Quasigroups and Related Systems **10** (2003), 1 − 28

Check character systems over quasigroups and loops

Galina B. Belyavskaya, Vladimir I. Izbash, Victor A. Shcherbacov

Abstract

In this paper we survey the known results concerning check character (or digit) systems with one check character based on quasigroups (loops, groups). These are codes with one control symbol detecting errors of specific types.

This survey includes the following sections: 1. Introduction. 2. Check character systems over groups. 3. Check character systems over quasigroups. 4. Check character systems over T-quasigroups. 5. Detection sets and detection rate. 6. Equivalence of check character systems. 7. Check character systems as n-ary operations.

1. Introduction

The aim of the present article is to survey the known results concerning check character (or digit) systems with one check character based on quasigroups (loops, groups).

A check digit system with one check character is an error detecting code $\mathfrak{C}$ over an alphabet A which arises by appending *a check digit* (symbol) a_n to every word $a_1a_2\dots a_{n-1} \in A^{n-1}$:

$$\mathfrak{C} : \begin{cases} A^{n-1} & \longrightarrow \quad A^n \\ a_1a_2\dots a_{n-1} & \longmapsto \quad a_1a_2\dots a_{n-1}a_n. \end{cases}$$

2000 Mathematics Subject Classification: 20N05, 20N15, 94B60, 94B65

Keywords: quasigroup, loop, group, automorphism, orthomorphism, code, n-ary quasigroup, check character system

The research described in this publication was made possible in part by Award No. MM2-3017 of the Moldovan Research and Development Association (MRDA) and the U.S. Civilian Research & Development Foundation for the Independent States of the Former Soviet Union (CRDF).

The purpose of using such a system is to detect transmission errors (which can arise once in a code word), in particular, made by human operators during typing of data.

The examples of check character systems used in practice are the following:

- the European Article Number (EAN) Code,
- the Universal Product Code (UPC),
- the International Standard Book Number (ISNB) Code,
- the system of the serial numbers of German banknotes,
- different bar-codes used in the service of transportation, automation of various processes and so on.

The control digit of a system based on a quasigroup (system over a quasigroup) is calculated by distinct check formulas (check equations) using quasigroup operations.

D. F. Beckley [1] and J. Verhoeff [27] investigated statistically errors made by human operators. They classified them as single errors (that is errors in only one component of a code word), (adjacent or neighbour) transpositions, i.e. errors of the form $\dots ab \dots \longrightarrow \dots ba \dots$, jump transpositions $(\dots abc \dots \to \dots cba \dots)$, twin errors $(\dots aa \dots \to \dots bb \dots)$, jump twin errors $(\dots aca \dots \to \dots bcb \dots)$ and phonetic errors $(\dots a0 \dots \to \dots 1a \dots,$ $a \geqslant 2)$. Single errors and transpositions are the most prevalent ones.

Table 1: Error types and their frequencies ([23]).

Error type		Relative frequency %	
		Verhoeff	Beckley
single error	$\dots a \dots \to \dots b \dots$	79.0 (60-95)	86
adjacent transposition	$\dots ab \dots \to \dots ba \dots$	10.2	8
jump transposition	$\dots abc \dots \to \dots cba \dots$	0.8	
twin error	$\dots aa \dots \to \dots bb \dots$	0.6	6
phonetic error ($a \geqslant 2$)	$\dots a0 \dots \to \dots 1a \dots$	0.5	
jump twin error	$\dots aca \dots \to \dots bcb \dots$	0.3	
other error		8.6	

Phonetic errors depend on the language and we shall not consider them here.

The work [27] of J. Verhoeff is the first significant publication that systematically studies systems for detection of errors made by human operators. It contains a survey of the decimal codes known in the begin of 1970-th.

A. Ecker and G. Poch in [12] have given a survey of elementary methods for the construction of check character systems (that is of the methods that do not use any mathematics other than simple arithmetical computations) and their analysis from mathematical point of view. In particular, the group-theoretical background of the known methods was explained and new codes were presented that stem from the theory of quasigroups. All methods using the modulo 10 sum can be described in the following way.

Let $a_1a_2\dots a_{n-1}$ $(n \geqslant 3)$ be a word over the alphabet $A = \{0, 1, \dots, 9\}$. The decimal code with one check digit $a_n \in A$ is defined by permutations $\delta_1, \delta_2, \dots, \delta_n$ on A together with the check equation

$$\sum_{i=1}^{n} \delta_i a_i \equiv c \pmod{10}, \quad c \in A$$

(usually $c = 0$), that is

$$a_n = \delta_n^{-1}(c - \sum_{i=1}^{n-1} \delta_i a_i) \pmod{10}.$$

Note that everywhere we do not use brackets for an application of a mapping. For example, we write αb instead of $\alpha\,(b)$.

So, the IBM code defined by the permutation

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

and the check equation

$$a_n + \delta a_{n-1} + a_{n-2} + \delta a_{n-3} + \dots \equiv c \text{ (mod10)}, \quad c \in A,$$

detects all single errors. Transposition errors will not be detected completely as the transposition 0 and 9 goes undetected. None of the jump transpositions or jump twin errors are detected. The generalized IBM code with the check equation

$$\sum_{i=1}^{n} \delta^{i-1} a_{n+1-i} \equiv c \text{ (mod10)}, \quad c \in A,$$

detects jump transpositions and jump twin errors with the defined accuracy.

In the paper [12] many other known elementary check systems modulo 10, 11 and $k > 11$ are presented with a short discussion concerning each system. More general group theoretical investigations are also considered which include all systems modulo different numbers. For that it is sufficient to take an arbitrary abelian (or non-abelian) group $G = G(+)$ and the following check equation

$$\sum_{i=1}^{n} \delta_i a_i = c \in G, \tag{1}$$

where $\delta_1, \delta_2, \ldots, \delta_n$ are fixed permutations of G.

So, the Universal Product Code (UPC) is a code with $G = Z_{10}(+)$, $n = 13$, $\delta_{2i-1} = \varepsilon = \delta_{13}$ and $\delta_{2i}a = 3a$ for $i = 1, \ldots, 6$, $c = 0$, where ε denotes the identity permutation. The check equations of the European Article Number (EAN) Code and the International Standard Book Number (ISNB) Code see in the end of the present article.

In Section 5 of [12] the possibility of constructing of check character systems based on Latin squares (or on quasigroups) is also investigated. The error detecting capability of such code may be better than of a modulo m check system.

A *Latin square of order* n is a square matrix with entries of n distinct elements each occurring exactly once in each row and column ([10]).

A *quasigroup* $Q(\cdot)$ is a binary operation $(\cdot)$ defined on the set Q such that for any two elements $a, b \in Q$ each of the equations $a \cdot x = b$, $y \cdot a = b$ has exactly one solution [10].

A *loop* is a quasigroup with the identity element e ($x \cdot e = e \cdot x = x$ for all $x \in Q$).

For example, the operation

$$a \cdot b = (ha + kb + l) \pmod n$$

where h, k, l are fixed integers from $Z_n = \{0, 1, \ldots, n-1\}$ with h and k relative prime to n defines a quasigroup on the set Z_n.

It is easy to verify that the multiplication table of a finite quasigroup is a Latin square. Conversely, a Latin square may be interpreted as a quasigroup.

H. P. Gumm [15] considers a check character system as an n-ary operation with the properties permitting to detect all single errors and all transposition errors. Later M. Damm in [8] and G. L. Mullen with V. Shcherbacov in [18] continued this approach and studied the considered systems related to n-ary operations (quasigroups). The work [8] of M. Damm contents as well a good survey of check character systems over groups and groups which are able to detect all transpositions (and all single errors).

Choosing $Q(\cdot)$ as a finite set endowed with an binary algebraic structure (a groupoid) one can take the following general check formulas for calculation of the control symbol a_n:

$$a_n = (\dots((\delta_1 a_1 \cdot \delta_2 a_2) \cdot \delta_3 a_3)\dots) \cdot \delta_{n-1} a_{n-1} \tag{2}$$

or

$$(\dots((\delta_1 a_1 \cdot \delta_2 a_2) \cdot \delta_3 a_3)\dots) \cdot \delta_n a_n = c \tag{3}$$

for fixed permutations δ_i of Q, $i = 1, 2, \dots, n$ and a fixed element c of Q.

It is easy to see that a (finite) check character system with check formula (2) or (3) detects all single errors if and only if $Q(\cdot)$ is a quasigroup. The other errors will be detected if and only if this quasigroup has specific properties.

Often a permutation δ_i in (2), (3) is chosen such that $\delta_i = \delta^{i-1}$, $i = 1, \dots, n$, for a fixed permutation δ of Q. In this case we obtain the following check formulas respectively:

$$a_n = (\dots((a_1 \cdot \delta a_2) \cdot \delta^2 a_3)\dots) \cdot \delta^{n-2} a_{n-1} \tag{4}$$

and

$$(\dots((a_1 \cdot \delta a_2) \cdot \delta^2 a_3)\dots) \cdot \delta^{n-1} a_n = c. \tag{5}$$

In the following sections we shall survey the check character systems over groups, quasigroups, loops, T-quasigroups, the check character systems considered as n-ary quasigroups, equivalences of check character systems.

The main attention will be focussed on check character systems over quasigroups and loops.

2. Check character systems over groups

Let $G(= G(\cdot)$ be a group with the identity e. Then the most general check equation is the equation (1) (usually $c = e$) and the formula (5) has the form

$$a_1 \cdot \delta a_2 \cdot \delta^2 a_3 \cdot \dots \cdot \delta^{n-1} a_n = e. \tag{6}$$

In [27] and [12] the conditions on a permutation δ_i (or δ) are given that make it possible to detect errors of different types. The error detection conditions for abelian groups (see Table 2) can be expressed by certain concepts that are recalled below. These conditions get more complicated when G is assumed to be non-abelian (see Table 3).

Before recall required concepts.

Definition 2.1 [10]. A *complete mapping* of a quasigroup (a group) is a bijective mapping $x \to \theta x$ of Q onto Q such that the mapping $x \to \eta x$ defined by $\eta x = x \cdot \theta x$ is again a bijective mapping of Q onto Q.

Definition 2.2 [11]. A permutation α of a group $G(+)$ is called an *orthomorphism* if $x - \alpha x = \beta x$ where β is a permutation of G and $-x$ is the opposite element for x in the group.

Definition 2.3 [23]. A permutation δ of $G(\cdot)$ is called *anti-symmetric* in a group (in a quasigroup) G if it fulfills the condition $x \cdot \delta y \neq y \cdot \delta x$ for all $x, y \in G, \quad x \neq y$.

In this paper are always composed from the right to the left.

Table 2: Conditions for error detection by (1) (by (6)), $n > 4$ with a finite abelian group

Error type	Conditions for all i
single error	δ_i (δ) permutation
adjacent transposition	$\delta_{i+1}\delta_i^{-1}$ (δ) orthomorphism
jump transposition	$\delta_{i+2}\delta_i^{-1}$ (δ^2) orthomorphism
twin error	$\delta_{i+1}\delta_i^{-1}$ (δ) complete mapping
jump twin error	$\delta_{i+2}\delta_i^{-1}$ (δ^2) complete mapping

Table 3: Conditions for error detection by (1), $n > 4$ with a finite non-abelian group

Error type	Conditions for all i, x, y, z
single error	δ_i permutation
adjacent transposition	$\delta_{i+1}\delta_i^{-1}$ anti-symmetric permutation
jump transposition	$x \cdot y \cdot \delta_{i+2}\delta_i^{-1} z \neq z \cdot y \cdot \delta_{i+2}\delta_i^{-1} x, \quad x \neq z$
twin error	$\delta_{i+1}\delta_i^{-1}$ complete mapping
jump twin error	$x \cdot y \cdot \delta_{i+2}\delta_i^{-1} x \neq z \cdot y \cdot \delta_{i+2}\delta_i^{-1} z, \quad x \neq z$

As it was pointed the transpositions are the most prevalent errors and their detection is connected with anti-symmetric mappings (see Table 3), so in the works [8], [9] of M. Damm and in the articles [13], [16], [17], [21], [22], [23], [24], [25] and [26] much attention is given to research of groups with anti-symmetric mappings. A survey of anti-symmetric mappings in different groups can be found in the article [23] of R. H. Schulz.

For the completeness we shall give the main results on the groups having anti-symmetric mappings in the order of their publication. Note that the results for abelian groups often follow as corollaries of known results concerning complete mappings.

- Abelian groups of order $m = 2n$ with n odd do not admit anti-symmetric mappings [23].

- The cyclic group G admits an anti-symmetric mapping if and only if $|G|$ is odd [23].

- All groups of odd order admit an anti-symmetric mappings [13].

- For $m > 2$ the symmetric group S_m and the alternating group A_m have anti-symmetric mappings [13].

- Every finite simple group except Z_2 has an anti-symmetric mapping [13].

- Every non-trivial finite p-group which is not a cyclic 2-group has anti-symmetric mappings [13].

- Every finite nilpotent group with a trivial or the non-cyclic Sylow 2-subgroup has an anti-symmetric mapping [13].

Taking into account these results J. A. Gallian and M. D. Mullin made the following

Conjecture 2.4 [13]. *All non-abelian groups have anti-symmetric mappings.*

This conjecture has been confirmed by S. Heiss at first for soluble groups in [16], later for each non-abelian group.

Theorem 2.5 [17]. *Every non-abelian group admits an anti-symmetric mapping.*

J. Verhoeff [27] has pointed out a number of anti-symmetric mappings of the dihedral groups D_5 and D_m, $m > 5$. We remember that the dihedral group D_m is a group of order $2m$ of such form

$$D_m = \langle d, s \mid d^m = e = s^2, \quad ds = sd^{-1} \rangle.$$

Note that within the group theory the dihedral group with $2m$ elements is usually denoted by D_{2m}.

Other anti-symmetric mappings of the dihedral groups were found in [15], [12], [13]. All these mappings give a possibility to obtain check character systems detecting all transpositions.

M. Damm proved the following important theorem.

Theorem 2.6 [8]. *For $m \geqslant 3$ odd there does not exist a check digit system over D_m which detects all jump transpositions or all twin errors or all jump twin errors.*

In [26] (see also [24]) all anti-symmetric mappings, automorphisms and anti-automorphisms of the dicyclic groups Q_2 (it is the quaternion group) and Q_3 of order 8 and 12, respectively, were obtained by computer search. These groups are

$$Q_2 = \langle a, b \ \mid \ a^4 = e, \quad b^2 = a^2, \quad ab = ba^{-1} \rangle$$

and

$$Q_3 = \langle a, b \ \mid \ a^6 = e, \quad b^2 = a^3, \quad ab = ba^{-1} \rangle.$$

Recall that an automorphism α of a group with the identity e is called regular if $\alpha x \neq x$ for each $x \neq e$ (such permutation α is called a fixed point free permutation).

Anti-symmetric automorphisms and anti-automorphisms of groups were considered by R. H. Schulz in [22], [23] and M. Damm in [8]. So, the following statement is proved.

Proposition 2.7 [23]. *An automorphism δ of a finite group G with the identity e is anti-symmetric if and only if δ does not fix any conjugacy class of $G\backslash\{e\}$. When G is abelian, then this is the case if and only if the automorphism δ is regular.*

Due to the works [27], [7], [12] necessary and sufficient conditions on a permutation (or on an automorphism) δ for detection each of five error types by a check digit system over a group G with check formula (6), $n > 4$ can be given in the following Table 4, where S_G (Aut$G$) denotes the set of all permutations (or the automorphism group, respectively) of G.

Table 4: Error detection of systems over groups with (6), $n > 4$

Error type	Conditions on δ, for all $x, y, z \in G$	
	$\delta \in S_G$	$\delta \in \operatorname{Aut} G$, $x \neq e$
single errors	none	none
transpositions	$x \cdot \delta y \neq y \cdot \delta x, x \neq y$	$\delta x \neq y^{-1}xy$
jump transpositions	$xy \cdot \delta^2 z \neq zy \cdot \delta^2 x$, $x \neq z$	$\delta^2 x \neq y^{-1}xy$
twin errors	$x \cdot \delta x \neq y \cdot \delta y$, $x \neq y$	$\delta x \neq y^{-1}x^{-1}y$
jump twin errors	$xy \cdot \delta^2 x \neq zy \cdot \delta^2 z$, $x \neq z$	$\delta^2 x \neq y^{-1}x^{-1}y$

Definition 2.8 [7]. Let G be a finite group. An automorphism δ of G is called *good* provided δx is not conjugate to x or x^{-1} and $\delta^2 x$ is not conjugate to x or x^{-1} for all $x \in G$, $x \neq e$, where x^{-1} is the inverse element for x.

Proposition 2.9 [7]. *A good automorphism is anti-symmetric and detects all single errors, transpositions, jump transpositions, twin errors and jump twin errors.*

In [7] it is shown that there are many groups possessing a good automorphism.

The class of groups having anti-symmetric mappings is extension closed according to

Theorem 2.10 [13]. *If G is a group with a normal subgroup H and there exist anti-symmetric mappings φ on H and ψ on G/H, then there exists an anti-symmetric mapping γ on G.*

3. Check character systems over quasigroups and loops

In this section we shall mainly survey new results concerning check character systems over quasigroups with check formulas (4) or (5) which are able to detect single errors, transpositions, jump transpositions, twin errors and jump twin errors in all digits of a code word (including the control digit).

Consider the following conditions which hold for all $a, b, c, d \in Q$ in a quasigroup $Q(\cdot)$, $\delta \in S_Q$:

(α_1) $\quad b \cdot \delta c \neq c \cdot \delta b$, if $b \neq c$;

(α_2) $ab \cdot \delta c \neq ac \cdot \delta b$, if $b \neq c$;
(α_3) $(a = d \cdot \delta^{n-2} b$ *and* $b = d \cdot \delta^{n-2} a) \Rightarrow (a = b)$;
(β_1) $dc \cdot \delta^2 b \neq bc \cdot \delta^2 d$, *if* $b \neq d$;
(β_2) $(ad \cdot c) \cdot \delta^2 b \neq (ab \cdot c) \cdot \delta^2 d$, *if* $b \neq d$;
(β_3) $(d = (a \cdot \delta^{n-3} b) \cdot c$ *and* $b = (a \cdot \delta^{n-3} d) \cdot c) \Rightarrow (b = d)$;
(γ_1) $b \cdot \delta b \neq c \cdot \delta c$ if $b \neq c$;
(γ_2) $ab \cdot \delta b \neq ac \cdot \delta c$ if $b \neq c$;
(γ_3) $(a = d \cdot \delta a$ *and* $b = d \cdot \delta b) \Rightarrow (b = a)$;
(σ_1) $bc \cdot \delta^2 b \neq dc \cdot \delta^2 d$, *if* $b \neq d$;
(σ_2) $(ab \cdot c) \cdot \delta^2 b \neq (ad \cdot c) \cdot \delta^2 d$, *if* $b \neq d$;
(σ_3) $(d = (a \cdot \delta^{n-3} d) \cdot c$ *and* $b = (a \cdot \delta^{n-3} b) \cdot c) \Rightarrow (b = d)$.

The main theorem of [4] that points necessary and sufficient conditions for detection of considered five error types by a check character system over a quasigroup with the check formula (4) or (5), $n > 4$ it is convenient to give in Table 5.

Table 5: Error detection of systems over quasigroups

Error type	Conditions on $\delta \in S_Q$, $n > 4$	
	Check formula (4)	Check formula (5)
single errors	none	none
transpositions	$(\alpha_1), (\alpha_2)$ and (α_3)	(α_1) and (α_2)
jump transpositions	$(\beta_1), (\beta_2)$ and (β_3)	(β_1) and (β_2)
twin errors	$(\gamma_1), (\gamma_2)$ and (γ_3)	(γ_1) and (γ_2)
jump twin errors	$(\sigma_1), (\sigma_2)$ and (σ_3)	(σ_1) and (σ_2)

It is clear from this table why formula (5) should be preferred. Note that the conditions for formula (5) do not depend on the size of n.

The conditions for transpositions, and jump transpositions with the check formula (4) were established earlier by R. H. Schulz in [20].

If a quasigroup $Q(\cdot)$ is a group and the check formula (5) is used, then the conditions (α_1), (β_1), (γ_1) and (δ_1) are both necessary and sufficiently, as they coincide with the conditions of Table 4, respectively.

If $Q(\cdot)$ is a quasigroup with the left identity e ($ex = x$ for all $x \in Q$) or a loop ($ex = xe = x$ for all $x \in Q$), then such conditions are correspondingly (α_2), (β_2), (γ_2) and (δ_2) [4].

Let $L_a x = ax, R_a x = xa$ for all $x \in Q$ in a quasigroup $Q(\cdot)$. The following statement is a corollary of the conditions from Table 5.

Proposition 3.1 [4]. *Let $Q(\cdot)$ be a finite quasigroup. Then*

- *condition (γ_1) holds if and only if the permutation δ is a complete mapping;*
- *condition (γ_2) holds if and only if the permutation δL_a^{-1} is a complete mapping for all $a \in Q$;*
- *condition (σ_1) holds if and only if the permutation $\delta^2 R_c^{-1}$ is a complete mapping for all $c \in Q$;*
- *condition (σ_2) holds if and only if the permutation $\delta^2 L_a^{-1} R_c^{-1}$ is a complete mapping for all $a, c \in Q$.*

In Corollary 3.2 below we shall observe that each conditions (γ_2), (σ_1) and (σ_2) can be associated with the notion of orthogonal Latin squares. That makes these conditions, in certain sense, "strong".

Two Latin squares $L_1 = ||a_{ij}||$ and $L_2 = ||b_{ij}||$ on m symbols are said to be *orthogonal* if every ordered pair of symbols occurs exactly once among the m^2 pairs (a_{ij}, b_{ij}), $i, j = 1, 2, \dots, m$ [10].

A *pair of orthogonal quasigroups* corresponds to a pair of orthogonal Latin squares and conversely.

Two quasigroups $Q(\cdot)$ and $Q(\circ)$ are called *orthogonal* if the system of equations

$$\begin{cases} x \cdot y = a \\ x \circ y = b \end{cases}$$

has an unique solution for all $a, b \in Q$.

Corollary 3.2 [4]. *If a finite quasigroup $Q(\cdot)$ satisfies the conditions γ_2 $((\sigma_1)$ or $(\sigma_2))$, then it has an orthogonal mate* (*pair*).

We can say more when $Q(\cdot)$ is a loop and δ is the identity permutation.

Recall that a *Moufang loop* is a loop which satisfies the Moufang identity $(zx \cdot y) \cdot x = z(x \cdot yx)$ (see [2], [10]).

Proposition 3.3 [4]. *If $Q(\cdot)$ is a loop, $\delta = \varepsilon$, $n > 4$, then*

- *properties (α_1) and (β_1) do not hold;*
- *from (σ_2) it follows (γ_2);*
- *in a Moufang loop* (*in particular, in a group*) *conditions (γ_1), (γ_2), (σ_1) and (σ_2) are equivalent.*

Corollary 3.4 [4].

- *It is impossible using a loop to detect all transpositions (jump transpositions, twin errors or jump twin errors) if check formula* (4) *is applied with* $\delta = \varepsilon$, $n > 4$.

- *A finite Moufang loop (a finite group) with check formula* (5), $\delta = \varepsilon$, $n > 4$ *does not detect all transpositions and jump transpositions, but detects all twin errors and all jump twin errors if and only if* $b^2 \neq d^2$ *for all* $b \neq d$ *(that is the identity permutation is a complete mapping).*

- *A check character system using a Moufang loop (a group) of odd order and check formula* (5) *with* $\delta = \varepsilon$, $n > 4$ *detects all twin errors and all jump twin errors.*

- *A check character system using an abelian group and coding formula* (5) *with* $\delta = \varepsilon$, $n > 4$ *detects all twin errors and all jump twin errors if and only if the group has odd order.*

These results show that check character systems over loops (groups) with formula (4) or (5) with $\delta = \varepsilon$, $n > 4$ cannot detect all transpositions and jump transpositions. In this case it is possible to use formula (4) or (5) with $\delta \neq \varepsilon$ for a quasigroup or it is possible to use formula (1) for a group.

4. Check character systems over T-quasigroups

There is another way to use groups for construction of check digit systems detecting these errors as well. Namely, instead of a group $Q(\circ)$ it is possible to take a quasigroup $Q(\cdot)$ which is isotopic to this group:

$$x \cdot y = \gamma^{-1}(\alpha x \circ \beta y)$$

where α, β, γ are permutations of Q [10, 2]. Such an idea is used in this section.

A quasigroup $Q(\cdot)$ is called a *T-quasigroup* if there exist an abelian group $Q(+)$ with automorphisms φ and ψ and a fixed element $g \in Q$ such that $x \cdot y = \varphi x + \psi y + g$ for all $x, y \in Q$ [19].

The concept of a T-quasigroup is a particular case of the concept of a quasigroup which is isotopic to an abelian group and it generalizes the concept of a medial quasigroup (see, for example, [2]).

Denote by $\operatorname{Ort} Q(+)$ the set of all orthomorphisms of a group $Q(+)$. Necessary and sufficient conditions for error detection of systems with formula (4) or (5), $n > 4$ are presented in Table 6 (see Theorems 1 and 3 of [5], respectively), where $Ix = -x$. The respective permutations that appear in Table 6 must be in $\operatorname{Ort} Q(+)$.

Table 6: Error detection of systems over T-quasigroups $x \cdot y = \varphi x + \psi y + g$

Error type	Conditions on δ permutations of $\operatorname{Ort} Q(+)$	
	Check formula (4)	Check formula (5)
single errors	none	none
transpositions	$\psi\delta\varphi^{-1}$, $\psi\delta\psi^{-1}\varphi^{-1}$, $I\psi\delta^{n-2}$	$\psi\delta\varphi^{-1}$, $\psi\delta\psi^{-1}\varphi^{-1}$
jump transpositions	$\psi\delta^2\varphi^{-2}$, $\psi\delta^2\psi^{-1}\varphi^{-2}$, $I\varphi\psi\delta^{n-3}$	$\psi\delta^2\varphi^{-2}$, $\psi\delta^2\psi^{-1}\varphi^{-2}$
twin errors	$I\psi\delta\varphi^{-1}$, $I\psi\delta\psi^{-1}\varphi^{-1}$, $\psi\delta$	$I\psi\delta\varphi^{-1}, I\psi\delta\psi^{-1}\varphi^{-1}$
jump twin errors	$I\psi\delta^2\varphi^{-2}$, $I\psi\delta^2\psi^{-1}\varphi^{-2}$, $\varphi\psi\delta^{n-3}$	$I\psi\delta^2\varphi^{-2}$, $I\psi\delta^2\psi^{-1}\varphi^{-2}$

In the both cases of the check formulas the conditions do not depend on the element $g \in Q$ and in the case of formula (5) the conditions do not depend on length $n > 4$ of a code word.

Corollary 4.1 [5]. *If in Table 6 δ is an automorphism of the abelian group $Q(+)$, then all described errors are detected if and only if the respective permutations are regular automorphisms.*

In [5] the conditions are also given when $\delta = I,\ \varepsilon,\ \varphi$ or ψ^{-1}. If $\delta = \varepsilon$, we obtain the conditions of Table 7.

According to Proposition 2 of [5] direct product of T-quasigroups detecting all errors of some type detects also all errors of the same type if formula (4) (or (5)) with $\delta = \varepsilon,\ n > 4$ is used.

In [5] a number of T-quasigroups is given satisfying all conditions from Table 6 (Table 7) if formula (4) (or (5)) is used with $\delta = \varepsilon$ and consequently, check character systems over such T-quasigroups with $\delta = \varepsilon$ are able to detect all of the five error types in contrast to check character systems over loops or groups (see Corollary 3.4).

