.

[73] **J.D. Phillips and D.Stanovský**, *Automated theorem proving in quasigroup and loop theory*, Artificial Intelligence Commun. **23** (2010), 267–283.

[74] **R.S. Pierce**, *Symmetric groupoids*, Osaka J. Math. **15** (1978), 51–76.

[75] **D.A. Robinson**, *A loop-theoretic study of right-sided quasigroups*, Ann. Soc. Sci. Bruxelles **93** (1979), 7–16.

[76] **E. Schröder**, *Über algorithmen und Calculi*, Arch. der Math. und Phys. **5** (1887), 225–278.

[77] **J.D.H. Smith**, *Finite distributive quasigroups*, Math. Proc. Cambridge Philos. Soc. **80** (1976), 37–41.

[78] **J.D.H. Smith**, *Commutative Moufang loops: the first 50 years*, Algebras Groups Geom. **2** (1985), 209–234.

[79] **J.D.H. Smith**, *An introduction to quasigroups and their representations*, Studies in Advanced Math., Chapman & Hall/CRC, Boca Raton (2007).

[80] **J.-P. Soublin**, *Étude algébrique de la notion de moyenne*, J. Math. Pures Appl. **50** (1971), 53–264.

[81] **D. Stanovský**, *Distributive groupoids are symmetric-by-medial: An elementary proof*, Comment. Math. Univ. Carolin. **49** (2008), 541–546.

[82] **D. Stanovský and P. Vojtěchovský**, *Abelian extensions and solvable loops*, Results in Math. **66** (2014), 367–384.

[83] **S.K. Stein**, *On the foundations of quasigroups*, Trans. Amer. Math. Soc. **85** (1957), 228–256.

[84] **S.K. Stein**, *Left-distributive quasigroups*, Proc. Amer. Math. Soc. **10** (1959), 577–578.

[85] **S.K. Stein**, *Homogeneous quasigroups*, Pacific J. Math. **14** (1964), 1091–1102.

[86] **A.K. Suschkewitsch**, *On a generalization of the associative law*, Trans. Amer. Math. Soc. **31** (1929), 204–214.

[87] **M. Takasaki**, *Abstractions of symmetric transformations*, (Japanese), Tôhoku Math. J. **49** (1943), 143–207.

[88] **K. Toyoda**, *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221–227.

[89] **N. Umaya**, *On symmetric structure of a group*, Proc. Japan Acad. **52** (1976), 174–176.

[90] **L. Vendramin**, *On the classification of quandles of low order*, J. Knot Theory Ramifications **21** (2012), no. 9, 1250088.

[91] **J. Vlachý**, *Small left distributive quasigroups*, Bachelor's Thesis, Charles University in Prague (2010), `https://is.cuni.cz/webapps/zzp`.

Received April 30, 2015

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic
Department of Information Systems and Mathematical Modeling, International IT University, Almaty, Kazakhstan
E-mail: stanovsk@karlin.mff.cuni.cz

Quasigroups and Related Systems **23** (2015), 129 − 163

Three lectures on automorphic loops

Petr Vojtěchovský

Abstract. These notes accompany a series of three lectures on automorphic loops to be delivered by the author at Workshops Loops '15 (Ohrid, Macedonia, 2015). Automorphic loops are loops in which all inner mappings are automorphisms.

The first paper on automorphic loops appeared in 1956 and there has been a surge of interest in the topic since 2010. The purpose of these notes is to introduce the methods used in the study of automorphic loops to a wider audience of researchers working in nonassociative mathematics.

In the first lecture we establish basic properties of automorphic loops (flexibility, power-associativity and the antiautomorphic inverse property) and discuss relations of automorphic loops to Moufang loops.

In the second lecture we expand on ideas of Glauberman and investigate the associated operation $(x^{-1}\backslash(y^2x))^{1/2}$ and similar concepts, using a more modern approach of twisted subgroups. We establish many structural results for commutative and general automorphic loops, including the Odd Order Theorem.

In the last lecture we look at enumeration and constructions of automorphic loops. We show that there are no nonassociative simple automorphic loops of order less than 4096, we study commutative automorphic loops of order pq and p^3, and introduce two general constructions of automorphic loops.

The material is newly organized and sometimes new, shorter proofs are given.

Contents

2010 Mathematics Subject Classification: Primary: 20N05.

Keywords: Automorphic loop, commutative automorphic loop, Γ-loop, Moufang loop, Bruck loop, Bol loop, Lie ring, twisted subgroup.

Research partially supported by the Simons Foundation Collaboration Grant 210176.

Introduction

The purpose of these notes is to give a gentle introduction into the theory of automorphic loops that nevertheless captures the main ideas of current investigation. Due to the limited scope of the lectures, not all proofs are included and not all known results about automorphic loops are stated. A survey article on automorphic loops that attempts to remedy both of these shortcomings is under preparation by the author and will appear elsewhere.

Let $Q = (Q, \cdot, \backslash, /, 1)$ be a loop, where we also write xy to denote the product $x \cdot y$. For $x \in Q$, let

$$L_x : Q \to Q,\ L_x(y) = xy \qquad \text{and} \qquad R_x : Q \to Q,\ R_x(y) = yx$$

be the *left* and *right translation by* x, respectively. The permutation group

$$\mathrm{Mlt}(Q) = \langle L_x,\, R_x \,:\, x \in Q\rangle$$

is called the *multiplication group of* Q, and its subloop

$$\mathrm{Inn}(Q) = \langle \varphi \in \mathrm{Mlt}(Q) \,:\, \varphi(1) = 1\rangle$$

is the *inner mapping group of* Q.

Denote by $\mathrm{Aut}(Q)$ the automorphism group of Q. An *automorphic loop* (or *A-loop*) is a loop Q in which every inner mapping is an automorphism, that is, $\mathrm{Inn}(Q) \le \mathrm{Aut}(Q)$. Note that groups are automorphic loops, but the converse is certainly not true.

The following multiplication table specifies a nonassociative automorphic loop of the smallest possible order, which we will call Q_6:

Q_6	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	6	3	5
3	3	5	1	2	6	4
4	4	3	6	5	1	2
5	5	6	2	1	4	3
6	6	4	5	3	2	1

.

Properties of Q_6 can be checked in the `GAP` [19] package `LOOPS` [38], for instance.

Bruck proved [5] that in any loop

$$\mathrm{Inn}(Q) = \langle L_{x,y},\, R_{x,y},\, T_x \,:\, x,\, y \in Q\rangle,$$

where

$$L_{x,y}(z) = (yx)\backslash(y(xz)), \quad R_{x,y}(z) = ((zx)y)/(xy), \quad \text{and} \quad T_x(y) = x\backslash(yx).$$

It is also well known that a mapping between two loops is a homomorphism of loops if and only if it respects the multiplication operation. Because this fact is of crucial importance for automorphic loops, we give a short proof:

Let $f : (A, \cdot_A, \backslash_A, /_A, 1_A) \to (B, \cdot_B, \backslash_B, /_B, 1_B)$ be a mapping between loops such that $f(x \cdot_A y) = f(x) \cdot_B f(y)$ for every x, $y \in A$. Then $f(x) \cdot_B f(x \backslash_A y) = f(x \cdot_A (x \backslash_A y)) = f(y)$ and therefore $f(x \backslash_A y) = f(x) \backslash_B f(y)$ for every x, $y \in Q$. The argument for right division is dual, and the property $f(1_A) = 1_B$ is obtained by cancelation from $f(1_A) = f(1_A \cdot_A 1_A) = f(1_A) \cdot_B f(1_A)$.

It follows that a loop Q is an automorphic loop if and only if for every x, $y \in Q$ the inner mappings $L_{x,y}$, $R_{x,y}$ and T_x respect multiplication. Consequently, the class of automorphic loops is a subvariety of the variety of loops, consisting of all loops satisfying the axioms

$$(yx)\backslash(y(x(uv))) = ((yx)\backslash(y(xu)))((yx)\backslash(y(xv))), \tag{A$_\ell$}$$

$$(((uv)x)y)/(xy) = (((ux)y)/(xy))(((vx)y)/(xy)), \tag{A$_r$}$$

$$x\backslash((uv)x) = (x\backslash(ux))(x\backslash(vx)). \tag{A$_m$}$$

In particular, subloops, factor loops and homomorphic images of automorphic loops are again automorphic loops.

We call a loop *left automorphic* if (A_ℓ) holds, *right automorphic* if (A_r) holds, and *middle automorphic* if (A_m) holds.

The axioms (A_ℓ), (A_r), (A_m) are somewhat long and intimidating, certainly much more so than the axiom

$$(xy)(zx) = (x(yz))x \tag{M}$$

defining Moufang loops, for instance. But the message of the axioms is easy to remember—“inner mappings respect multiplication”—and, as we shall see, automorphic loops are very much amenable to algebraic investigation.

Such an investigation started in earnest in 1956 with the work of Bruck and Paige [6]. We will retrace some of their steps, for instance by proving that automorphic loops are power-associative. The main contribution of [6], which we will not follow here, was to demonstrate that diassociative automorphic loops share many properties with Moufang loops (which are always diassociative, by Moufang's theorem [36]).

The conjecture that every diassociative automorphic loop is Moufang is implicit in [6], but its proof remained elusive for 45 years. The conjecture was established for the special case of commutative loops by Osborn in 1958 [41]. Since commutative Moufang loops are automorphic by [5] (or see Proposition 1.14), it follows from Osborn's result that commutative Moufang loops are precisely commutative diassociative automorphic loops. The full conjecture was finally confirmed by Kinyon, Kunen and Phillips in 2002 [33].

Following a few sporadic results in late 1900s and early 2000s, of which we mention [14, 17, 32, 39, 43], automorphic loops became one of the focal areas in loop theory after the work of Jedlička, Kinyon and the author on commutative automorphic loops [25, 26] was circulated. It is worth mentioning that some results of [25] were first obtained by automated deduction [35], which remains influential in this field. But once the initial hurdles were cleared, the theory opened up to more traditional modes of investigation.

New results by many authors followed in quick succession. We mention two highlights: Odd Order Theorem for automorphic loops [34], and solvability of finite commutative automorphic loops [23].

The field remains active and we hope that these survey notes will attract new researchers to automorphic loops and related areas. Open problems can be found in the last section of this paper.

From now on we will employ the following notational conventions in order to save parentheses and improve legibility. The division operations are less binding than juxtaposition, and the explicit $\cdot$ multiplication is less binding than divisions and juxtaposition. For instance, $x/y\cdot y\backslash zy$ means $(x/y)(y\backslash(zy))$.

Lecture 1: Basic properties

In this section we establish some basic properties of automorphic loops. Most of these properties were known already to Bruck and Paige [6], except that they were not aware of the fact that automorphic loops have the antiautomorphic inverse property (see [29] or Proposition 1.4) and its consequences (one of the axioms (A_ℓ), (A_r) can be ommitted by Theorem 1.6, and the left and right nuclei coincide by Theorem 1.11). Of course, they also did not know that diassociative automorphic loops are Moufang [33], a result that we have incorporated without proof into Theorem 1.12.

Many proofs presented in this section shorten older arguments. We do not hesitate to prove even folklore results to better show to the reader that most result in this section can be derived quickly from first principles. In this spirit, consider:

Lemma 1.1. *Let Q be a loop and $\varphi\in\mathrm{Aut}(Q)$. Then*

$$\varphi L_x^{\pm1}\varphi^{-1}=L_{\varphi(x)}^{\pm1},\quad \varphi R_x^{\pm1}\varphi^{-1}=R_{\varphi(x)}^{\pm1},$$
$$\varphi T_x^{\pm1}\varphi^{-1}=T_{\varphi(x)}^{\pm1},\quad \varphi L_{x,y}^{\pm1}\varphi^{-1}=L_{\varphi(x),\varphi(y)}^{\pm1},\quad \varphi R_{x,y}^{\pm1}\varphi^{-1}=R_{\varphi(x),\varphi(y)}^{\pm1}$$

for every x, $y\in Q$.

Proof. We have $\varphi L_x\varphi^{-1}(y)=\varphi(x\cdot\varphi^{-1}(y))=\varphi(x)\cdot\varphi(\varphi^{-1}(y))=\varphi(x)\cdot y=L_{\varphi(x)}(y)$, so $\varphi L_x\varphi^{-1}=L_{\varphi(x)}$. Then $\varphi L_x^{-1}\varphi^{-1}=(\varphi L_x\varphi^{-1})^{-1}=L_{\varphi(x)}^{-1}$. The argument for R_x is similar. Then $\varphi T_x\varphi^{-1}=\varphi L_x^{-1}R_x\varphi^{-1}=\varphi L_x^{-1}\varphi^{-1}\varphi R_x\varphi^{-1}=L_{\varphi(x)}^{-1}R_{\varphi(x)}=T_{\varphi(x)}$, and so on. □

Thus in any loop Q, the automorphism group $\mathrm{Aut}(Q)$ acts on $\mathrm{Mlt}(Q)$ and on $\mathrm{Inn}(Q)$ by conjugation, mapping left inner mappings to left inner mappings, and so on. If Q is an automorphic loop, then the action of $\mathrm{Aut}(Q)$ induces an action of $\mathrm{Inn}(Q)$.

1.1. Flexibility and power-associativity

A loop Q is *flexible* if $x(yx) = (xy)x$ holds for every x, $y \in Q$. A consequence of flexibility is that every element x has a (unique) two-sided inverse x^{-1}. Indeed, if x^ℓ, x^r ar the left and right inverses of x, respectively, then $x = x(x^\ell x) = (xx^\ell)x$, so $xx^\ell = 1 = xx^r$ and $x^\ell = x^r$.

Proposition 1.2 ([6, p. 311])**.** *Every middle automorphic loop is flexible.*

Proof. Suppose that Q satisfies (A_m). Then $T_x(xy) = T_x(x) \cdot T_x(y)$, and multiplying this equality by x on the left yields $(xy)x = x(x\backslash xx \cdot x\backslash yx) = x(x \cdot x\backslash yx) = x(yx)$. □

We remark that there exists a loop (of order 6) that is both left and right automorphic, yet does not posses two-sided inverses, so is also not flexible.

A loop Q is said to be *power-associative* if for every $x \in Q$ the subloop $\langle x\rangle$ of Q generated by x is associative. For a prime p, a power-associative loop Q is said to be a *p-loop* if every element of Q has order that is a power of p.

Assuming two-sided inverses, a general strategy for proving power-associativity is as follows: Define *nominal powers* $x^{[n]}$ by letting $x^{[0]} = 1$, $x^{[k+1]} = xx^{[k]}$ and $x^{[-k]} = (x^{[k]})^{-1}$. Then it is not hard to show by induction that Q is power-associative if and only if

$$x^{[i]}(x^{[j]}x^{[k]}) = (x^{[i]}x^{[j]})x^{[k]} \tag{1.1}$$

for all i, j, $k \in \mathbb{Z}$. A typical proof of (1.1) in a given variety of loops is based on a careful induction. In automorphic loops, however, Bruck and Paige [6] employed an ingenious argument that we will essentially follow here.