Table 7: Error detection of systems over T-quasigroups $x \cdot y = \varphi x + \psi y + g$

Error type	Conditions on φ, ψ if $\delta = \varepsilon, n > 4$ in (5)
single errors	none
transpositions	φ, $\varphi\psi^{-1}$ are regular
jump transpositions	φ^2, $\varphi^2\psi^{-1}$ are regular
twin errors	$I\varphi^1$, $I\varphi\psi^{-1}$ are regular
jump twin errors	$I\varphi^2$, $I\varphi^2\psi^{-1}$ are regular

5. Detection sets and detection rate of check digit systems

For any check character system over a quasigroup it is possible to define a detection set and a detection rate (percentage) of errors of each type. In Table 2 of [23] (see also [27] and [14]) a rate of detection for a check character system over a group of order q with check formula (6), $n > 4$ is pointed out. This information we give in Table 8, where detection sets M_T, M_{jT}, M_{TE}, M_{jTE} of transpositions, twin errors and jump twin errors respectively are defined in the following way:

$$M_T = \{(a,b) \in Q^2 \,|\, a \cdot \delta b \neq b \cdot \delta a,\ a \neq b\},$$

$$M_{jT} = \{(a,b,c) \in Q^3 \,|\, ab \cdot \delta^2 c \neq cb \cdot \delta^2 a,\ a \neq c\},$$

$$M_{TE} = \{(a,b) \in Q^2 \,|\, a \cdot \delta a \neq b \cdot \delta b,\ a \neq b\},$$

$$M_{jTE} = \{(a,b,c) \in Q^3 \,|\, ab \cdot \delta^2 a \neq cb \cdot \delta^2 c,\ a \neq c\}.$$

Note that these sets are considered as detection sets of the respective errors, since if $(a,b) \in M_T$ (or $(a,b) \in M_{TE}$), then the transposition $\dots ab \dots \to \dots ba \dots$ (or the twin error $\dots aa \dots \to \dots bb \dots$, respectively) will be detected.

If $(a,b,c) \in M_{jT}$ (or $(a,b,c) \in M_{jTE}$), then the jump transposition $\dots abc \dots \to \dots cba \dots$ (or the jump error $\dots aba \dots \to \dots cbc \dots$, respectively) will be defined.

The maximal number of the pairs (a, b) with $a \neq b$ (the triples (a, b, c) with $a \neq c$) in a group of order q is $q(q-1)$ (or $q^2(q-1)$, respectively), so we obtain a percentage (or a rate) of detection from Table 8 (compare with Table 4).

Table 8: Detection of errors by check character systems over groups of order q

Error type	Detection set	Percentage of detection
transpositions	M_T	$\lvert M_T\rvert/q(q-1)$
jump transpositions	M_{jT}	$\lvert M_{jT}\rvert/q^2(q-1)$
twin errors	M_{TE}	$\lvert M_{TE}\rvert/q(q-1)$
jump twin errors	M_{jTE}	$\lvert M_{jTE}\rvert/q^2(q-1)$

Let $S(Q(\cdot), \delta)$ denote a check character system over a quasigroup of order q with the check formula (5), $n > 4$. For such a system detection sets M_T^δ, M_{jT}^δ, M_{TE}^δ and M_{jTE}^δ are more complicated and are defined in the following way [6]:

$$M_T^\delta = U_1^\delta \cup V_1^\delta,$$

where

$$U_1^\delta = \{(b, c) \in Q^2 \mid b \cdot \delta c \neq c \cdot \delta b,\ b \neq c\},$$
$$V_1^\delta = \{(a, b, c) \in Q^3 \mid ab \cdot \delta c \neq ac \cdot \delta b,\ b \neq c\};$$

$$M_{jT}^\delta = U_2^\delta \cup V_2^\delta,$$

where

$$U_2^\delta = \{(b, c, d) \in Q^3 \mid bc \cdot \delta^2 d \neq dc \cdot \delta^2 b,\ b \neq d\},$$
$$V_2^\delta = \{(a, b, c, d) \in Q^4 \mid (ab \cdot c) \cdot \delta^2 d \neq (ad \cdot c)\delta^2 b,\ b \neq d\};$$

$$M_{TE}^\delta = U_3^\delta \cup V_3^\delta,$$

where

$$U_3^\delta = \{(b, c) \in Q^2 \mid b \cdot \delta b \neq c \cdot \delta c,\ b \neq c\},$$
$$V_3^\delta = \{(a, b, c) \in Q^3 \mid ab \cdot \delta b \neq ac \cdot \delta c,\ b \neq c\};$$

$$M^{\delta}_{jTE} = U^{\delta}_4 \cup V^{\delta}_4,$$

where

$$U^{\delta}_4 = \{(b, c, d) \in Q^3 \mid bc \cdot \delta^2 b \neq dc \cdot \delta^2 d,\ b \neq d\},$$

$$V^{\delta}_4 = \{(a, b, c, d) \in Q^4 \mid (ab \cdot c) \cdot \delta^2 b \neq (ad \cdot c)\delta^2 d,\ b \neq d\}.$$

The set U^{δ}_i, $i = 1, 2, 3, 4$, points out the corresponding detected errors in the first digits of code words, while the set V^{δ}_i, $i = 1, 2, 3, 4$, defines the detected errors in the rest positions beginning with the second position.

Generally, the sets U^{δ}_i and V^{δ}_i are dependent, moreover, for quasigroups with the left identity e the set V^{δ}_i completely defines the set U^{δ}_i (by $a = e$) $i = 1, 2, 3, 4$.

Now we note that

$$\max(|U^{\delta}_i|) = q(q-1),\ \ \max(|V^{\delta}_i|) = q^2(q-1)\ \ \text{for}\ \ i = 1, 3$$

and

$$\max(|U^{\delta}_i|) = q^2(q-1),\ \ \max(|V^{\delta}_i|) = q^3(q-1)\ \ \text{for}\ \ i = 2, 4,$$

so

$$\max(|U^{\delta}_i| + |V^{\delta}_i|) = q(q^2-1)\ \ \text{for}\ \ i = 1, 3$$

and

$$\max(|U^{\delta}_i| + |V^{\delta}_i|) = q^2(q^2-1)\ \ \text{for}\ \ i = 2, 4.$$

Taking into account the above-mentioned we shall obtain Table 9 and Table 10 which contain estimations of percentage (i.e. the rate) r^{δ} of detection errors for a system $S(Q(\cdot), \delta)$ over a quasigroup $Q(\cdot)$, over a quasigroup with the left identity or over a loop, respectively [6].

Table 9: Detection of errors by systems over quasigroups of order q

Error types	Detection set	Percentage of detection
transpositions	$M^{\delta}_T = U^{\delta}_1 \cup V^{\delta}_1$	$r^{\delta}_1 \leqslant (\lvert U^{\delta}_1\rvert + \lvert V^{\delta}_1\rvert)/q(q^2-1)$
jump transpositions	$M^{\delta}_{JT} = U^{\delta}_2 \cup V^{\delta}_2$	$r^{\delta}_2 \leqslant (\lvert U^{\delta}_2\rvert + \lvert V^{\delta}_2\rvert)/q^2(q^2-1)$
twin errors	$M^{\delta}_{TE} = U^{\delta}_3 \cup V^{\delta}_3$	$r^{\delta}_3 \leqslant (\lvert U^{\delta}_3\rvert + \lvert V^{\delta}_3\rvert)/q(q^2-1)$
jump twin errors	$M^{\delta}_{JTE} = U^{\delta}_4 \cup V^{\delta}_4$	$r^{\delta}_4 \leqslant (\lvert U^{\delta}_4\rvert + \lvert V^{\delta}_4\rvert)/q^2(q^2-1)$

Table 10: Detection of errors by systems over quasigroups with the left identity or over loops of order q

Error type	Detection set	Percentage of detection
transpositions	$M_T^\delta = V_1^\delta$	$r_1^\delta = \lvert V_1^\delta\rvert / q^2(q-1)$
jump transpositions	$M_{JT}^\delta = V_2^\delta$	$r_2^\delta = \lvert V_2^\delta\rvert / q^3(q-1)$
twin errors	$M_{TE}^\delta = V_3^\delta$	$r_3^\delta = \lvert V_3^\delta\rvert / q^2(q-1)$
jump twin errors	$M_{JTE}^\delta = V_4^\delta$	$r_4^\delta = \lvert V_4^\delta\rvert / q^3(q-1)$

If $Q(\cdot)$ is a group of order q, then $|V_i| = q|U_i|$ and we obtain from Table 10 the detection rates of Table 8.

6. Equivalence of check character systems

The concepts of detection sets and detection rate allow to consider equivalence relations between check character systems over the same quasigroup (loop or group) as systems with the same detection rate of the same error type by means of a classification of permutations δ.

In [27] J. Verhoeff suggested some transformations preserving detection rate using automorphisms and translations of a group. These ideas were used by M. Damm in [8] and R. H. Schulz in [23, 24, 25].

The concept of automorphism equivalent permutations δ_1 and δ_2 for a group of [23] one can carry over a quasigroup.

Definition 6.1 [6]. A permutation δ_2 is called *automorphism equivalent to a permutation* δ_1 ($\delta_2 \sim \delta_1$) for a quasigroup $Q(\cdot)$ if there exists an automorphism α of $Q(\cdot)$ such that $\delta_2 = \alpha\delta_1\alpha^{-1}$.

The following proposition for quasigroups repeats Proposition 6.6 of [23] for a groups.

Proposition 6.2 [6]. *Automorphism equivalence is an equivalence relation* (*that is reflexive, symmetric and transitive*).

If δ_1 and δ_2 are automorphism equivalent for a quasigroup $Q(\cdot)$, then the systems $S(Q(\cdot), \delta_1)$ and $S(Q(\cdot), \delta_2)$ detect the same percentage of transpositions (*jump transpositions, twin errors, jump twin errors*).

According to computations by S. Giese [14] there are 1706 equivalence classes of anti-symmetric mappings (these detect all transpositions) with respect to automorphism equivalence in the dihedral group D_5 of order 10. S. Giese distinguished 6 types of classes according to the detection rate of other errors in this group and defined detection rate of all 5 error types weighted with their relative frequencies. Unweighted error detection rate in D_5 depends on length n of code words (see Table 8 of [23]).

There exist exactly 1152 anti-symmetric mappings in the quaternion group, which constitute 48 equivalence classes of size 24 each with respect to automorphism equivalence [26, 24, 25]. In these articles it is pointed out that the dicyclic group Q_3 has 1.403.136 anti-symmetric mappings. They form 3.456 equivalence classes with respect to automorphism equivalence. Types of check digit systems over the groups Q_2 and Q_3 and their detection rates are presented as well in these articles.

Definition 6.3 [23]. Permutations δ_1 and δ_2 are called *weak equivalent for a group* $G(\cdot)$ if there exist elements $a, b \in G$ and an automorphism $\alpha \in \operatorname{Aut} G(\cdot)$ such that

$$\delta_2 = R_a \alpha^{-1} \delta_1 \alpha L_b, \quad a, b \in G,$$

where $R_a x = xa,\ L_a x = ax$ for all $x \in G$.

For a loop the notion of weak equivalence was generalized in [6].

Recall that the left, right, middle nuclei of a loop $Q(\cdot)$ are respectively the sets [2]:

$$N_l = \{a \in Q |\, ax \cdot y = a \cdot xy\ for\ all\ x, y \in Q\},$$
$$N_r = \{a \in Q |\, x \cdot ya = xy \cdot a\ for\ all\ x, y \in Q\},$$
$$N_m = \{a \in Q |\, xa \cdot y = x \cdot ay\ for\ all\ x, y \in Q\}.$$

The nucleus N of a loop is the intersection of the left, right and middle nuclei:

$$N = N_l \cap N_r \cap N_m.$$

In a group $Q(\cdot)$ the nucleus N coincides with Q.

Definition 6.4 [6]. A permutation δ_2 of a set Q is called *weakly equivalent to a permutation* δ_1 ($\delta_2 \overset{w}{\sim} \delta_1$) *for a loop* $Q(\cdot)$ if there exist an automorphism α of the loop and elements $p, q \in N$ such that

$$\delta_2 = R_p \alpha \delta_1 \alpha^{-1} L_q,$$

where $R_p x = xp,\ L_q x = qx,\ N$ is the nucleus of the loop.

The following statement is generalization for loops of Proposition 6.2 of [23] (see also [8], [27]) for groups.

Proposition 6.5 [6].

a) *Weak equivalence is an equivalence relation for a loop.*

b) *If $\delta_1 \overset{w}{\sim} \delta_2$, then systems $S(Q(\cdot), \delta_1)$ and $S(Q(\cdot), \delta_2)$ over a loop $Q(\cdot)$ detect the same percentage of transpositions (twin errors).*

c) *If, in addition, δ_1 is an automorphism of the loop $Q(\cdot)$, then these systems detect the same percentage of transpositions (jump transpositions, twin errors and jump twin errors).*

Corollary 6.6 [6]. *If $Q(\cdot)$ is a loop (a group), N is its nucleus, $p, q \in N$ (or $p, q \in Q$, respectively), then*

a) *systems $S(Q(\cdot), \varepsilon)$ and $S(Q(\cdot), R_pL_q)$ detect the same percentage of transpositions (jump transpositions, twin errors and jump twin errors);*

b) *systems $S(Q(\cdot), R_pL_q)$ over a loop can not detect all transpositions (all jump transpositions).*

Corollary 6.7 [6]. *A system $S(Q(\cdot), R_pL_q)$ over a Moufang loop of odd order with nucleus N, $p, q \in N$ detects all twin errors and all jump twin errors.*

In [6] there can be found an example of an eight-element loop together with weak equivalent permutations of this loop that are related to check character systems which have the equal detection percentage of the same errors.

7. Check character systems as n-ary operations

It is possible to consider a code $Q^n \rightarrow Q^{n+1} : a_1a_2 \dots a_n \rightarrow a_1a_2 \dots a_na_{n+1}$ with one control symbol a_{n+1} as an n-ary operation f, setting

$$f(a_1, a_2, \dots, a_n) = a_{n+1}.$$

Such approach to check character systems detecting all single errors and all adjacent transpositions was used by H. P. Gumm in [15] and later by M. Damm in [8]. G. L. Mullen and V. Shcherbacov [18] considered check character systems with n-ary quasigroup operation detecting (jump) transpositions and (jump) twin errors not only in adjacent positions.

Definition 7.1 [3]. A non-empty set Q with n-ary operation f such that in the equation $f(x_1, x_2, \dots, x_n) = x_{n+1}$ any n elements of $x_1, x_2, \dots, x_n$, x_{n+1} define the last one uniquely is called an *n-ary quasigroup* (or an n-quasigroup) $Q(f)$.

Definition 7.2 [8]. Let $g : D^{n+1} \to D$, where $D = \{0, 1, \dots, m-1\}$, $c \in D$, be a mapping. The set

$$P_{g,c} = \{(d_n, d_{n-1}, \dots, d_0) \in D^{n+1} \,|\, g(d_n, \dots, d_0) = c\}$$

is called an *implicit check system over base m* if

1. $g(d_n, \dots, d_i, \dots, d_0) = g(d_n, \dots, d_i', \dots, d_0) = c$ implies $d_i = d_i'$.
2. $g(d_n, \dots, d_i, d_{i-1}, \dots, d_0) = g(d_n, \dots, d_{i-1}, d_i, \dots, d_0) = c$ implies $d_i = d_{i-1}$.
3. for all $d_n, \dots, d_1 \in D$ there exists $d_0 \in D$ such that

$$g(d_n, \dots, d_1, d_0) = c.$$

Definition 7.3 [8]. Let $D = \{0, 1, \dots, m-1\}$ and let $f : D^n \to D$ be a mapping. The set

$$P_f' = \{(d_n, \dots, d_0) \in D^{n+1} \,|\, f(d_n, \dots, d_1) = d_0\}$$

is called an *explicit check system over base m* if

1. $f(d_n, \dots, d_i, \dots, d_1) = f(d_n, \dots, d_i', \dots, d_1)$ implies $d_i = d_i'$.
2. $f(d_n, \dots, d_i, d_{i-1}, \dots, d_1) = f(d_n, \dots, d_{i-1}, d_i, \dots, d_1)$ implies $d_i = d_{i-1}$.
3. $f(d_n, \dots, d_2, d_0) = d_1$, where $f(d_n, \dots, d_1) = d_0$ implies $d_1 = d_0$.

Both these check systems detect all single errors and adjacent transpositions including the control symbol. The operation f from Definition 7.3 is a finite n-ary quasigroup (see property 1) with additional properties 2 and 3. M. Damm proved the following general result concerning the existence of implicit (explicit) check systems (see [15] as well).

Theorem 7.4 [8]. *For each base $m > 2$ and all $n \geqslant 2$ there exists a mapping $f : D^n \to D$ (respectively $D^{n+1} \to D$) such that P_f $(P_{g,c})$ defines a check system.*

A connection between an implicit check system and some explicit check system over base m is established in [8] when an n-ary ($(n{+}1)$-ary) operation f (g) is a composition of binary quasigroups.

Theorem 7.5 [8].

1. *For each explicit check system P_f where f is a composition of $n-1$ binary quasigroups $*_i$, that is*

$$f(d_n,\, d_{n-1},\, \dots,\, d_1) = (\dots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-2} \dots) *_2 d_1$$

there exists a quasigroup $*_1$ and an element $c \in D$ such that the equivalence

$$f(d_n,\, \dots,\, d_1) = d_0 \Longleftrightarrow g(d_n,\, \dots,\, d_0) = c$$

holds for $g(d_n,\, \dots,\, d_0) = f(d_n,\, \dots,\, d_1) *_1 d_0$.

2. *For every implicit check system $P(g,c)$ where g is a composition of n quasigroups $*_i$:*

$$g(d_n,\, \dots,\, d_0) = (\dots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-2} \dots) *_1 d_0$$

there exists a quasigroup $*_2'$ such that the equivalence

$$f(d_n,\, \dots,\, d_1) = d_0 \Longleftrightarrow g(d_n,\, \dots,\, d_0) = c$$

holds for $f = ((\dots((d_n *_n d_{n-1}) *_{n-1} d_{n-2}) *_{n-2} \dots) *_3 d_2) *_2' d_1$.

Definition 7.6 [8]. An n-ary quasigroup $Q(f)$ is called *anti-symmetric* if

$$f(x_n,\, \dots,\, x_i,\, x_{i-1},\, \dots,\, x_1) = f(x_n,\, \dots,\, x_{i-1},\, x_i,\, \dots,\, x_1)$$

implies $x_i = x_{i-1}$.

The following statement is often useful.

Lemma 7.7 [8]. *If $Q(f)$ is an anti-symmetric n-quasigroup and φ, ψ are permutations of Q, then $Q(\bar{f})$ where*

$$\bar{f}(x_n,\, \dots,\, x_1) = \psi^{-1} f(\varphi x_n,\, \varphi x_{n-1},\, \dots,\, \varphi x_1)$$

is an anti-symmetric n-quasigroup.

From Theorem 7.4 it follows

Corollary 7.8 [15]. *For each $n \geqslant 2$ and all $m > 2$ there exists an anti-symmetric n-quasigroup of base m.*

Let

$$\hat{f}(x_n, x_{n-1}, \ldots, x_1) = x_0 \Longleftrightarrow f(x_0, x_1, \ldots, x_{n-1}) = x_n.$$

It is valid the following

Theorem 7.9 [8].

1. *Every n-quasigroup detects all single errors. If g is an anti-symmetric n-quasigroup, then $P_{g,c}$ is an implicit check system for any $c \in D$.*
2. *P'_f is an explicit check system if and only if $P'_{\hat{f}}$ is an explicit check system.*
3. *P'_f is an explicit check system if and only if f and $\hat{f}$ are anti-symmetric n-quasigroups.*

Implicit check systems with the check formula

$$g(x_n, x_{n-1}, \ldots, x_0) = (\ldots((x_n *_n x_{n-1}) *_{n-1} x_{n-2}) \ldots) *_1 x_0 = c, \quad (7)$$

where $*_i$, $i = 1, 2, \ldots, n$, is a binary quasigroup, occupy a special position among the check systems researched by M. Damm.

Theorem 7.10 [8]. *$(n+1)$-Ary quasigroup $Q(g)$, where*

$$g(x_n, \ldots, x_0) = (\ldots(x_n *_n x_{n-1}) *_{n-1} \ldots) *_1 x_0$$

is anti-symmetric if and only if $*_n$ is anti-symmetric and each row of the quasigroup $*_{i+1}$ is an anti-symmetric mapping of $*_i$, $i = 1, 2, \ldots, (n-1)$.

Theorem 7.11 [8]. *Every quasigroup $*_i$ in a check system with the formula (7) has an anti-symmetric mapping. If such system detects all twin errors, then each quasigroup has a complete mapping. If it defines all jump twin errors, then every quasigroup, except $*_n$, has a complete mapping.*

Theorem 7.12 [8]. *Let $Q(*_i)$ be a quasigroup in a check system with the check formula (7) which detects all twin errors. Then the quasigroup $Q(*_i)$, $i = 1, 2, \ldots, n-1$, is orthogonal to the quasigroup $*'_i$ defined by*

$$x *'_i y = z \Longleftrightarrow z *_{i+1} y = x.$$

Definition 7.13 [8]. A binary quasigroup $Q(*)$ is called *total anti-symmetric* if it is anti-symmetric ($x * y = y * x$ implies $x = y$) and the equality $(c * x) * y = (c * y) * x$ implies $x = y$ for all c, x, $y \in Q$.

M. Damm in [8] has pointed out that a check system with the check formula

$$(\dots((x_n * x_{n-1}) * x_{n-2}) \dots) * x_0 = d,$$

where $*$ is a binary quasigroup, defines (implicit) check system if and only if $*$ is a total anti-symmetric quasigroup. He also gives an algorithm of computer construction of total anti-symmetric binary quasigroups. For the following check formula

$$\varphi^n x_n * \varphi^{n-1} x_{n-1} * \varphi^{n-2} x_{n-2} * \dots * \varphi x_1 * x_0 = 0,$$

where $Q(*)$ is the dihedral group D_3 (D_4 or D_5), M. Damm in [8] using computer found total anti-symmetric permutations with good possibilities to detect errors of all five types.

G. L. Mullen and V. Shcherbacov [18] continued research of check character systems as n-ary operations, considering a code $a_1 a_2 \dots a_n \longrightarrow a_1 a_2 \dots a_n a_{n+1}$ over a finite alphabet Q as an n-ary operation f, setting

$$f(a_1, a_2, \dots, a_n) = a_{n+1}.$$

Such code they call an *n-ary code* (Q, f). If f is an n-ary quasigroup operation, then this code is called an *n-quasigroup code.*

An n-ary code detects all single errors if and only if it is an n-quasigroup code.

In [18] it is shown that all n-ary quasigroup codes (Q, f) over the same alphabet Q ($|Q| = q$) (arity n is fixed) have in some sense equal possibilities to detect all possible types of errors.

More refined n-ary quasigroup codes which are able to detect transpositions and twin errors (not necessary in adjacent positions) are being researched.

Let x_m^n, where $m \leqslant n$, denote the sequence $x_m, x_{m+1}, \dots, x_n$, and $\overline{1, n} = \{1, 2, \dots, n\}$, let $Q(f)$ be an n-ary quasigroup: $f(x_1^n) = x_{n+1}$.

Changing in $f(x_1^n)$ elements $x_{k_1}, x_{k_2}, \dots, x_{k_m}$ respectively for some fixed elements $a_1, a_2, \dots, a_m$ we obtain a new $(n-m)$-ary quasigroup operation which is called a *retract* of the quasigroup $Q(f)$ [3].

Definition 7.14 [18]. A retract of a form $f\left(a_i^{i-1},\, x_i,\, a_{i+1}^{i+k-1},\, x_{i+k},\, a_{i+k+1}^n\right)$ of an n-ary quasigroup $Q(f)$ where a_i^{i-1}, a_{i+1}^{i+k-1}, a_{i+k+1}^n are some fixed elements of Q, $i \in \overline{1,\, n-k}$, $k \in \overline{1,\, n-1}$ is called an $(i,\, i+k)$ *binary retract* of the quasigroup $Q(f)$.

Definition 7.15 [18]. A binary anti-symmetric quasigroup $Q(\cdot)$ is called *totally anti-commutative* if $x \cdot x = y \cdot y$ implies $x = y$ for all $x, y \in Q$ (compare with the Definition 7.13).

The following theorem determines properties of n-ary quasigroup codes which are able to detect all (not necessarily neighbour) transpositions and twin errors in the information symbols of a code word.

Theorem 7.16. *An $(n-1)$-ary quasigroup code $(Q,\, f)$, $n > 3$ with check equation $f(x_1^{n-1}) = x_n$ detects each transposition and twin error on the places $(i,\, i+k)$, $i \in \overline{1,\, n-k-1}$, $k \in \overline{1,\, n-2}$ if and only if all $(i,\, i+k)$ binary retracts of the n-ary quasigroup $Q(f)$ are totally anti-commutative.*

Remark. Note that for the check formula $g(x_1^n) = c$, where c is a fixed element, analogous properties in general case are sufficient but not necessary as it is pointed in Theorem 2 of [18]. However, it is valid when g is an n-ary abelian group isotope (see Theorems 7.20 and 7.22).

Definition 7.17 [18]. An n-ary quasigroup $Q(g)$ of the form

$$\gamma g(x_1,\, x_2,\, \dots,\, x_n) = \gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_n x_n$$

where $Q(+)$ is a group, $\gamma_1,\, \gamma_2,\, \dots,\, \gamma_n$ are permutations of Q is called an *n-ary group isotope.*

Definition 7.18 [18]. An n-quasigroup $Q(g)$ of the form

$$g(x_1,\, x_2,\, \dots,\, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n + a = \sum_{i=1}^{n} \alpha_i x_i + a,$$

where $Q(+)$ is an abelian group, $\alpha_1,\, \alpha_2,\, \dots,\, \alpha_n$ are automorphisms of the group $Q(+)$, a is a fixed element of Q, is called an *n-T-quasigroup.*

Proposition 7.19 [18]. *In an n-ary group isotope $Q(g)$ of the form*

$$g(x_1,\, x_2,\, \dots,\, x_n) = \gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_n x_n$$

a) *all $(i,\, i+1)$ $(i \in \overline{1,\, n-1})$ binary retracts are totally anti-commutative quasigroups if and only if all binary quasigroups of the form $\gamma_i x_i + \gamma_{i+1} x_{i+1}$ are totally anti-commutative;*

b) *all* $(i,\, i+k)$ $(i \in \overline{1,\, n-k},\ k \in \overline{1,\, n-1})$ *binary retracts are totally anti-commutative quasigroups if and only if all binary quasigroups of the form* $\gamma_i x_i + t + \gamma_{i+k} x_{i+k}$ *for all fixed element* t, *are totally anti-commutative.*

Theorem 7.20 [18]. *A code* $Q(g)$, *where* g *is an abelian group isotope, with the check equation* $\sum\limits_{i=1}^{n} \gamma_i x_i = 0$, *where* 0 *is the zero of the abelian group* $Q(+)$, *detects any transposition and twin error on the places* $(i,\, i+1)$, $i \in \overline{1,\, n-1}$, $(i,\, i+2)$, $i \in \overline{1,\, n-2}$ *if and only if all binary quasigroups of the form* $\gamma_i x_i + \gamma_{i+1} x_{i+1}$ *and of the form* $\gamma_i x_i + \gamma_{i+2} x_{i+2}$ *are totally anti-commutative.*

Proposition 7.21 [18]. *A binary T-quasigroup* $Q(\cdot)$ *of the form* $x \cdot y = \alpha x + \beta y + a$ *is totally anti-commutative if and only if the mappings* $\alpha - \beta$ *and* $\alpha + \beta$ *are automorphisms of the group* $Q(+)$.