Note that for any loop Q and a subset A of $\mathrm{Aut}(Q)$ the set

$$\mathrm{Fix}(A) = \{x \in Q \,:\, \varphi(x) = x \text{ for every } \varphi \in A\}$$

of common fixed points of automorphisms from A is a subloop of Q.

Proposition 1.3 ([6, Theorems 2.4 and 2.6])**.** *Every automorphic loop is power-associative and satisfies $(x^iy)x^j = x^i(yx^j)$, $x^i(x^jy) = x^j(x^iy)$, $(yx^i)x^j = (yx^j)x^i$ for every i, $j \in \mathbb{Z}$.*

Proof. Our loop Q is flexible by Proposition 1.2, which implies that $x \in \mathrm{Fix}(L_{y,x})$ and hence $\langle x\rangle \le \mathrm{Fix}(L_{y,x})$. In particular, $(xy)x^{[j]} = x(yx^{[j]})$. (Note that we have not used (A_r) yet.) This means that the inner mapping $R^{-1}_{yx^{[j]}}R_{x^{[j]}}R_y$ fixes x, thus also $x^{[i]}$, and we have $(x^{[i]}y)x^{[j]} = x^{[i]}(yx^{[j]})$. As a special case we obtain (1.1), which implies power-associativity. Then x^i is well-defined, coincides with $x^{[i]}$, and $(x^iy)x^j = x^i(yx^j)$ follows.

The inner mapping $R_{xy}^{-1}L_xR_y$ trivially fixes x, so also x^i. This shows that $R_{x^iy}^{-1}L_{x^i}R_y$ fixes x, so also x^j, and $x^i(x^jy) = x^j(x^iy)$ follows. The last identity is proved dually. □

Note that the identities of Proposition 1.3 say that for a fixed x in an automorphic loop Q, the group $\langle L_{x^i},\, R_{x^i} \,:\, i \in \mathbb{Z}\rangle$ is commutative.

1.2. Antiautomorphic inverse property

A loop with two-sided inverses has the *antiautomorphic inverse property* if it satisfies the identity

$$(xy)^{-1} = y^{-1}x^{-1}. \tag{1.2}$$

We are now going to show that every automorphic loop has the antiautomorphic inverse property. For reasons that become clear, we prove a seemingly stronger result, assuming only (A_ℓ) and (A_m). We give a shorter proof than in [29].

Proposition 1.4 (compare [29, Proposition 7.4]). *Every loop that is both left and middle automorphic has the antiautomorphic inverse property.*

Proof. In the proof of Proposition 1.3 we established $(xy)x^{[j]} = x(yx^{[j]})$ using only (A_ℓ) and (A_m). In particular, we can use $(xy)x^{-1} = x(yx^{-1})$ below. Consider $\psi = L_y^{-1}L_xL_{x\backslash y} = L_{x\backslash y,x} \in \mathrm{Aut}(Q)$. Since $\psi((x\backslash y)^{-1}) = y\backslash x$, we also have $\psi(x\backslash y) = (y\backslash x)^{-1}$. Then $(y\backslash x)^{-1}\cdot y^{-1} = (y\backslash x)^{-1}\cdot y\backslash 1 = \psi(x\backslash y)\psi((x\backslash y)\backslash x^{-1}) = \psi(x^{-1}) = y\backslash(x\cdot(x\backslash y)x^{-1}) = y\backslash(x(x\backslash y)\cdot x^{-1}) = y\backslash yx^{-1} = x^{-1}$. Then (1.2) follows by substituting yx for x. □

In general, the antiautomorphic inverse property has a similar effect as commutativity in the sense that it allows one to deduce properties about right concepts from properties of left concepts, and vice versa. In the following well-known lemma, let J be the inversion mapping $x \mapsto x^{-1}$.

Lemma 1.5. *Let Q be an antiautomorphic inverse property loop. Then the inversion mapping J is an involutory antiautomorphism of Q. Moreover, $JL_xJ = R_{x^{-1}}$ and $JL_{x,y}J = R_{x^{-1},y^{-1}}$ for every x, $y \in Q$.*

Proof. With x, $y \in Q$ we have $JL_xJ(y) = (xy^{-1})^{-1} = yx^{-1} = R_{x^{-1}}(y)$, so $JL_xJ = R_{x^{-1}}$. Then $JL_{x,y}J = JL_{yx}^{-1}J \cdot JL_yJ \cdot JL_xJ = R_{(yx)^{-1}}^{-1}R_{y^{-1}}R_{x^{-1}} = R_{x^{-1}y^{-1}}^{-1}R_{y^{-1}}R_{x^{-1}} = R_{x^{-1},y^{-1}}$. □

We now easily arrive at the following important result:

Theorem 1.6 (compare [29, Theorem 7.1]). *The following properties are equivalent for a loop Q:*

(*i*) *Q is automorphic,*

(*ii*) *Q is left and middle automorphic,*

(*iii*) *Q is right and middle automorphic.*

Proof. Thanks to the duality, it suffices to establish the implication $(ii) \Rightarrow (i)$. Suppose that Q is left and middle automorphic. By Proposition 1.4, Q has the antiautomorphic inverse property. By Lemma 1.5, J is an antiautomorphism and $R_{x^{-1},y^{-1}} = JL_{x,y}J$ is an automorphism, being a composition of an automorphism and two antiautomorphisms. □

We can further exploit the inversion mapping J.

Lemma 1.7 ([34, Lemma 2.7]). *Let Q be an automorphic loop. Then J centralizes* $\mathrm{Inn}(Q)$*. Moreover, $L_{x,y} = R_{x^{-1},y^{-1}}$ and $T_x^{-1} = T_{x^{-1}}$ for every x, $y \in Q$.*

Proof. Because $\varphi(x^{-1}) = \varphi(x)^{-1}$ for every $x \in Q$ and $\varphi \in \mathrm{Aut}(Q)$, the inversion mapping J centralizes $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$. Combining this with Lemma 1.5 yields $L_{x,y} = JL_{x,y}J = R_{x^{-1},y^{-1}}$. Using this fact and Proposition 1.3 yields $T_xT_{x^{-1}} = L_x^{-1}R_xL_{x^{-1}}^{-1}R_{x^{-1}} = R_xR_{x^{-1}}L_x^{-1}L_{x^{-1}}^{-1} = R_{x^{-1},x}L_{x,x^{-1}}^{-1} = R_{x^{-1},x}R_{x^{-1},x}^{-1} = 1$. □

1.3. Nuclei

As usual, define the *left*, *middle* and *right nucleus* of a loop Q by

$$\begin{aligned} N_\ell(Q) &= \{a \in Q \,:\, a(xy) = (ax)y \text{ for all } x,\, y \in Q\},\\ N_m(Q) &= \{a \in Q \,:\, x(ay) = (xa)y \text{ for all } x,\, y \in Q\},\\ N_r(Q) &= \{a \in Q \,:\, x(ya) = (xy)a \text{ for all } x,\, y \in Q\}, \end{aligned}$$

respectively, and the *nucleus* of Q by $N(Q) = N_\ell(Q) \cap N_m(Q) \cap N_r(Q)$.

It is easy to observe that all the nuclei are associative subloops of Q. In general loops, there is no relationship between the three nuclei $N_\ell(Q)$, $N_m(Q)$ and $N_r(Q)$. On the other hand, it is well known (see below) that in inverse property loops all nuclei coincide.

Recall that a loop with two-sided inverses has the *left inverse property* if $x^{-1}(xy) = y$ holds, the *right inverse property* if $(xy)y^{-1} = x$ holds, and the *inverse property* if it has both the left and right inverse properties.

Proposition 1.8 ([5, Theorem VII.2.1]). *In antiautomorphic inverse property loops the left and right nuclei coincide. In inverse property loops all nuclei coincide.*

Proof. Suppose that Q satisfies (1.2). Then the condition $ax{\cdot}y = a{\cdot}xy$ is equivalent to $y^{-1} \cdot x^{-1}a^{-1} = y^{-1}x^{-1} \cdot a^{-1}$, so $N_\ell(Q) = N_r(Q)$. Now suppose that Q has the inverse property. From $(xy)^{-1}x = (xy)^{-1}(xy \cdot y^{-1}) = y^{-1}$ we deduce (1.2), so it remains to show that $N_\ell(Q) = N_m(Q)$. If $ax \cdot y = a \cdot xy$ then $y = (ax)^{-1}(a \cdot xy)$, and substituting $x = a^{-1}u^{-1}$, $y = ua \cdot v$ yields $ua \cdot v = y = u \cdot av$. The other inclusion follows by a similar argument. □

Suppose that Q is an automorphic loop. We know from Proposition 1.4 that Q has the antiautomorphic inverse property, and thus that $N_\ell(Q) = N_r(Q)$ by Proposition 1.8. But taking $x = 2$ and $y = 3$ in Q_6 shows that Q does not necessarily have the left or right inverse property, so there is no *a priori* reason why the nuclei of Q should coincide. In fact, there are automorphic loops Q satisfying the strict inclusion $N(Q) = N_\ell(Q) = N_r(Q) < N_m(Q)$. Theorem 1.11 shows that no other inclusions among nuclei arise in automorphic loops.

Call a subloop S of a loop Q *characteristic* if $\varphi(S) = S$ for every $\varphi \in \mathrm{Aut}(Q)$.

In general loops, nuclei are not necessarily normal subloops, but they are always characteristic subloops. For instance, if $a \in N_\ell(Q)$ and $\varphi \in \mathrm{Aut}(Q)$ then $\varphi(a) \cdot \varphi(x)\varphi(y) = \varphi(a \cdot xy) = \varphi(ax \cdot y) = \varphi(a)\varphi(x) \cdot \varphi(y)$ shows that $\varphi(a) \in N_\ell(Q)$.

In automorphic loops, nuclei are therefore normal subloops thanks to this easy but important fact:

Lemma 1.9 ([6, Theorem 2.2])**.** *Let Q be an automorphic loop and S a characteristic subloop of Q. Then S is normal in Q.*

Proof. A subloop S is normal in Q if and only if $\varphi(S) = S$ for every $\varphi \in \mathrm{Inn}(Q)$. □

Lemma 1.10. *Let Q be an automorphic loop. Then $T_xT_y(a) = T_{yx}(a)$ for every $a \in N_\ell(Q) = N_r(Q)$.*

Proof. We have already shown that $N_\ell(Q) = N_r(Q)$ is a characteristic subloop of Q. Let $u = T_x(y)$ (that is, $xu = yx$). Because $a \in N_r(Q)$, we also have $T_{xu}(a) \in N_r(Q)$, and so $x(uT_{xu}(a)) = (xu)T_{xu}(a) = a(xu)$. Since $a \in N_\ell(Q)$, we then have $T_xT_y(a) = T_x(y\backslash ay) = T_x(y)\backslash T_x(ay) = T_x(y)\backslash(x\backslash(ay)x) = T_x(y)\backslash(x\backslash a(yx)) = u\backslash(x\backslash a(xu)) = u\backslash(x\backslash x(uT_{xu}(a))) = T_{xu}(a) = T_{yx}(a)$. □

Theorem 1.11. *Let Q be an automorphic loop. Then $N(Q) = N_\ell(Q) = N_r(Q) \leq N_m(Q)$ and all nuclei are normal subloops of Q.*

Proof. All nuclei are normal by Lemma 1.9. Let $A = N_\ell(Q) = N_r(Q)$. It remains to prove that $A \leq N_m(Q)$. Note that $L_{x,y}$ and $R_{x,y}$ fix A pointwise, while $(xa)y = x(ay)$ holds if and only if $M_{x,y}(a) = a$, where $M_{x,y} = L_x^{-1}R_y^{-1}L_xR_y$.

Given $a \in A$, we want to show that $M_{x,y}(a) = a$. Now,

$$M_{x,y} = (L_x^{-1}R_x)(R_x^{-1}R_y^{-1}R_{xy})(R_{xy}^{-1}L_{xy})(L_{xy}^{-1}L_xL_y)(L_y^{-1}R_y),$$

and thus $M_{x,y} = T_xR_{x,y}^{-1}T_{xy}^{-1}L_{y,x}T_y$. While evaluating $M_{x,y}$ at a, we never leave the normal subloop A, so $M_{x,y}(a) = T_xT_{xy}^{-1}T_y(a)$. By Lemma 1.10, $M_{x,y}(a) = T_xT_{xy}^{-1}T_y(a) = T_x(T_yT_x)^{-1}T_y(a) = a$. □

The middle nucleus is important in automorphic loops but its role is not fully understood.

1.4. Diassociativity and the Moufang property

Up to this point we have carefully proved all the results. In this subsection we skip some proofs and refer the reader to the literature.

A loop has the *left alternative property* if it satisfies $x(xy) = (xx)y$ and the *right alternative property* if $x(yy) = (xy)y$ holds. A loop Q is *diassociative* if any two elements of Q generate an associative subloop.

By Moufang's theorem [36], Moufang loops are diassociative. The loop Q_6 with $x = 2$ and $y = 3$ shows that automorphic loops need not have the left alternative property nor the right alternative property so, in particular, they need not be diassociative.

Bruck and Paige proved in [6, Theorem 2.4] that the following properties are equivalent for an automorphic loop Q: Q is diassociative; Q satisfies both left and right inverse properties; Q satisfies both left and right alternative properties. Moreover, as we have already mentioned in the introduction, every diassociative automorphic loop is Moufang [33]. Thanks to Proposition 1.4, we can refine these results as follows:

Theorem 1.12. *The following properties are equivalent for an automorphic loop* Q :

(*i*) *Q has the left alternative property*

(*ii*) *Q has the right alternative property,*

(*iii*) *Q has the left inverse property,*

(*iv*) *Q has the right inverse property,*

(*v*) *Q is diassociative,*

(*vi*) *Q is Moufang.*

Proof. Suppose that Q has the left alternative property. Then Proposition 1.4 implies that $(yx \cdot x)^{-1} = x^{-1} \cdot x^{-1}y^{-1} = x^{-1}x^{-1} \cdot y^{-1} = (y \cdot xx)^{-1}$, so Q has the right alternative property. A similar argument finishes the equivalence of (*i*) and (*ii*), and also proves the equivalence of (*iii*) and (*iv*). The rest follows from [6, 33]. □

We conclude this section with Bruck's proof of the fact that commutative Moufang loops are automorphic. The argument is based on nice observations about autotopisms and companions of pseudo-automorphisms, which we review.

Let Q be a loop. A triple (f, g, h) of bijections $Q \to Q$ is an *autotopism* if $f(x)g(y) = h(xy)$ holds for every x, $y \in Q$. It is easy to see that the coordinatewise product (composition) of autotopisms is an autotopism.

If a bijection f of Q and $c \in Q$ satisfy the identity $f(x) \cdot f(y)c = f(xy)c$, then f is called a *pseudo-automorphism* of Q with *companion c*.

Lemma 1.13 (compare [5, Lemma VII.2.1]). *Let Q be a loop and (f, g, h) an autotopism of Q such that $f(1) = 1$. Then $g = h$ and $g(x) = f(x)c$, where $c = g(1)$. Hence f is a pseudo-automorphism with companion $c = g(1)$.*

Proof. We have $g(x) = f(1)g(x) = h(1 \cdot x) = h(x)$, so $g = h$. Also, $f(x)c = f(x)g(1) = h(x) = g(x)$. Finally, $f(x) \cdot f(y)c = f(x)g(y) = h(xy) = g(xy) = f(xy)c$. □

Proposition 1.14 ([5, Lemma VII.3.3]). *Commutative Moufang loops are automorphic.*

Proof. Let Q be a commutative Moufang loop. Let f be a pseudo-automorphism of Q with companion c. Then $f(x) \cdot cf(y) = f(x) \cdot f(y)c = f(xy)c = f(yx)c = f(y) \cdot f(x)c = f(x)c \cdot f(y)$ for every x, $y \in Q$, so $c \in N_m(Q)$. Since Q is an inverse property loop, its nuclei coincide by Proposition 1.8 and we have $c \in N_r(Q)$. Then c can be canceled in $f(x) \cdot f(y)c = f(xy)c$ and $f \in \mathrm{Aut}(Q)$ follows.

It therefore suffices to prove that the mappings $L_{x,y}$ are pseudo-automorphisms. The Moufang identity (M) is equivalent to the statement that $\varphi_x = (L_x, R_x, R_x L_x)$ is an autotopism of Q. Then $\varphi_{yx}^{-1}\varphi_y\varphi_x$ is an autotopism with first component $L_{x,y}$. By Lemma 1.13, $L_{x,y}$ is a pseudo-automorphism. □

Lecture 2: Associated operations

Many of the concepts presented in this section can be traced to two influential papers [20, 21] on loops of odd order written by Glauberman in the 1960s. In his study of Moufang loops $(Q, \cdot)$ of odd order [21], the most important idea was to associate another loop $(Q, \bullet)$ with $(Q, \cdot)$, defined by $x \bullet y = x^{1/2}yx^{1/2}$, where $x^{1/2}$ is the unique square root of x in $(Q, \cdot)$. The resulting loop $(Q, \bullet)$ is an instance of what would nowadays be called a Bruck loop (or a K-loop). This made Glauberman study Bruck loops of odd order and their left multiplication groups in detail [20] and establish a number of key results for them (see Theorem 2.2). He then transferred the results from Bruck loops to Moufang loops.

We follow a similar approach but in a more general setting of twisted subgroups. We show how to associate left Bruck loops with uniquely 2-divisible left Bol loops and with uniquely 2-divisible automorphic loops. We then follow [22] and establish a one-to-one correspondence between left Bruck loops of odd order and a certain class of commutative loops containing commutative automorphic loops of odd order. This will allow us to prove an analog of Theorem 2.2 for commutative automorphic loops. Finally, as in [34] we establish a one-to-one correspondence between uniquely 2-divisible automorphic loops whose associated left Bruck loop is associative and a certain class of uniquely 2-divisible Lie rings. This eventually leads to the Odd Order Theorem for automorphic loops. For the convenience of the reader, the correspondence results are visualized in Figure 2.

2.1. Bruck loops

A loop Q is a *left Bol loop* if it satisfies the *left Bol identity*

$$x(y(xz)) = (x(yx))z. \tag{2.3}$$

It is well known that left Bol loops have the left inverse property.

The following result gives a nice axiomatization of left Bol loops in the variety of magmas with inverses.

Lemma 2.1 ([31, (3.10)] and [42, Theorem 4.1])**.** *Let $(Q,\cdot)$ be a groupoid with an identity element and two-sided inverses satisfying* (2.3)*. Then $(Q,\cdot)$ is a left Bol loop.*

Consequently, a nonempty subset of a left Bol loop is a subloop if it is closed under mutiplication and inverses.

A *left Bruck loop* is a left Bol loop with the *automorphic inverse property* $(xy)^{-1} = x^{-1}y^{-1}$.

Here is an omnibus result on Bruck loops of odd order compiled from [20, 21]. Recall that the *left multiplication group* of Q is defined by $\mathrm{Mlt}_\ell(Q) = \langle L_x : x \in Q\rangle$.

Theorem 2.2 (Glauberman)**.** *Let Q be a left Bruck loop of odd order. Then Q is solvable. If $H \leq Q$ then $|H|$ divides $|Q|$. If p is a prime dividing $|Q|$ then there is $x \in Q$ such that $|x| = p$. Sylow p-subloops and Hall π-subloops of Q exist. The left multiplication group $\mathrm{Mlt}_\ell(Q)$ of Q is of odd order.*

If also $|Q| = p^k$ for an odd prime p, then Q is centrally nilpotent.

2.2. Twisted subgroups

A subset S of a group G is a *twisted subgroup* of G if it contains the identity element of G, is closed under inverses, and is closed under the binary operation $(x,y) \mapsto xyx$.

Note that a twisted subgroup is not necessarily a subgroup, but every twisted subgroup S is closed under powers. Indeed, it suffices to show that all positive powers of $x \in S$ belong to S, and we get this by induction on k from $x^{k+2} = xx^kx$.

Call a subset U of a loop Q *uniquely* 2*-divisible* if the squaring map $Q \to Q$, $x \mapsto x^2$ restricts to a bijection on U. In this case, for every $x \in U$ there is a unique element $x^{1/2} \in U$ such that $(x^{1/2})^2 = x$. If U happens to be power associative and $x \in U$ has odd order n, then $x^{1/2} = x^{(n+1)/2}$, so the square root of x is a positive power of x. If U happens to be closed under inverses, then $((x^{-1})^{1/2})^2 = x^{-1} = (x^{1/2}x^{1/2})^{-1} = (x^{1/2})^{-1}(x^{1/2})^{-1} = ((x^{1/2})^{-1})^2$ shows that $(x^{-1})^{1/2}$ is equal to $(x^{1/2})^{-1}$.

Proposition 2.3 (compare [20, Lemma 3])**.** *Let G be a group and S a uniquely* 2*-divisible twisted subgroup of G. Then $(S,\circ)$ with multiplication*

$$x \circ y = (xy^2x)^{1/2}$$

is a left Bruck loop. Moreover, the powers in $(S,\cdot)$ and $(S,\circ)$ coincide.

Proof. If x, $y \in S$ then $y^2 \in S$, $xy^2x \in S$ and $(xy^2x)^{1/2} \in S$. Hence $(S, \circ)$ is a groupoid. Since $1 \circ x = x = x \circ 1$ and $x^{-1} \circ x = (x^{-1}x^2x^{-1})^{1/2} = 1 = (xx^{-2}x)^{1/2} = x \circ x^{-1}$, we see that $(S, \circ)$ has identity element 1 and two-sided inverses. Note that $x \circ (y \circ x) = (xyx^2yx)^{1/2} = ((xyx)^2)^{1/2} = xyx$. Thus $x \circ (y \circ (x \circ z)) = (xyxz^2xyx)^{1/2} = (xyx) \circ z = (x \circ (y \circ x)) \circ z$. By Lemma 2.1, $(S, \circ)$ is a left Bol loop in which inverses coincide with those of $(S, \cdot)$. It is a left Bruck loop thanks to $(x \circ y)^{-1} = ((xy^2x)^{1/2})^{-1} = ((xy^2x)^{-1})^{1/2} = (x^{-1}y^{-2}x^{-1})^{1/2} = x^{-1} \circ y^{-1}$. The inductive step $x \circ x^{n+1} = (xx^{2n+2}x)^{1/2} = x^{n+2}$ shows that powers in $(S, \cdot)$ and $(S, \circ)$ coincide. □

A twisted subgroup of a uniquely 2-divisible group need not be uniquely 2-divisible (consider $\mathbb{Z}$ in $(\mathbb{Q}, +)$). But note that if G is a group of odd order then any twisted subgroup S of G is uniquely 2-divisible.

The next result shows that in many varieties of loops the concepts "uniquely 2-divisible" and "of odd order" coincide for finite loops.

Lemma 2.4. *Let Q be a finite power-associative loop in which $|x|$ divides $|Q|$ for every $x \in Q$. Then the following conditions are equivalent:*

(*i*) *Q is uniquely 2-divisible,*

(*ii*) *$|Q|$ is odd,*

(*iii*) *$|x|$ is odd for every $x \in Q$.*

Proof. Condition (*ii*) implies (*iii*) by the assumption that $|x|$ divides $|Q|$. Conversely, if (*iii*) holds then the inversion mapping $x \mapsto x^{-1}$ is an involution with a unique fixed point $x = 1$, so $|Q|$ is odd.

If (*i*) holds then $x^2 = 1$ implies $x = 1$, so (*iii*) holds. Conversely, if (*iii*) holds, then $|x| = 2n + 1$ implies $(x^{n+1})^2 = x^{2n+2} = x$, so the squaring map is onto Q. Thanks to finiteness of Q, it is also one-to-one, and (*i*) follows. □

2.3. Bruck loops associated with Bol and automorphic loops

If G is a uniquely 2-divisible group, Proposition 2.3 with $S = G$ yields a uniquely 2-divisible left Bruck loop $(G, \circ)$, the (*left*) *Bruck loop associated with G*.

Proposition 2.3 cannot be used directly to associate left Bruck loops with nonassociative loops Q. The trick is to work with a certain twisted subgroup S of $\mathrm{Mlt}(Q)$ instead and then project the operation $\circ$ from S to Q. The classical example is that of uniquely 2-divisible left Bol loops, which we recall in Proposition 2.5.

Proposition 2.5 ([18]). *Let $(Q, \cdot)$ be a left Bol loop. Then $L_Q = \{L_x : x \in Q\}$ is a twisted subgroup of $\mathrm{Mlt}_\ell(Q)$ satisfying*

$$L_xL_yL_x = L_{x(yx)}. \tag{2.4}$$

If $(Q,\cdot)$ is also uniquely 2-divisible, then L_Q is uniquely 2-divisible and $(Q,\circ)$ with multiplication

$$x\circ y = (x(y^2x))^{1/2} \tag{2.5}$$

is a left Bruck loop in which powers coincide with those of $(Q,\cdot)$. When Q is finite then any subloop of $(Q,\cdot)$ is a subloop of $(Q,\circ)$.

Proof. We have $1 = L_1 \in L_Q$, $L_x^{-1} = L_{x^{-1}} \in L_Q$ thanks to the left inverse property, and (2.4) follows from (2.3). Therefore L_Q is a twisted subgroup of $\mathrm{Mlt}_\ell(Q)$. An easy induction with (2.4) shows that $L_x^n = L_{x^n}$ for every $n \geq 0$.

Suppose that $(Q,\cdot)$ is uniquely 2-divisible. The mapping $Q \to L_Q$, $x \mapsto L_x$ is a bijection since $L_x(1) = x$. Since $(L_{x^{1/2}})^2 = L_{(x^{1/2})^2} = L_x$, it follows that L_Q is uniquely 2-divisible with $L_x^{1/2} = L_{x^{1/2}}$. By Proposition 2.3, $(L_Q,\circ)$ with multiplication $L_x \circ L_y = (L_xL_y^2L_x)^{1/2} = L_{(x(y^2x))^{1/2}}$ is a left Bruck loop with powers coinciding with those of $\mathrm{Mlt}_\ell(Q)$.

We claim that $\varphi : (L_Q,\circ) \to (Q,\circ)$, $L_x \mapsto x$ is an isomorphism of loops. Indeed, φ is clearly a bijection and $\varphi(L_x \circ L_y) = \varphi(L_{(x(y^2x))^{1/2}}) = (x(y^2x))^{1/2} = x\circ y = \varphi(L_x)\circ\varphi(L_y)$.

Finally, suppose that Q is finite and $S \leq (Q,\cdot)$. To show that S is a subloop of $(Q,\circ)$, it suffices to prove that it is closed under inverses and under the multiplication $\circ$. The former is true because the inverses in $(Q,\cdot)$ and $(Q,\circ)$ coincide, and the latter is true because $(S,\cdot)$ is closed under $\cdot$ and square roots (being positive integral powers in the finite case). □

A twisted subgroup in $\mathrm{Mlt}(Q)$ is harder to find for automorphic loops. For $x \in Q$ define

$$P_x = R_xL_{x^{-1}}^{-1}.$$

Note that in automorphic loops we have $P_x = L_{x^{-1}}^{-1}R_x$ by Proposition 1.3.

Proposition 2.6 ([34, Proposition 4.2])**.** *Let $(Q,\cdot)$ be an automorphic loop. Then $P_Q = \{P_x : x \in Q\}$ is a twisted subgroup of $\mathrm{Mlt}(Q)$ satisfying*

$$P_xP_yP_x = P_{P_x(y)} = P_{(x^{-1}\backslash y)x}. \tag{2.6}$$

If $(Q,\cdot)$ is also uniquely 2-divisible, then P_Q is uniquely 2-divisible and $(Q,\circ)$ with multiplication

$$x\circ y = ((x^{-1}\backslash y^2)x)^{1/2} = (x^{-1}\backslash y^2x)^{1/2} \tag{2.7}$$

is a left Bruck loop in which powers coincide with those of $(Q,\cdot)$. When Q is finite then any subloop of $(Q,\cdot)$ is a subloop of $(Q,\circ)$.

Proof. We have $1 = P_1 \in P_Q$. Proposition 1.3 and Lemma 1.7 yield

$$P_xP_{x^{-1}} = R_xL_{x^{-1}}^{-1}R_{x^{-1}}L_x^{-1} = L_{x^{-1}}^{-1}R_{x^{-1}}L_x^{-1}R_x = T_{x^{-1}}T_x = 1,$$

so $P_x^{-1} = P_{x^{-1}} \in P_Q$. The identity (2.6) is nontrivial; see [34, Proposition 3.4] for a proof. Therefore P_Q is a twisted subgroup of $\mathrm{Mlt}(Q)$. An easy induction with (2.6) yields $P_x^n = P_{x^n}$ for every $n \geq 0$, using $P_x(x^i) = (x^{-1}\backslash x^i)x = x^{i+2}$.

Suppose that $(Q,\cdot)$ is uniquely 2-divisible. The mapping $Q \to P_Q$, $x \mapsto P_x$ is a bijection since $P_x(1) = x^2$. Since $P_{x^{1/2}}^2 = P_{(x^{1/2})^2} = P_x$, it follows that P_Q is uniquely 2-divisible with $P_x^{1/2} = P_{x^{1/2}}$. By Proposition 2.3, $(P_Q, \circ)$ with multiplication $P_x \circ P_y = (P_x P_y^2 P_x)^{1/2} = P_{((x^{-1}\backslash y^2)x)^{1/2}}$ is a left Bruck loop with powers coinciding with those of $\mathrm{Mlt}(Q)$. Note that $(x^{-1}\backslash y)x = x^{-1}\backslash yx$ by Proposition 1.3.

We conclude as in the proof of Proposition 2.5, using the bijection $P_x \mapsto x$. □

When $(Q,\cdot)$ is a uniquely 2-divisible automorphic loop, we call $(Q,\circ)$ from Proposition 2.6 the *left Bruck loop associated with* $(Q,\cdot)$.

It is worth noting that in left Bol loops we have $x^{-1}\backslash y^2 = xy^2$ thanks to the left inverse property. So, in left Bol loops, the operation (2.5) of Proposition 2.5 coincides with the operation (2.7) of Proposition 2.6. But neither result is a special case of the other.