Theorem 7.22 [18]. *A code* $(Q,\, g)$, *where* g *is an* n*-T-quasigroup, with the check equation*

$$g(x_1, x_2, \dots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n = 0$$

detects

a) *any transposition error on the place* $(i,\, i+1)$, $i \in \overline{1,\, n-1}$ *(i.e. any transposition) if and only if the mapping* $\alpha_i - \alpha_{i+1}$ *is an automorphism of the group* $Q(+)$;

b) *any transposition error on the place* $(i,\, i+2)$, $i \in \overline{1,\, n-2}$ *(i.e. any jump transposition) if and only if the mapping* $\alpha_i - \alpha_{i+2}$ *is an automorphism of* $Q(+)$;

c) *any twin error on the place* $(i,\, i+1)$, $i \in \overline{1,\, n-1}$ *if and only if the mapping* $\alpha_i + \alpha_{i+1}$ *is an automorphism of* $Q(+)$;

d) *any twin error on the place* $(i,\, i+2)$, $i \in \overline{1,\, n-2}$ *(i.e. any jump twin error) if and only if the mapping* $\alpha_i + \alpha_{i+2}$ *is an automorphism of* $Q(+)$.

We note that the check formula of Theorem 7.22 is the check formula (1) where the permutations $\alpha_1, \alpha_2, \dots, \alpha_n$ are automorphisms of the abelian group $Q(+)$.

G. L. Mullen and V. Shcherbacov use Theorem 7.22 for construction a number of examples of codes based on n-T-quasigroups which detect all five types of the considered errors. They also give modifications of the ISBN-code and the EAN-code with better possibilities than the known codes.

In the ISBN-code $(Z_{11},\, g)$, $n = 10$ the check formula

$$1{\cdot}x_1{+}2{\cdot}x_2{+}3{\cdot}x_3{+}4{\cdot}x_4{+}5{\cdot}x_5{+}6{\cdot}x_6{+}7{\cdot}x_7{+}8{\cdot}x_8{+}9{\cdot}x_9{+}10{\cdot}x_{10} \equiv 0 \,(\mathrm{mod}\, 11)$$

is changed for

$$1{\cdot}x_1{+}3{\cdot}x_2{+}5{\cdot}x_3{+}7{\cdot}x_4{+}9{\cdot}x_5{+}10{\cdot}x_6{+}8{\cdot}x_7{+}6{\cdot}x_8{+}4{\cdot}x_9{+}2{\cdot}x_{10} \equiv 0 \,(\mathrm{mod}\, 11).$$

The last check formula allows to detect single errors and all error types of Theorem 7.22.

In the EAN-code $(Z_{10},\, g)$, $n = 13$, instead of the check formula

$$x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12} + x_{13} = 0$$

the formula

$$x_1 + 3x_2 + 9x_3 + 7x_4 + x_5 + 3x_6 + 9x_7 + 7x_8 + x_9 + 3x_{10} + 9x_{11} + 7x_{12} + x_{13} = 0$$

is proposed which has the better capability then the first one.

Acknowledgment. The authors thank A. Diordiev for the help at design of the given survey.

References

[1] **D. F. Beckley**: *An optimum systems with modulo* 11, The Computer Bulletin **11** (1967), 213 – 215.

[2] **V. D. Belousov**: *Foundations of the Theory of Quasigroups and Loops*, (in Russian), Nauka, Moscow 1967.

[3] **V. D. Belousov**: *n-Ary Quasigroups*, (in Russian), Sţiinta, Kishinev 1972.

[4] **G. B. Belyavskaya, V. I. Izbash, and G. L. Mullen**: *Check character systems using quasigroups: I* , (to appear).

[5] **G. B. Belyavskaya, V. I. Izbash, and G. L. Mullen**: *Check character systems using quasigroups: II*, (to appear).

[6] **G. B. Belyavskaya**: *On check character systems over quasigroups and loops*, Algebra and Discrete Math., (to appear).

[7] **C. Broecker, R. H. Schulz and G. Stroth**: *Check character systems using Chevalle groups*, Designs, Codes and Cryptography, DESI. **10** (1997), 137 – 143.

[8] **H. M. Damm**: *Prüfziffersysteme über Qasigruppen*, Diplomarbeit, Philipps-Universität Marburg 1998.

[9] **H. M. Damm**: *Check digit systems over groups and anti-symmetric mappings*, Archiv der Mathematik **75** (2000), 413 – 421.

[10] **J. Dénes and A. D. Keedwell**: *Latin Squares and their Applications*, Académiai Kiadó, Budapest 1974.

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

[12] **A. Ecker and G. Poch**: *Check character systems*, Computing **37** (1986), 277 – 301.

[13] **J. A. Gallian and M. D. Mullin**: *Groups with anti-symmetric mappings*, Arch. Math. **65** (1995), 273 – 280.

[14] **S. Giese**: *Äquivalenz von Prüfzeichensystemen am Beispil der Diedergruppe* D_5, Staatsexamensarbeit FU Berlin, 1999.

[15] **H. P. Gumm**: *A new class of check-digit methods for arbitrary number systems*, IEEE Trans. Inf. Th. IT, **31** (1985), 102 – 105.

[16] **S. Heiss**: *Anti-symmetric mappings for finite solvable groups*, Arch. Math. **69** (1997), 445 – 454.

[17] **S. Heiss**: *Anti-symmetric mappings for finite groups*, Preprint, 1999.

[18] **G. L. Mullen and V. A. Shcherbacov**: *Properties of codes with one check symbol from a quasigroup point of view*, Bulletinul Acad. Sci. Rep. Moldova, ser. Matematica no. **3** (2002), 71 – 86.

[19] **P. Nemec and T. Kepka**: *T-quasigroups, I,* Acta Univ. Carolinae **12** (1971), 39 – 49.

[20] **R. H. Schulz**: *A note on check character systems using Latin squares*, Diskrete Math. **97** (1991), 371 – 375.

[21] **R. H. Schulz**: *Some check digit systems over non-abelian group*, Mitt. der Math. Ges. Hamburg **12** (1991), 819 – 827.

[22] **R. H. Schulz**: *Check character systems over groups and orthogonal Latin squares*, Applic. Algebra in Eng., Comm. and Computing, AAECC, **7** (1996), 125 – 132.

[23] **R. H. Schulz**: *On check digit systems using anti-symmetric mappings*, In it Numbers, Information and Complexity, Kluwer Acad. Publ. Boston 2000, 295 – 310.

[24] **R. H. Schulz**: *Equivalence of check digit systems over the dicyclic groups of order 8 and 12*, In *Mathematikdidaktik aus Begeisterung für die Mathematik*, Klett Verlag, Stuttgart 2000, 227 – 237.

[25] **R. H. Schulz**: *Check character systems and anti-symmetric mappings*, In *Computational Discrete Mathematics, LNCS* **2122** (2001), 136 – 147.

[26] **S. Ugan**: *Prüfzeichensysteme über dizyklishen Gruppen der Ordnung* 8 *und* 12, Diplomarbeit, FU Berlin, FB Mathematik & Informatik 1999.

[27] **J. Verhoeff**: *Error detecting decimal codes*, **29**, Math. Centre Tracts. Math. Centrum Amsterdam, 1969.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
str. Academiei 5
MD-2028 Chisinau
Moldova

Received May 28, 2003

e-mail: gbel@math.md (G.B.Belyavskaya)
vizb@math.md (V.I.Izbash)
scerb@math.md (V.A.Shcherbacov)

Quasigroups and Related Systems **10** (2003), 29 – 64

Quasigroups constructed from cycle systems

Curt C. Lindner

Abstract

An m-cycle system of order n is a pair (S,C), where C is a collection of edge disjoint m-cycles which partitions the edge set of the complete undirected graph K_n with vertex set S. If the m-cycle system (S,C) has the additional property that every pair of vertices $a \neq b$ are joined by a path of length 2 (and therefore exactly one) in an m-cycle of C, then (S,C) is said to be 2-perfect. Now given an m-cycle system (S,C) we can define a binary operation "$\circ$" on S by $a \circ a = a$ and if $a \neq b$, $a \circ b = c$ and $b \circ a = d$ if and only if the cycle $(\dots, d, a, b, c, \dots) \in C$. This is called the Standard Construction and it is well known that the groupoid $(S,\circ)$ is a quasigroup (which can be considered to be the "multiplicative" part of a universal algebra quasigroup $(S,\circ,\backslash,/)$) if and only if (S,C) is 2-perfect. The class of 2-perfect m-cycle systems is said to be *equationally defined* if and only if there exists a *variety* of universal algebra quasigroups V such that the finite members of V are *precisely* all universal algebra quasigroups whose multiplicative parts can be constructed from 2-perfect m-cycle systems using the Standard Construction. This paper gives a survey of results showing that 2-perfect m-cycle systems can be equationally defined for $m = 3, 5$, and 7 only. Similar results are obtained for m-perfect $(2m+1)$-cycle systems using the Opposite Vertex Construction (too detailed to go into here). We conclude with a summary of similar results (without details) for 2-perfect and m-perfect directed cycle systems.

1. Introduction

Sometimes people in combinatorics, algebra, and universal algebra see things differently. The following three definitions are a good illustration of this principle.

2000 Mathematics Subject Classification: 05B15, 05C38, 20N05
Keywords: quasigroup, m-cycle system

Definition 1.1. An *$n \times n$ latin square* (or a *latin square of order n*) is an $n \times n$ array such that each of the integers $1, 2, 3, \ldots, n$ occurs exactly once in each row and column.

Example 1.2. Latin square of order 5.

1	3	2	5	4
5	2	4	1	3
4	5	3	2	1
3	1	5	4	2
2	4	1	3	5

Definition 1.3. A *quasigroup* is a pair $(Q, \circ)$, where "$\circ$" is a binary operation on Q such that for all not necessarily distinct $a, b \in Q$, the equations

$$\begin{cases} a \circ x = b, \\ y \circ a = b \end{cases}$$

have unique solutions.

The fact that the solutions are unique guarantees that no element occurs twice in any row or column of the table for "$\circ$". If Q is finite, each element occurs exactly once in each row and column, and hence the table for a *finite* quasigroup of order n is nothing more than a latin square of order n with a headline and sideline.

Example 1.4. Quasigroup of order 5.

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

Definition 1.5. A *universal algebra quasigroup* of order n is an ordered 4-tuple $(Q, \circ, \backslash, /)$, where "$\circ$", "$\backslash$", and "$/$" are binary operations on the set Q called "multiplication", "left division", and "right division" respectively, satisfying the four identities

$$\begin{cases} x \circ (x \backslash y) = y, \\ x \backslash (x \circ y) = y, \\ (x/y) \circ y = x, \\ (x \circ y)/y = x. \end{cases}$$

This definition is a good bit more complicated than the first two, necessitating a more detailed explanation.

To begin with each of $(Q,\circ)$, $(Q,\backslash)$, and $(Q,/)$ is a quasigroup. For example to see that $(Q,\backslash)$ is a quasigroup, let $a,b\in Q$. Then $a\backslash(a\circ b)=b$ guarantees that the equation $a\backslash x=b$ has a solution. Further, if $a\backslash x_1 = a\backslash x_2$, then $x_1 = a\circ(a\backslash x_1) = a\circ(a\backslash x_2) = x_2$ guarantees that the solution is unique. Similarly the equation $y\backslash a = b$ has a unique solution. An analogous argument shows that $(Q,\circ)$ and $(Q,/)$ are quasigroups as well. Furthermore, the binary operations "$\circ$", "$\backslash$", and "$/$" have the symbiotic relationships

$$\begin{cases} a\circ b=c & \text{if and only if} \quad a\backslash c=b,\\ a\circ b=c & \text{if and only if} \quad c/b=a.\end{cases}$$

The first of these follows from the identities $x\backslash(x\circ y)=y$ and $x\circ(x\backslash y)=y$, while the second follows from the identities $(x\circ y)/y=x$ and $(x/y)\circ y = x$. Because of this symbiotic relationship only one of "$\circ$", "$\backslash$", and "$/$ is necessary to define all three. In everything that follows we will always use $(Q,\circ)$ to define $(Q,\circ,\backslash,/)$.

Example 1.6. Universal algebra quasigroup of order 5.

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

$\backslash$	1	2	3	4	5
1	1	3	2	5	4
2	4	2	5	3	1
3	5	4	3	1	2
4	2	5	1	4	3
5	3	1	4	2	5

$/$	1	2	3	4	5
1	1	4	5	2	3
2	5	2	1	3	4
3	4	1	3	5	2
4	3	5	2	4	1
5	2	3	4	1	5

On the other hand, *any* quasigroup $(Q,\circ)$ can be considered to be the multiplication part of a universal algebra quasigroup as follows: define "$\backslash$" and "$/$" in terms of "$\circ$" by

$$\begin{cases} a\backslash b=c & \text{if and only if} \quad a\circ c=b,\\ a/b=c & \text{if and only if} \quad c\circ b=a.\end{cases}$$

It is not difficult to see that $(Q,\circ,\backslash,/)$ satisfies the four identities $x\circ(x\backslash y) = y$, $x\backslash(x\circ y)=y$, $(x/y)\circ y=x$, and $(x\circ y)/y=x$. For example to see that the identity $(x \circ y)/y = x$ is satisfied, let $a \circ b = c$. Then $c/b = a$ and so $(a \circ b)/b = c/b = a$. The proofs that the other identities are satisfied by $(Q, \circ, \backslash, /)$ are just as easy.

Hence we can think of *any* quasigroup $(Q, \circ)$ as being the "multiplicative" part of a universal algebra quasigroup.

From now on we will use juxtaposition to indicate "multiplicative" in quasigroup identities. So, for example, the defining identities for a quasigroup become $x(x\backslash y) = y$, $x\backslash(xy) = y$, $(x/y)y = x$, and $(xy)/y = x$.

Now all of this might seem unnecessary at first, but for what we are going to do in this paper it is necessary! Here's the reason why. We are going to talk about *varieties* of quasigroups; i.e., classes of quasigroups defined by sets of quasigroup identities. Hence we need the universal algebra definition of a quasigroup.

2. A small amount of universal algrebra

Since any quasigroup can be considered to be the "multiplicative" part of a universal algebra quasigroup we will frequently drop the quantification "universal algebra" in front of quasigroup. The context will make clear what we are talking about.

A *variety* of quasigroups is a class of *universal algebra quasigroups* which is closed under the taking of subquasigroups, direct products, and homomorphic images. A very famous theorem due to G. Birkhoff [6] says that a variety V of quasigroups can be *equationally defined.* That is to say, if V is a variety of quasigroups, there exists a collection of quasigroup identities I such that V is *precisely* the set of *all* quasigroups which satisfy these identities. The identities I are called a *defining set* of identities for the variety V. (Actually Birkhoff proved a much more general result than this, but we are interested in quasigroups only, and so have edited the statement of Birkhoff's Theorem to quasigroups.) There is, of course, nothing unique about a defining set of identities. The converse is trivial; i.e., if I is a collection of quasigroup identities, the class of all quasigroups satisfying these identities is closed under the taking of subquasigroups, direct products, and homomorphic images, and so is a variety. Hence, to prove that a class of quasigroups $\mathcal{C}$ is NOT a variety, it suffices to produce a quasigroup in $\mathcal{C}$ having a homomorphic image which does NOT belong to $\mathcal{C}$. The following Folk Theorem and Folk Corollary are exactly what is needed to do this.

Theorem 2.1 (Folk Theorem). *The mapping α is a homomorphism of the universal algebra quasigroup $(Q_1, \circ_1, \backslash_1, /_1)$ onto the universal algebra quasigroup $(Q_2, \circ_2, \backslash_2, /_2)$ if and only if α is a homomorphism of $(Q_1, \circ_1)$ onto $(Q_2, \circ_2)$.*

Proof. One way is trivial. So let α be a homomorphism of the quasigroup $(Q_1, \circ_1)$ onto the quasigroup $(Q_2, \circ_2)$. Let $a\backslash_1 b = c$. Then $a \circ_1 c = b$, $(a \circ_1 c)\alpha = b\alpha$, $a\alpha \circ_2 c\alpha = b\alpha$, and $a\alpha\backslash_2 b\alpha = c\alpha$.

Similarly $a/_1 b = c$ gives $c \circ_1 b = a$, $(c \circ_1 b)\alpha = a\alpha$, $c\alpha \circ_2 b\alpha = a\alpha$, and $a\alpha/_2 b\alpha = c\alpha$. □

Corollary 2.2 (Folk Corollary). *A class of universal algebra quasigroups is closed under the taking of homomorphic images if and only if its class of multiplicative parts is closed under the taking of homomorphic images.* □

Hence, in order to show that a class of universal algebra quasigroups $\mathcal{C}$ is NOT a variety it suffices to construct a universal algebra quasigroup belonging to $\mathcal{C}$ whose multiplicative part has a homomorphic image onto a quasigroup which cannot be the multiplicative part of a universal algebra quasigroup belonging to $\mathcal{C}$.

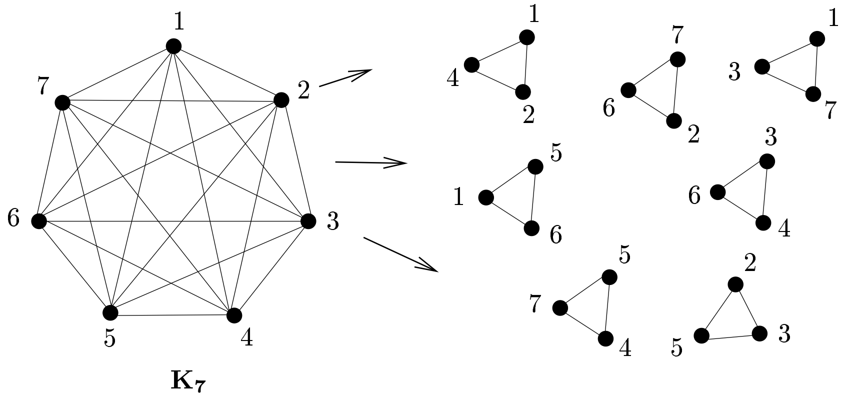
The object of this survey is an account of the struggle to achieve the solution to the problem of determining whether or not certain classes of quasigroups obtained from decomposing the edge set of the complete undirected graph into cycles form the *finite* members of a variety of quasigroups. We will now be a good deal more specific than this! And what better place to start than with Steiner triple systems!

3. Steiner triple systems

A *Steiner triple system* (or triple system) of order n is a pair (S, T), where T is a collection of edge disjoint triangles which partition the edge set of K_n (= the complete undirected graph on n vertices) with vertex set S.

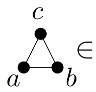
It is well-known [12] that the *spectrum* (= the set of all n such that a triple system of order n exists) for triple systems is precisely the set of all $n \equiv 1$ or $3 \pmod 6$.

Example 3.1. Steiner triple system of order 7.



Now given a triple system (S, T) we can define a groupoid $(S, \circ)$ as follows (the Standard Construction):

(1) $a \circ a = a$, for all $a \in S$, and

(2) if $a \neq b$, $a \circ b = b \circ a = c$, where  $\in T$.

Example 3.2. Groupoid constructed from Example 3.1.

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

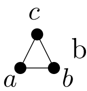
Inspection shows that the groupoid $(S, \circ)$ constructed above is actually a quasigroup which, as previously noted, is the multiplicative part of the universal algebra quasigroup $(S, \circ, \backslash, /)$.

Not only is $(S, \circ)$ a quasigroup, but it satisfies each of the *equivalent* sets of identities:

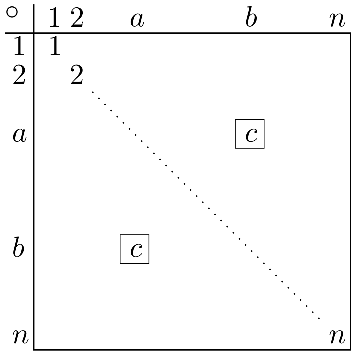
$$I_1 = \begin{cases} x^2 = x \\ (yx)x = y \\ xy = yx \end{cases} \qquad \text{and} \qquad I_2 = \begin{cases} x \backslash x = x \\ (yx) \backslash y = x \\ (yx)/y = x \end{cases}$$

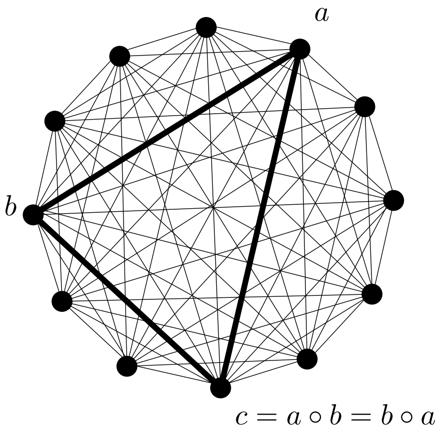
(A quasigroup satisfies the identities I_1 if and only if it satisfies the identities I_2.) In what follows we will *always* use the identities I_1.

It turns out that the groupoid constructed from *any* triple system using the Standard Construction is always a quasigroup and always satisfies the identities I_1.

Denote the triangle  by any cyclic shift of (a, b, c) or (b, a, c) and let (S, T) be a triple system and $(S, \circ)$ the groupoid constructed from T using the Standard Construction. Suppose $a \circ x = a \circ y$. If $a = x$, then $a = a \circ x = a \circ y$ implies $y = a$, since otherwise $(a, y, d) \in T$ and $a \circ y = d \neq a$. If $a \neq x$, then $a \neq y$, and (a, x, c), $(a, y, c) \in T$ implies $x = y$. Hence $(S, \circ)$ is row latin (= each element occurs exactly once in each row). Trivially $a \circ b = b \circ a$ ($(S, \circ)$ is commutative) and so $(S, \circ)$ is column latin as well. Hence $(S, \circ)$ is a quasigroup. As noted above $(S, \circ)$ satisfies $x^2 = x$ and $xy = yx$. To see that $(S, \circ)$ satisfies $(yx)x = y$ as well is easy. To begin with $(a \circ a) \circ a = a \circ a = a$. If $a \neq b$ and $(a, b, c) \in T$, then $(a \circ b) \circ b = c \circ b = a$.

What is of extreme importance to us in this discussion is that the converse is also true. That is to say, any finite quasigroup satisfying the three identities $x^2 = x$, $(yx)x = y$, and $xy = yx$ can be constructed from a triple system using the Standard Construction. So, let $(S, \circ)$ be a quasigroup of order n satisfying the three identities above, and define a collection C of triangles as follows: for each $a \neq b \in S$ place the triangle $(a, b, a \circ b = b \circ a = c)$ in C.





K_n

In order to show that the triangles in C are an edge disjoint collection of triangles which partition the edge set of K_n we must show that (i) every edge is in a triangle of C and (ii) the triangle $(a, b, a \circ b = b \circ a = c)$ constructed from the edge $\{a,b\}$ is the same triangle as the triangle constructed from each of the edges $\{b,c\}$ and $\{c,a\}$. Trivially each edge is in a triangle of C and so we can proceed to (ii). This is where the identities come into play. The triangle constructed from $\{b,c\}$ is $(b,c,b\circ c = c\circ b = (a\circ b)\circ b = a) = (b,c,a) = (a,b,c)$ and the triangle constructed from $\{c,a\}$ is $(c,a,c\circ a = a\circ c = a\circ(a\circ b) = b) = (c,a,b) = (a,b,c)$. Hence (S,C) is a triple system.

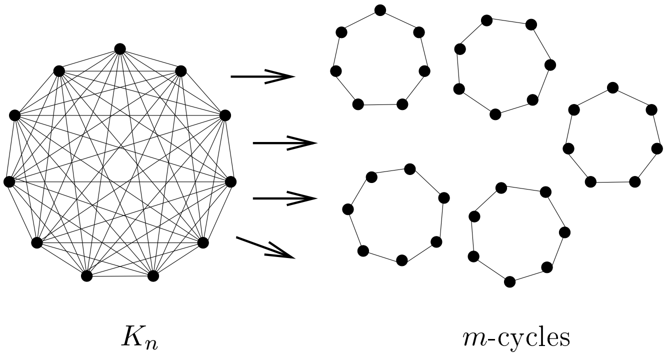
Not only is (S,C) a triple system but the triangles (a,b,c) in C all have the property that $a\circ b = b\circ a = c$, $b\circ c = c\circ b = a$, and $a\circ c = c\circ a = b$. It follows that if we apply the Standard Construction to (S,C) we get the quasigroup $(S,\circ)$ that we started with. We have the following theorem.

Theorem 3.3. *Let V be the variety of quasigroups defined by the identities $x^2 = x$, $xy = yx$, and $(yx)x = y$. A finite quasigroup belongs to V if and only if its multiplicative part can be constructed from a Steiner triple system using the Standard Construction.* □

Remark. Among other things Theorem 3.3 says that the spectrum for the finite quasigroups in the variety defined by the identities $x^2 = x$, $xy = yx$, and $(yx)x = y$ is precisely the set of all $n \equiv 1$ or $3 \pmod 6$, since this is the spectrum for Steiner triple systems. There is no particular reason for the defining identities to all be "multiplicative". However, the identities $I_1 = \{x^2 = x,\ xy = yx,\ (yx)x = y\}$ have been used "forever" to define *Steiner quasigroups* and there's no sense in changing now!

4. m-cycle systems

An *m-cycle system* is a pair (S,C), where C is a collection of edge disjoint m-cycles which partition the edge set of the complete undirected graph K_n with vertex set S. The number n is called the order of the m-cycle system (S,C).

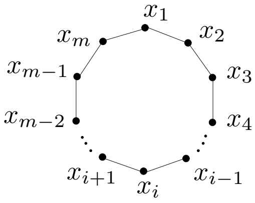


So, for example, a Steiner triple system is a 3-cycle system.

Fairly recently, the necessary and sufficient conditions for the existence of an m-cycle system of order n have been determined to be [1, 30];

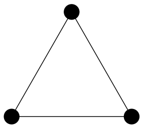
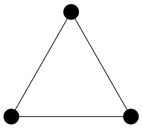
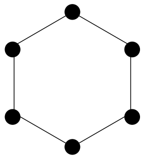
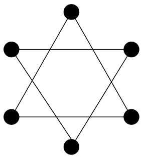
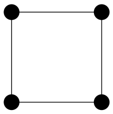
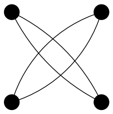
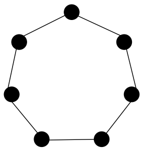
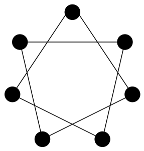
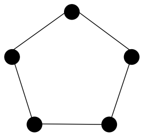
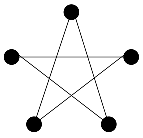
$$\begin{cases} (1) \quad n \geqslant m, \text{ if } n > 1, \\ (2) \quad n \text{ is odd, and} \\ (3) \quad n(n-1)/2m \text{ is an integer.} \end{cases}$$

In what follows we will denote the m-cycle



by any cyclic shift of $(x_1, x_2, x_3, \ldots, x_n)$ or $(x_1, x_m, x_{m-1}, x_{m-2}, \ldots, x_2)$.

If $c = (x_1, x_2, x_3, \ldots, x_m)$ is an m-cycle we will denote by $c(2)$ the collection of edges $\{x_i, x_{i+2}\}, i = 1, 2, \ldots, m$. The graph $c(2)$ is called the *distance* 2 *graph* of the cycle c.

m-cycle	distance 2 graph	m-cycle	distance 2 graph
	 3-cycle		 disjoint 3-cycles
	 disjoint double edges		 7-cycle
	 5-cycle		

Distance 2 graphs of m-cycles for $m = 3, 4, 5, 6$, and 7

An m-cycle system (S,C) of *order* n is said to be 2-*perfect* provided the collection of graphs $C(2)=\{c(2)\mid c\in C\}$ covers the edge set of K_n. This is *equivalent* to saying that for every pair of vertices $a\neq b$, there is *exactly* one cycle of the form $(\cdots,a,x,b,\cdots)\in C$; i.e., *exactly* one cycle in C in which a and b are joined by a path of length 2.

Example 4.1. (two 6-cycle systems of order 13, one 2-perfect and one not 2-perfect.)