We can now easily deduce Cauchy's and Lagrange's theorems for automorphic loops of odd order from Theorem 2.2.

Theorem 2.7. *Let Q be an automorphic loop of odd order. If S is a subloop of Q then $|S|$ divides $|Q|$. If p is a prime dividing $|Q|$ then Q contains an element of order p.*

Proof. Let $(Q,\circ)$ be the left Bruck loop associated with Q. If $S \leq Q$ then $(S,\circ) \leq (Q,\circ)$ by Proposition 2.6. By Theorem 2.2, $|S|$ divides $|Q|$. Let p be a prime dividing $|Q|$. Then there is $x \in (Q,\circ)$ of order p by Theorem 2.2. Because powers in Q and $(Q,\circ)$ coincide, x has also order p in Q. □

Corollary 2.8. *Every automorphic loop of prime order is associative.*

Note that we cannot easily use Proposition 2.6 to obtain the Odd Order Theorem for automorphic loops from the Odd Order Theorem for Bruck loops, for instance. The difficulty lies in the fact that it is not clear how subloops of $(Q,\circ)$ are related to subloops of $(Q,\cdot)$.

2.4. Correspondence with Bruck loops

By Proposition 2.6, if $(Q,\cdot)$ is a uniquely 2-divisible automorphic loop then P_Q is a twisted subgroup of $\mathrm{Mlt}(Q)$ satisfying (2.6), which induces a left Bruck loop operation $(Q,\circ)$ by $x \circ y = (x^{-1}\backslash y^2 x)^{1/2}$. However, there exist distinct uniquely 2-divisible automorphic loops with the same associated left Bruck loops, so it is not possible to find an inverse to the mapping $(Q,\cdot) \mapsto (Q,\circ)$.

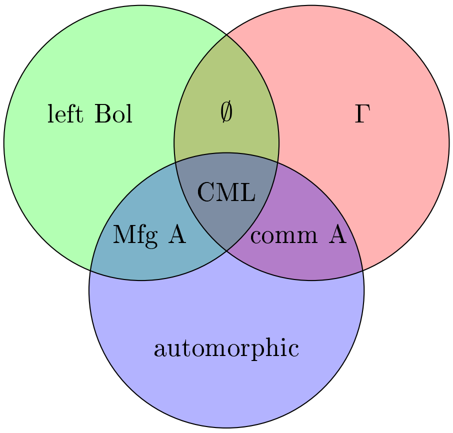


Figure 1: Intersections among left Bol loops, automorphic loops and Γ-loops.

In an attempt to find a correspondence between uniquely 2-divisible left Bruck loops and some class of loops, Greer [22] defined a technical variety of loops as follows.

A loop Q is a *Γ-loop* if it is commutative, has the automorphic inverse property, satisfies $L_xL_{x^{-1}} = L_{x^{-1}}L_x$ and $P_xP_yP_x = P_{P_x(y)}$. Note that the last condition is just (2.6). By [22, Theorem 3.5], Γ-loops are power-associative.

Figure 1 gives a Venn diagram of intersections of the varieties of left Bol loops, automorphic loops and Γ-loops. Here is a full justification for the diagram. If Q is an automorphic Γ-loop then it is a commutative automorphic loop; conversely, a commutative automorphic loop is certainly automorphic and it satisfies the automorphic inverse property by Proposition 1.4, the relation $L_xL_{x^{-1}} = L_{x^{-1}}L_x$ by Proposition 1.3, and (2.6) by [34, Proposition 3.4]. If Q is left Bol and automorphic then the antiautomorphic inverse property implies that Q is Moufang (and automorphic); the converse is trivial. If Q is left Bol and a Γ-loop then it is a commutative Moufang loop. If Q is Moufang and a Γ-loop then it is a commutative Moufang loop. Finally, a commutative Moufang loop is automorphic by Proposition 1.14.

When $(Q, \cdot)$ is a uniquely 2-divisible Γ-loop, we can use the same construction as in the case of uniquely 2-divisible automorphic loops to obtain the *associated left Bruck loop* $(Q, \circ)$, namely $x \circ y = (x^{-1}\backslash y^2x)^{1/2}$. In the end, the variety of Γ-loops was chosen so that the proof of this result can mimic the proof in the automorphic case. (For instance, the difficult identity (2.6) is part of the definition of Γ-loops.) See [22, Theorem 4.9] for details.

Following Greer, we will now show how to construct a left Bruck loop Q from a Γ-loop of odd order. (See the discussion after Lemma 2.11 for an obstacle in the more general uniquely 2-divisible case.) We will actually use the twisted subgroup

L_Q again, but with a different operation.

On a uniquely 2-divisible group $(G, \cdot)$, let

$$x * y = xy[y, x]^{1/2}, \tag{2.8}$$

where $[x, y] = x^{-1}y^{-1}xy$ is the usual commutator.

Straightforward, albeit nontrivial calculation with the commutator in groups yields:

Lemma 2.9 ([22, Theorem 2.5]). *Let $(G, \cdot)$ be a uniquely 2-divisible group. Then $(G, *)$ defined by (2.8) is a Γ-loop. Powers in $(G, \cdot)$ and $(G, *)$ coincide.*

Let us now consider a twisted subgroup seemingly unrelated to L_Q; see [4, 18, 20]. For a group G and $\tau \in \mathrm{Aut}(G)$ let

$$K(\tau) = \{x \in G \,:\, \tau(x) = x^{-1}\}.$$

We claim that $K(\tau)$ is a twisted subgroup of G. Indeed, $1 \in K(\tau)$ is clear, if $x \in K(\tau)$ then $\tau(x^{-1}) = \tau(x)^{-1} = (x^{-1})^{-1}$, so $x^{-1} \in K(\tau)$, and if x, $y \in K(\tau)$ then $\tau(xyx) = \tau(x)\tau(y)\tau(x) = x^{-1}y^{-1}x^{-1} = (xyx)^{-1}$, so $xyx \in K(\tau)$.

Lemma 2.10 (compare [18, Theorem 4.3]). *Let G be a group and $\tau \in \mathrm{Aut}(G)$. Let S be a twisted subgroup of G such that $S \subseteq K(\tau)$ and $\langle S\rangle = G$. Then $\{x^2 \,:\, x \in K(\tau)\} \subseteq S$. In particular, if G is a uniquely 2-divisible group then $S = K(\tau)$.*

Proof. Let $x \in K(\tau)$. Then $x^2 = x\tau(x^{-1})$. Since $\langle S\rangle = G$, there are $x_1, \dots, x_n \in S$ such that $x = x_1 \cdots x_n$. Then $x\tau(x^{-1}) = x_1 \cdots x_n\tau(x_n^{-1} \cdots x_1^{-1}) = x_1 \cdots x_n\tau(x_n^{-1}) \cdots \tau(x_1^{-1}) = x_1 \cdots x_n x_n \cdots x_1$, where we have used $x_i \in S \subseteq K(\tau)$. An easy induction on n shows that the element $x_1 \cdots x_n x_n \cdots x_1$ belongs to the twisted subgroup S.

We have proved $\{x^2 \,:\, x \in K(\tau)\} \subseteq S \subseteq K(\tau)$. Suppose that G is uniquely 2-divisible. The squaring map is then injective on any twisted subgroup, and we claim that it is surjective on $K(\tau)$, so that $K(\tau)$ is uniquely 2-divisible. Indeed, if $x \in K(\tau)$ then $\tau(x^{1/2}) = \tau(x)^{1/2} = (x^{-1})^{1/2} = (x^{1/2})^{-1}$, so $x^{1/2} \in K(\tau)$. It follows that $K(\tau) = \{x^2 \,:\, x \in K(\tau)\}$, and $S = K(\tau)$. □

Lemma 2.11 (compare [22, Lemma 4.3]). *Let G be a uniquely 2-divisible group and let $\tau \in \mathrm{Aut}(G)$. Then $K(\tau)$ is a subloop of the Γ-loop $(G, *)$.*

Proof. By Lemma 2.9, $(G, *)$ is a Γ-loop. If x, $y \in K(\tau)$ then $\tau(x * y) = \tau(xy[y, x]^{1/2}) = \tau(x)\tau(y)[\tau(y), \tau(x)]^{1/2} = x^{-1}y^{-1}[y^{-1}, x^{-1}]^{1/2} = x^{-1} * y^{-1} = (x * y)^{-1}$, where we have used the automorphic inverse property in the last step.

Let us now consider left division in $(G, *)$. The following statements are equivalent: $x * a = y$, $xa[a, x]^{1/2} = y$, $[a, x] = (a^{-1}x^{-1}y)^2$, $ax = ya^{-1}x^{-1}y$, $ay^{-1}a = x^{-1}yx^{-1}$, $(ay^{-1})^2 = x^{-1}yx^{-1}y^{-1}$, $a = (x^{-1}yx^{-1}y^{-1})^{1/2}y$. Since this is a term in $(G, \cdot)$, we can easily show that $K(\tau)$ is closed under left division in $(G, *)$. □

We would now like to apply Lemmas 2.9 and 2.11. However, there are examples of uniquely 2-divisible left Bruck loops Q with $G = \mathrm{Mlt}_\ell(Q)$ not uniquely 2-divisible, so the lemmas cannot be applied directly. We therefore focus on the odd case.

Proposition 2.12 ([22]). *Let $(Q, \cdot)$ be a left Bruck loop of odd order and let $G = \mathrm{Mlt}_\ell(Q, \cdot)$. Then $(L_Q, *)$ is a Γ-loop, and $(Q, *)$ with multiplication*

$$x * y = (L_x * L_y)(1) = (L_x L_y [L_y, L_x]^{1/2})(1)$$

is a Γ-loop.

Proof. Proposition 2.5 shows that L_Q is a twisted subgroup of $\mathrm{Mlt}_\ell(Q, \cdot)$. Let τ be the conjugation on $\mathrm{Sym}(Q)$ by the inversion map J of $(Q, \cdot)$. For x, $y \in Q$, we have $JL_xJ(y) = J(xy^{-1}) = x^{-1}y = L_{x^{-1}}(y) = L_x^{-1}(y)$ by the automorphic inverse property and the left inverse property. Because $\langle L_Q \rangle = G$, the established identity $\tau(L_x) = JL_xJ = L_{x^{-1}} = L_x^{-1}$ shows that $\tau \in \mathrm{Aut}(G)$ and also that $L_Q \subseteq K(\tau)$.

By Theorem 2.2, $|G|$ is odd. By Lemma 2.4, G is uniquely 2-divisible. Lemma 2.10 with $S = L_Q$ then gives $L_Q = K(\tau)$. By Lemma 2.11, $(L_Q, *) = (K(\tau), *)$ is a subloop of the Γ-loop $(G, *)$. Finally, as usual, we transfer the operation $*$ from $(L_Q, *)$ to $(Q, *)$ by the isomorphism $L_x \mapsto x$. □

For a left Bruck loop $(Q, \cdot)$ of odd order, we call $(Q, *)$ from Proposition 2.12 the *Γ-loop associated with* $(Q, \cdot)$.

Greer went on to establish the announced one-to-one correspondence, and more:

Theorem 2.13 ([22, Theorem 5.2]). *There is a categorical equivalence between left Bruck loops of odd order and Γ-loops of odd order. Given a Γ-loop $(Q, \cdot)$ of odd order, we let $(Q, \circ)$ be the associated left Bruck loop with multiplication $x \circ y = (x^{-1} \backslash y^2 x)^{1/2}$. Conversely, given a Bruck loop $(Q, \circ)$ of odd order, we let $(Q, \cdot)$ be the associated Γ-loop with multiplication $x \cdot y = (L_x L_y [L_y, L_x]^{1/2})(1)$, where L_x is the left translation in $(Q, \circ)$.*

Solvability, Lagrange and Cauchy theorems for commutative automorphic loops of odd order were for the first time established in [25]. (See Theorems 3.11 and 3.12 for the even case.) The fact that commutative automorphic loops of odd order p^k (p a prime) are centrally nilpotent was proved independently in [9] and [27].

Theorem 2.13 allows us to obtain these and additional results from Glauberman's Theorem 2.2 not only for commutative automorphic loops of odd order but also for the larger class of Γ-loops of odd order.

Theorem 2.14 ([22, Section 6]). *Let Q be a Γ-loop of odd order. Then Q is solvable and the Lagrange and Cauchy theorems hold for Q. Moreover, there are Sylow p- and Hall π-subloops in Q.*

If also $|Q| = p^k$ for an odd prime p, then Q is centrally nilpotent.

2.5. Correspondence with Lie rings

The correspondence between left Bruck loops of odd order and Γ-loops of odd order covered all commutative automorphic loops of odd order as a subclass of Γ-loops, but it did not cover all automorphic loops of odd order. In [34], a one-to-one correspondence was found between uniquely 2-divisible automorphic loops whose associated left Bruck loop is an abelian group on the one hand, and uniquely 2-divisible Lie rings satisfying conditions (2.10), (2.11) on the other hand (see Theorem 2.18). This partial correspondence is sufficient to establish the Odd Order Theorem for automorphic loops (Theorem 2.21). In this subsection we sketch the proofs of these results.

We start with a construction of Wright [46]. Let us call $(Q,+,[.,.])$ an *algebra* if $(Q,+)$ is a an abelian group and $[.,.]$ is biadditive, that is $[x+y,z]=[x,z]+[y,z]$ and $[x,y+z]=[x,y]+[x,z]$ for every x, y, $z\in Q$. In this situation, for every $x\in Q$ define

$$\mathrm{ad}^\ell_x : Q\to Q,\ \mathrm{ad}^\ell_x(y)=[x,y],\quad \mathrm{ad}^r_x : Q\to Q,\ \mathrm{ad}^r_x(y)=[y,x]$$

to be the *left* and *right adjoint maps of* x, respectively. Note that ad^ℓ_x, ad^r_x are just the left and right translations with respect to the binary operation $[.,.]$, respectively. Finally, for $x\in Q$ define

$$\ell_x=\mathrm{id}_Q-\mathrm{ad}^\ell_x,\quad r_x=\mathrm{id}_Q-\mathrm{ad}^r_x.$$

Proposition 2.15 (see [46, Proposition 8] and [34, Lemma 5.1])**.** *Let $(Q,+,[.,.])$ be an algebra. Define a groupoid $(Q,\cdot)$ by*

$$x\cdot y=x+y-[x,y]. \tag{2.9}$$

Then $(Q,\cdot)$ is a loop (necessarily with identity element 0) if and only if

$$\ell_x \text{ and } r_x \text{ are bijections of } Q \tag{2.10}$$

for every $x\in Q$.

When $(Q,\cdot)$ is a loop with left and right translations L_x, R_x, respectively, then

$$L_x(y)=x+\ell_x(y),\ R_x(y)=x+r_x(y),\ L_x^{-1}(y)=\ell_x^{-1}(y-x),\ R_x^{-1}(y)=r_x^{-1}(y-x).$$

Moreover, $L_{x,y}=\ell_{yx}^{-1}\ell_y\ell_x$, $R_{x,y}=r_{xy}^{-1}r_yr_x$ and $T_x=\ell_x^{-1}r_x$.

Proof. We have $0\cdot x=x=x\cdot 0$ for every $x\in Q$. Note that $x\cdot y=x+\ell_x(y)=y+r_y(x)$. Hence L_x bijects if and only if ℓ_x bijects, and R_y bijects if and only if r_y bijects.

The formulas for L_x, R_x, L_x^{-1}, R_x^{-1} are straightforward. Let us calculate $L_{x,y}$. Note that every ℓ_x is additive, being a sum of two additive maps. We have

$$\begin{aligned}L_{x,y}(z)&=L_{yx}^{-1}L_yL_x(z)=L_{yx}^{-1}L_y(x+\ell_x(z))=L_{yx}^{-1}(y+\ell_y(x+\ell_x(z)))\\&=\ell_{yx}^{-1}(y+\ell_y(x)+\ell_y\ell_x(z)-yx)=\ell_{yx}^{-1}(yx+\ell_y\ell_x(z)-yx)\\&=\ell_{yx}^{-1}\ell_y\ell_x(z).\end{aligned}$$

Similarly for $R_{x,y}$ and T_x. □

Following Wright, we call $(Q,\cdot)$ the *linear groupoid* of the algebra $(Q,+,[.,.])$, and the *linear loop* of $(Q,+,[.,.])$ if (2.10) holds. In view of Proposition 2.15, it is easy to express but difficult to understand in terms of properties of $[.,.]$ when the linear loop $(Q,\cdot)$ is automorphic. We therefore specialize to the setting of Lie rings.

An algebra $(Q,+,[.,.])$ is *alternating* if $[x,x]=0$ for every $x\in Q$. Every alternating algebra is *skew-symmetric*, that is, $[x,y]=-[y,x]$. (Proof: Expand $0=[x+y,x+y]$.)

We say that an algebra $(Q,+,[.,.])$ is *uniquely* 2*-divisible* if the abelian group $(Q,+)$ is uniquely 2-divisible.

If $(Q,+,[.,.])$ is alternating, then $x\cdot x=x+x-[x,x]=2x$, so the associated linear groupoid is uniquely 2-divisible if and only if $(Q,+,[.,.])$ is uniquely 2-divisible.

A *Lie ring* is an alternating algebra $(Q,+,[.,.])$ in which $[.,.]$ satisfies the *Jacobi identity* $[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0$.

Even for Lie rings it is not easy to characterize when the associated linear loop is automorphic. We therefore analyze a stronger condition, namely ℓ_x and r_x being automorphisms.

Lemma 2.16 (compare [34, Proposition 5.2]). *Let $(Q,+,[.,.])$ be a Lie ring and let $(Q,\cdot)$ be defined by* (2.9)*. Then $(Q,\cdot)$ is a loop and all mappings ℓ_x, r_x are automorphisms of $(Q,\cdot)$ if and only if conditions* (2.10) *and*

$$[[x,Q],[x,Q]]=0 \tag{2.11}$$

hold for every $x\in Q$. In such a case, $(Q,\cdot)$ is automorphic.

Proof. By Proposition 2.15, $(Q,\cdot)$ is a loop if and only if (2.10) holds. We therefore assume that (2.10) holds and investigate when the bijections ℓ_x, r_x are automorphisms of $(Q,\cdot)$. Using skew-symmetry and the Jacobi identity freely, we have

$$\begin{aligned}
\ell_x(u)\ell_x(v) &= \ell_x(u)+\ell_x(v)-[\ell_x(u),\ell_x(v)]\\
&= u-[x,u]+v-[x,v]-[u-[x,u],v-[x,v]]\\
&= (u+v-[u,v])-[x,u+v]+([u,[x,v]]+[[x,u],v])-[[x,u],[x,v]]\\
&= (u+v-[u,v])-[x,u+v]+[x,[u,v]]-[[x,u],[x,v]]\\
&= (u+v-[u,v])-[x,u+v-[u,v]]-[[x,u],[x,v]]\\
&= uv-[x,uv]-[[x,u],[x,v]]=\ell_x(uv)-[[x,u],[x,v]].
\end{aligned}$$

Therefore $\ell_x\in\mathrm{Aut}(Q,\cdot)$ if and only if (2.11) holds. The calculation for r_x is similar.

By Proposition 2.15, $\mathrm{Inn}(Q,\cdot)\le\langle\ell_x,r_x : x\in Q\rangle$. Therefore, if ℓ_x, $r_x\in\mathrm{Aut}(Q,\cdot)$ for every $x\in Q$, the loop $(Q,\cdot)$ is automorphic. □

Our eventual goal is to prove the Odd Order Theorem for automorphic loops, so we focus on the uniquely 2-divisible case.

Lemma 2.17. *Let $(Q,+,[.,.])$ be a uniquely 2-divisible Lie ring satisfying (2.10) and (2.11). Let $(Q,\cdot)$ be the (uniquely 2-divisible automorphic) linear loop of $(Q,+,[.,.])$. Let $(Q,\circ)$ be the (uniquely 2-divisible) left Bruck loop associated with $(Q,\cdot)$. Then $(Q,\circ)=(Q,+)$ is an abelian group.*

Proof. We have $x^2=x+x-[x,x]=2x$, so $x^{1/2}=x/2$. Also, $x(-x)=x+(-x)+[x,-x]=0$ shows $x^{-1}=-x$. Then $x\circ y=(x^{-1}\backslash y^2x)^{1/2}=((-x)\backslash(2y)x)/2$. Therefore, the condition $x\circ y=x+y$ is equivalent to $(2y)x=(-x)\cdot(2(x+y))$, which is equivalent to $2y+x-[2y,x]=-x+2(x+y)-[-x,2(x+y)]$, which follows easily because $[.,.]$ is alternating and biadditive. □

We have shown how to construct uniquely 2-divisible automorphic loops from certain uniquely 2-divisible Lie rings. In order to build a correspondence, we now need to return from uniquely 2-divisible automorphic loops $(Q,\cdot)$ to Lie rings, i.e., we need to build operations $+$ and $[.,.]$ on $(Q,\cdot)$. Lemma 2.17 suggests to restrict our attention to the class of uniquely 2-divisible automorphic loops whose associated left Bruck loop is an abelian group, and set $x+y=x\circ y$. This approach works. See [34] for a proof.

Theorem 2.18 ([34, Theorem 5.7])**.** *Suppose that $(Q,+,[\cdot,\cdot])$ is a uniquely 2-divisible Lie ring satisfying (2.10) and (2.11). Then $(Q,\cdot)$ defined by (2.9) is a uniquely 2-divisible automorphic loop whose associated left Bruck loop $(Q,\circ)$ is an abelian group (in fact, $(Q,\circ)=(Q,+)$).*

Conversely, suppose that $(Q,\cdot)$ is a uniquely 2-divisible automorphic loop whose associated left Bruck loop $(Q,\circ)$ is an abelian group. Then $(Q,\circ,[\cdot,\cdot])$ defined by

$$[x,y]=x\circ y\circ(xy)^{-1} \tag{2.12}$$

is a uniquely 2-divisible Lie ring satisfying (2.10) and (2.11).

Furthermore, the two constructions are inverse to one another. Subrings (resp. ideals) of the Lie ring are subloops (resp. normal subloops) of the corresponding automorphic loop, and subloops (resp. normal subloops) closed under square roots are subrings (resp. ideals) of the corresponding Lie ring.

Figure 2 summarizes what we have learned so far. In the figure, all algebras are of odd order, left Bruck loops are blue, Γ-loops are red, automorphic loops are green, and Lie rings satisfying (2.10) and (2.11) are cyan. Dotted lines represent abelian groups. Automorphic loops whose associated left Bruck loops are associative are dashed green. Shaded regions represent one-to-one correspondences. Except for the associated operation $x\cdot y=L_xL_y[L_y,L_x]^{1/2}(1)$, all associated operations make sense in the uniquely 2-divisible case, too.

We now work toward the Odd Order Theorem for automorphic loops.

Lemma 2.19 ([34, Lemma 5.8])**.** *Let $(Q,+,[.,.])$ be a uniquely 2-divisible Lie ring. Then (2.11) holds if and only if $(Q,+,[.,.])$ is solvable of length 2, that is, $[[Q,Q],[Q,Q]]=0$.*

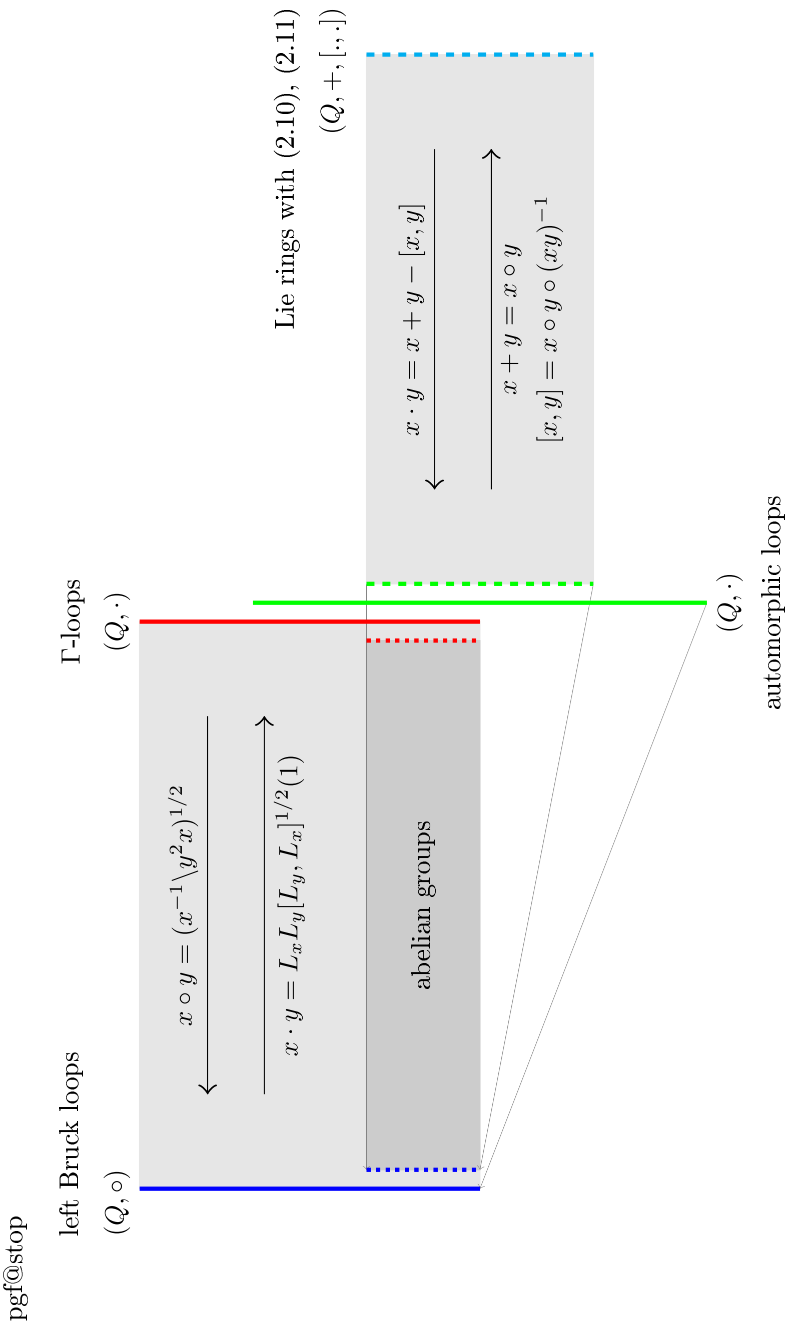


Figure 2: Associated operations between left Bruck loops, Γ-loops, automorphic loops and Lie rings of odd order.

Lemma 2.20 ([34, Lemma 6.5]). *Let $(Q,\cdot)$ be an automorphic loop of odd order, let $(Q,\circ)$ be the associated left Bruck loop, and let S be a characteristic subloop of $(Q,\circ)$. Then S is a normal subloop of $(Q,\cdot)$.*

Proof. Since $x\circ y = (x^{-1}\backslash y^2x)^{1/2}$, we have $\mathrm{Aut}(Q,\cdot)\leq\mathrm{Aut}(Q,\circ)$. Thus S is invariant under $\mathrm{Inn}(Q,\cdot)\leq\mathrm{Aut}(Q,\cdot)$. Let u, $v\in S$. We will show that vu and $v/u\in S$. Let $w=v^{1/2}$. Since powers in $(Q,\cdot)$ and $(Q,\circ)$ coincide, $w\in S$. Then $T_u((u\circ w)^2) = (T_u(u\circ w))^2 = (T_u(u)\circ T_u(w))^2 = (u\circ T_u(w))^2 = u^{-1}\backslash T_u(w)^2u = u^{-1}\backslash T_u(v)u = L_{u^{-1}}^{-1}R_uT_u(v) = L_{u^{-1}}^{-1}L_u^{-1}R_u^2(v)$ is an element of S, where we have used Proposition 1.3 in the last equality. Since $L_uL_{u^{-1}}\in\mathrm{Inn}(Q,\cdot)$, it follows that $R_u^2(v)\in S$. By induction, $R_u^{2m}(v)\in S$ for every m. By Lemma 2.4, $|u| = 2m+1$ for some m. Then $R_u^{2m+1}\in\mathrm{Inn}(Q,\cdot)$, so also $R_u^{-2m}R_u^{2m+1}(v) = vu$ and $R_u^{-2m-2}R_u^{2m+1}(v) = v/u\in S$. By the antiautomorphic inverse property for $(Q,\cdot)$, $v\backslash u\in S$, too.

We have shown that S is a subloop of $(Q,\cdot)$. It is a normal subloop because S is invariant under $\mathrm{Inn}(Q,\cdot)$. □

Theorem 2.21 ([34, Theorem 6.6]). *Automorphic loops of odd order are solvable.*

Proof. Let $(Q,\cdot)$ be a minimal counterexample. If S is a nontrivial, proper normal subloop of $(Q,\cdot)$ then, by minimality, both S and $(Q,\cdot)/S$ are solvable automorphic loops of odd order. This contradicts the nonsolvability of $(Q,\cdot)$. Therefore $(Q,\cdot)$ is simple.

Let $(Q,\circ)$ be the associated left Bruck loop. By Theorem 2.2, $(Q,\circ)$ is solvable and so the derived subloop $D=(Q,\circ)'$ is a proper subloop of $(Q,\circ)$. Since D is a characteristic subloop of $(Q,\circ)$, Lemma 2.20 shows that D is normal in $(Q,\cdot)$. Since $(Q,\cdot)$ is simple, $D=1$ and $(Q,\circ)$ is an abelian group.

Recall that powers in $(Q,\cdot)$ and $(Q,\circ)$ agree. Let p be a prime divisor of $|Q|$ and let $Q_p=\{x\in Q\,:\,x^p=1\}$. Then Q_p is a characteristic subloop of $(Q,\circ)$, hence a normal subloop of $(Q,\cdot)$. By Theorem 2.7, Q_p is nontrivial, so $Q_p=Q$ because $(Q,\cdot)$ is simple. Thus $(Q,\cdot)$ has exponent p, $(Q,\circ)$ has exponent p, and $(Q,\circ)$ is an elementary abelian p-group.