(i) 2-*perfect*: $S=\{1,2,3,4,5,6,7,8,9,10,11,12,13\}$, and
$C_1=\{(5,9,11,8,13,12),\ (6,10,12,9,1,13),(7,11,13,10,2,1),$
$(8,12,1,11,3,2),(9,13,2,12,4,3),(10,1,3,13,5,4),(11,2,4,1,6,5),$
$(12,3,5,2,7,6),(13,4,6,3,8,7),(1,5,7,4,9,8),(2,6,8,5,10,9),$
$(3,7,9,6,11,10),(4,8,10,7,12,11)\}.$

(ii) *not* 2-*perfect*: $S=\{1,2,3,4,5,6,7,8,9,10,11,12,13\}$, and
$C_2=\{(1,2,13,3,12,7),(2,3,1,4,13,8),(3,4,2,5,1,9),(4,5,3,6,2,10),$
$(5,6,4,7,3,11),(6,7,5,8,4,12),(7,8,6,9,5,13),(8,9,7,10,6,1),$
$(9,10,8,11,7,2),(10,11,9,12,8,3),(11,12,10,13,9,4),$
$(12,13,11,1,10,5),(13,1,12,2,11,6)\}.$

None of the edges $\{1,4\},\{2,5\},\{3,6\},\{4,7\},\{5,7\},\{6,9\},\{7,10\},\{8,11\},$
$\{9,12\},\{10,13\},\{1,11\},\{2,12\},\{3,13\},\{1,7\},\{2,8\},\{3,9\},\{4,10\},\{5,11\},$
$\{6,12\},\{7,12\},\{1,8\},\{2,9\},\{3,10\},\{4,11\},\{5,12\},\{6,13\}$
are covered by the graphs in $C_2(2)$. *Check it out*!

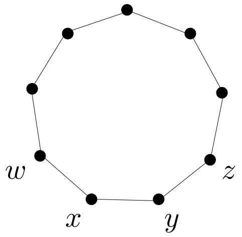
Although the spectrum for m-cycle systems (= set of all n such that an m-cycle system of order n exists) has recently been settled, the spectrum for m-cycle systems with the very strong additional property of being 2-perfect is far from settled. The spectrum for 2-perfect m-cycle systems has been determined for $m=3,5,6$, and 7 as well as for few other values of m [28]. However, knowing the spectrum for 2-perfect m-cycle systems is not necessary in what follows.

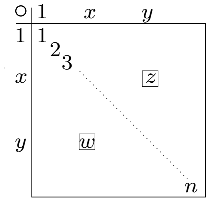
Given an m-cycle system (S,C) we can define a binary operation "$\circ$" on S called the *Standard Construction* (an *extrapolation* of the Standard Construction for Steiner triple systems) as follows:

The standard construction

(1) $x\circ x=x$, for all $x\in S$, and

(2) if $x\neq y$, $x\circ y=z$ and $y\circ x=w$ if and only if $(\cdots,w,x,y,z,\cdots)\in C$.





Example 4.2. (The Standard Construction applied to the 6-cycle systems in Example 4.1.)

$\circ_1$	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	10	13	2	7	5	11	9	12	4	3	8	6
2	7	2	11	1	3	8	6	12	10	13	4	5	9
3	10	8	3	12	2	4	9	7	13	11	1	6	5
4	6	11	9	4	13	3	5	10	8	1	12	2	7
5	8	7	12	10	5	1	4	6	11	9	2	13	3
6	4	9	8	13	11	6	2	5	7	12	10	3	1
7	2	5	10	9	1	12	7	3	6	8	13	11	4
8	5	3	6	11	10	2	13	8	4	7	9	1	12
9	13	6	4	7	12	11	3	1	9	5	8	10	2
10	3	1	7	5	8	13	12	4	2	10	6	9	11
11	12	4	2	8	6	9	1	13	5	3	11	7	10
12	11	13	5	3	9	7	10	2	1	6	4	12	8
13	9	12	1	6	4	10	8	11	3	2	7	5	13

$\circ_2$	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	13	2	13	2	10	12	9	3	5	13	2	6
2	7	2	1	3	1	3	11	13	10	4	6	1	3
3	4	8	3	2	4	2	4	12	1	11	5	7	2
4	3	5	9	4	3	5	3	5	13	2	12	6	8
5	9	4	6	10	5	4	6	4	6	1	3	13	7
6	8	10	5	7	11	6	5	7	5	7	2	4	1
7	2	9	11	6	8	12	7	6	8	6	8	3	5
8	6	3	10	12	7	9	13	8	7	9	7	9	4
9	5	7	4	11	13	8	10	1	9	8	10	8	10
10	11	6	8	5	12	1	9	11	2	10	9	11	9
11	10	12	7	9	6	13	2	10	12	3	11	10	12
12	13	11	13	8	10	7	1	3	11	13	4	12	11
13	12	1	12	1	9	11	8	2	4	12	1	5	13

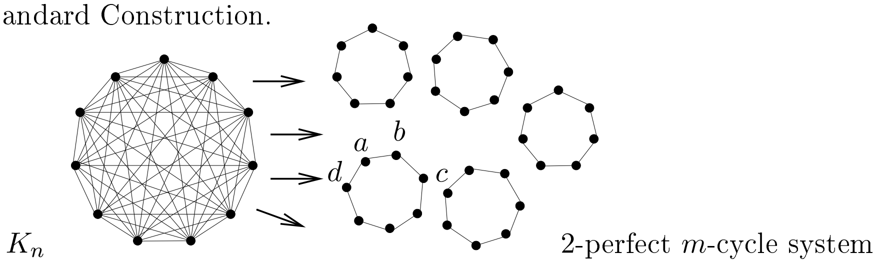
Now a cursory glance at the above example shows that the groupoid obtained from the 2-perfect 6-cycle system in Example 4.1 using the Standard Construction is a quasigroup, while the groupoid obtained from the 6-cycle system which is not 2-perfect using the Standard Construction is nowhere close to being a quasigroup. (For example, $1 \circ_2 2 = 1 \circ_2 4 = 13$.) The natural question to ask at this point is: does being 2-perfect have anything to do with the groupoid constructed from an m-cycle system being a quasigroup? The following Folk Theorem shows that the answer to this question is "**you bet it does**!"

Theorem 4.3 (Folk Theorem). *Let (S, C) be an m-cycle system. The groupoid constructed from (S, C) using the Standard Construction is a quasigroup if and only if (S, C) is 2-perfect.*

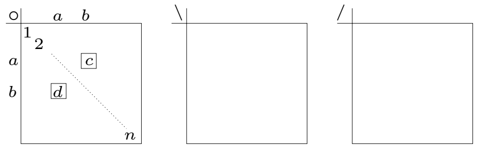
Proof. Suppose (S, C) is 2-perfect. We need to show that for all a, $b \in S$ the equations $a \circ x = b$ and $y \circ a = b$ have *unique* solutions. Now $a \circ a = a$ by definition for all $a \in S$; and we cannot have $a \circ b = a$ or $c \circ a = a$ for $b \neq a$ or $c \neq a$, since we cannot have cycles in C that look like $(\cdots, a, b, a \cdots)$ or $(\cdots c, a, a, \cdots)$. Hence $a \circ x = a$ and $y \circ a = a$ have unique solutions. So let $a \neq b \in S$ and $(\cdots, y, a, b, \cdots) \in C$. Then $y \circ a = b$. This is unique since the edge $\{a, b\}$ belongs to exactly one m-cycle of C. Since (S, C) is 2-perfect there is *exactly* one cycle $(\cdots, a, x, b, \cdots) \in C$ and so $a \circ x = b$ is unique. Hence $(S, \circ)$ is a quasigroup.

Now assume $(S, \circ)$ is a quasigroup and let $a \neq b \in S$. Then the equation $a \circ x = b$ has a *unique* solution and so there is *exactly* one m-cycle of the form $(\cdots, a, x, b, \cdots)$ in C. Hence (S, C) is 2-perfect. □

In what follows we will say that the class of 2-perfect m-cycle systems is *equationally defined* if and only if there exists a variety of quasigroups V with the property that the finite quasigroups in V are precisely the quasigroups whose multiplicative parts can be constructed from 2-perfect m-cycle systems using the Standard Construction. In other words, $(Q, \circ, \backslash, /) \in V$ if and only if $(Q, \circ)$ can be constructed from a 2-perfect m-cycle system using the Standard Construction.



$V =$



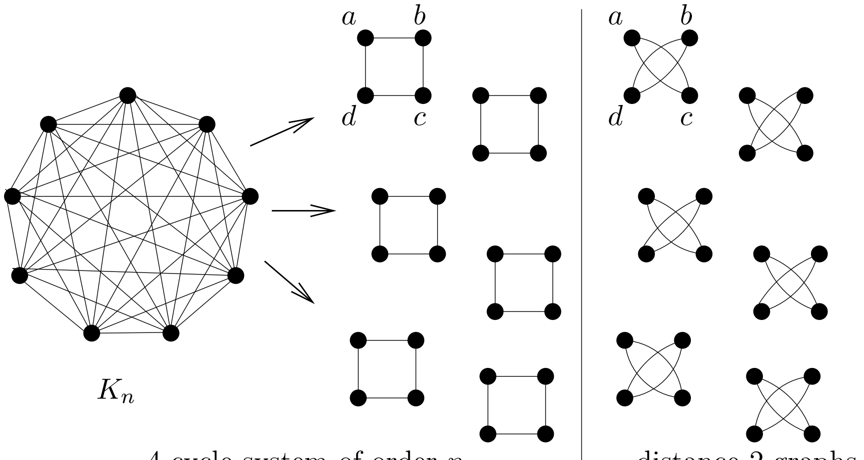
A finite quasigroup belongs to the variety of quasigroups V iff its multiplicative part can be constructed from a 2 perfect m cycle system using the Standard Construction.

Question. *For which* $m \geqslant 3$ *is the class of* 2*-perfect* m*-cycle systems equationally defined* ?

Since a triangle is a 3-cycle, Theorem 3.3 shows that the class of Steiner triple systems is equationally defined. We will now show that the class of 2-perfect m-cycle systems is equationally defined for $m = 3, 5$, and 7 ONLY. In each case we will give a set of defining identities for the variety.

5. 4-cycle systems

It is well-known (see A. Kotzig [13]) that the spectrum for 4-cycle systems is the set of all $n \equiv 1 \pmod 8$. Unfortunately, 4-cycle systems are *never* 2-perfect. This is easy to see. Let (S, C) be a 4-cycle system of order n. Then $|C| = \binom{n}{2}/4$. The distance 2 graph of each 4-cycle (a, b, c, d) in C consists of the four edges $\{a, b\}, \{a, b\}, \{c, d\}, \{c, d\}$. Hence a distinct listing of the edges belonging to the distance 2 graphs contains at most $2|C| = \binom{n}{2}/2$ edges, and so there are not enough edges to cover the edge set of K_n.



4-cycle system of order n

distance 2 graphs

Distance 2 graphs of a 4-cycle system

So much for 4-cycle systems!

6. 5-cycle systems

Unlike 3-cycle systems which are always 2-perfect and 4-cycle systems which are never 2-perfect, 5-cycle systems, just like the 6-cycle systems in Example 4.1, are sometimes 2-perfect and sometimes not 2-perfect.

Example 6.1. 2-perfect 5-cycle system of order 5 and two 5-cycle systems of order 11; one 2-perfect and the other not 2-perfect.

(1) 2-*perfect*: $S = \{1,2,3,4,5\}$, and $C = \{(1,2,3,4,5),(1,3,5,2,4)\}$.

(2) 2-*perfect*: $S = \{1,2,3,4,5,6,7,8,9,10,11\}$, and
$C_1 = \{(1,3,9,5,4),(2,4,10,6,5),\ (3,5,11,7,6),\ (4,6,1,8,7),$
$(5,7,2,9,8),\ (6,8,3,10,9),\ (7,9,4,11,10),\ (8,10,5,1,11),$
$(9,11,6,2,1),\ (10,1,7,3,2),\ (11,2,8,4,3)\}$.

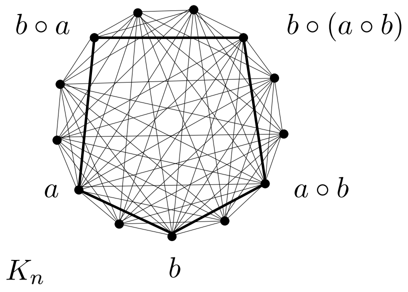
(3) *Not* 2-*perfect*: $S = \{1,2,3,4,5,6,7,8,9,10,11\}$, and
$C_2 = \{(1,3,10,5,4),\ (2,4,11,6,5),\ (3,5,1,7,6),\ (4,6,2,8,7),$
$(5,7,3,9,8),\ (6,8,4,10,9),\ (7,9,5,11,10),\ (18,10,6,1,11),$
$(9,11,7,2,1,),\ (10,1,8,3,2),\ (11,2,9,4,3)\}$.

In 1966 Alex Rosa [29] proved that the spectrum for 5-cycle systems is precisely the set of all $n \equiv 1$ or 5 (mod 10). Except for the unique 5-cycle system of order 5, none of the 5-cycle systems constructed by Rosa are 2-perfect. Almost 20 years later the 2-perfect spectrum for 5-cycle systems was determined by C. C. Lindner and D. R. Stinson [25] who showed that the 2-perfect spectrum is the same as the spectrum for 5-cycle systems, except that there does not exist a 2-perfect 5-cycle system of order 15. This is all quite interesting, but just as for 3-cycle systems, it plays no part in the determination of whether or not the class of 2-perfect 5-cycle systems is equationally defined.

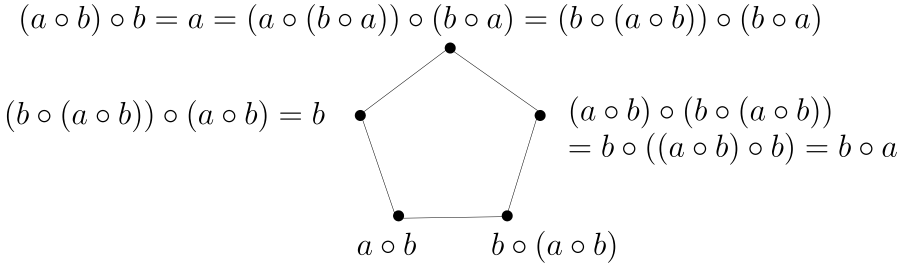
Theorem 6.2. *The class of* 2-*perfect* 5-*cycle systems can be equationally defined. The set of identities* $x^2 = x$, $(yx)x = y$, *and* $x(yx) = y(xy)$ *is a defining set of identities.*

Proof. Let V be the variety of quasigroups defined by the identities $x^2 = x$, $(yx)x = y$, and $x(yx) = y(xy)$. Let (S, C) be a 2-perfect 5-cycle system and $(S, \circ)$ the quasigroup constructed from (S, C) using the Standard Construction. To begin with, $(S, \circ)$ satisfies $x^2 = x$ by definition and so the other two identities are satisfied for $a = b$. Now suppose $a \neq b$ and $(a, b, c, d, e) \in C$. Then $(a \circ b) \circ b = c \circ b = a$ and $a \circ (b \circ a) = a \circ e = d = b \circ c = b \circ (a \circ b)$ and so the identities $(yx)x = y$ and $x(yx) = y(xy)$ are satisfied as well.

Hence $(S, \circ)$ belongs to the variety V. To finish the proof we need to show that every finite quasigroup belonging to V (= satisfying the defining set of identities) can be constructed from a 2-perfect 5-cycle system using the Standard Construction. The proof is more or less the same as for 3-cycle systems, except a bit more tedious. So, let $(S, \circ)$ be a quasigroup of order n satisfying the defining identities and define a collection of 5-cycles C as follows: for each $a \neq b \in S$, $(a, b, a \circ b, b \circ (a \circ b), b \circ a) \in C$.



We need to show that (i) $a, b, a \circ b, b \circ (a \circ b)$, and $b \circ a$ are distinct (so that $(a, b, a \circ b, b \circ (a \circ b), b \circ a)$ is indeed a 5-cycle), (ii) every edge of K_n belongs to a 5-cycle of C, (iii) each edge belonging to $(a, b, a \circ b, b \circ (a \circ b), b \circ a)$ determines exactly the same 5-cycle, and (iv) the Standard Construction applied to (S, C) gives the quasigroup $(S, \circ)$ that we started with. Parts (i) and (ii) are straightforward so we will go straight to (iii). We will show that the edge $\{a \circ b, b \circ (a \circ b)\}$ determines the same 5-cycle as the edge $\{a, b\}$. The best way to do this is with a picture.


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

The other cases are similar. This shows that (S, C) is a 2-perfect 5-cycle system (Theorem 4.3). Inherent in the proof of (iii) is $(x, a, b, y, z) \in C$ if and only if $a \circ b = y$ and $b \circ a = x$. Hence the Standard Construction applied to (S, C) gives the quasigroup $(S, \circ)$ that we started with (proving (iv)). □

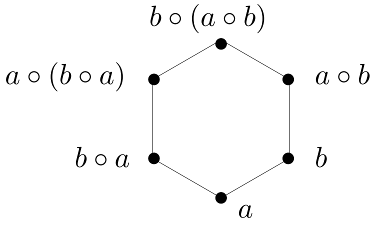
Remark . As with 3-cycle systems, there is no particular reason that the defining identities are all "multiplicative", other than the fact that the author happens to like them. Other collections involving all three operations are possible. For example, $x^2 = x$, $yx = y/x$, and $y/x = x\backslash(y(xy))$. The only requirement is that a quasigroup satisfies the defining identities if and only if its multiplicative part can be constructed from a 2-perfect 5-cycle system using the Standard Construction.

7. 2-perfect 6-cycle systems

The spectrum for 6-cycle systems is precisely the set of all $n \equiv 1$ or 9 (mod 12). This was determined by Alex Rosa and Charlotte Huang [11]. The 2-perfect spectrum is another matter and was determined in 1991 by C. C. Lindner, K. T. Phelps, C. Rodger, and E. J. Billington [4, 20] to be the same as for 6-cycle systems with the exception of $n = 9$, for which no 2-perfect 6-cycle system exists. As with the previous cases, knowing the 2-perfect spectrum has nothing to do with the problem of whether or not the class of 2-perfect 6-cycle systems can be equationally defined. In what follows a quasigroup $(S, \circ)$ is said to be *antisymmetric* provided $a \circ b \neq b \circ a$ for all $a \neq b \in S$. Denote by $\mathcal{C}$ the class of *all* finite antisymmetric quasigroups satisfying the three identities $x^2 = x, (yx)x = y$, and $(xy)(y(xy)) = x(yx)$.

Theorem 7.1. *$\mathcal{C}$ consists precisely of all quasigroups which can be constructed from 2-perfect 6-cycle systems using the Standard Construction.*

Proof. It is straightforward to see that the quasigroup constructed from a 2-perfect 6-cycle system (S, C) using the Standard Construction satisfies the three identities $x^2 = x$, $(yx)x = y$, and $(xy)(x(xy)) = x(yx)$. Antisymmetry comes from the fact that $(\cdots, d, a, b, c, \cdots) \in C$ gives $a \circ b = c \neq d = b \circ a$. Now let $(S, \circ)$ be an antisymmetric quasigroup satisfying the three identities above. Define a collection of 6-cycles C as follows: for each $a \neq b \in S$ place the 6-cycle $(a, b, a \circ b, b \circ (a \circ b), a \circ (b \circ a), b \circ a)$ in C. The proof that (S, C) is a 2-perfect 6-cycle system from which $(S, \circ)$ can be constructed using the Standard Construction follows the proof in Theorem 6.2 using the picture



□

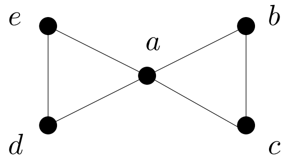
Corollary 7.2. *If I is a defining set of identities for 2-perfect 6-cycle systems and $V(I)$ is the variety of quasigroups defined by I, then the finite members of $V(I)$ are $\mathcal{C}$.* □

Here's where the trouble begins. Varieties are defined by identities *not* properties, and being antisymmetric is a property. Hence the three identities $x^2 = x$, $(yx)x = y$, and $(xy)(y(xy)) = x(yx)$ PLUS antisymmetry does NOT define a variety of quasigroups. So the problem of determining whether or not the class of 2-perfect 6-cycle systems is equationally defined is equivalent to proving or disproving the existence of a collection of quasigroup identities I so that the variety $V(I)$ defined by I has the property that the finite members of $V(I)$ are $\mathcal{C}$. This remained an open problem for years until D. E. Bryant proved in 1992 that no such variety exists [7, 8]. The proof that Bryant gave was to construct a 2-perfect 6-cycle system (S, C) such that the quasigroup $(S, \circ) \in \mathcal{C}$ constructed from (S, C) using the Standard Construction has a homomorphic image onto a quasigroup which cannot be constructed from a 2-perfect 6-cycle system using the Standard Construction and so does not belong to $\mathcal{C}$. It then follows that $\mathcal{C}$ cannot constitute the finite members of a variety $V(I)$, since any homomorphic image of any quasigroup in $\mathcal{C}$ would have to be in $V(I)$, and since it is finite would have to be in $\mathcal{C}$ as well (and therefore constructable from a 2-perfect 6-cycle system using the Standard Construction).

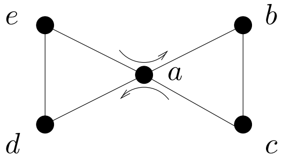
We give a sketch of Bryant's proof in the next section.

8. 2-perfect 6-cycle systems cannot be equationally defined

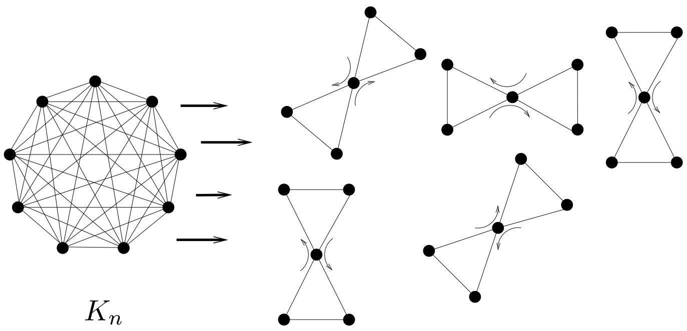
In order to prove that the class of 2-perfect 6-cycle systems cannot be equationally defined we will need to use a decomposition of K_n called a *bowtie system.* This calls for a definition. A *bowtie* is a closed 6-trail of the form (a, b, c, a, d, e), where $a, b, c, d,$ and e are *distinct.* So that there is no confusion, the closed 6-trail (a, b, c, a, d, e) consists of the 6 edges $\{a, b\}$, $\{b, c\}$, $\{c, a\}$, $\{a, d\}$, $\{d, e\}$, and $\{e, a\}$. Now, the graph of these edges is



which is also the graph of the bowtie (a, b, c, a, e, d). To differentiate between these two bowties we will use the picture

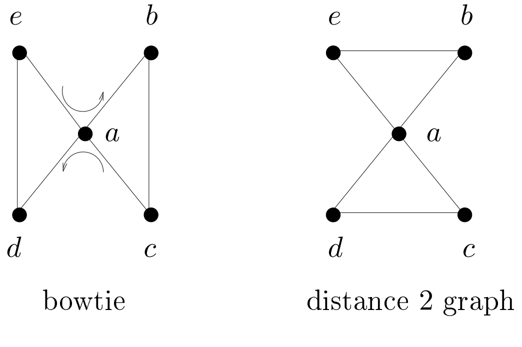


to represent the bowtie (a, b, c, a, d, e). A *bowtie system* of order n is a pair (S, B), where B is a collection of bowties which partition the edge set of K_n with vertex set S.



Bowtie system of order n

Just as with m-cycle systems, the bowtie system (S, B) is said to be 2-perfect provided the collection of distance 2 graphs of the bowties in B covers the edge set of K_n.



bowtie distance 2 graph

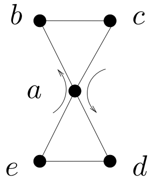
Theorem 8.1 (E. J. Billington and C. C. Lindner [5]). *The spectrum for 2-perfect bowtie systems is the set of all* $n \equiv 1$ *or* 9 $(mod\ 12)$, $n \geqslant 21$. □

Now given a 2-perfect bowtie system (S, B) we can define a binary operation "$\circ$" on S called the Standard Construction as follows:

The standard construction

(1) $x \circ x = x$, for all $x \in S$, and

(2) if $x \neq y$, $x \circ y = z$ and $y \circ x = w$ if and only if $(\cdots w, x, y, z, \cdots) \in B$.



$\circ$	a	b	c	d	e	n
	1 2					
a		$\boxed{c}$	$\boxed{b}$	$\boxed{e}$	$\boxed{d}$	
b	$\boxed{e}$		$\boxed{a}$			
c	$\boxed{d}$	$\boxed{a}$				
d	$\boxed{c}$				$\boxed{a}$	
e	$\boxed{b}$			$\boxed{a}$		
n						n

Just as with the Standard Construction for m-cycle systems the groupoid $(S, \circ)$ is a quasigroup if and only if (S, B) is 2-perfect. The proof follows the proof of Theorem 4.3. With all of the above information in hand we can now sketch the proof of the following theorem.

Theorem 8.2 (D. E. Bryant [7, 8]). *The class of* 2*-perfect* 6*-cycle systems CANNOT be equationally defined.*

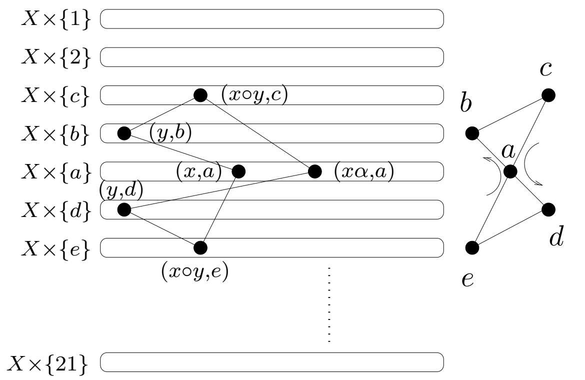
Proof. We will construct a quasigroup of order 273 which can be constructed from a 2-perfect 6-cycle system using the Standard Construction having a homomorphic image of order 21 which cannot be constructed from a 2-perfect 6-cycle system using the Standard Construction.

Let (X, C_1) be the 2-perfect 6-cycle system of order 13 in Example 4.1 and let (Y, B) be a 2-perfect bowtie system of order 21 (see Theorem 8.1). Let $S = X \times Y$ and define a collection of 6-cycles C_2 as follows:

(1) $((x, i), (y, i), (z, i), (u, i), (v, i), (w, i)) \in C_2$ for every $(x, y, z, u, v, w) \in C_1$ and every $i \in Y$, and

(2) let $(X, \circ)$ be any quasigroup of order 13, α a derangement on X, and for each $(a, b, c, a, d, e) \in B$ and each x, $y \in X$ (x, y not necessarily distinct) place the 6-cycle $((x, a), (y, b), (x \circ y, c), (x\alpha, a), (y, d), (x \circ y, e))$ in C_2.

It is straightforward to see that (S, C_2) is a 2-perfect 6-cycle system.



place a copy of (X, C_1) on each $X \times \{i\}$

Now let $(S, \circ_2)$ be the quasigroup constructed from (S, C_2) using the Standard Construction and $(Y, \circ_3)$ the quasigroup constructed from (Y, B) using the Standard Construction.

Define the mapping $\beta : S \overset{\text{onto}}{\longrightarrow} Y$ by $(x, i)\beta = i$. It is straightforward to see that β is a homomorphism of $(S, \circ_2)$ onto $(Y, \circ_3)$ (and therefore a homomorphism of $(S, \circ_2, \backslash_2, /_2)$ onto $(Y, \circ_3, \backslash_3, /_3)$). Now let (a, b, c, a, d, e) be any bowtie in (Y, B). Then $b \circ_3 c = a = c \circ_3 b, b \neq c$, and so $(Y, \circ_3)$ is definitely NOT antisymmetric. Since the multiplicative part of a quasigroup constructed from a 2-perfect 6-cycle system using the Standard Construction is *always* antisymmetric, $(Y, \circ_3)$ cannot be constructed from a 2-perfect 6-cycle system using the Standard Construction. It follows that the class of 2-perfect 6-cycle systems cannot be equationally defined. □

9. 7-cycle systems

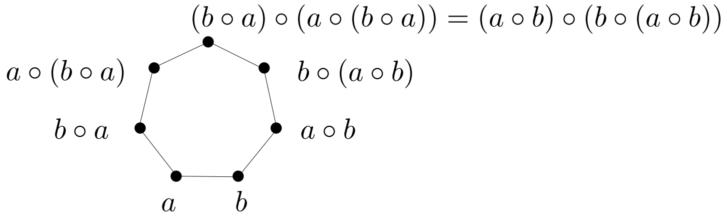
So far we have shown that the classes of 2-perfect 3-cycle and 5-cycle systems can be equationally defined, the class of 2-perfect 6-cycle systems cannot be equationally defined, and 4-cycle systems are not even worth discussing.