By Theorem 2.18, $(Q,\circ,[\cdot,\cdot])$ defined by (2.12) is a Lie ring satisfying (2.10) and (2.11). By Lemma 2.19, $(Q,\circ,[\cdot,\cdot])$ is solvable (of class 2). Since $(Q,\circ)$ is an elementary abelian p-group, we may view $(Q,\circ,[\cdot,\cdot])$ as a finite dimensional Lie algebra over $GF(p)$. Since $(Q,\cdot)$ is simple, Theorem 2.18 also implies that $(Q,\circ,[\cdot,\cdot])$ is either a simple Lie algebra or an abelian Lie algebra (that is, $[Q,Q]=0$). The former case contradicts solvability of $(Q,\circ,[\cdot,\cdot])$, and so $(Q,\circ,[\cdot,\cdot])$ is an abelian Lie algebra. But then $x\cdot y = x\circ y\circ[x,y] = x\circ y$, so $(Q,\cdot)$ is an abelian group, a contradiction with nonsolvability of $(Q,\cdot)$. □

Lecture 3: Enumerations and constructions

In this section we first show how to efficiently search for finite simple automorphic loops, temporarily suspending the notation $\circ$ and $*$ from previous sections. Then we discuss (commutative) automorphic loops of order pq and p^3. Finally, we give two useful constructions of automorphic loops.

3.1. Enumerating all left automorphic loops

Let G be a permutation group on a finite set $Q = \{1, \dots, d\}$, and let $H \leq G$. The first goal of this section is to present a naive algorithm for constructing all loops $(Q, *)$ on Q with identity element 1 so that $\mathrm{Mlt}_\ell(Q, *) \leq G$ and $H \leq \mathrm{Aut}(Q, *)$. Since $\mathrm{Mlt}_\ell(Q, *)$ acts transitively on Q and $\varphi(1) = 1$ holds for every $\varphi \in H$, let us assume from the start that G is transitive on Q and $H \leq G_1$.

We then specialize this algorithm to construct all left automorphic loops $(Q, *)$ on Q satisfying $\mathrm{Mlt}_\ell(Q, *) = G$. In the next subsection we will add the requirement that $(Q, *)$ be simple. The exposition follows [29].

Lemma 3.1. *Let $Q = \{1, \dots, d\}$ be a finite set and let $L = \{\ell_x : x \in Q\}$ be a subset of* $\mathrm{Sym}(Q)$*. Then $(Q, *)$ defined by $x * y = \ell_x(y)$ is a loop with identity element* 1 *if and only if*

(i) ℓ_1 is the identity mapping on Q, and

(ii) $\ell_x(1) = x$ for every $x \in Q$, and

(iii) $\ell_x^{-1}\ell_y$ is fixed-point free for every x, $y \in Q$ with $x \neq y$.

Proof. Condition (i) holds iff $x = \ell_1(x) = 1 * x$ for every $x \in Q$. Condition (ii) hold iff $x = \ell_x(1) = x * 1$ for every $x \in Q$. So (i) and (ii) together are equivalent to $(Q, *)$ having 1 as the identity element. Since $L \subseteq \mathrm{Sym}(Q)$, all the left translations of $(Q, *)$ are bijections. Let $z \in Q$. Then z is not a fixed point of $\ell_x^{-1}\ell_y$ if and only if $x * z \neq y * z$. Therefore condition (iii) holds if and only if all right translations of $(Q, *)$ are one-to-one. We are done by finiteness of Q. □

We therefore have the following naive algorithm for constructing all loops on Q with identity element 1: Construct all subsets $\{\ell_x : x \in Q\}$ of $\mathrm{Sym}(Q)$ and check that conditions $(i) - (iii)$ of Lemma 3.1 hold.

We will show how to speed up the algorithm if we are only interested in left automorphic loops, essentially by adding left translation not one at a time but rather one conjugacy class at a time.

Lemma 3.2. *Let Q be a loop.*

(i) A bijection $\varphi : Q \to Q$ is an automorphism of Q if and only if $\varphi L_x \varphi^{-1} = L_{\varphi(x)}$ for every $x \in Q$.

(ii) If $\varphi \in \mathrm{Aut}(Q)$ fixes x then $L_x\varphi = \varphi L_x$.

Proof. The following conditions, universally quantified for $y \in Q$, are equivalent: $\varphi L_x \varphi^{-1} = L_{\varphi(x)}$, $\varphi(x\varphi^{-1}(y)) = \varphi(x)y$, $\varphi(xy) = \varphi(x)\varphi(y)$. To prove (ii), consider $\varphi \in \mathrm{Aut}(Q)$ that fixes x, and note that $L_x\varphi(y) = x\varphi(y) = \varphi(x)\varphi(y) = \varphi(xy) = \varphi L_x(y)$ for every $y \in Q$. □

Algorithm 3.3.
Input: A set $Q = \{1, \dots, d\}$, a transitive permutation group G on Q, and $H \le G_1$.

Output: All loops $(Q, *)$ on Q with identity element 1 such that $\mathrm{Mlt}_\ell(Q,*) \le G$ and $H \le \mathrm{Aut}(Q,*)$.

Step 1: Let $\ell_1 = 1_G$, and let $X \subseteq Q \setminus \{1\}$ be a set of orbit representatives for the natural action of H on $Q \setminus \{1\}$. (The condition $\ell_1 = 1_G$ is forced by Lemma 3.1(i).)

Step 2: For all $x \in X$, let

$$\mathcal{L}_x = \{\ell_x \in G : \ell_x(1) = x,\ \ell_x \text{ is fixed-point free, and } \ell_x \in C_G(H_x)\}.$$

If $\mathcal{L}_x = \emptyset$, stop with failure. (This is a set of candidates for ℓ_x. The first two conditions are necessary by Lemma 3.1. The last condition is necessary by Lemma 3.2(ii). Note that if $\mathcal{L}_x$ is nonempty, it suffices to find one $\ell \in \mathcal{L}_x$ and set $\mathcal{L}_x = \ell(C_G(H_x)_1)$.)

Step 3: For all $x \in X$, let

$$\begin{aligned}\mathbb{L}_x = \{\ell_x^H\ &: \ell_x \in \mathcal{L}_x,\ |\ell_x^H| = |H(x)|,\\ &\ell_x^{-1}\ell \text{ is fixed-point free for every } \ell \in \ell_x^H \text{ with } \ell \neq \ell_x\}.\end{aligned}$$

If $\mathbb{L}_x = \emptyset$, stop with failure. (By Lemma 3.2, the desired $L = \{\ell_x : x \in Q\}$ is a union of H-conjugacy classes in G. The set $\mathbb{L}_x$ is a set of candidates for the H-conjugacy class containing ℓ_x. The condition $|\ell_x^H| = |H(x)|$ is forced by Lemma 3.2(i). The second condition is forced by Lemma 3.1(iii).)

Step 4: Construct a graph Γ on $V = \bigcup_{x\in X} \mathbb{L}_x$ by letting $(\ell_x^H, \ell_y^H) \in \mathbb{L}_x \times \mathbb{L}_y$ to be an edge if and only if $(\ell_x^H)^{-1}(\ell_y^H)$ consists of fixed-point free permutations. (Note that it suffices to check that $\ell_x^{-1}\ell_y^H$ consists of fixed-point free permutations. Indeed, if $\psi\ell_x\psi^{-1}(z) = \varphi\ell_y\varphi^{-1}(z)$ for some $z \in Q$, then $\ell_x(\psi^{-1}(z)) = (\psi^{-1}\varphi)\ell_y(\psi^{-1}\varphi)^{-1}(\psi^{-1}(z))$.)

Step 5: Find all subsets C of V such that C is a clique in Γ and $\sum_{v\in C} |v| = |Q|-1$. If there are no such C, stop with failure. Else return all loops $Q(L) = (Q,*)$, where $L = L(C) = \{\ell_1\} \cup \bigcup_{v \in C} v = \{\ell_x : x \in Q\}$ and $x*y = \ell_x(y)$. (The clique property accounting for $|Q|-1$ left translations is at this stage necessary and sufficient by Lemmas 3.1 and 3.2.)

Denote by $\mathcal{A}_\ell^{\le}(Q,G)$ all left automorphic loops $(Q,*)$ defined on Q with identity element 1 and satisfying $\mathrm{Mlt}_\ell(Q,*) \le G$, by $\mathcal{A}_\ell^{=}(Q,G)$ all loops $(Q,*) \in \mathcal{A}_\ell^{\le}(Q,G)$ with $\mathrm{Mlt}_\ell(Q,*) = G$, and by $\mathcal{A}^{=}(Q,G)$ all loops $(Q,*) \in \mathcal{A}_\ell^{\le}(Q,G)$ that are automorphic and satisfy $\mathrm{Mlt}(Q,*) = G$. Let also $\mathcal{C}(Q,G,H)$ be the set of all loops $(Q,*)$ obtained by Algorithm 3.3 with input Q, G and H.

Lemma 3.4. *Let G be a transitive permutation group on $Q = \{1, \dots, d\}$. Then $\mathcal{A}_\ell^=(Q,G) \subseteq \mathcal{C}(Q,G,G_1) \subseteq \mathcal{A}_\ell^\leq(Q,G)$. Moreover, $\mathcal{A}^=(Q,G) \subseteq C(Q,G,G_1)$.*

Proof. First let $(Q,*) \in \mathcal{A}_\ell^=(Q,G)$. Then $\mathrm{Inn}_\ell(Q,*) = \mathrm{Mlt}_\ell(Q,*)_1 = G_1$, and therefore $(Q,*) \in \mathcal{C}(Q,G,G_1)$. Now let $(Q,*) \in C(Q,G,G_1)$. Then $\mathrm{Mlt}_\ell(Q,*) \leq G$ because every left translation of $(Q,*)$ is in G. Since $\mathrm{Inn}_\ell(Q,*) = \mathrm{Mlt}_\ell(Q,*)_1 \leq G_1 \leq \mathrm{Aut}(Q,*)$, the loop $(Q,*)$ is left automorphic. Finally, let $(Q,*) \in \mathcal{A}^=(Q,G)$. Then $\mathrm{Mlt}_\ell(Q,*) \leq G$ and $G_1 = \mathrm{Mlt}(Q,*)_1 = \mathrm{Inn}(Q,*) \leq \mathrm{Aut}(Q,*)$. Thus $(Q,*) \in \mathcal{C}(Q,G,G_1)$. □

Lemma 3.4 can be used to find all left automorphic loops on the set $Q = \{1, \dots, d\}$ with identity element 1. It suffices to apply the lemma to all transitive groups G in Q and discard duplicate loops.

3.2. Searching for finite simple automorphic loops

Recall that a loop Q is said to be *simple* if it has no normal subloops except for Q and 1.

In principle, Algorithm 3.3 returns all finite left automorphic loops, and hence also all finite simple automorphic loops. In practice, the algorithm is too slow to get to even moderately large orders. In this section we will describe improvements to the algorithm so that it can check for simple automorphic loops of order up to several thousands.

The key results are due to Albert and Vesanen. Albert's result is easy to prove, Vesanen's not so much.

Theorem 3.5 ([3, Theorem 8])**.** *A loop Q is simple if and only if its multiplication group* $\mathrm{Mlt}(Q)$ *acts primitively on Q.*

Theorem 3.6 ([45])**.** *Let Q be a finite loop. If* $\mathrm{Mlt}(Q)$ *is solvable then Q is solvable.*

Recall that a partition of Q is said to be *trivial* if it is of the form $\{Q\}$ or of the form $\{\{x\} : x \in Q\}$. A group $G \leq \mathrm{Sym}(Q)$ *preserves* a partition $\{B_1, \dots, B_n\}$ of Q if for every $\varphi \in G$ and every $1 \leq i \leq n$ there is $1 \leq j \leq n$ such that $\varphi(B_i) = B_j$. A transitive permutation group $G \leq \mathrm{Sym}(Q)$ is *primitive* if it does not preserve any nontrivial partition of Q. The *degree* of G is the cardinality of Q.

It is easy to see that every 2-transitive group $G \leq \mathrm{Sym}(Q)$ is primitive. (Consider a nontrivial partition $\{B_1, \dots, B_n\}$ with $n \geq 1$, B_1 containing distinct elements x, y, and let $z \in B_2$. Let $\varphi \in G$ be such that $\varphi(x) = x$ and $\varphi(y) = z$. Then $\varphi(B_1) \neq B_j$ for every $1 \leq j \leq n$.) Unlike finite 2-transitive groups, finite primitive groups are not classified [13]. `GAP` contains a library of all primite groups of degree < 2500. `MAGMA` [12] contains a library of all primitive groups of degree < 4096.

Lemma 3.7. *If Q is a loop of order bigger than 4 and $H \leq \mathrm{Aut}(Q)$ then H is not 3-transitive on $Q \setminus \{1\}$.*

Proof. Suppose that H is 3-transitive on $Q \setminus \{1\}$. Let x, $y \in Q$ be such that $|\{1, x, y\}| = 3$ and $z = xy \neq 1$. Then $\{x, y, z\}$ is a subset of $Q \setminus \{1\}$ of cardinality 3. Let $\varphi \in H$ be such that $\varphi(x) = x$, $\varphi(y) = y$ and $\varphi(z) \neq z$. (Here we use $|Q| > 4$.) We reach a contradiction with $\varphi(z) = \varphi(xy) = \varphi(x)\varphi(y) = xy = z$. □

Proposition 3.8. *All finite simple nonassociative automorphic loops are found in the set $\bigcup \mathcal{C}(Q, G, G_1)$, where the union is taken over sets Q of even order and over primitive groups $G \leq \mathrm{Sym}(Q)$ that are not solvable and not* 4*-transitive.*

Proof. Let $(Q, *)$ be a finite simple nonassociative automorphic loop of order $d > 1$ with the identity element 1. Let $G = \mathrm{Mlt}(Q, *)$. If $(Q, *)$ is solvable then it is an abelian group, a contradiction. By Theorem 2.21, we can assume that d is even. By Theorem 3.6, G is not solvable. If G is 4-transitive, then $G_1 \leq \mathrm{Aut}(Q, *)$ is 3-transitive on $Q \setminus \{1\}$, a contradiction with Lemma 3.7. It remains to show that $(Q, *) \in \mathcal{C}(Q, G, G_1)$. This follows from Lemma 3.4. □

Let $(Q, *) \in \bigcup \mathcal{C}(Q, G, G_1)$, where the union is as in Proposition 3.8. Suppose that we run the algorithm by incrementally increasing the cardinality of Q, and, for a fixed $d = |Q|$, by incrementally increasing the order of G. When should we catalog $(Q, *)$ as a newly found finite simple nonassociative automorphic loop? We first calculate the order of $M = \mathrm{Mlt}(Q, *) \leq G$. If $|M| < |G|$ then $(Q, *)$ is guaranteed to be automorphic (since $\mathrm{Inn}(Q, *) = M_1 \leq G_1 \leq \mathrm{Aut}(Q, *)$) but either M is not as in Proposition 3.8 or we have already seen $(Q, *)$ in $\mathcal{C}(Q, M, M_1)$, so we do not store $(Q, *)$. If $|M| > |G|$ then $(Q, *)$ is either not automorphic (checking this is expensive), or we will see the same loop later in $\mathcal{C}(Q, M, M_1)$, so we again do not store it. If $|M| = |G|$ then $(Q, *)$ is a finite simple nonassociative automorphic loop and we store it (upon checking for isomorphism against all already stored loops with the same multiplication group).

This search has been carried out in [29] for $d < 2500$ and recently by Cameron and Leemans [7] for $d < 4096$. The result is somewhat surprising:

Proposition 3.9. *There are no finite simple nonassociative automorphic loops of order less than* 4096*.*

We remark that Algorithm 3.3 finds numerous finite simple nonassociative left automorphic loops.

Are there any finite simple nonassociative commutative automorphic loops? The search for finite simple commutative automorphic loops can be reduced to orders 2^k by the following result (whose proof, incidentally, required another associated operation to show that a product of two squares is a square):

Theorem 3.10 ([25])**.** *Let Q be a finite commutative automorphic loop. Then Q is a direct product $A \times B$, where $A = \{x \in Q : |x| = 2^n$ for some $n\}$ and $B = \{x \in Q : |x|$ is odd$\}$. Morever, $|A| = 2^m$ for some m and $|B|$ is odd.*

With this decomposition at hand, we easily get:

Theorem 3.11 ([25]). *Let Q be a finite commutative automorphic loop. Then the Cauchy and Lagrange theorems hold for Q.*

It is much harder to deduce solvability in the even case. Grishkov, Kinyon and Nagy used advanced results on Lie algebras to prove:

Theorem 3.12 ([23]). *Every finite commutative automorphic loop is solvable.*

Thus there are no finite simple nonassociative commutative automorphic loops.

3.3. Commutative automorphic loops of order pq

Recall that a power-associative loop Q is a p-loop if every element of Q has order that is a power of p. From Theorem 3.11 we easily deduce that, for an odd prime p, a finite automorphic loop is a p-loop if and only if $|Q|$ is a power of p.

Let us now consider finite commutative automorphic loops. Unlike in abelian groups, the direct factor B from Theorem 3.10 does not necessarily decompose as a direct product of p-loops. In fact, for certain odd primes $p > q$, Drápal constructed a nonassociative commutative automorphic loop Q of order pq, which therefore does not factor as a direct product of an automorphic loop of order p and an automorphic loop of order q. We will discuss his construction at the end of this subsection. First we have a look at commutative automorphic loops of order pq in general.

Lemma 3.13. *Let Q be a power-associative loop. Then $Q/Z(Q)$ is never a nontrivial cyclic group.*

Proof. Suppose that $Q/Z(Q)$ is cyclic of order $m > 1$. Then there is $x \in Q \setminus Z(Q)$ such that $xZ(Q)$ has order m in $Q/Z(Q)$ and $Q = \bigcup_{0 \le i < m} x^i Z(Q)$. Therefore any element of Q can be written as $x^i a$ for some $0 \le i < m$ and $a \in Z(Q)$. With three elements of Q written in this form, we calculate

$$(x^i a \cdot x^j b) \cdot x^k c = (x^i x^j) x^k \cdot abc = x^i (x^j x^k) \cdot abc = x^i a \cdot (x^j b \cdot x^k c),$$

where we have used a, b, $c \in Z(Q)$ and power-associativity for $\langle x \rangle$. Hence Q is a group, and the result follows from the well-known fact that, in groups, $Q/Z(Q)$ is never a nontrivial cyclic group. □

Niederreiter and Robinson proved the following result while studying Bol loops of order pq:

Proposition 3.14 ([40]). *Let Q be a left Bol loop of order pq with odd primes $p > q$. Then Q contains a unique subloop of order p.*

Lemma 3.15. *Let Q be a nonassociative commutative automorphic loop of order pq with odd primes $p > q$. Then $Z(Q) = 1$, Q contains a normal subgroup S of order p, and all elements of $Q \setminus S$ have order q.*

Proof. We have $Z(Q) < Q$ by assumption. If $1 < Z(Q)$ then $Q/Z(Q)$ is isomorphic to $\mathbb{Z}_p$ or to $\mathbb{Z}_q$ by Corollary 2.8, a contradiction with Lemma 3.13. Hence $Z(Q) = 1$.

By Theorem 2.14, Q is solvable. Let $S = Q' < Q$. We have $1 < S$, else Q is an abelian group. Let $|S| = s$ and $\{s,t\} = \{p,q\}$. Then $|Q/S| = t$, and both S and Q/S are cyclic groups of prime order. Let $x \in Q \setminus S$. Then $|\langle xS\rangle| = |Q/S| = t$, so t divides $|x|$. By Theorem 2.7, either $|x| = st = pq$ or $|x| = t$. If $|x| = pq$ then $Q = \langle x\rangle$ is a group, a contradiction. Hence $|x| = t$.

Let $(Q,\circ)$ be the associated left Bruck loop. By Proposition 3.14, $(Q,\circ)$ contains a unique subloop of order p. Since powers in $(Q,\circ)$ and $(Q,\cdot)$ coincide, it follows that Q contains precisely $p-1$ elements of order p. Hence $s = p$. □

We will need the following two results:

Theorem 3.16 ([30])**.** *Let Q be a loop such that* $\mathrm{Inn}(Q)$ *is a cyclic group. Then Q is an abelian group.*

Theorem 3.17 (Albert)**.** *Let S be a normal subgroup of Q, and let $L_S = \{L_x : x \in S\}$. For a permutation group G on Q, let $G_S = \{\varphi \in G : \varphi|_S = \mathrm{id}_S\}$ and $G_{Q/S} = \{\varphi \in G : \varphi(xS) = xS$ for every $x \in Q\}$. Then* $\mathrm{Mlt}(Q)_S = L_S \cdot \mathrm{Inn}(Q)$, $\mathrm{Mlt}(Q)_{Q/S} = L_S \cdot \mathrm{Inn}(Q)_{Q/S}$ *and* $\mathrm{Inn}(Q/S) \cong (\mathrm{Mlt}(Q)_S)/(\mathrm{Mlt}(Q)_{Q/S})$.

Proposition 3.18. *Let Q be a nonassociative commutative automorphic loop of order pq with odd primes $p > q$. Then there is a normal subgroup $C \cong \mathbb{Z}_p$ of* $\mathrm{Inn}(Q)$ *such that* $\mathrm{Inn}(Q)/C$ *is a cyclic group of order dividing* $p-1$.

Proof. Let S be the unique normal subgroup of order p in Q, whose existence is guaranteed by Lemma 3.15. Consider the mapping $f : \mathrm{Inn}(Q) \to \mathrm{Aut}(S)$, $f(\varphi) = \varphi|_S$. Since $\varphi|_S\psi|_S(x) = \varphi|_S(\psi(x)) = \varphi(\psi(x)) = (\varphi\psi)|_S(x)$ for every $x \in S$, the mapping f is a homomorphism. Its kernel is equal to $C = \{\varphi \in \mathrm{Inn}(Q) : \varphi|_S = \mathrm{id}_S\}$. Now, $\mathrm{Aut}(S) \cong \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ is cyclic, so $\mathrm{Inn}(Q)/C \le \mathrm{Aut}(S)$ is a cyclic group of order dividing $p-1$. If C is trivial, we deduce that $\mathrm{Inn}(Q)$ is cyclic and Theorem 3.16 then implies that Q is an abelian group, a contradiction. Thus C is nontrivial.

Let $S = \langle s\rangle$ and fix $t \in Q\setminus S$. Since $L_s(St) = s(St) = (sS)t = St$, the mapping $\psi = L_s|_{St}$ is a bijection on St. We claim that ψ is a p-cycle. Suppose this is not the case. Since ψ has no fixed points and p is a prime, ψ must contain nontrivial cycles of distinct lengths. Then a suitable power of ψ, say ψ^i, has more than 1 but less than p fixed points. Without loss of generality, let t be a fixed point of ψ^i. Then $\alpha = L_t^{-1}L_s^iL_t \in \mathrm{Mlt}(Q)$ fixes 1. Thus $\alpha \in \mathrm{Inn}(Q) \le \mathrm{Aut}(Q)$, and $\alpha|_S \in \mathrm{Aut}(S)$. Moreover, since $\alpha|_S$ is conjugate to ψ^i, they have the same cycle structure. The fixed points of $\alpha|_S$ then determine a nontrivial proper subgroup of $S \cong \mathbb{Z}_p$, a contradiction.

Since Q/S is of prime order q, it is an abelian group and $\mathrm{Inn}(Q/S) = 1$. Then Theorem 3.17 gives $1 = \mathrm{Inn}(Q/S) \cong (L_S \cdot \mathrm{Inn}(Q))/(L_S \cdot \mathrm{Inn}(Q)_{Q/S})$, so $\mathrm{Inn}(Q) = \mathrm{Inn}(Q)_{Q/S}$. In other words, every $\varphi \in \mathrm{Inn}(Q)$ satisfies $\varphi(xS) = xS$ for every $x \in Q$.

Consider $1 \neq \varphi \in C$. Then φ is determined by the value on t, and $t \neq \varphi(t) \in St$. Because $\psi = L_s|_{St}$ is a p-cycle, there exists some $0 < j < p$ such that $\psi^j(t) = \varphi(t)$. Furthermore, $\varphi(s^k t) = s^k\varphi(t) = L_{s^k}\psi^j(t) = \psi^j L_{s^k}(t) = \psi^j(s^k t)$ by Proposition 1.3, so $\varphi|_{St} = \psi^j$. Because ψ^j is a p-cycle and $\varphi^k|_{St} = \psi^{jk}$ for every k, the elements φ, φ^2, …, $\varphi^p = 1$ are distinct and account for all elements of C. Hence $C \cong \mathbb{Z}_p$. □

Construction 3.19 ([16, Propositions 3.1 and 3.6]). *Let p be an odd prime and $t \in \mathbb{Z}_p$. Define a partial map $f_t : \mathbb{Z}_p \to \mathbb{Z}_p$ by $f_t(x) = (x+1)(tx+1)^{-1}$. Suppose that for every $i \geq 1$ the value $f_t^i(0)$ is defined and there is a unique $x \in \mathbb{Z}_p$ such that $f_t^i(x) = 0$. Let $d = |\{f_t^i(0) : i \geq 1\}|$. Then $\mathbb{Z}_p \times \mathbb{Z}_d$ with multiplication*

$$(i,a)(j,b) = (i+j, (a+b)(1+tf_t^i(0)f_t^j(0))^{-1})$$

is a commutative automorphic loop.

Proposition 3.20 ([28]). *Construction 3.19 yields a nonassociative commutative automorphic loop of order pq for odd primes $p > q$ if and only if q divides $p^2 - 1$, in which case it yields only one such loop up to isomorphism.*

Thanks to Proposition 3.18, all commutative automorphic loops of order pq could be classified by the *tour de force* of classifying all loops with trivial center and metacyclic inner mapping group, a program of Drápal that is nearing completion (see, for instance, [15]). Another, perhaps easier approach, is to classify all left Bruck loops of order pq, and then use Theorem 2.13. In particular, if there is a unique nonassociative left Bruck loop of order pq and q divides p^2-1, then it must correspond to a unique nonassociative commutative automorphic loop of order pq, constructed by Construction 3.19.

3.4. Commutative automorphic loops of order p^3

Proposition 3.21 ([26]). *Let p be an odd prime and Q a commutative automorphic loop. If $|Q| \in \{p, 2p, 4p, p^2, 2p^2, 4p^2\}$ then Q is an abelian group.*

Proof. By Theorem 3.10, it suffices to prove that all commutative automorphic loops Q of odd order p and p^2 are groups. For $|Q| = p$ this is a special case of Corollary 2.8, for instance. When $|Q| = p^2$ then $Z(Q)$ is nontrivial by Theorem 2.14, and the case $|Z(Q)| = p$ is excluded by Lemma 3.13. □

In view of Proposition 3.21, commutative automorphic loops of order p^3 (for any prime p) are of interest. As above, we can easily show that if such a loop is nonassociative of odd order p^3 then $Z(Q) \cong \mathbb{Z}_p$ and $Q/Z(Q) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. There are commutative automorphic loops of order 8 with trivial center [26].

Consider the following construction of [26]. Let $n \geq 2$ be an integer. The *overflow indicator* $(.,.)_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \{0,1\}$ is defined by

$$(x,y)_n = \begin{cases} 1, & \text{if } x+y \geq n, \\ 0, & \text{otherwise.} \end{cases}$$

For a, $b \in \mathbb{Z}_n$, define $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$ on $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$ by

$$\begin{aligned}&(x_1, x_2, x_3)(y_1, y_2, y_3)\\ &\quad= (x_1 + y_1 + (x_2 + y_2)x_3y_3 + a(x_2, y_2)_n + b(x_3, y_3)_n,\ x_2 + y_2,\ x_3 + y_3).\end{aligned}$$

Then $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$ is a commutative automorphic loop of order n^3, $Z(Q) = N_\ell(Q) = \mathbb{Z}_n \times 0 \times 0$, and $N_m(Q) = \mathbb{Z}_n \times \mathbb{Z}_n \times 0$.

It turns out that all nonassociative commutative automorphic loops of odd order p^3 are of the form $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$. This was shown by De Barros, Grishkov and the author, who studied quotients of free 2-generated nilpotent class 2 commutative automorphic loops and also proved:

Theorem 3.22 ([10]). *For every prime p, there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism, including the three abelian groups $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.*

The structure of the free 2-generated commutative automorphic loop of nilpotency class 2 can be found in [10, Theorem 2.3], which is proved by careful associator calculus. Lemma 3.23 below gives some insight, and once again shows that the middle nucleus is of key importance in automorphic loops.

Recall that the *associator* (x, y, z) is defined by $(xy)z = x(yz) \cdot (x, y, z)$.

Lemma 3.23 ([10, Lemmas 2.1 and 2.2]). *Let Q be a commutative loop of nilpotency class 2 (that is, $Q/Z(Q)$ is an abelian group). Then $(x, y, x) = 1$, $(x, y, z) = (z, y, x)^{-1}$ and $(x, y, z)(y, z, x)(z, x, y) = 1$ for every x, y, $z \in Q$. Moreover, Q is automorphic if and only if $(xy, u, v) = (x, u, v)(y, u, v)$ for every x, y, u, $v \in Q$.*

In the automorphic case, we have $(xy, u, v) = (x, u, v)(y, u, v)$, $(x, y, uv) = (x, y, u)(x, y, v)$, and $(x, yu, v) = (x, v, y)(x, v, u)(y, x, v)(u, x, v)$.

The structure of the free 2-generated commutative automorphic loop of nilpotency class 3 is also known, cf. [11, Theorem 5.4].

3.5. Two constructions of automorphic loops

We conclude the lecture notes with two constructions of automorphic loops.