The spectrum for 7-cycle systems is the set of all $n \equiv 1$ or 7 (mod 14). (See A. Rosa [29].) The spectrum for 2-perfect 7-cycle systems is *exactly the same* as for 7-cycle systems and was determined in 1991 by Elisabetta Manduchi [26].

It turns out that the class of 2-perfect 7-cycle systems can be equationally defined.

Theorem 9.1. *The class of 2-perfect 7-cycle systems can be equationally defined. The set of identities $x^2 = x$, $(yx)x = y$, and $(xy)(y(xy)) = (yx)(x(yx))$ is a defining set of identities.*

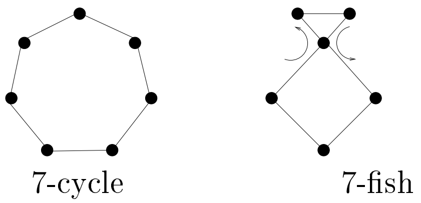
Proof. Let V be the variety of quasigroups defined by the identities $x^2 = x$, $(yx)x = y$, and $(xy)(y(xy)) = (yx)(x(yx))$, and let (S, C) be a 2-perfect 7-cycle system and $(S, \circ)$ the quasigroup constructed from (S, C) using the Standard Construction. Since $a \circ a = a$, for all $a \in S$, by definition, all three identities are satisfied for $a = b$. Now suppose $a \neq b$ and let $(a, b, c, d, e, f, g) \in C$. Then $(b \circ a) \circ a = g \circ a = b$ and $(a \circ b) \circ (b \circ (a \circ b)) = c \circ (b \circ c) = c \circ d = e = g \circ f = (b \circ a) \circ (a \circ g) = (b \circ a) \circ (a \circ (b \circ a))$ and so the identities $(yx)x = y$ and $(xy(y(xy)) = (yx)(x(yx))$ are satisfied. It follows that every quasigroup constructed from a 2-perfect 7-cycle system using the Standard Construction belongs to the variety V defined by the three identities $x^2 = x$, $(yx)x = y$, and $(xy)(y(xy)) = (yx)(x(yx))$. We must now show that every finite quasigroup belonging to the variety V can be constructed from a 2-perfect 7-cycle system using the Standard Construction. The proof is a bit tedious, but perfectly straightforward, and follows the proofs in Theorems 6.2 and 7.1 using the picture


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

□

Remark. Other collections of defining identities are possible of course, including collections involving all three operations.

Remark. The interested reader may feel a bit *uneasy* at this point for the following reason. Maybe the class of 2-perfect 7-cycle systems really cannot be equationally defined. Why not copy the argument in Theorem 8.2 to construct a quasigroup from a 2-perfect 7-cycle system having a homomorphism onto a quasigroup constructed from a 2-perfect "closed 7-trail system" so that the quasigroup constructed from this closed 7-trail system cannot be constructed from a 2-perfect 7-cycle system? The answer is simple: there are only two closed trails of length 7; here they are!



Closed trails of length 7

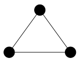
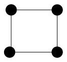
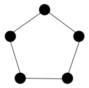
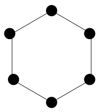
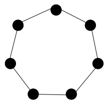
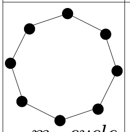
Since 4-cycle systems cannot be 2-perfect, “7-fish systems” cannot be 2-perfect. Hence the argument in Theorem 8.2 is not possible.

10. 2-perfect m-cycle systems cannot be equationally defined for m $\geqslant$ 8

Let’s recap what we’ve done so far: the classes of 2-perfect 3, 5, and 7 cycle systems can be equationally defined; the class of 6-cycle systems *cannot* be equationally defined; and the Standard Construction applied to 4-cycle systems never gives a quasigroup. In [9] it is shown that the class of 2-perfect m-cycle systems cannot be equationally defined for $m \geqslant slant8$. The construction to show this is an extrapolation of the construction used to show that 2-perfect 6-cycle systems cannot be equationally defined. Although the construction is similar the details are extremely tedious and since this is a survey with the intent of popularizing connections between universal algebra and graph theory, the author has decided to omit these details and refer the interested reader to [9, 19].

Theorem 10.1. *If $m \geqslant slant8$, 2-perfect m-cycle systems cannot be equationally defined.* □

11. Summary of results for 2-perfect m-cycle systems

K_n	*2 perfect spectrum*	*Equationally defined*
	$n \equiv 1$ *or* $3 (mod 6)$ *T.P.Kirkman* [12]	YES $\left\{\begin{array}{l} x^2=x \\ (yx)x=y \\ xy=yx \end{array}\right.$
		
	$n \equiv 1$ *or* $5 (mod\ 10)$ $n \neq 15$ *C.C.Lindner* *D.R.Stinson* [25]	YES $\left\{\begin{array}{l} x^2=x \\ (yx)x=y \\ x(yx)=y(xy) \end{array}\right.$
	$n \equiv 1$ *or* $9 (mod\ 12)$ $n \neq 9$ *E.J.Billington* *C.C.Lindner* *K.T.Phelps* *C.A.Rodger* [4, 20]	NO *D.E.Bryant* [7, 8]
	$n \equiv 1 (mod\ 14)$ *or* $n \equiv 7 (mod\ 14)$ *E.Manduchi* [26]	YES $\left\{\begin{array}{l} x^2=x \\ (yx)x=y \\ (xy)(y(xy))= \\ (yx)(x(yx)) \end{array}\right.$
 $m{-}cycle$ $m \geqslant 8$	*See* [28]	NO *D.E.Bryant* *C.C.Lindner* [9]

12. The Opposite Vertex Construction

Now it doesn't take the wisdom of a saint to see that there are lots of binary operations that can be defined on an m-cycle system other than the Standard Construction. One such binary operation is the *Opposite Vertex Construction.*

Let (S, C) be an m-cycle system of order n and denote by $C(k)$ the collection of distance k graphs of cycles in C. If the graphs in $C(k)$ partition K_n with vertex set S, then (S, C) is said to be *k-perfect.* This is *equivalent* to saying that for every pair of vertices $a \neq b$, there is *exactly* one cycle belonging to C in which a and b are joined by a path of length k. Up to now we have considered only 2-perfect m-cycle systems.

Now given a $(2m+1)$-cycle system we can define an idempotent $(x^2 = x)$ commutative $(xy = yx)$ groupoid as follows.

The opposite vertex construction

Let (S, C) be a $(2m + 1)$ cycle system and define a binary operation $\circ$ by:
(1) $x \circ x = x$, all $x \in S$, and
(2) if $x \neq y, x \circ y = y \circ x =$ the vertex opposite the edge $\{x, y\}$ in the cycle containing $\{x, y\}$.

It is immediate that $(S, \circ)$ is a quasigroup if and only if (S, C) is *m-perfect.*

Example 12.1. 2-perfect 5-cycle system of order 11 and quasigroup constructed using the Opposite Vertex Construction.

$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, $C = \{(1, 9, 4, 3, 5), (2, 10, 5, 4, 6), (3, 11, 6, 5, 7), (4, 1, 7, 6, 8), (5, 2, 8, 7, 9), (6, 3, 9, 8, 10), (7, 4, 10, 9, 11), (8, 5, 11, 10, 1), (9, 6, 1, 11, 2), (10, 7, 2, 1, 3), (11, 8, 3, 2, 4)\}$.

$\circ$	1	2	3	4	5	6	7	8	9	10	11
1	1	10	7	6	4	2	8	11	3	5	9
2	10	2	11	8	7	5	3	9	1	4	6
3	7	11	3	1	9	8	6	4	10	2	5
4	6	8	1	4	2	10	9	7	5	11	3
5	4	7	9	2	5	3	11	10	8	6	1
6	2	5	8	10	3	6	4	1	11	9	7
7	8	3	6	9	11	4	7	5	2	1	10
8	11	9	4	7	10	1	5	8	6	3	2
9	3	1	10	5	8	11	2	6	9	7	4
10	5	4	2	11	6	9	1	3	7	10	8
11	9	6	5	3	1	7	10	2	4	8	11

Inspection reveals that this quasigroup satisfies the 3 quasigroup identities $I(5) = \{x^2 = x,\ xy = yx,\ ((xy)\backslash x)y = (xy)\backslash y\}$.

Example 12.2. 3-perfect 7-cycle system of order 7 and quasigroup constructed using the Opposite Vertex Construction.

$S = \{1, 2, 3, 4, 5, 6, 7\}$,

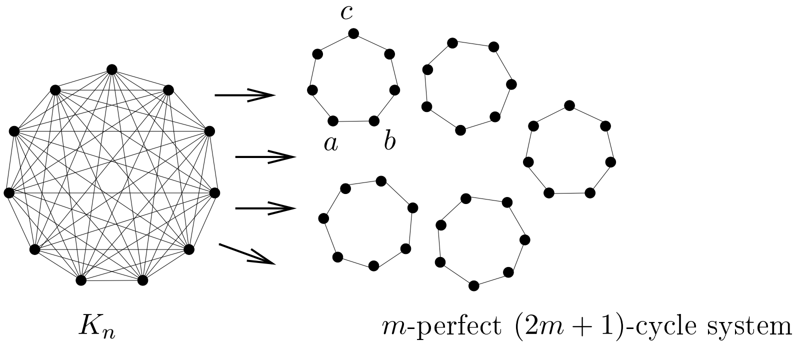
$C = \{(1, 2, 3, 4, 5, 6, 7),\ (1, 3, 5, 7, 2, 4, 6),\ (1, 4, 7, 3, 6, 2, 5)\}$.

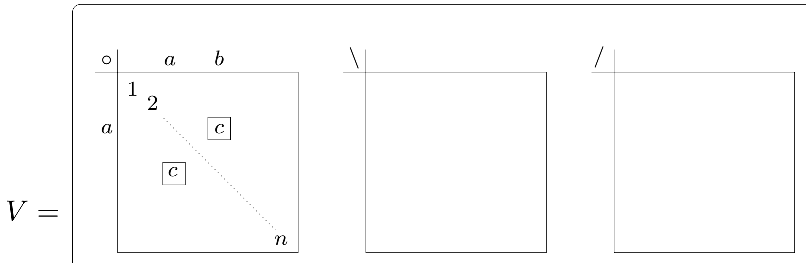
$\circ$	1	2	3	4	5	6	7
1	1	5	2	6	3	7	4
2	5	2	6	3	7	4	1
3	2	6	3	7	4	1	5
4	6	3	7	4	1	5	2
5	3	7	4	1	5	2	6
6	7	4	1	5	2	6	3
7	4	1	5	2	6	3	7

Inspection reveals that this quasigroup satisfies the 3 quasigroup identities $I(7) = \{x^2 = x,\ xy = yx,\ x\backslash((xy)\backslash x) = ((xy)\backslash x)(y\backslash((xy)\backslash y))\}$.

Examples 12.1 and 12.2 *illustrate* the fact (which is easy to prove) that the quasigroups constructed from 2-perfect 5-cycle systems using the Opposite Vertex Construction *always* satisfy the identities in $I(5)$ and the quasigroups constructed from 3-perfect 7-cycle systems using the Opposite Vertex Construction *always* satisfy the identities in $I(7)$.

In what follows to say that m-perfect $(2m + 1)$-cycle systems are *equationally defined* means that there exists a variety of quasigroups V such that a *finite* quasigroup belongs to the variety V if and only if its multiplicative part can be constructed from an m-perfect $(2m+1)$-cycle system using the Opposite Vertex Construction.





A *finite* quasigroup belongs to the variety of quasigroups V iff its multiplicative part can be constructed from an m-perfect $2m+1$-cycle system using the Opposite Vertex Construction.

We will show that m-perfect $(2m+1)$-cycle systems can be equationally defined for $m = 1, 2,$ and 3 only. We already know that 1-perfect 3-cycle systems (= Steiner triple systems) can be equationally defined, since the Opposite Vertex Construction and the Standard Construction are the same for 3-cycles.

The following two lemmas establish a fundamental relationship between 2-perfect $(2m+1)$-cycle systems and m-perfect $(2m+1)$-cycle systems.

Lemma 12.3. *If (Q, C) is a 2-perfect $(2m+1)$-cycle system, then $C(2)$ is an m-perfect $(2m+1)$-cycle system and $C(2)(m) = C$. Furthermore, if $(Q, \circ_1, \backslash_1, /_1)$ is the quasigroup constructed from (Q, C) using the Standard Construction and $(Q, \circ_2, \backslash_2, /_2)$ is the quasigroup constructed from $C(2)$ using the Opposite Vertex Construction, then $\circ_1 = \backslash_2, \backslash_1 = \circ_2$, and $/_1$ and $/_2$ are transposes.*

Proof. Let $(x_1, x_2, x_3, \dots, x_{2m+1}) \in C$. Then

$$(x_1, x_3, x_5, \dots, x_{2m+1}, x_2, x_4, \dots, x_{2m}) \in C(2).$$

Since (Q, C) is 2-perfect, $(Q, C(2))$ is a $(2m+1)$-cycle system. It is immediate that the distance m graph of $(x_1, x_3, x_5, \dots, x_{2m+1}, x_2, x_4, \dots, x_{2m})$ is $(x_1, x_2, x_3, \dots, x_{2m+1})$ and so $C(2) = C$ and $(Q, C(2))$ is m-perfect. Now let $(Q, \circ_1, \backslash_1, /_1)$ be the quasigroup constructed from (Q, C) using the Standard Construction and $(Q, \circ_2, \backslash_2, /_2)$ the quasigroup constructed from $(Q, C(2))$ using the Opposite Vertex Construction. Then

$$\begin{cases} x_1 \circ_1 x_2 = x_3, & x_1 \circ_2 x_3 = x_2 \\ x_1 \backslash_1 x_3 = x_2, & x_1 \backslash_2 x_2 = x_3 \\ x_3 /_1 x_2 = x_1, & x_2 /_2 x_3 = x_1. \end{cases}$$

It follows that $\circ_1 = \backslash_2, \backslash_1 = \circ_2$, and $/_1$ and $/_2$ are transposes. □

Lemma 12.4. *If (Q, C) is an m-perfect $(2m{+}1)$-cycle system, then $C(m)$ is a 2-perfect $(2m{+}1)$-cycle system and $C(m)(2) = C$. Further, if $(Q, \circ_1, \backslash_1, /_1)$ is the quasigroup constructed from (Q, C) using the Opposite Vertex Construction and $(Q, \circ_2, \backslash_2, /_2)$ the quasigroup constructed from $C(m)$ using the Standard Construction, then $\circ_1 = \backslash_2$, $\backslash_1 = \circ_2$, and $/_1$ and $/_2$ are transposes.*

Proof. Similar to Lemma 12.3. □

Now let $w(x, y)$ be any quasigroup word in the free quasigroup on the two generators x and y. Denote by $sw(x, y)$ the word obtained from $w(x, y)$ by replacing "$\circ$" with "$\backslash$", "$\backslash$" with "$\circ$", and any subword of the form "$a(x, y)/b(x, y)$" with "$b(x, y)/a(x, y)$". If I is any set of quasigroup identities set $S(I) = \{sw(x, y) = sv(x, y) \mid w(x, y) = v(x, y) \in I\}$. (Note that $S(S(I)) = I$.) We have the following lemma.

Lemma 12.5. *If $(Q, \circ_1, \backslash_1, /_1)$ and $(Q, \circ_2, \backslash_2, /_2)$ are quasigroups where $\circ_1 = \backslash_2$, $\backslash_1 = \circ_2$, and $/_1$ and $/_2$ are transposes, then one of these quasigroups satisfies the set of identities I if and only if the other quasigroup satisfies the identities $S(I)$.* □

Example 12.6. Let $(Q, \circ_1, \backslash_1, /_1)$ and $(Q, \circ_2, \backslash_2, /_2)$ be given by the accompanying quasigroups. Then $\circ_1 = \backslash_2, \backslash_1 = \circ_2$, and $/_1$ and $/_2$ are transposes. It is straightforward to see that $(Q, \circ_1, \backslash_1, /_1)$ satisfies the identities

$$I = \{x^2 = x, \quad y(x/(xy)) = (xy)\backslash y, \quad ((xy)\backslash y)x = x/(xy)\}$$

and $(Q, \circ_2, \backslash_2, /_2)$ satisfies the identities

$$S(I) = \{x\backslash x = x, \quad y\backslash((x\backslash y)/x) = (x\backslash y)y, \quad ((x\backslash y)y)\backslash x = (x\backslash y)/x\}.$$

$\circ_1$	1	2	3	4	5
1	1	4	2	5	3
2	4	2	5	3	1
3	2	5	3	1	4
4	5	3	1	4	2
1	3	1	4	2	5

$\circ_2$	1	2	3	4	5
1	1	3	5	2	4
2	5	2	4	1	3
3	4	1	3	5	2
4	3	5	2	4	1
5	2	4	1	3	5

Lemma 12.7. *m-perfect $(2m{+}1)$-cycle systems can be equationally defined if and only if 2-perfect $(2m + 1)$-cycle systems can be equationally defined.*

Proof. Suppose 2-perfect $(2m+1)$-cycle systems are equationally defined and let I be a defining set of identities. *Claim*: $S(I)$ is a defining set of identities for m-perfect $(2m+1)$-cycle systems. If $(Q, \circ_1, \backslash_1, /_1)$ satisfies $S(I)$, then the quasigroup $(Q, \circ_2, \backslash_2, /_2)$ satisfies I, where $\circ_2 = \backslash_1, \backslash_2 = \circ_1$, and $/_2$ and $/_1$ are transposes (Lemma 12.5). Let (Q, C) be the 2-perfect $(2m+1)$-cycle system from which $(Q, \circ_2, \backslash_2, /_2)$ is constructed using the Standard Construction. Then $(Q, C(2))$ is m-perfect and if $(Q, \circ_3, \backslash_3, /_3)$ is the quasigroup constructed from $(Q, C(2))$ using the Opposite Vertex Construction, then $\circ_3 = \backslash_2 = \circ_1$, $\backslash_3 = \circ_2 = \backslash_1$, and $/_3$ and $/_2$ are transposes (Lemma 12.3). Since $/_2$ and $/_1$ are transposes $/_3 = /_1$. Hence $(Q, \circ_3, \backslash_3, /_3) = (Q, \circ_1, \backslash_1, /_1)$ and so $(Q, \circ_1, \backslash_1, /_1)$ can be constructed from an m-perfect $(2m+1)$-cycle system using the Opposite Vertex Construction.

Now let (Q, C) be m-perfect. Then $(Q, C(m))$ is 2-perfect and so the quasigroup $(Q, \circ_2, \backslash_2, /_2)$ constructed from $(Q, C(m))$ using the Standard Construction satisfies the identities I. If $(Q, \circ_1, \backslash_1, /_1)$ is the quasigroup constructed from (Q, C) using the Opposite Vertex Construction, then (Lemma 12.4) $\circ_1 = \backslash_2$, $\backslash_1 = \circ_2$, and $/_1$ and $/_2$ are transposes. Hence by Lemma 12.5 the quasigroup $(Q, \circ_1, \backslash_1, /_1)$ satisfies the identities $S(I)$. Combining all of the above shows that if 2-perfect $(2m+1)$-cycle systems are equationally defined then so are m-perfect $(2m+1)$-cycle systems.

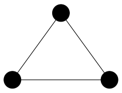
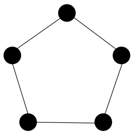
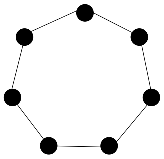
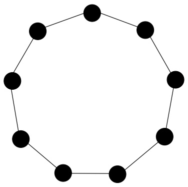
The proof of the converse is identical. □

Theorem 12.8 (C. C. Lindner and C. A. Rodger [21]). *m-perfect $(2m+1)$-cycle systems can be equationally defined for $m = 1, 2$ and 3 only.*

Proof. 2-perfect $(2m+1)$-cycle systems can be equationally defined for $m = 1, 2$, and 3 only. □

13. Summary of results for m-perfect $(\mathbf{2m+1})$-cycle systems

The accompaning table is a summary of the results on equationally defining m-perfect $(2m+1)$-cycle systems (using the Opposite Vertex Construction). The defining identities in each case are not necessarily “translations” of the corresponding identities used to define 2-perfect $(2m+1)$-cycle systems. It is nevertheless straightforward to see that, in fact, they are defining identities. The reason for their inclusion here is that they are appealing to the author.

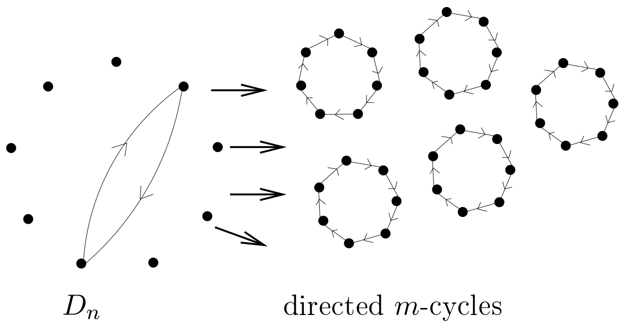
K_n	m-perfect spectrum	Equationally defined (using the Opposite Vertex Construction)
	$n \equiv 1$ or $3 \pmod 6$ Steiner triple system [12]	YES $\begin{cases} x^2 = x \\ xy = yx \\ (yx)x = y \end{cases}$
	$n \equiv 1$ or $5 \pmod{10}$ $n \neq 15$ C.C.Lindner D.R.Stinson [25]	YES $\begin{cases} x^2 = x \\ xy = yx \\ ((xy) \setminus x)y = (xy) \setminus y \end{cases}$
	$n \equiv 1$ or $7 \pmod{14}$ E.Manduchi [26]	YES $\begin{cases} x^2 = x \\ xy = yx \\ x \setminus ((xy) \setminus x) = \\ ((xy) \setminus x)(y \setminus ((xy) \setminus y)) \end{cases}$
 $(2m+1)$-cycle $2m+1 \geqslant 9$	See [28]	NO C.C.Lindner C.A.Rodger [21]

14. Directed cycle systems

A natural question to ask at this point is: "are there analogues of the Standard Construction and Opposite Vertex Construction for *directed m-cycle systems* (as opposed to the results we have surveyed so far = undirected m-cycle systems)?" The answer is YES!

Since there is a limit to the length of this paper, we will give here the directed analogues of the Standard and Opposite Vertex Constructions *without details*. The interested reader can find plenty of details in [10, 21].

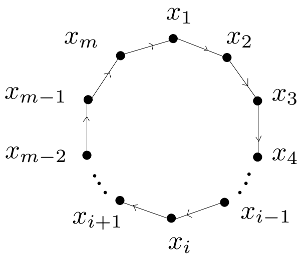
A *directed m-cycle system* of order n is a pair (S, C), where C is an edge disjoint collection of directed m-cycles which partitions the edge set of D_n (the complete directed graph on n vertices) with vertex set S.



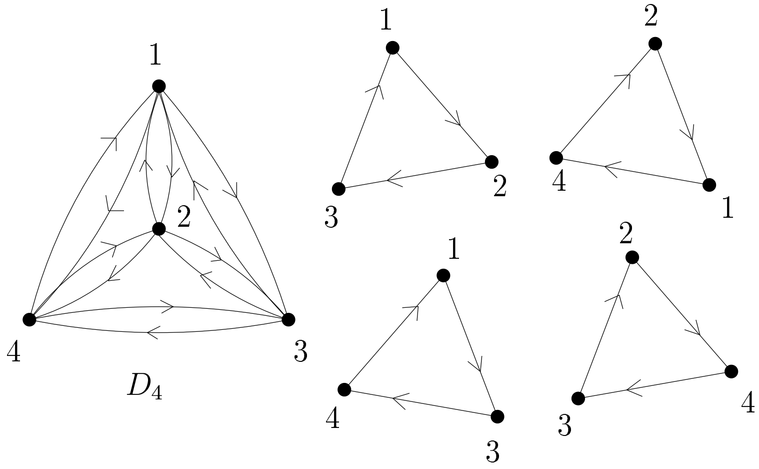
Quite recently, the necessary and sufficient conditions for the existence of a directed m-cycle system of order n have been determined to be [2]:

$$\begin{cases} (1)\ \ n \geqslant m,\ \text{if } n > 1, \\ (2)\ \ n(n-1)/m \quad \text{is an integer, and} \\ (3)\ \ (n,m) \neq (4,4), (6,3),\ \text{or } (6,6). \end{cases}$$

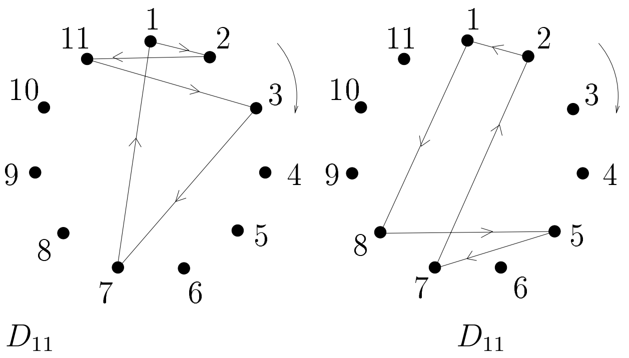
In what follows we will denote the directed m-cycle by any cyclic shift of $< x_1, x_2, x_3, \ldots, x_m >$ and the edge from a to b by $< a, b >$.



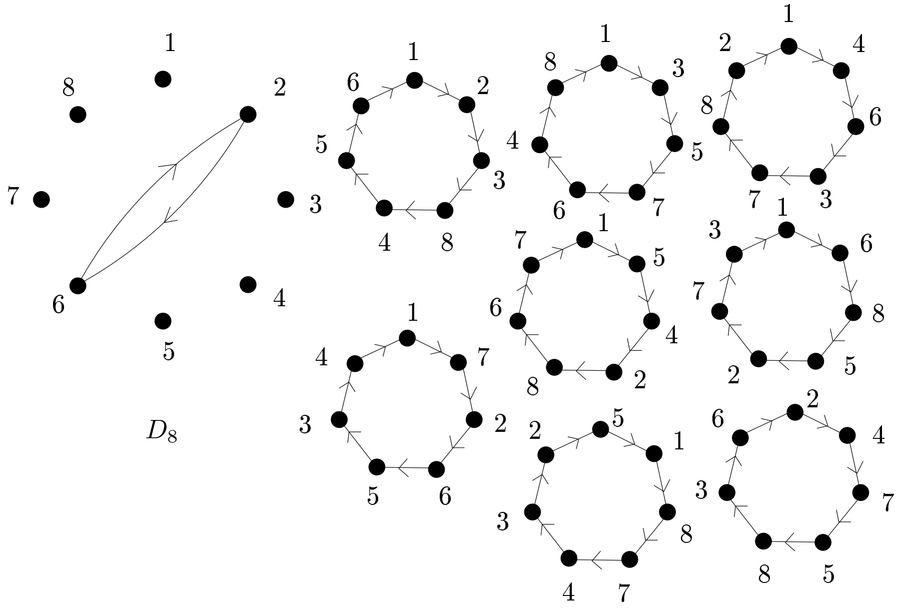
Example 14.1. Directed 3-cycle system of order 4.



Example 14.2. Directed 5-cycle system of order 11.



Example 14.3. Directed 7-cycle system of order 8.



Now given a directed cycle system (S, C) we can define two binary operations on S as follows:

The directed standard construction

Let (S, C) be a directed m-cycle system of order n and define a binary operation $\circ$ on S by:

(1) $x \circ x = x$, for all $x \in S$, and

(2) if $x \neq y$, $x \circ y = z$ if and only if $< \ldots, x, y, z, \cdots > \in S$.

The directed opposite vertex construction

Let (S, C) be a directed $(2m + 1)$-cycle system of order n and define a binary operation $\circ$ on S by:

(1) $x \circ x = x$, for all $x \in S$, and

(2) if $x \neq y, x \circ y =$ the vertex opposite the edge $< x, y >$ in the directed cycle containing $< x, y >$.

CAUTION. Since the edges $< a, b >$ and $< b, a >$ belong to different cycles, the vertex opposite $< a, b >$ is not necessarily the same vertex as the vertex opposite $< b, a >$. For example, in Example 14.2 the vertex opposite the edge $< 1, 2 >$ is 3, while the vertex opposite the edge $< 2, 1 >$ is 5.

The directed m-cycle system (S, C) of order n is said to be *k-perfect* if and only if $(S, C(k))$ partitions D_n, where $C(k)$ is the collection of distance k graphs of the cycles in C. This is equivalent to saying that for each $a \neq b \in S$, a and b are connected by a path of length k from a to b in a cycle of C and a path of length k from b to a in a cycle of C.

It is straightforward to see that the directed 3-cycle system of order 4 in Example 14.1 is 2-perfect; the directed 5-cycle system in Example 14.2 is NOT 2-perfect; and the directed 7-cycle system in Example 14.3 is 3-perfect.

As with undirected cycles, the groupoid (S, C) constructed from a directed m-cycle system using the Directed Standard Construction is a quasigroup if and only if (S, C) is 2-perfect and the groupoid constructed from a directed $(2m + 1)$-cycle system using the Directed Opposite Vertex Construction is a quasigroup if and only if (S, C) is m perfect. This is easy to prove (so we will omit the proof).

Example 14.4. Quasigroup constructed from Example 14.1 using the Directed Standard Construction.

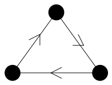
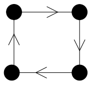
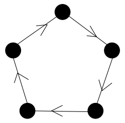
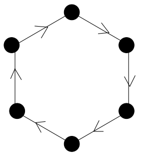
$\circ$	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

Example 14.5. Quasigroup constructed from Example 14.3 using the Directed Opposite Vertex Construction.

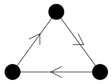
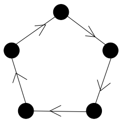
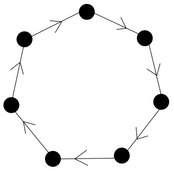
∘	1	2	3	4	5	6	7	8
1	1	4	6	7	8	2	5	3
2	3	2	5	8	7	4	6	1
3	5	8	3	2	4	7	1	6
4	6	7	1	4	2	8	3	5
5	4	1	7	6	5	3	8	2
6	8	5	2	3	1	6	4	7
7	2	3	8	5	6	1	7	4
8	7	6	4	1	3	5	2	8

Just as was the case for undirected cycle systems, the class of 2-perfect (m-perfect) directed m-cycle ($(2m+1)$-cycle) systems is *equationally defined* if and only if there exists a variety of quasigroups V such that the finite quasigroups in V are *precisely* the quasigroups whose multiplicative parts can be constructed from 2-perfect (m-perfect) directed m-cycle ($(2m+1)$-cycle) systems using the Directed Standard Construction (Directed Opposite Vertex Construction).

Summary of results for 2-perfect directed m-cycle systems

D_n	2-perfect spectrum	Equationally defined
	$n \equiv 0$ or 1 (mod 3) $n \neq 6$ N.S.Mendelsohn [27]	$\begin{cases} x^2 = x \\ x(yx) = y \end{cases}$
	$n \equiv 0$ or 1 (mod 4) $n \neq 4$ or 8 [3]	$\begin{cases} x^2 = x \\ (xy)(y(xy)) = x \end{cases}$
	$n \equiv 0$ or 1 (mod 5) $n \neq 6$ or 10 and possibly $n = 15$ and 20 [3]	$\begin{cases} x^2 = x \\ (y(xy))((xy)(y(xy))) = x \end{cases}$
 m-cycle $m \geqslant 6$	?	NO D.E.Bryant C.C.Lindner [10]

Summary of results for m-perfect directed (2m + 1)-cycle systems

D_n	m-perfect spectrum	Equationally defined
	$n \equiv 0$ or 1 (mod 3) $n \neq 6$ N.S.Mendelsohn [27]	$\begin{cases} x^2 = x \\ x(yx) = y \end{cases}$
	$n \equiv 0$ or 1 (mod 5) $n \neq 6$ or 10 and possibly $n = 15$ and 20 [3]	$\begin{cases} x^2 = x \\ y(x/(xy)) = (xy)\backslash y \\ ((xy)\backslash y)x = x/(xy) \end{cases}$
 $(2m + 1)$-cycle $2m + 1 \geqslant 7$	?	NO C.C.Lindner C.A.Rodger [21]

15. Concluding remarks

The initial part of this survey is a rewriting of a survey paper by the author for a talk in Adelaide at the AustMS meetings at Flinders University in 1996 [17]. The sections on the Opposite Vertex Construction and the directed analogues of the Standard Construction and the Opposite Vertex Construction have been added. Other "perfect" graph decompositions are possible, and the interested reader is referred to [15, 16, 17, 22, 23, 24] for additional reading on the subject.

Finally, as mentioned throughout this set of notes, knowing the spectrum for 2-perfect m-cycle systems and 2-perfect directed m-cycle systems is not necessary in determining whether or not a 2-perfect class is equationally defined. However, it is certainly comforting to know the spectrum for the 2-perfect classes that can be equationally defined. The author would like to point out that the determination of the 2-perfect spectrums for $m = 5, 6$ and 7 for undirected cycles and $m = 4$ and 5 for directed cycles is a difficult undertaking.

The general problem of determining the 2-perfect spectrum for both undirected and directed m-cycle systems is an open and extremely difficult problem.

Well, I could go on and on. However, this set of notes is long enough as it is, and so I will end with the immortal words of Porky Pig:

THAT'S ALL FOLKS!

References

[1] **B. Alspach and H. Gavlas**: *Cycle decompositions of K_n and $K_n - I$*, J. Combinatorial Theory B **81** (2001), 77 – 99.

[2] **B. Alspach, H. Gavlas, M. Šajna, and H. Verrall**: *Cycle decompositions IV: Complete directed graphs and fixed length directed cycles*, J. Combinatorial Theory B, (to appear).

[3] **F. E. Bennett**: *Recent progress on the existence of perfect Mendelsohn designs*: J. Statistical Planning and Inference **94** (2001), 121 – 138.

[4] **E. J. Billington and C. C. Lindner**: *The spectrum for lambda-fold 2-perfect 6-cycle systems*, European J. Combinatorics **13** (1992), 5 – 14.

[5] **E. J. Billington and C. C. Lindner**: *The spectrum for 2-perfect bowtie systems*, Discrete Math. **135** (1994), 61 – 68.

[6] **G. Birkhoff**: *On the structure of abstract algebras*, Proc. Cambridge Phil. Soc. **31** (1935), 433 – 454.

[7] **D. E. Bryant**: *Varieties of p-quasigroups*, Australasian J. Combinatorics **6** (1992), 229 – 243.

[8] **D. E. Bryant**: *Varieties of quasigroups arising from 2-perfect m-cycle systems*, Designs, Codes and Cryptography **2** (1992), 159 – 168.

[9] **D. E. Bryant and C. C. Lindner**: *2-perfect m-cycle systems can be equationally defined for $m = 3, 5$, and 7 only*, Algebra Universalis **35** (1996), 1 – 7.

[10] **D. E. Bryant and C. C. Lindner**: *2-perfect directed m-cycle systems can be equationally defined for $m = 3, 4$ and 5 only*, J. Statistical Planning and Inference **56** (1996), 57 – 63.

[11] **C. Huang and A. Rosa**: *Another class of balanced graph designs: balanced circuit designs*, Discrete Math. **12** (1975), 269 – 293.

[12] **T. P. Kirkman**: *On a problem in combinations*, Cambridge and Dublin Math. J. **2** (1847), 191 – 204.

[13] **A. Kotzig**: *On cycle decompositions of the complete graph into 4k-gons* (Russian), Mat.-fiz. Časopis **15** (1965), 227 – 233.

[14] **E. R. Lamken and R. M. Wilson**: *Decompositions of edge-colored complete graphs*, J. Combinatorial Theory, Ser. A **89** (2000), 149 – 200.

[15] **E. M. Li Marzi**: *Perfect* 7*-cycle systems*, Appl. Discr. Math. (to appear).

[16] **E. M. Li Marzi and F. Rania**: *On equationally definable* m*-cycle systems*, Rendiconti Semin. Mat. Messina - Serie II Tomo XXIV Supplemento al N°5, 87 – 93.

[17] **C. C. Lindner**: *Graph theory and universal algebra go hand in hand*, Australian Math. Soc. Gazette **24** (1997), 191 – 215.

[18] **C. C. Lindner**: *A partial* 4*-cycle system of order* n *can be embedded in a* 4*-cycle system of order at most* $2n + 15$, Bull. ICA **37** (2003), 88 – 93.

[19] **C. C. Lindner, E. M. Li Marzi, F. Rania and R. M. Wilson**: $\{2, 3\}$*-perfect* m*-cycle systems are equationally defined for* $m = 7, 8, 9$, *and* 11 *only*, (to appear).

[20] **C. C. Lindner, K. T. Phelps and C. A. Rodger**: *The spectrum for* 2*-perfect* 6*-cycle systems*, J. Combinatorial Theory, Ser. A **57** (1991), 76 – 85.

[21] **C. C. Lindner and C. A. Rodger**: *On equationally defining* m*-perfect* $(2m + 1)$*-cycle systems*, J. Combinatorial Designs **5** (1994), 301 – 309.

[22] **C. C. Lindner and C. A. Rodger**: *The complete solution of the problem of equationally defining closed trail systems of* K_n, Bull. ICA **11** (1994), 84 – 95.

[23] **C. C. Lindner and C. A. Rodger**: *On equationally defining extended cycle systems*, Discrete Math. **173** (1997), 1 – 14.

[24] **C. C. Lindner and C. A. Rodger**: *A connection between varieties of quasigroups and graph decompositions*, Discrete Math. (Perspectives), (to appear).

[25] **C. C. Lindner and D. R. Stinson**: *Steiner pentagon systems*, Discrete Math. **52**, (1984), 67 – 74.

[26] **E. Manduchi**: *Steiner heptagon systems*, Ars Combinatoria **31** (1991), 105 – 115.

[27] **N. S. Mendelsohn**: *A natural generalization of Steiner triple systems*, In *Computers in number theory*, Academic Press, New York 1971, 323 – 338.

[28] **C. A. Rodger**: *Cycle systems*, In *The CRC Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, eds.), CRC Press 1996, 266 – 270.

[29] **A. Rosa**: *On cyclic decompositions of the complete graph into polygons with an odd number of edges*, (in Slovak), Časopis Pěstov. Mat. **91** (1966), 53 – 63.

[30] **M. Šajna**: *Cycle decompositions III: complete graphs and fixed length cycles*, J. Combinatorial Designs **10** (2002), 27 – 78.

Department of Discrete and Statistical Sciences
Auburn University
Auburn
Alabama 36849
USA
e-mail: lindncc@mail.auburn.edu

Received May 23, 2003

Quasigroups and Related Systems **10** (2003), 65 − 94

Octonions, simple Moufang loops and triality

Gábor P. Nagy and Petr Vojtěchovský

Abstract

Nonassociative finite simple Moufang loops are exactly the loops constructed by Paige from Zorn vector matrix algebras. We prove this result anew, using geometric loop theory. In order to make the paper accessible to a broader audience, we carefully discuss the connections between composition algebras, simple Moufang loops, simple Moufang 3-nets, S-simple groups and groups with triality. Related results on multiplication groups, automorphisms groups and generators of Paige loops are provided.

Contents

2000 Mathematics Subject Classification: 20N05, 20D05
Keywords: simple Moufang loop, Paige loop, octonion, composition algebra, classical group, group with triality, net

The first author was supported by the FKFP grant 0063/2001 of the Hungarian Ministry for Education and the OTKA grants nos. F042959 and T043758. The second author partially supported by the Grant Agency of Charles University, grant number 269/2001/B-MAT/MFF.

1 Introduction

The goal of this paper is to present the classification of finite simple Moufang loops in an accessible and uniform way to a broad audience of researchers in nonassociative algebra. The results are not new but the arguments often are. Although not all proofs are included, our intention was to leave out only those proofs that are standard (that is those that can be found in many sources), those that are purely group-theoretical, and those that require only basic knowledge of loop theory. We have rewritten many proofs using geometric loop theory—a more suitable setting for this kind of reasoning. To emphasize the links to other areas of loop theory and algebra, we comment on definitions and results generously, although most of the remarks we make are not essential later in the text.

Here is a brief description of the content of this paper. After reviewing some basic properties of loops, nets and composition algebras, we construct a family of simple Moufang loops from the Zorn alternative algebras. These loops are also known as Paige loops. We then briefly discuss the multiplication groups of Paige loops, because these are essential in the classification.

With every Moufang loop we associate a Moufang 3-net, and with this 3-net we associate a group with triality. An S-homomorphism is a homomorphism between two groups with triality that preserves the respective triality automorphisms. This leads us to the concept of S-simple groups with triality, which we classify. The group with triality G associated with a simple Moufang loop L must be S-simple. Moreover, when L is nonassociative G must be simple. This is the moment when we use results of Liebeck concerning the classification of finite simple groups with triality. His work is based on the classification of finite simple groups. The fact that there are no other nonassociative finite simple Moufang loops besides finite Paige loops then follows easily.

Building on the geometric understanding we have obtained so far, we determine the automorphism groups of all Paige loops constructed over perfect fields. We conclude the paper with several results concerning the generators of finite Paige loops and integral Cayley numbers. All these results are mentioned because they point once again towards classical groups. Several problems and conjectures are pondered in the last section.

A few words concerning the notation: As is the habit among many loop theorists, we write maps to the right of their arguments, and therefore compose maps from left to right. The only exception to this rule are some traditional maps, such as the determinant det. A subloop generated by S will be denoted by $\langle S\rangle$. The symmetric group on n points is denoted by S_n.

2 Loops and nets

We now give a brief overview of definitions and results concerning loops and nets. Nets (also called webs in the literature) form the foundations of the geometric loop theory. All material covered in 2.1–2.3 can be found in [4] and [25], with proofs. We refer the reader to [25, Ch. II] and [8, Ch. VIII, X] for further study of nets.

2.1 Quasigroups and loops

Let $Q = (Q, \cdot)$ be a groupoid. Then Q is a *quasigroup* if the equation $x \cdot y = z$ has a unique solution in Q whenever two of the three elements x, y, $z \in Q$ are specified. Quasigroups are interesting in their own right, but also appear in combinatorics under the name *latin squares* (more precisely, multiplication tables of finite quasigroups are exactly latin squares), and in universal algebra, where subvarieties of quasigroups are often used to provide an instance of some universal algebraic notion that cannot be demonstrated in groups or other rigid objects. We ought to point out that in order to define the variety of quasigroups equationally, one must introduce additional operations $\backslash$ and $/$ for left and right division, respectively.

A quasigroup Q that possesses an element e satisfying $e \cdot x = x \cdot e = x$ for every $x \in Q$ is called a *loop* with *neutral element* e. The vastness of the variety of loops dictates to focus on some subvariety, usually defined by an identity approximating the associative law. (Associative loops are exactly groups.) In this paper, we will be concerned with *Moufang loops*, which are loops satisfying any one of the three equivalent *Moufang identities*

$$((xy)x)z = x(y(xz)), \quad ((xy)z)y = x(y(zy)), \quad (xy)(zx) = (x(yz))x, \quad (1)$$

and in particular with simple Moufang loops (see below). Every element x of a Moufang loop is accompanied by its *two-sided inverse* x^{-1} satisfying $xx^{-1} = x^{-1}x = e$. Any two elements of a Moufang loop generate a subgroup, and thus $(xy)^{-1} = y^{-1}x^{-1}$.

Each element x of a loop Q gives rise to two permutations on Q, the *left translation* $L_x : y \mapsto xy$ and the *right translation* $R_x : y \mapsto yx$. The group $\mathrm{Mlt}\,Q$ generated by all left and right translations is known as the *multiplication group* of Q. The subloop $\mathrm{Inn}\,Q$ of $\mathrm{Mlt}\,Q$ generated by all maps $L_xL_yL_{yx}^{-1}$, $R_xR_yR_{xy}^{-1}$ and $R_xL_x^{-1}$, for x, $y \in Q$, is called the *inner mapping group* of Q. It consists of all $\varphi \in \mathrm{Mlt}\,Q$ such that $e\varphi = e$.

A subloop S of Q is *normal* in Q if $S\varphi = S$ for every $\varphi \in \mathrm{Inn}\,Q$. The loop Q is said to be *simple* if the only normal subloops of Q are Q and $\{e\}$.

In any loop Q, the *commutator* of x, $y \in Q$ is the unique element $[x, y] \in Q$ satisfying $xy = (yx)[x, y]$, and the *associator* of x, y, $z \in Q$ is the unique element $[x, y, z] \in Q$ satisfying $(xy)z = (x(yz))[x, y, z]$. We prefer to call the subloop $C(Q)$ of Q consisting of all elements x such that $[x, y] = [y, x] = e$ for every $y \in Q$ the *commutant* of Q. (Some authors use the name *centrum* or *Moufang center*.) The subloop $N(Q)$ consisting of all $x \in Q$ such that $[x, y, z] = [y, x, z] = [y, z, x] = e$ holds for every y, $z \in Q$ is known as the *nucleus* of Q. Then $Z(Q) = C(Q) \cap N(Q)$ is the *center* of Q, which is always a normal subloop of Q.

2.2 Isotopisms versus isomorphisms

Quasigroups and loops can be classified up to isomorphism or up to isotopism. When Q_1, Q_2 are quasigroups, then the triple (α, β, γ) of bijections from Q_1 onto Q_2 is an *isotopism* of Q_1 onto Q_2 if $x\alpha \cdot y\beta = (x \cdot y)\gamma$ holds for every x, $y \in Q_1$. An isotopism with $Q_1 = Q_2$ is called an *autotopism*. Every isomorphism α gives rise to an isotopism (α, α, α). The notion of isotopism is superfluous in group theory, as any two groups that are isotopic are already isomorphic.

In terms of multiplication tables, Q_1 and Q_2 are isotopic if the multiplication table of Q_2 can be obtained from the multiplication table of Q_1 by permuting the rows (by α), the columns (by β), and by renaming the elements (by γ). Isotopisms are therefore appropriate morphisms for the study of quasigroups and loops. On the other hand, every quasigroup is isotopic to a loop, which shows that the algebraic properties of isotopic quasigroups can differ substantially. Fortunately, the classification of finite simple Moufang loops is the same no matter which kind of equivalence (isotopism or isomorphism) we use. This is because (as we shall see) there is at most one nonassociative finite simple Moufang loop of a given order, up to isomorphism.

A loop L is a *G-loop* if every loop isotopic to L is isomorphic to L. So, finite simple Moufang loops are G-loops.

2.3 Loops and 3-nets

Let $k > 2$ be an integer, $\mathcal{P}$ a set, and $\mathcal{L}_1, \dots, \mathcal{L}_k$ disjoint sets of subsets of $\mathcal{P}$. Put $\mathcal{L} = \bigcup \mathcal{L}_i$. We call the elements of $\mathcal{P}$ and $\mathcal{L}$ *points* and *lines*, respectively, and use the common geometric terminology, such as "all lines through the point P", etc. For $\ell \in \mathcal{L}_i$, we also speak of a *line of type* i or an i*-line.* Lines of the same type are called *parallel.*

The pair $(\mathcal{P}, \mathcal{L})$ is a k*-net* if the following axioms hold:

1) Distinct lines of the same type are disjoint.

2) Two lines of different types have precisely one point in common.

3) Through any point, there is precisely one line of each type.

Upon interchanging the roles of points and lines, we obtain *dual* k*-nets.* In that case, the points can be partitioned into k classes so that:

1′) Distinct points of the same type are not connected by a line.

2′) Two points of different types are connected by a unique line.

3′) Every line consists of k points of pairwise different types.

There is a natural relation between loops and 3-nets. Let us first start from a loop L and put $\mathcal{P} = L \times L$. Define the line classes

$$\begin{aligned}
\mathcal{L}_1 &= \{\{(x,c) \mid x \in L\} \mid c \in L\}, \\
\mathcal{L}_2 &= \{\{(c,y) \mid y \in L\} \mid c \in L\}, \\
\mathcal{L}_3 &= \{\{(x,y) \mid x, y \in L,\, xy = c\} \mid c \in L\}.
\end{aligned}$$

Then, $(\mathcal{P}, \mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3)$ is a 3-net. The lines of these classes are also called *horizontal, vertical* and *transversal lines,* respectively. The point

$O = (e, e)$ is the *origin* of the net.

Let us now consider a 3-net $(\mathcal{P}, \mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3)$. Let $O \in \mathcal{P}$ be an arbitrary point, and let ℓ, k be the unique horizontal and vertical lines through O, respectively. Then the construction of Figure 1 defines a loop operation on ℓ with neutral element O.

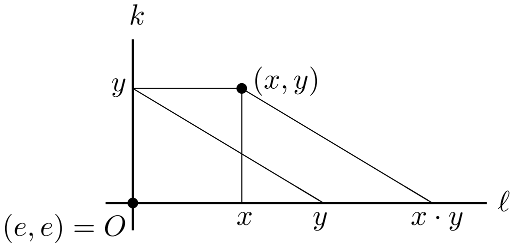


Figure 1: The geometric definition of the coordinate loop.

Since the parallel projections are bijections between lines of different type, we can index the points of k by points of ℓ, thus obtaining a bijection between $\mathcal{P}$ and $\ell \times \ell$. The three line classes are determined by the equations $X = c$, $Y = c$, $XY = c$, respectively, where c is a constant. We say that (ℓ, O) is a *coordinate loop* of the 3-net $(\mathcal{P}, \mathcal{L})$.

2.4. Collineations and autotopisms

Let $\mathcal{N} = (\mathcal{P}, \mathcal{L})$ be a 3-net. *Collineations* are line preserving bijective maps $\mathcal{P} \to \mathcal{P}$. The group of collineations of $\mathcal{N}$ is denoted by $\text{Coll}\,\mathcal{N}$. A collineation induces a permutation of the line classes. There is therefore a group homomorphism from $\text{Coll}\,\mathcal{N}$ to the symmetric group S_3. The kernel of this homomorphism consists of the *direction preserving collineations.*

Let L be the coordinate loop of $\mathcal{N} = (\mathcal{P}, \mathcal{L})$ with respect to some origin $O \in \mathcal{P}$. Let $\varphi : \mathcal{P} \to \mathcal{P}$ be a bijection. Then φ preserves the line classes 1 and 2 if and only if it has the form $(x, y) \mapsto (x\alpha, y\beta)$ for some bijections α, $\beta : L \to L$. Moreover, if φ preserves the line classes 1 and 2 then φ also preserves the third class if and only if there is a bijection $\gamma : L \to L$ such that the triple (α, β, γ) is an autotopism of L. Automorphisms of L can be characterized in a similar way (see Lemma 7.2).

2.5. Bol reflections

Let $\mathcal{N}$ be a 3-net and $\ell_i \in \mathcal{L}_i$, for some i. We define a certain permutation σ_{ℓ_i} on the point set $\mathcal{P}$ (cf. Figure 2). For $P \in \mathcal{P}$, let a_j and a_k be the lines through P such that $a_j \in \mathcal{L}_j$, $a_k \in \mathcal{L}_k$, and $\{i, j, k\} = \{1, 2, 3\}$.

Then there are unique intersection points $Q_j = a_j \cap \ell_i$, $Q_k = a_k \cap \ell_i$. We define $P\sigma_{\ell_i} = b_j \cap b_k$, where b_j is the unique j-line through Q_k, and b_k the unique k-line through Q_j. The permutation σ_{ℓ_i} is clearly an involution satisfying $\mathcal{L}_j\sigma_{\ell_i} = \mathcal{L}_k$, $\mathcal{L}_k\sigma_{\ell_i} = \mathcal{L}_j$. If it happens to be the case that σ_{ℓ_i} is a collineation, we call it the *Bol reflection with axis* ℓ_i.

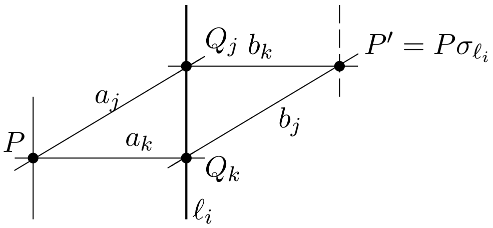


Figure 2: The Bol reflection with axis ℓ_i.

Obviously, every Bol reflection fixes a line pointwise (namely its axis) and interchanges the other two line classes. In fact, it is easy to see that any collineation with this property is a Bol reflection. Then for any $\gamma \in \operatorname{Coll}\mathcal{N}$ and $\ell \in \mathcal{L}$ we must have $\gamma^{-1}\sigma_\ell\gamma = \sigma_{\ell\gamma}$, as $\gamma^{-1}\sigma_\ell\gamma$ is a collineation fixing the line $\ell\gamma$ pointwise. In words, the set of Bol reflections of $\mathcal{N}$ is invariant under conjugations by elements of the collineation group of $\mathcal{N}$.

Let $\ell_i \in \mathcal{L}_i$, $i = 1, 2, 3$, be the lines through some point P of $\mathcal{N}$. As we have just seen, $\sigma_{\ell_1}\sigma_{\ell_2}\sigma_{\ell_1} = \sigma_{\ell_3}$, since $\ell_3\sigma_{\ell_1} = \ell_2$. Therefore $(\sigma_{\ell_1}\sigma_{\ell_2})^3 = \mathrm{id}$ and $\langle\sigma_{\ell_1}, \sigma_{\ell_2}, \sigma_{\ell_3}\rangle$ is isomorphic to S_3. This fact will be of importance later.

A 3-net $\mathcal{N}$ is called a *Moufang* 3-*net* if σ_ℓ is a Bol reflection for every line ℓ. The terminology is justified by Bol, who proved that $\mathcal{N}$ is a Moufang 3-net if and only if all coordinate loops of $\mathcal{N}$ are Moufang [4, p. 120].

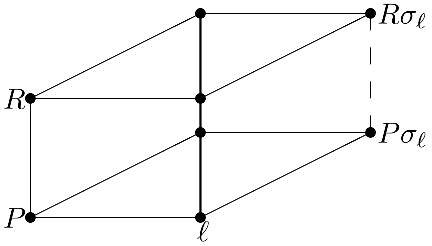


Figure 3: The 2-Bol configuration.

The configuration in Figure 3 is called the 2-*Bol configuration.* Using the other two directions of axes, we obtain 1- and 3-Bol configurations. With these configurations at hand, we see that the net $\mathcal{N}$ is Moufang if and only if all its Bol configurations close (i.e., $R\sigma_\ell$ and $P\sigma_\ell$ are collinear). See [25, Sec. II.3] for more on closures of net configurations.

3 Composition algebras

The most famous nonassociative Moufang loop is the multiplicative loop of real octonions. Recall that octonions are built up from quaternions in a way analogous to the construction of quaternions from complex numbers, or complex numbers from real numbers. Following Springer and Veldkamp [22], we will imitate this procedure over any field. We then construct a countable family of finite simple Moufang loops, one for every finite field $GF(q)$.

Let F be a field and V a vector space over F. A map $N : V \to F$ is a *quadratic form* if $\langle\ ,\ \rangle : V\times V \to F$ defined by $\langle u, v\rangle = (u+v)N - uN - vN$ is a bilinear form, and if $(\lambda u)N = \lambda^2(uN)$ holds for every $u \in V$ and $\lambda \in F$.