Construction 3.24 ([24]). *Let R be a commutative ring, V an R-module and $E = \mathrm{End}_R(V)$ the ring of R-endomorphisms of V. Let $(W, +) \le (E, +)$ be such that*

(*i*) *$ab = ba$ for every a, $b \in W$, and*

(*ii*) *$1 + a$ is invertible for every $a \in W$.*

Define multiplication on $W \times V$ by

$$(a, u)(b, v) = (a + b,\ (1 + b)(u) + (1 - a)(v)).$$

Then $(W \times V, \cdot)$ is an automorphic loop.

A special case of this construction was first given in [27] in an effort to shed some light on automorphic loops of order p^3. (Automorphic loops of order p^2 are known to be groups by [8] or by [34, Theorem 6.1].) A slight variation on Construction 3.24 was also given in [37] in characteristic 2.

An important special case of Construction 3.24 can be given as follows: Let $R = k < K = V$, where $k < K$ is a field extension. Let W be a k-subspace of K such that $k1 \cap W = 0$. We can identify $a \in W$ with the k-endomorphism of K given by $b \mapsto ba$ (the right translation by a in $(K, \cdot)$). Then it is easy to see (cf. [24]) that the conditions (i) and (ii) of Construction 3.24 are satisfied, and we obtain an automorphic loop $Q_{k<K}(W) = Q_{R,V}(W)$ on $W \times K$.

Let us come back to automorphic loops of order p^3. In order to obtain them as loops $Q_{k<K}(W)$, we choose $k = \mathbb{F}_p$ to be the field of order p and $K = \mathbb{F}_{p^2}$ a quadratic field extension of k. If p is odd, we can find all suitable k-subspaces W as follows: The field K can be identified with $\{x + y\sqrt{d} \,:\, x,\, y \in k\}$, where $d \in k$ is not a square. Let

$$W_0 = k\sqrt{d} \text{ and } W_a = k(1 + a\sqrt{d}) \text{ for } 0 \neq a \in k.$$

Then every W_a is a 1-dimensional k-subspace of K such that $k1 \cap W_a = 0$. Conversely, if W is a 1-dimensional k-subspace of K such that $k1 \cap W = 0$, there is $a + b\sqrt{d}$ in W with $a,\, b \in k,\, b \neq 0$. If $a = 0$ then $W = W_0$. Otherwise $a^{-1}(a + b\sqrt{d}) = 1 + a^{-1}b\sqrt{d} \in W$, and $W = W_{a^{-1}b}$. Hence there is a one-to-one correspondence between the elements of k and 1-dimensional k-subspaces W of K satisfying $k1 \cap W = 0$, given by $a \mapsto W_a$.

Proposition 3.25 ([24]). *Let p be a prime and $\mathbb{F}_p = k < K = \mathbb{F}_{p^2}$.*

(*i*) *Suppose that p is odd. If $a,\, b \in k$, then the automorphic loops $Q_{k<K}(W_a)$, $Q_{k<K}(W_b)$ of order p^3 are isomorphic if and only if $a = \pm b$. In particular, there are $(p+1)/2$ pairwise nonisomorphic automorphic loops of order p^3 of the form $Q_{k<K}(W)$, where we can take $W \in \{W_a : 0 \leq a \leq (p-1)/2\}$.*

(*ii*) *Suppose that $p = 2$. Then there are 2 pairwise nonisomorphic automorphic loops of order p^3 of the form $Q_{k<K}(W)$.*

We do not claim that Proposition 3.25 accounts for all automorphic loops of order p^3.

Finally, we present a construction reminiscent of generalized dihedral groups.

Construction 3.26 ([1]). *Let $(G, +)$ be an abelian group and $m > 1$ an even integer. Let $\alpha \in \operatorname{Aut}(G)$. Define multiplication on $\mathbb{Z}_m \times G$ by*

$$(i, u)(j, v) = (i + j, \alpha^{ij}((-1)^j u + v)).$$

Then the resulting loop $\operatorname{Dih}(m, G, \alpha)$ is automorphic if and only if $m = 2$ or $\alpha^2 = 1$.

Aboras [2] obtained many structural properties of the dihedral-like automorphic loops $\mathrm{Dih}(m, G, \alpha)$, which are of interest because they account for many small automorphic loops.

The special case of Construction 3.26 with $m = 2$ was originally introduced in [34], and the following result was obtained there:

Theorem 3.27 ([34, Corollary 9.9])**.** *Let p be an odd prime, and let Q be a loop of order $2p$. Then Q is automorphic if and only if it is isomorphic to the cyclic group $\mathbb{Z}_{2p}$ or to a dihedral-like loop $\mathrm{Dih}(2, \mathbb{Z}_p, \alpha)$ for some $\alpha \in \mathrm{Aut}(\mathbb{Z}_p)$. There are precisely p pairwise nonisomorphic automorphic loops of order $2p$.*

Coming back full circle, the automorphic loop Q_6 from the introduction is isomorphic to the loop $\mathrm{Dih}(2, \mathbb{Z}_3, \alpha)$, where α is the unique nontrivial automorphism of $\mathbb{Z}_3$.

4. Open problems

Problem 4.1. *Is there a finite simple nonassociative automorphic loop?*

Problem 4.2. *Is there an automorphic loop of odd order with trivial middle nucleus?*

Problem 4.3. *If Q is a finite automorphic loop and $H \leq Q$, does $|H|$ divide $|Q|$?*

Let p be a prime.

Problem 4.4. *Find an elementary proof of the fact that automorphic loops of order p^2 are groups.*

Problem 4.5. *Classify automorphic loops of order p^3.*

Problem 4.6. *Classify commutative automorphic loops of order p^4.*

Problem 4.7. *Classify left Bruck loops of order pq and p^2q, where p, q are distinct odd primes.*

Problem 4.8. *Classify* (*commutative*) *automorphic loops of order pq and p^2q, where p, q are distinct odd primes.*

Problem 4.9. *Study free commutative automorphic loops with k free generators and of nilpotency class n. Already the cases $(k, n) = (2, 4)$ and $k \geq 3$ are open.*

Problem 4.10. *Study in detail the mapping $\Phi : (Q, \cdot) \mapsto (Q, \circ)$ that associates a uniquely 2-divisible left Bruck loop $(Q, \circ)$ to a uniquely 2-divisible automorphic loop $(Q, \cdot)$ via $x \circ y = (x^{-1} \backslash y^2 x)^{1/2}$. In particular, what is the image of Φ? If $(Q, \circ) \in \mathrm{im}(\Phi)$, is there also a commutative automorphic loop $(Q, \cdot)$ such that $(Q, \circ) = \Phi(Q, \cdot)$?*

Problem 4.11. *Can Proposition* 2.12 *be extended from left Bruck loops of odd order to uniquely* 2*-divisible left Bruck loops, perhaps under different correspondence?*

Problem 4.12. *Let* $(Q, +, [.,.])$ *be an algebra in which the condition* (2.10) *holds, and let* $(Q, \cdot)$ *be the associated linear loop with multiplication* $x \cdot y = x + y - [x, y]$. *Characterize when* $(Q, \cdot)$ *is an automorphic loop* (*beyond the obvious equational characterization*). *Are there interesting classes of algebras for which* $(Q, \cdot)$ *is always automorphic?*

Problem 4.13. *Let* $(Q, +, [.,.])$ *be a Lie ring satisfying* (2.10). *Characterize when the associated linear loop* $(Q, \cdot)$ *is automorphic* (*beyond the obvious equational characterization*).

An alternative theory of solvability in loop theory has been developed in [44], based on concepts from universal algebra (congruence modular varieties). Let us call this solvability *congruence solvability.* Congruence solvability is in general a stronger concept than solvability. To see whether congruence solvability is the right concept for loops, theorems previously proved for (classical) solvability in loops should be revisited. In particular:

Problem 4.14. *Are left Bruck* (*Moufang, commutative automorphic, automorphic*) *loops of odd order congruence solvable?*

Acknowledgment. I thank Michael Kinyon for useful conversations on the Greer correspondence, Přemysl Jedlička for comments on Construction 3.19, Aleš Drápal for the key idea in the proof of Proposition 3.18, and an anonymous referee for a few improvements to the presentation.

References

[1] **M. Aboras**, *Dihedral-like constructions of automorphic loops*, Comment. Math. Univ. Carolin. **55** (2014), 269–284.

[2] **M. Aboras**, *Dihedral-like constructions of automorphic loops*, PhD thesis, University of Denver, May 2015, preprint.

[3] **A.A. Albert**, *Quasigroups I*, Trans. Amer. Math. Soc. **54** (1943), 507–519.

[4] **M. Aschbacher**, *Near subgroups of finite groups*, J. Group Theory **1** (1998), 113–129.

[5] **R.H. Bruck**, *A survey of binary systems*, third printing, corrected, Ergebnisse der Mathematik und ihrer Grenzgebiete **20**, Springer Verlag, 1971.

[6] **R.H. Bruck and L.J. Paige**, *Loops whose inner mappings are automorphisms*, Ann. of Math. (**2**) **63** (1956), 308–323.

[7] **P. Cameron and D. Leemans**, e-mail correspondence, August 2014.

[8] **P. Csörgő**, *All automorphic loops of order p^2 for some prime p are associative*, J. Algebra Appl. **12** (2013), no. **6**, 1350013, 8 pp.

[9] **P. Csörgő**, *Multiplication groups of commutative automorphic p-loops of odd order are p-groups*, J. Algebra **350** (2012), 77–83.

[10] **D.A.S. De Barros, A. Grishkov and P. Vojtěchovský**, *Commutative automorphic loops of order p^3*, J. Algebra Appl. **11** (2012), no. **5**, 1250100, 15 pages.

[11] **D.A.S. De Barros, A. Grishkov and P. Vojtěchovský**, *The free commutative automorphic* 2*-generated loop of nilpotency class* 3, Comment. Math. Univ. Carolin. **53** (2012), 321–336.

[12] **W. Bosma, J. Cannon and C. Playoust**, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[13] **J.D. Dixon and B. Mortimer**, *Permutation groups*, Graduate Texts in Mathematics, Springer, New York, 1996.

[14] **A. Drápal**, *A-loops close to code loops are groups*, Comment. Math. Univ. Carolin. **41** (2000), 245–249.

[15] **A. Drápal**, *Orbits of inner mapping groups*, Monatsh. Math. **134** (2002), 191–206.

[16] **A. Drápal**, *A class of commutative loops with metacyclic inner mapping groups*, Comment. Math. Univ. Carolin. **49** (2008), 357–382.

[17] **A. Figula**, *Affine reductive spaces of small dimension and left A-loops*, Results Math. **49** (2006), no. **1**–**2**, 45–79.

[18] **T. Foguel, M.K. Kinyon and J.D. Phillips**, *On twisted subgroups and Bol loops of odd order*, Rocky Mountain J. Math. **36** (2006), no. **1**, 183–212.

[19] **The GAP Group**, GAP – Groups, Algorithms, and Programming, Version 4.4.10; 2007. `http://www.gap-system.org`

[20] **G. Glauberman**, *On loops of odd order I*, J. Algebra **1** (1964), 374–396.

[21] **G. Glauberman**, *On loops of odd order II*, J. Algebra **2** (1968), 393–414.

[22] **M. Greer**, *A class of loops categorically isomorphic to Bruck loops of odd order*, Commun. Algebra **42** (2014), 3682–3697.

[23] **A. Grishkov, M. Kinyon and G.P. Nagy**, *Solvability of commutative automorphic loops*, Proc. Amer. Math. Soc. **142** (2014), 3029–3037.

[24] **A. Grishkov, M. Rasskazova and P. Vojtěchovský**, *Automorphic loops arising from module endomorphisms*, preprint.

[25] **P. Jedlička, M. Kinyon and P. Vojtěchovský**, *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), 365–384.

[26] **P. Jedlička, M. Kinyon and P. Vojtěchovský**, *Constructions of commutative automorphic loops*, Commun. Algebra **38** (2010), 3243–3267.

[27] **P. Jedlička, M. Kinyon and P. Vojtěchovský**, *Nilpotency in automorphic loops of prime power order*, J. Algebra **350** (2012), 64–76.

[28] **P. Jedlička and D. Simon**, *On commutative A-loops of order pq*, J. Algebra Appl. **14** (2015), no. **3**, 1550041, 20 pp.

[29] **K.W. Johnson, M.K. Kinyon, G.P. Nagy and P. Vojtěchovský**, *Searching for small simple automorphic loops*, LMS J. Comput. Math. **14** (2011), 200–213.

[30] **T. Kepka and M. Niemenmaa**, *On loops with cyclic inner mapping groups*, Arch. Math. (Basel) **60** (1993), no. **3**, 233–236.

[31] **H. Kiechle**, *Theory of K-loops*, Lecture Notes in Math. **1778**, Springer-Verlag, Berlin, 2002.

[32] **M. Kikkawa**, *Geometry of homogeneous Lie loops*, Hiroshima Math. J. **5** (1975), 141–179.

[33] **M.K. Kinyon, K. Kunen and J.D. Phillips**, *Every diassociative A-loop is Moufang*, Proc. Amer. Math. Soc. **130** (2002), 619–624.

[34] **M.K. Kinyon, K. Kunen, J.D. Phillips and P. Vojtěchovský**, *The structure of automorphic loops*, Trans. Amer. Math. Soc., in press.

[35] **W.W. McCune**, *Prover9 and Mace4*, version 2009-11A. `http://www.cs.unm.edu/~mccune/prover9/`

[36] **R. Moufang**, *Zur Struktur von Alternativkörpern* (German), Math. Ann. **110** (1935), 416–430.

[37] **G.P. Nagy**, *On centerless commutative automorphic loops*, Comment. Math. Univ. Carolin. **55** (2014), 485–491.

[38] **G.P. Nagy and P. Vojtěchovský**, *LOOPS: Computing with quasigroups and loops in GAP*, version 2.0.0, computational package for GAP, `http://www.math.du.edu/loops`

[39] **P.T. Nagy and K. Strambach**, *Loops as invariant sections in groups, and their geometry*, Canad. J. Math **46** (1994), 1027–1056.

[40] **H. Niederreiter and K.H. Robinson**, *Bol loops of order pq*, Math. Proc. Cambridge Philos. Soc. **89** (March 1981), 241–256.

[41] **J.M. Osborn**, *A theorem on A-loops*, Proc. Amer. Math. Soc. **9** (1958), 347–349.

[42] **J.D. Phillips and P. Vojtěchovský**, *A scoop from groups: equational foundations for loops*, Comment. Math. Univ. Carolin. **49** (2008), 279–290.

[43] **K.K. Shchukin**, *Nilpotency of the multiplication group of an A-loop* (Russian), Mat. Issled. **102** (1988), 116–117.

[44] **D. Stanovský and P. Vojtěchovský**, *Commutator theory for loops*, J. Algebra **399** (2014), 290–322.

[45] **A. Vesanen**, *Solvable groups and loops*, J. Algebra **180** (1996), 862–876.

[46] **C.R.B. Wright**, *On the multiplication group of a loop*, Illinois J. Math. **13** (1969), 660–673.

Received May 4, 2015

Department of Mathematics, University of Denver 2280 S Vine St., Denver, Colorado 80208, U.S.A.
E-mail: petr@math.du.edu