When $f : V \times V \to F$ is a bilinear form, then u, $v \in V$ are *orthogonal* (with respect to f) if $(u, v)f = 0$. We write $u \perp v$. The *orthogonal complement* $W^\perp$ of a subspace $W \le V$ is the subspace $\{v \in V;\ v \perp w$ for every $w \in W\}$. The bilinear form f is said to be *non-degenerate* if $V^\perp = 0$. A quadratic form N is *non-degenerate* if the bilinear form $\langle\ ,\ \rangle$ associated with N is non-degenerate. When N is non-degenerate, the vector space V is said to be *nonsingular*. A subspace W of (V, N) is *totally isotropic* if $uN = 0$ for every $u \in W$. All maximal totally isotropic subspaces of (V, N) have the same dimension, called the *Witt index*. If N is non-degenerate and $\dim V \le \infty$ then the Witt index cannot exceed $\dim V/2$.

In this paper, an *algebra* over F is a vector space over F with bilinear multiplication. Specifically, we do not assume that multiplication in an algebra is associative.

A *composition algebra* $C = (C, N)$ over F is an algebra with a multiplicative neutral element e such that the quadratic form $N : C \to F$ is non-degenerate and

$$(uv)N = uNvN \tag{2}$$

holds for every u, $v \in C$. In this context, the quadratic form N is called a *norm*.

When $\langle\ ,\ \rangle$ is the bilinear form associated with the norm N, the *conjugate* of $x \in C$ is the element $\overline{x} = \langle x, e\rangle e - x$. Every element $x \in C$ satisfies

$$x^2 - \langle x, e\rangle x + (xN)e = 0$$

(cf. [22, Prop. 1.2.3]), and thus also $x\overline{x} = \overline{x}x = (xN)e$. In particular, the multiplicative inverse of x is $x^{-1} = (xN)^{-1}\overline{x}$, as long as $xN \ne 0$. Furthermore, $0 \ne x \in C$ is a zero divisor if and only if $xN = 0$.

3.1 The Cayley-Dickson process

Let $C = (C, N)$ be a composition algebra over F and $\lambda \in F^* = F \setminus \{0\}$. Define a new product on $D = C \times C$ by

$$(x,\, y)(u,\, v) = (xu + \lambda \overline{v} y,\, vx + y\overline{u}),$$

where x, y, u, v are elements of C. Also define the norm M on D by

$$(x,\, y)M = xN - \lambda(yN),$$

where x, $y \in C$. By [22, Prop. 1.5.3], if C is associative then $D = (D, M)$ is a composition algebra. Moreover, D is associative if and only if C is commutative and associative. The above procedure is known as the *Cayley-Dickson process.*

We would now like to construct all composition algebras by iterating the Cayley-Dickson process starting with F. However, there is a twist when F is of characteristic 2. Namely, when $\operatorname{char} F = 2$ then F is not a composition algebra since $\langle x, x\rangle = (x+x)N - xN - xN = 0$ for every $x \in F$, thus $\langle x, y\rangle = \langle x, \lambda x\rangle = \lambda\langle x, x\rangle = 0$ for every x, $y \in F$, and N is therefore degenerate. The situation looks as follows:

Theorem 3.1 (Thm. 1.6.2. [22]). *Every composition algebra over F is obtained by iterating the Cayley-Dickson process, starting from F if* $\operatorname{char} F$ *is not equal to* 2*, and from a* 2*-dimensional composition algebra when* $\operatorname{char} F$ *is equal to* 2*. The possible dimensions of a composition algebra are* 1*,* 2*,* 4 *and* 8*. Composition algebras of dimension* 1 *or* 2 *are commutative and associative, those of dimension* 4 *are associative but not commutative, and those of dimension* 8 *are neither commutative nor associative.*

A composition algebra of dimension 2 *over F is either a quadratic field extension of F or is isomorphic to $F \oplus F$.*

For a generalization of composition algebras into dimension 16 we refer the reader to [26].

3.2 Split octonion algebras

Composition algebras of dimension 8 are known as *octonion algebras.* Since there is a parameter λ in the Cayley-Dickson process, it is conceivable (and sometimes true) that there exist two octonion algebras over F that are not isomorphic.

A composition algebra (C, N) is called *split* if there is $0 \neq x \in C$ such that $xN = 0$. By [22, Thm. 1.8.1], over any field F there is exactly one split composition algebra in dimension 2, 4 and 8, up to isomorphism. As we have already noticed, split composition lgebras are precisely composition algebras with zero divisors. The unique split octonion algebra over F will be denoted by $\mathbb{O}(F)$. (It is worth mentioning that when F is finite then every octonion algebra over F is isomorphic to $\mathbb{O}(F)$, cf. [22, p. 22].)

All split octonion algebras $\mathbb{O}(F)$ were known already to Zorn, who constructed them using the *vector matrices*

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}, \tag{3}$$

where a, $b \in F$ and α, β are vectors in F^3. The norm N is given as the "determinant" $\det x = ab - \alpha \cdot \beta$, where $\alpha \cdot \beta$ is the usual dot product

$$(\alpha_1, \alpha_2, \alpha_3) \cdot (\beta_1, \beta_2, \beta_3) = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3.$$

The conjugate of x is

$$\overline{x} = \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}, \tag{4}$$

and two vector matrices are multiplied according to

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}, \tag{5}$$

where $\beta \times \delta$ is the usual vector product

$$(\beta_1, \beta_2, \beta_3) \times (\delta_1, \delta_2, \delta_3) = (\beta_2\delta_3 - \beta_3\delta_2,\ \beta_3\delta_1 - \beta_1\delta_3,\ \beta_1\delta_2 - \beta_2\delta_1).$$

The reader can think of this *Zorn vector algebra* anytime we speak of $\mathbb{O}(F)$.

It turns out that every composition algebra satisfies the *alternative laws*

$$(xy)x = x(yx), \quad x(xy) = x^2y, \quad (xy)y = xy^2.$$

This is an easy corollary of the (not so easy) fact that composition algebras satisfy the Moufang identities (1), cf. [22, Prop. 1.4.1].

4 A class of classical simple Moufang loops

4.1 Paige loops

Although the octonion algebra $\mathbb{O}(F)$ satisfies the Moufang identities, it is not a Moufang loop yet, since it is not even a quasigroup ($0 \cdot x = 0$

for every $x \in \mathbb{O}(F)$). Denote by $M(F)$ the subset of $\mathbb{O}(F)$ consisting of all elements of norm (determinant) 1. We have $\det x \det y = \det xy$ since $\mathbb{O}(F)$ is a composition algebra, which means that $M(F)$ is closed under multiplication. The neutral element of $M(F)$ is

$$e = \begin{pmatrix} 1 & (0,0,0) \\ (0,0,0) & 1 \end{pmatrix},$$

and the two-sided inverse of $x \in M(F)$ is $x^{-1} = \overline{x}$, where x is as in (3) and $\overline{x}$ is as in (4).

Let Z be the center of the Moufang loop $M(F)$. We have $Z = \{e\}$ when $\operatorname{char} F = 2$, and $Z = \{e, -e\}$ when $\operatorname{char} F \neq 2$. Denote by $M^*(F)$ the Moufang loop $M(F)/Z$.

Theorem 4.1 (Paige [23]). *Let F be a field and $M^*(F)$ the loop of Zorn vector matrices of norm one modulo the center, multiplied according to* (5)*. Then $M^*(F)$ is a nonassociative simple Moufang loop. When $F = GF(q)$ is finite, the order of $M^*(F)$ is $\frac{1}{d}q^3(q^4-1)$, where $d = (2, q-1)$.*

The noncommutative loops $M^*(F)$ of Theorem 4.1 are sometimes called *Paige loops.*

In the remaining part of this section, we investigate the multiplication groups of loops $M(F)$ and $M^*(F)$ constructed over an arbitrary field F.

4.2 Orthogonal groups

Let V be a vector space over F with a non-degenerate quadratic form $N : V \to F$. A linear transformation $f : V \to V$ is *orthogonal with respect to N* if it preserves N, i.e., if $(xf)N = xN$ for all $x \in V$. Then f preserves the associated bilinear form $\langle\ ,\ \rangle$ as well:

$$\begin{aligned} \langle xf, yf \rangle &= (xf + yf)N - (xf)N - (yf)N \\ &= (x + y)N - (x)N - (y)N \\ &= \langle x, y \rangle. \end{aligned}$$

The group consisting of all orthogonal transformations of (V, N) is known as the *orthogonal group* $O(V) = O(V, N)$. The determinant of an orthogonal transformation is ±1. Orthogonal transformations with determinant 1 form the *special orthogonal group* $SO(V)$. The elements of $SO(V)$ are called *rotations.* One usually denotes by $\Omega(V)$ the commutator subgroup $O'(V)$ of $O(V)$. By definition, every element of $\Omega(V)$ is a rotation, and we would like to see which rotations belong to $\Omega(V)$.

Take an element $g \in SO(V)$ and consider the map $1 - g : x \mapsto x - xg$. Define the bilinear form χ_g on $V(1-g)$ by $(u,v)\chi_g = \langle u, w\rangle$, where w is an arbitrary vector from V satisfying $w(1-g) = v$. Then χ_g is well-defined and non-degenerate, by [27, Thm. 11.32]. Recall that the *discriminant* $\mathrm{discr}(f)$ of a bilinear form f with respect to some basis is the determinant of its matrix. Whether or not the discriminant of χ_g is a square in F does not depend on the choice of the basis in $V(1-g)$. This property characterizes elements of $\Omega(V)$.

Lemma 4.2 (11.50 Thm. [27]). *The rotation $g \in SO(V)$ belongs to $\Omega(V)$ if and only if* $\mathrm{discr}(\chi_g) \in F^2$.

Pick any element $\sigma \in O(V)$ with $\sigma^2 = \mathrm{id}$. The two subspaces

$$\begin{aligned} U &= V(\sigma - 1) = \{x\sigma - x \mid x \in V\},\\ W &= V(\sigma + 1) = \{x\sigma + x \mid x \in V\} \end{aligned}$$

are orthogonal to each other. Indeed,

$$\langle x\sigma - x, y\sigma + y\rangle = \langle x\sigma, y\rangle - \langle x, y\sigma\rangle = \langle x\sigma, y\rangle - \langle x\sigma, y\sigma^2\rangle = 0.$$

The subspace W consists of vectors invariant under σ. If W is a non-singular hyperplane (that is, a subspace of dimension $\dim V - 1$) then σ is called a *symmetry with respect to W*. (If $\mathrm{char}(F) = 2$ then σ is usually called a *transvection*.) If σ is a symmetry with respect to W and $g \in O(V)$, the conjugate $\sigma^g = g^{-1}\sigma g$ is a symmetry with respect to Wg.

4.3 Multiplication groups of Paige loops

Let now $V = \mathbb{O}(F)$ be the split octonion algebra over F. We identify the vector matrix

$$x = \begin{pmatrix} x_0 & (x_1, x_2, x_3) \\ (x_4, x_5, x_6) & x_7 \end{pmatrix}$$

with the column vector $(x_0, \dots, x_7)^t$, and we use the canonical basis of F^8 as the basis of V. Since $\langle x, y\rangle = \det(x+y) - \det x - \det y = x_7y_0 - x_4y_1 - x_5y_2 - x_6y_3 - x_1y_4 - x_2y_5 - x_3y_6 + x_0y_7$, the bilinear from $\langle x, y\rangle$ can be expressed as x^tJy, where

$$J = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{6}$$

Recall that $M(F)$ consists of all elements of $\mathbb{O}(F)$ that are of norm 1.

Lemma 4.3. *For every $a \in M(F)$, we have $L_a, R_a \in \Omega(V)$.*

Proof. We only deal with the case L_a. Since $aN = 1$, we have $L_a \in O(V)$, by (2). Let $a = (a_0, \ldots, a_7)^t$ and write matrix maps to the left of their arguments. Then L_a can be identified with

$$\begin{pmatrix} a_0 & 0 & 0 & 0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & 0 & 0 & 0 & a_6 & -a_5 & a_1 \\ 0 & 0 & a_0 & 0 & -a_6 & 0 & a_4 & a_2 \\ 0 & 0 & 0 & a_0 & a_5 & -a_4 & 0 & a_3 \\ a_4 & 0 & -a_3 & a_2 & a_7 & 0 & 0 & 0 \\ a_5 & a_3 & 0 & -a_1 & 0 & a_7 & 0 & 0 \\ a_6 & -a_2 & a_1 & 0 & 0 & 0 & a_7 & 0 \\ 0 & a_4 & a_5 & a_6 & 0 & 0 & 0 & a_7 \end{pmatrix}.$$

Routine calculation yields $\det(L_a) = (aN)^4$, and $L_a \in SO(V)$ follows. By Lemma 4.2, it suffices to show $\operatorname{discr}(\chi_{L_a}) \in F^2$.

Assume first that $(e-a)N \neq 0$. Then $V(1-L_a) = V(e-a) = V$, and $((e-a)^{-1}v)(1-L_a) = v$ for every $v \in V$. Thus $(u,v)\chi_{La} = \langle u, vL_{e-a}^{-1}\rangle$, and the matrix of χ_{L_a} is JL_{e-a}^{-1}, where J is as in (6). Therefore $\operatorname{discr}(\chi_{L_a}) = \det(J)\det(L_{e-a})^{-1} = ((e-a)N)^{-4} \in F^2$.

Suppose now $(e-a)N = 0$ and exclude the trivial case $e-a \in F$. Define the elements

$$e_0 = \begin{pmatrix} 1 & (0,0,0) \\ (0,0,0) & 0 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 & (1,0,0) \\ (0,0,0) & 0 \end{pmatrix},$$
$$e_2 = \begin{pmatrix} 0 & (0,1,0) \\ (0,0,0) & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 & (0,0,1) \\ (0,0,0) & 0 \end{pmatrix}$$

and

$$f_0 = (e-a)e_0 = \begin{pmatrix} 1-a_0 & (0,0,0) \\ (-a_4,-a_5,-a_6) & 0 \end{pmatrix},$$
$$f_1 = (e-a)e_1 = \begin{pmatrix} 0 & (1-a_0,0,0) \\ (0,-a_3,a_2) & -a_4 \end{pmatrix},$$
$$f_2 = (e-a)e_2 = \begin{pmatrix} 0 & (0,1-a_0,0) \\ (a_3,0,-a_1) & -a_5 \end{pmatrix},$$
$$f_3 = (e-a)e_3 = \begin{pmatrix} 0 & (0,0,1-a_0) \\ (-a_2,a_1,0) & -a_6 \end{pmatrix}.$$

The vectors e_i span a totally isotropic subspace of V and $f_i \in (e-a)V$. Since $\langle (e-a)x, (e-a)y\rangle = (e-a)N\langle x,y\rangle = 0$, $(e-a)V$ is totally isotropic as well. In particular, $\dim((e-a)V) \leqslant 4$.

Assume $a_0 \neq 1$. Then, the vectors f_i are linearly independent and hence form a basis of $(e-a)V$. The matrix $M=(m_{ij})$ of χ_{L_a} with respect to the basis $\{f_0,\, f_1,\, f_2,\, f_3\}$ satisfies $m_{ij} = (f_i,f_j)\chi_{L_a} = \langle f_i, e_j\rangle$, which yields

$$M = \begin{pmatrix} 0 & a_4 & a_5 & a_6 \\ -a_4 & 0 & a_3 & -a_2 \\ -a_5 & -a_3 & 0 & a_1 \\ -a_6 & a_2 & -a_1 & 0 \end{pmatrix},$$

by calculation. Then $\mathrm{discr}(\chi_{L_a}) = \det M = (a_1a_4 + a_2a_5 + a_3a_6)^2 \in F^2$.

The special case $a_0 = 1$ can be calculated similarly. □

For the rest of this section, let ι denote the conjugation map $x \mapsto \overline{x}$. Note that $\iota \in O(V)$ and $e\iota = e$.

Lemma 4.4. *Any element $g \in O(V)$ with $eg = e$ commutes with ι.*

Proof. We have $\overline{x}g = (\langle x,e\rangle e - x)g = \langle x,e\rangle eg - xg = \langle xg, eg\rangle eg - xg = \langle xg, e\rangle e - xg = \overline{xg}$. □

Lemma 4.5. *For an arbitrary element $g \in O(V)$, we define $\iota^g = g^{-1}\iota g$. Put $a = eg$. Then $aN = 1$ and $x\iota^g = a\overline{x}a$ holds for all $x \in V$.*

Proof. On the one hand, $aN = (eg)N = eN = 1$, therefore $a\overline{a} = e$ and $a^{-1} = \overline{a}$. On the other hand, $g = hL_a$ for some h with $eh = e$. By the previous lemma, $\iota^g = L_a^{-1}\iota L_a$ and $x\iota^g = ((xL_a^{-1})\iota)L_a = a(\overline{a^{-1}x}) = a\overline{x}a$. □

The map $-\iota : x \mapsto -\bar{x}$ is a symmetry with respect to the 7-dimensional nonsingular hyperplane

$$H = \left\{ \left(\begin{array}{cc} x_0 & (x_1, x_2, x_3) \\ (x_4, x_5, x_6) & -x_0 \end{array} \right) \middle| \; x_i \in F \right\}.$$

The conjugate $-\iota^g$ is a symmetry with respect to Hg. This means that

$$\mathcal{C} = \{-\iota^g \mid g \in O(V)\} = \{-L_a^{-1} \iota L_a \mid a \in M(F)\}$$

is a complete conjugacy class consisting of symmetries.

Theorem 4.6. *The multiplication group of $M(F)$ is $\Omega(\mathbb{O}(F), N)$.*

Proof. By Lemma 4.3, $\mathrm{Mlt}(M(F)) \leqslant \Omega(V)$. We have $(ax)\iota = x\iota\,\bar{a}$, which implies

$$\iota\iota^g = \iota L_a^{-1} \iota L_a = R_a L_a$$

and

$$\iota^g \iota^h = (\iota\iota^g)^{-1}(\iota\iota^h) = (R_a L_a)^{-1}(R_b L_b) \in \mathrm{Mlt}(M(F))$$

for $g, h \in O(V)$. Let us denote by $\mathcal{D}$ the set consisting of $\iota^g\iota^h$, $g, h \in O(V)$. $\mathcal{D}$ is clearly an invariant subset of $O(V)$. By [1, Thm. 5.27], $\mathcal{D}$ generates $\Omega(V)$, which proves $\mathrm{Mlt}(M(F)) = \Omega(\mathbb{O}(F), N)$. □

Finally, we determine the multiplication groups of Paige loops.

Corollary 4.7. *The multiplication group of the Paige loop $M^*(F)$ is the simple group $P\Omega(\mathbb{O}(F), N) = P\Omega_8^+(F)$.*

Proof. The surjective homomorphism $\varphi : M(F) \to M^*(F)$, $x \mapsto \pm x$ induces a surjective homomorphism $\Phi : \mathrm{Mlt}(M(F)) \to \mathrm{Mlt}(M^*(F))$. On the one hand, the kernel of Φ contains $\pm\mathrm{id}$. On the other hand $P\Omega(V) = \Omega(V)/\{\pm\mathrm{id}\}$ is a simple group, cf. [1, Thm. 5.27]. Since $\mathrm{Mlt}(M^*(F))$ is not trivial, we must have $\mathrm{Mlt}(M^*(F)) = P\Omega(V)$. Finally, the norm N has maximal Witt index 4, therefore the notation $P\Omega_8^+(F)$ is justified. □

Remark 4.8. The result of Theorem 4.6 is *folklore,* that is, most of the authors (Freudenthal, Doro, Liebeck, etc.) use it as a *well-known* fact without making a reference. The authors of the present paper are not aware of any reference, however, especially one that would handle all fields at once.

5 Groups with triality

5.1 Triality

Let G be a group. We use the usual notation $x^y = y^{-1}xy$ and $[x,y] = x^{-1}y^{-1}xy = x^{-1}x^y$ for x, $y \in G$. Let α be an automorphism of G, then $x\alpha$ will be denoted by x^α as well, and $[x,\alpha]$ will stand for $x^{-1}x^\alpha$. The element $\alpha^y \in \operatorname{Aut} G$ maps x to $x^{y^{-1}\alpha y} = ((x^{y^{-1}})^\alpha)^y$.

Let S_n be the symmetric group on $\{1,\dots,n\}$. $G \times H$ and $G \rtimes H$ will stand for the direct and semidirect product of G and H, respectively. In the latter case, H acts on G.

We have the following definition due to Doro [10].

Definition 5.1. The pair (G,S) is called a *group with triality*, if G is a group, $S \leqslant \operatorname{Aut} G$, $S = \langle \sigma, \rho \mid \sigma^2 = \rho^3 = (\sigma\rho)^2 = 1\rangle \cong S_3$, and for all $g \in G$ the *triality identity*

$$[g,\sigma]\,[g,\sigma]^\rho\,[g,\sigma]^{\rho^2} = 1$$

holds.

The principle of triality was introduced by Cartan [6] in 1938 as a property of orthogonal groups in dimension 8, and his examples motivated Tits [28]. Doro was the first one to define the concept of an abstract group with triality, away from any context of a given geometric or algebraic object.

Definition 5.2. Let $(G_i, \langle \sigma_i, \rho_i\rangle)$, $i = 1,2$ be groups with triality. The homomorphism $\varphi : G_1 \to G_2$ is an *S-homomorphism* if $g\sigma_1\varphi = g\varphi\sigma_2$ and $g\rho_1\varphi = g\varphi\rho_2$ hold for all $g \in G_1$. The kernel of an S-homomorphism is an S-invariant normal subgroup. The group with triality G is said to be *S-simple* if it has no proper S-invariant normal subgroups.

The following examples of groups with triality are of fundamental importance. They are adopted from Doro [10].

Example 5.3. Let A be a group, $G = A^3$, and let σ, $\rho \in \operatorname{Aut} G$ be defined by $\sigma : (a_1,a_2,a_3) \mapsto (a_2,a_1,a_3)$ and $\rho : (a_1,a_2,a_3) \mapsto (a_2,a_3,a_1)$. Then G is a group with triality with respect to $S = \langle \sigma, \rho\rangle$.

Example 5.4. Let A be a group with $\varphi \in \operatorname{Aut} A$, $\varphi \neq \mathrm{id}_A$, satisfying $x\,x^\varphi\,x^{\varphi^2} = 1$ for all $x \in A$. Put $G = A \times A$, $\sigma : (a_1,a_2) \mapsto (a_2,a_1)$ and $\rho : (a_1,a_2) \mapsto (a_1^\varphi, a_2^{\varphi^{-1}})$. Then G is a group with triality with respect to $S = \langle \sigma, \rho\rangle$.

If A is of exponent 3 and $\varphi = \mathrm{id}_A$ then G is a group with triality in a wider sense, meaning that the triality identity is satisfied but S is not isomorphic to S_3.

Example 5.5. Let V be a two-dimensional vector space over a field of characteristic different from 3. Let S be the linear group generated by the matrices

$$\rho = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then the additive group of V and S form a group with triality.

Remark 5.6. If A is a simple group then the constructions in Examples 5.3 and 5.4 yield S-simple groups with triality. Obviously, if (G, S) is a group with triality and G is simple (as a group) then (G, S) is S-simple. Below, we are concerned with the converse of this statement.

5.2 Triality of Moufang nets

In the following, (G, S) stands for a group G with automorphism group S isomorphic to S_3. Let $\sigma,\ \rho \in S$ be such that $\sigma^2 = \rho^3 = \mathrm{id}$. Let the three involutions of S be $\sigma_1 = \sigma$, $\sigma_2 = \sigma\rho$ and $\sigma_3 = \rho\sigma = \sigma\rho^2$. Finally, the conjugacy class σ_i^G will be denoted by $\mathcal{C}_i$.

The following lemma gives a more conceptual reformulation of Doro's triality. (It is similar to Lemma 3.2 of [17], attributed by Liebeck to Richard Parker.)

Lemma 5.7. *The pair (G, S) is a group with triality if and only if $(\tau_i\tau_j)^3 = \mathrm{id}$ for every $\tau_i \in \mathcal{C}_i$, $\tau_j \in \mathcal{C}_j$, where $i,\ j \in \{1,\ 2,\ 3\}$ and $i \neq j$. In this case, $(G, \langle \tau_i, \tau_j \rangle)$ is a group with triality as well.*

Proof. The condition of the first statement claims something about the conjugacy classes $\mathcal{C}_i$, which do not change if we replace S by $\langle \tau_i, \tau_j \rangle$. This means that the first statement implies the second one.

For the first statement, it suffices to investigate the case $i = 1$, $j = 3$, $\tau_1 = \sigma^g$ and $\tau_3 = \sigma\rho^2$, with arbitrary $g \in G$. Then the following equations are equivalent for every $g \in G$:

$$\begin{aligned}
1 &= (\sigma^g(\sigma\rho^2))^3, \\
1 &= \sigma^g(\sigma\rho^2) \cdot \sigma^g(\sigma\rho^2) \cdot \sigma^g(\sigma\rho^2), \\
1 &= [g, \sigma]\rho^2 \cdot [g, \sigma]\rho^2 \cdot [g, \sigma]\rho^2, \\
1 &= [g, \sigma] \cdot \rho^{-1}[g, \sigma]\rho \cdot \rho[g, \sigma]\rho^2, \\
1 &= [g, \sigma]\, [g, \sigma]^{\rho}\, [g, \sigma]^{\rho^2}.
\end{aligned}$$

This finishes the proof. □

The next lemma already foreshadows the relation between Moufang 3-nets and groups with triality.

Lemma 5.8. *Let P be a point of the Moufang 3-net $\mathcal{N}$. Denote by ℓ_1, ℓ_2 and ℓ_3 the three lines through P with corresponding Bol reflections σ_1, σ_2, σ_3. Then the collineation group $S = \langle \sigma_1, \sigma_2, \sigma_3 \rangle \cong S_3$ acts faithfully on the set $\{\ell_1, \ell_2, \ell_3\}$. This action is equivalent to the induced action of S on the parallel classes of $\mathcal{N}$.*

Proof. As we have demonstrated in Section 2, the conjugate of a Bol reflection is a Bol reflection. Thus $\sigma_1\sigma_2\sigma_1 = \sigma_3 = \sigma_2\sigma_1\sigma_2$, which proves the first statement. The rest is trivial. □

Using these lemmas, we can prove two key propositions.

Proposition 5.9. *Let $\mathcal{N}$ be a Moufang 3-net and let M be the group of collineations generated by all Bol reflections of $\mathcal{N}$. Let $M_0 \leqslant M$ be the direction preserving subgroup of M. Let us fix an arbitrary point P of $\mathcal{N}$ and denote by S the group generated by the Bol reflections with axes through P. Then $M_0 \lhd M$, $M = M_0S$, and the pair (M_0, S) is a group with triality.*

Proof. $M_0 \lhd M = M_0S$ is obvious. Thus S is a group of automorphism of M_0 by conjugation. By Lemma 5.7, it is sufficient to show $\langle \sigma_i^g, \sigma_j^h \rangle \cong S_3$ for all g, $h \in M_0$, where σ_i and σ_j are the reflections on two different lines through P. Since g, h preserve directions, the axes of σ_i^g and σ_j^h intersect in some point P'. Hence $\langle \sigma_1^g, \sigma_2^h \rangle \cong S_3$, by Lemma 5.8. □

The converse of the proposition is true as well.

Proposition 5.10. *Let (G, S) be a group with triality. The following construction determines a Moufang 3-net $\mathcal{N}(G, S)$. Let the three line classes be the conjugacy classes $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$. By definition, three mutually non-parallel lines $\tau_i \in \mathcal{C}_i$ $(i = 1, 2, 3)$ intersect in a common point if and only if*

$$\langle \tau_1, \tau_2, \tau_3 \rangle \cong S_3.$$

Moreover, if $G_1 = [G, S]S = \langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$, then the group $M(\mathcal{N})$ generated by the Bol reflections of $\mathcal{N}$ is isomorphic to $G_1/Z(G_1)$.

Proof. By definition, parallel lines do not intersect. When formulating the triality identity as in Lemma 5.7, we see that two non-parallel lines have a point in common such that there is precisely one line from the third parallel class incident with this point. This shows that $\mathcal{N}(G,S)$ is a 3-net indeed.

The Moufang property follows from the construction immediately, since one can naturally associate an involutorial collineation to any line $\tau_i \in \mathcal{C}_i$, namely the one induced by τ_i on G. This induced map $\bar{\tau}_i$ interchanges the two other parallel classes $\mathcal{C}_j$, $\mathcal{C}_k$ and fixes the points on its axis, that is, it normalizes the S_3 subgroups containing τ_i.

Finally, since a Bol reflection acts on the line set in the same way that the associated $\mathcal{C}_i$-element acts on the set $\cup\mathcal{C}_j$ by conjugation, we have the isomorphism $M(\mathcal{N}) \cong G_1/Z(G_1)$. □

Remark 5.11. From the point of view of dual 3-nets, the point set is the union of the three classes $\mathcal{C}_i$, and lines consist of the intersections of an S_3 subgroup with each of the three classes.

Remark 5.12. One finds another construction of groups with triality using the geometry of the associated 3-net in P. O. Mikheev's paper [18]. A different approach to groups with triality is given in J. D. Phillips' paper [24].

5.3 Triality collineations in coordinates

At this point, we find it useful to write down the above maps in the coordinate system of the 3-net. If we denote by $\sigma_m^{(v)}, \sigma_m^{(h)}, \sigma_m^{(t)}$ the Bol reflections with axes $X = m$, $Y = m$, $XY = m$, respectively, then we have

$$\begin{aligned}
\sigma_m^{(v)} &: (x,y) \mapsto (m(x^{-1}m), m^{-1}(xy)),\\
\sigma_m^{(h)} &: (x,y) \mapsto ((xy)m^{-1}, (my^{-1})m),\\
\sigma_m^{(t)} &: (x,y) \mapsto (my^{-1}, x^{-1}m).
\end{aligned}$$

This yields

$$\begin{aligned}
\sigma_m^{(v)}\sigma_1^{(v)} &: (x,y) \mapsto (m^{-1}(xm^{-1}), my),\\
\sigma_m^{(h)}\sigma_1^{(h)} &: (x,y) \mapsto (xm, (m^{-1}y)m^{-1}),\\
\sigma_{m^{-1}}^{(t)}\sigma_1^{(t)} &: (x,y) \mapsto (mx, ym).
\end{aligned}$$

These are direction preserving collineations generating G.

They can be written in the form $\sigma_m^{(v)}\sigma_1^{(v)} = (L_m^{-1}R_m^{-1}, L_m)$, $\sigma_m^{(h)}\sigma_1^{(h)} = (R_m, L_m^{-1}R_m^{-1})$ and $\sigma_m^{(t)}\sigma_1^{(t)} = (L_m, R_m)$ as well. The associated autotopisms are

$$(L_m^{-1}R_m^{-1}, L_m, L_m^{-1}), \quad (R_m, L_m^{-1}R_m^{-1}, R_m^{-1}), \quad (L_m, R_m, L_mR_m),$$

respectively. By the way, the fact that these triples are autotopisms is equivalent with the Moufang identities (1).

6 The classification of nonassociative finite simple Moufang loops

6.1 Simple 3-nets

The classification of finite simple Moufang loops is based on the classification of finite simple groups with triality. Using the results of the previous section, the classification can be done in the following steps.

Proposition 6.1. *Let $\varphi : \mathcal{N}_1 \to \mathcal{N}_2$ be a map between two 3-nets that preserves incidence and directions.*

(i) Suppose that $\varphi(P_1) = P_2$ holds for the points $P_1 \in \mathcal{N}_1$, $P_2 \in \mathcal{N}_2$. Then φ defines a homomorphism $\bar{\varphi} : L_1 \to L_2$ in a natural way, where L_i is the coordinate loop of the 3-net $\mathcal{N}_i$ with origin P_i. Conversely, the loop homomorphism $\bar{\varphi} : L_1 \to L_2$ uniquely determines a collineation $\mathcal{N}_1 \to \mathcal{N}_2$, namely φ.

(ii) Suppose that the 3-nets $\mathcal{N}_i$ $(i = 1, 2)$ are Moufang and φ is a collineation onto. Let us denote by (M_i, S) the group with triality that corresponds to the 3-net $\mathcal{N}_i$. Then the maps $\sigma_\ell \mapsto \sigma_{\ell\varphi}$ induce a surjective S-homomorphism $\tilde{\varphi} : M_1 \to M_2$, where σ_ℓ is the Bol reflection in $\mathcal{N}_1$ with axis ℓ. Conversely, an S-homomorphism $M_1 \to M_2$ defines a direction preserving collineation between the 3-nets $\mathcal{N}(M_1, S)$ and $\mathcal{N}(M_2, S)$.

Proof. The first part of statement (i) follows from the geometric definition of the loop operation in a coordinate loop; the second part is trivial. For the (ii) statement, it is sufficient to see that a relation of the reflections σ_ℓ corresponds to a point-line configuration of the 3-net, and that the φ-image of the configuration induces the same relation on the reflections $\sigma_{\varphi(\ell)}$. The converse follows from Proposition 5.10. □

In the sense of the proposition above, we can speak of *simple* 3-*nets*, that is, of 3-nets having only trivial homomorphisms. The next proposition follows immediately.

Proposition 6.2. *If L is a simple Moufang loop, then the associated* 3*-net $\mathcal{N}$ is simple as well. That is, the group (M_0, S) with triality determined by $\mathcal{N}$ is S-simple.*

6.2 S-simple groups with triality

The structure of S-simple groups with triality is rather transparent. It is clear that G is S-simple if and only if it has no S-invariant proper nontrivial normal subgroups.

Let G be such a group and let $N \lhd G$ be an arbitrary proper normal subgroup of G. Let us denote by N_i the images of N under the elements of S, $i = 1, \dots, 6$.

Since the union and the intersection of the groups N_i is an S-invariant normal subgroup of G, we have $G = N_1 \cdots N_6$ and $\{1\} = N_1 \cap \ldots \cap N_6$. If $N_i \cap N_j$ is a proper subgroup of N_i for some i, $j = 1, \dots, 6$, then we replace N_i by $N_i \cap N_j$. We can therefore assume that the groups N_i intersect pairwise trivially. Since S acts transitively on the groups N_i, one of the following cases must occur:

Case A. G is a simple group. In this case, there is no proper normal subgroup N.

Case B. The number of distinct groups N_i is 2. Then $N = N^\rho$, $M = N^\sigma$, $G = NM$, $N \cap M = \{1\}$ and elements of N and M commute. Every element $g \in G$ can be written as $g = ab^\sigma$. ρ induces an automorphism φ on N. Then, $g^\sigma = a^\sigma b = ba^\sigma$ and $g^\rho = a^\rho b^{\sigma\rho} = a^\rho b^{\rho^{-1}\sigma} = a^\varphi b^{\varphi^{-1}\sigma}$.

Moreover, applying the triality identity on $a \in N$, we obtain

$$(a^{\varphi^2} a^\varphi a)^{-1} (a a^\varphi a^{\varphi^2})^\sigma = 1,$$

which is equivalent with the identity $a a^\varphi a^{\varphi^2} = 1$. This means that the map $N \times N \to G$, $(a, b) \mapsto ab^\sigma$ defines an S-isomorphism between G and the construction in Example 5.4.

However, a result of Khukhro claims that the existence of the automorphism φ of N implies that N is nilpotent of class at most 3 (see [16, p. 223], [20, Thm. 3.3]). Therefore, no S-simple group with triality can be constructed in this case.

Case C. The number of distinct groups N_i is 3: $N = N_1$, $N^\rho = N_2$, $N^{\rho^2} = N_3$. We can assume $N_1^\sigma = N_1$ and $N_2^\sigma = N_3$.

Case C/1. Assume that $M = N_1 \cap (N_2N_3)$ is a proper subgroup of N_1. Then $M^\rho \in N_1^\rho = N_2 \subseteq N_2N_3$, similarly $M^{\rho^2} \in N_2N_3$. Moreover, $M^\sigma = N_1^\sigma \cap (N_2^\sigma N_2^\sigma) = M$. Hence, $MM^\rho M^{\rho^2}$ is a proper S-invariant normal subgroup of G, a contradiction.

Case C/2. Assume $N_1 \cap (N_2N_3) = \{1\}$. Then $G = N_1 \times N_2 \times N_3 \cong N^3$. By the triality identity, we have $a^{-1}a^\sigma \in N_1 \cap (N_2N_3)$ for any $a \in N_1$, thus, $a^\sigma = a$. Consider the map $\Phi : N^3 \to G$, $\Phi(a, b, c) = ab^\rho c^{\rho^2}$. By

$$(ab^\rho c^{\rho^2})^\sigma = ac^\rho b^{\rho^2} \qquad \text{and} \qquad (ab^\rho c^{\rho^2})^\rho = ca^\rho b^{\rho^2},$$

Φ defines an S-isomorphism between G and the group with triality in Example 5.3.

Case C/3. Assume $N_1 \subseteq N_2N_3$, G noncommutative. We have $G = N_1 \times N_2 \cong N^2$. Since G is S-simple, we must have $Z(G) = \{1\}$ and $Z(N) = \{1\}$. Let us assume that $a^\rho = a_1a_2$ with $1 \neq a_1 \in N_1$, $a_2 \in N_2$ for some element $a \in N_1 = N$. Take $b \in N$ with $a_1b \neq ba_1$. Every element of N_1 commutes with every element of N_2. This implies

$$1 \neq [a_1a_2, b] = [a^\rho, b] \in N \cap N^\rho,$$

a contradiction.

Case C/4. If G is commutative and S-simple, then we are in the situation of Example 5.5. The proof is left to the reader.

We summarize these results in the following proposition. In the finite case the result was proved by S. Doro [10]. In the infinite case, it is due to G. P. Nagy and M. Valsecchi [20].

Proposition 6.3. *Let G be a noncommutative S-simple group with triality. Then either G is simple or $G = A \times A \times A$, where A is a simple group and the triality automorphisms satisfy $(a, b, c)^\rho = (c, a, b)$, $(a, b, c)^\sigma = (a, c, b)$.*

6.3 The classification

Lemma 6.4. *Let $G = A \times A \times A$ be an S-simple group with triality. Then the associated loop is isomorphic to the group A.*

Proof. We leave to the reader to check that an associative simple Moufang loop A has $G = A \times A \times A$ as a group with triality. Since the group with triality determines the 3-net uniquely, and since groups are G-loops, that is, the coordinate loop does not depend on the choice of the origin, we are done. □

Also the following result is due to Doro, but the way of proving is based on the geometric approach, hence new.

Lemma 6.5 (Doro). *Assume that G is a group with triality such that ρ is an inner automorphism. Then the associated Moufang loop has exponent* 3.

Proof. Let ρ be an inner automorphism of G. We assume G to be a group of direction preserving collineations of the 3-net $\mathcal{N}$ associated with L. We consider ρ as a collineation of $\mathcal{N}$ permuting the directions cyclicly. We denote by Γ^+ the collineation group of $\mathcal{N}$ generated by G and ρ. Γ^+ consists of collineations which induce an even permutation on the set of directions.

Let $\alpha \in G$ be a direction preserving collineation which induces ρ on G and put $r = \alpha^{-1}\rho$. Obviously, $\Gamma^+ = \langle G, r\rangle$, hence $r \in Z(\Gamma^+)$. Moreover, since Γ^+ is invariant under σ, we have $r^\sigma \in Z(\Gamma^+)$.

Let τ be a Bol reflection whose axis is parallel to the axis of σ. On the one hand, $\sigma\tau \in G$ and

$$\sigma\tau = r^{-1}\sigma\tau r = (\sigma^r\sigma)(\sigma\tau^r)$$

holds. On the other hand, $\sigma^r\sigma = r^{-1}r^\sigma \in Z(\Gamma^+)$ and $\sigma\tau^r \in \Gamma^+$. Therefore,

$$(\sigma\tau)^3 = (\sigma^r\sigma)^3\,(\sigma\tau^r)^3 = \mathrm{id}$$

by the modified triality property, cf. Lemma 5.7.

Assume now that the axis of the Bol reflections σ and τ are vertical with equation $X = e$ and $X = a$. As we have seen in Section 5.3, the coordinate forms of these maps are $(x, y)\sigma = (x^{-1}, xy)$ and $(x, y)\tau = (ax^{-1}a, a^{-1}(xy))$. This implies $(x, y)\sigma\tau = (axa, a^{-1}y)$ and $(x, y)(\sigma\tau)^3 = (a^3xa^3, a^{-3}y)$. By $(\sigma\tau)^3 = \mathrm{id}$, we have $a^3 = 1$. Since we chose τ arbitrarily, L must be of exponent 3. □

Corollary 6.6. *If G is a finite group with triality which determines a noncommutative simple Moufang loop then all triality automorphisms are outer.*

Proof. Assume that σ is an inner automorphism. Then so are σ^ρ and $\rho = \sigma^\rho\sigma$. We have the same implication if we suppose $\sigma\rho$ or $\rho\sigma$ to be inner. In any case, ρ will be inner and L will be a finite Moufang loop of exponent 3. By [13, Thm. 4], L is either not simple or commutative. □

Theorem 6.7 (Liebeck's Theorem [17]). *The only finite simple groups with triality are the simple groups $(P\Omega_8^+(q), S)$. The triality automorphisms are uniquely determined up to conjugation. (They are the so called graph automorphisms of $P\Omega_8^+(q)$.)*

Corollary 6.8 (Thm. [17]). *The only nonassociative finite simple Moufang loops are the Paige loops $M^*(q) = M^*(GF(q))$, where q is a prime power.*

7 Automorphism groups of Paige loops over perfect fields

Now that we have found all nonassociative finite simple Moufang loops, we will determine their automorphism groups. In fact, we will determine $\operatorname{Aut} M^*(F)$ whenever F is perfect. Recall that a field of characteristic p is *perfect* if the Frobenius map $x \mapsto x^p$ is an automorphism of F. The approach here is based on [21].

7.1 The automorphisms of the split octonion algebras

Let C be a composition algebra over F. A map $\alpha : C \to C$ is a *linear automorphism* (resp. *semilinear automorphism*) of C if it is a bijective F-linear (resp. F-semilinear) map preserving the multiplication, i.e., satisfying $(uv)\alpha = (u\alpha)(v\alpha)$ for every u, $v \in C$. It is well known that the group of linear automorphisms of $\mathbb{O}(F)$ is isomorphic to the Chevalley group $G_2(F)$, cf. [11, Sec. 3], [22, Ch. 2]. The group of semilinear automorphisms of $\mathbb{O}(F)$ is therefore isomorphic to $G_2(F) \rtimes \operatorname{Aut} F$.

Since every linear automorphism of a composition algebra is an isometry [22, Sec. 1.7], it induces an automorphism on the loops $M(F)$ and $M^*(F)$. The following result—that is interesting in its own right—shows that every element of $\mathbb{O}(F)$ is a sum of two elements of norm one. Consequently, $\operatorname{Aut} \mathbb{O}(F) \le \operatorname{Aut} M^*(F)$.

Theorem 7.1 (Thm. 3.3 [29]). *Let F be any field and $\mathbb{O}(F)$ the split octonion algebra over F. Then every element of $\mathbb{O}(F)$ is a sum of two elements of norm one.*

Proof. As before, we identify $\mathbb{O}(F)$ with the Zorn vector matrix algebra over F, where the norm is given by the determinant. Let

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$$

be an element of $\mathbb{O}(F)$. First assume that $\beta \neq 0$. Note that for every $\lambda \in F$ there is $\gamma \in F^3$ such that $\gamma \cdot \beta = \lambda$. Pick $\gamma \in F^3$ so that $\gamma \cdot \beta = a + b - ab + \alpha \cdot \beta$. Then choose $\delta \in \gamma^\perp \cap \alpha^\perp \neq 0$. This choice guarantees that $(a-1)(b-1)-(\alpha-\gamma)\cdot(\beta-\delta) = ab-a-b+1-\alpha\cdot\beta+\gamma\cdot\beta = 1$. Thus

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = \begin{pmatrix} 1 & \gamma \\ \delta & 1 \end{pmatrix} + \begin{pmatrix} a-1 & \alpha-\gamma \\ \beta-\delta & b-1 \end{pmatrix}$$

is the desired decomposition of x into a sum of two elements of norm 1. Note that the above procedure works for every α.

Now assume that $\beta = 0$. If $\alpha \neq 0$, we use a symmetrical argument as before to decompose x. It remains to discuss the case when $\alpha = \beta = 0$. Then the equality

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & (1,0,0) \\ (-1,0,0) & 0 \end{pmatrix} + \begin{pmatrix} 0 & (-1,0,0) \\ (1,0,0) & b \end{pmatrix}$$

does the job. □

An automorphism $f \in \operatorname{Aut} M^*(F)$ will be called *(semi)linear* if it is induced by a (semi)linear automorphism of $\mathbb{O}(F)$.

7.2 Geometric description of loop automorphisms

By considering extensions of automorphisms of $M^*(F)$, it was proved in [29] that $\operatorname{Aut} M^*(2)$ is isomorphic to $G_2(2)$. The aim of this section is to generalize this result (although using different techniques) and prove that every automorphism of $\operatorname{Aut} M^*(F)$ is semilinear, provided F is perfect. We reach this aim by identifying $\operatorname{Aut} M^*(F)$ with a certain subgroup of the automorphism group of the group with triality associated with $M^*(F)$.

To begin with, we recall the geometrical characterization of automorphisms of a loop, as promised in Subsection 2.3.

Lemma 7.2 (Thm. 10.2 [3]). *Let L be a loop and $\mathcal{N}$ its associated 3-net. Any direction preserving collineation which fixes the origin of $\mathcal{N}$ is of the form $(x, y) \mapsto (x\alpha, y\alpha)$ for some $\alpha \in \operatorname{Aut} L$. Conversely, the map $\alpha : L \to L$ is an automorphism of L if and only if $(x, y) \mapsto (x\alpha, y\alpha)$ is a direction preserving collineation of $\mathcal{N}$.*

We will denote the map $(x, y) \mapsto (x\alpha, y\alpha)$ by φ_α. Before reading any further, recall Propositions 5.9 and 5.10.

Proposition 7.3. *Let L be a Moufang loop and $\mathcal{N}$ its associated 3-net. Let M be the group of collineations generated by the Bol reflections of $\mathcal{N}$, M_0 the direction preserving part of M, and $S \cong S_3$ the group generated by the Bol reflections whose axis contains the origin of $\mathcal{N}$. Then $\operatorname{Aut} L \cong C_{\operatorname{Aut} M_0}(S)$.*

Proof. As the set of Bol reflections of $\mathcal{N}$ is invariant under conjugations by collineations, every element $\varphi \in \operatorname{Coll}\mathcal{N}$ normalizes the group M_0 and induces an automorphism $\widehat{\varphi}$ of M. It is not difficult to see that φ fixes the three lines through the origin of $\mathcal{N}$ if and only if $\widehat{\varphi}$ centralizes (the involutions of) S.

Pick $\alpha \in \operatorname{Aut} L$, and let $\widehat{\varphi_\alpha}$ be the automorphism of M_0 induced by the collineation φ_α. As φ_α fixes the three lines through the origin, $\widehat{\varphi_\alpha}$ belongs to $C_{\operatorname{Aut} M_0}(S)$, by the first paragraph.

Conversely, an element $\psi \in C_{\operatorname{Aut} M_0}(S)$ normalizes the conjugacy class of σ in M_0S and preserves the incidence structure defined by the embedding of $\mathcal{N}$. This means that $\psi = \widehat{\varphi}$ for some collineation $\varphi \in \operatorname{Coll}\mathcal{N}$. Now, ψ centralizes S, therefore φ fixes the three lines through the origin. Thus φ must be direction preserving, and there is $\alpha \in \operatorname{Aut} L$ such that $\varphi = \varphi_\alpha$, by Lemma 7.2. □

7.3 The automorphisms of Paige loops

Theorem 7.4. *Let F be a perfect field. Then the automorphism group of the nonassociative simple Moufang loop $M^*(F)$ constructed over F is isomorphic to the semidirect product $G_2(F) \rtimes \operatorname{Aut} F$. Every automorphism of $M^*(F)$ is induced by a semilinear automorphism of the split octonion algebra $\mathbb{O}(F)$.*

Proof. We fix a perfect field F, and assume that all simple Moufang loops and Lie groups mentioned below are constructed over F.

The group with triality associated with M^* is the multiplicative group $\operatorname{Mlt} M^* \cong D_4$, and the graph automorphisms of D_4 are exactly the triality automorphisms of M^* (cf. [11], [10]). To be more precise, Freudenthal proved this for the reals and Doro for finite fields, however they based their arguments only on the root system and parabolic subgroups, and that is why their result is valid over any field.

By [11], $C_{D_4}(\sigma) = B_3$, and by [17, Lemmas 4.9, 4.10 and 4.3], $C_{D_4}(\rho) = G_2$. As $G_2 < B_3$, by [14, p. 28], we have $C_{D_4}(S_3) = G_2$.

Since F is perfect, $\operatorname{Aut} D_4$ is isomorphic to $\Delta \rtimes (\operatorname{Aut} F \times S_3)$, by a result of Steinberg (cf. [7, Chapter 12]). Here, Δ is the group of the inner and diagonal automorphisms of D_4, and S_3 is the group of graph automorphisms of D_4. When $\operatorname{char} F = 2$ then no diagonal automorphisms exist, and $\Delta = \operatorname{Inn} D_4$. When $\operatorname{char} F \neq 2$ then S_3 acts faithfully on $\Delta / \operatorname{Inn} D_4 \cong C_2 \times C_2$. Hence, in any case, $C_\Delta(S_3) = C_{D_4}(S_3)$. Moreover, for the field and graph automorphisms commute, we have $C_{\operatorname{Aut} D_4}(S_3) = C_{D_4}(S_3) \rtimes \operatorname{Aut} F$.

We have proved $\operatorname{Aut} M^* \cong G_2 \rtimes \operatorname{Aut} F$. The last statement follows from the fact that the group of linear automorphisms of the split octonion algebra is isomorphic to G_2. □

8. Related results, prospects and open problems

We conclude with a few results and open problems concerning simple Moufang loops.

8.1. Generators for finite Paige loops

It is well known that every finite simple group is generated by at most 2 elements. This result requires the classification of finite simple groups, and was finalized in [2]. Since any two elements of a Moufang loop generate a subgroup, no nonassociative Moufang loop can be 2-generated. The following theorem can be proved using some classical results on generators of groups $SL(2,q)$, cf. [31]:

Theorem 8.1. *Every Paige loop $M^*(q)$ is 3-generated. When $q > 2$, the generators can be chosen as*

$$\begin{pmatrix} 0 & e_1 \\ -e_1 & \lambda \end{pmatrix}, \quad \begin{pmatrix} 0 & e_2 \\ -e_2 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix},$$

where λ is a primitive element of $GF(q)$, and e_i is the 3-vector whose only nonzero coordinate is in position i and is equal to 1. When $q = 2$, the generators can be chosen as

$$\begin{pmatrix} 1 & e_1 \\ e_1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & e_2 \\ e_2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & e_3 \\ e_3 & 1 \end{pmatrix}.$$

8.2. Generators for integral Cayley numbers of norm one

Let $C = (C, N)$ be a real composition algebra. The *set of integral elements* of C is the maximal subset of C containing 1, closed under multiplication and subtraction, and such that both aN and $a + \overline{a}$ are integers for each a in the set.

Let $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ be the classical real composition algebras, i.e., those obtained from $\mathbb{R}$ by the Cayley-Dickson process with parameter $\lambda = -1$. The real octonions $\mathbb{O}$ are often called *Cayley numbers*. For $C \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$, there is a unique set of integral elements of C. (For instance, when $C = \mathbb{C}$

this set is known as the Gaussian integers.) When $C = \mathbb{O}$, there are seven such sets, all isomorphic, as Coxeter showed in [9].

We use the notation of [9] here. Let J be one of the sets of integral elements in $\mathbb{O}$, and let $J' = \{x \in J |\ xN = 1\}$. Then $|J'| = 240$, and $J'/\{1, -1\}$ is isomorphic to $M^*(2)$. (This may seem strange, however, $M^*(2)$ is a subloop of any $M^*(q)$, too.) Hence, by Theorem 8.1, $J'/\{1, -1\}$ must be 3-generated. Let i, j, k be the usual units in $\mathbb{H}$, and let e be the unit that is added to $\mathbb{H}$ when constructing $\mathbb{O}$. Following Dickson and Coxeter, let $h = (i + j + k + e)/2$. Then one can show that i, j and h generate $J'/\{1, -1\}$ (multiplicatively). Since $i^2 = -1$, it follows that every set of integral elements of unit norm in $\mathbb{O}$ is 3-generated, too. See [30] for details.

8.3. Problems and conjectures

Problem 8.2. *Find a presentation for $M^*(q)$ in the variety of Moufang loops, possibly based on the generators of Theorem* 8.1.

Problem 8.3. *Find (necessarily infinite) nonassociative simple Moufang loops that are not Paige loops.*

Conjecture 8.4. *Let L be a nonassociative simple Moufang loop and let $H = \mathrm{Mlt}(L)_e$ be the stabilizer of the neutral element in the multiplication group of L. Then H is simple.*

Problem 8.5. *Find a function $f : \mathbb{N} \to \mathbb{N}$ such that the order of the multiplication group of a Moufang loop of order n is less that $f(n)$.*

For the finite Paige loop $M^*(q)$, we have

$$\begin{aligned} |M^*(q)| &= \frac{1}{d}q^3(q^4-1), \\ |P\Omega_8^+(q)| &= \frac{1}{d^2}q^{12}(q^2-1)(q^4-1)^2(q^6-1), \end{aligned}$$

where $d = (2, q-1)$. Hence $|\,\mathrm{Mlt}(M^*(q))| < 4|M^*(q)|^4$ holds. This motivated us to state:

Conjecture 8.6. *The function $f(n) = 4n^4$ solves Problem* 8.5.

References

[1] **E. Artin:** *Geometric Algebra*, Interscience Publishers, New York, 1957.

[2] **M. Aschbacher, R. Guralnick:** *Some applications of the first cohomology group*, J. Algebra **90** (1984), 446 – 460.

[3] **A. Barlotti, K. Strambach:** *The geometry of binary systems*, Advances Math. **49** (1983), 1 – 105.

[4] **R. H. Bruck:** *A Survey of Binary Systems*, Springer-Verlag, Berlin-Heidelberg-New York, 1958.

[5] **R. H. Bruck:** *What is a loop?*, in Studies in Modern Algebra, A. A. Albert (ed.), MAA Studies in Mathematics, 1963, 59 – 99.

[6] **E. Cartan:** *Leçons sur la Théorie des Spineurs*, Hermann et Cie., Paris, 1938.

[7] **R. W. Carter:** *Simple groups of Lie type*, Wiley Interscience, 1972.

[8] **O. Chein, H. O. Pflugfelder, J. D. H. Smith:** *Quasigroups and Loops: Theory and Applications*, Sigma Series in Pure Mathematics **8**, Heldermann Verlag Berlin, 1990.

[9] **H. S. M. Coxeter:** *Integral Cayley numbers*, Duke Mathematical Journal **13**, No. **4**, December 1946. Reprinted in H. S. M. Coxeter, *Twelve Geometric Essays*, Southern Illinois University Press, 1968.

[10] **S. Doro:** *Simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **83** (1978), 377 – 392.

[11] **H. Freudenthal:** *Oktaven, Ausnahmegruppen und Oktavengeometrie*, Geometria Dedicata **19** (1985), 1 – 63.

[12] **M. Funk, P. T. Nagy:** *On collineation groups generated by Bol reflections*, J. Geom. **41** (1993), 63 – 78.

[13] **G. Glauberman:** *On loops of odd order II*, J. Algebra **8** (1968), 383 – 414.

[14] **D. Gorenstein, R. Lyons, R. Solomon:** *The classification of the finite simple groups*, No. 3. Part I, Mathematical Surveys and Monographs **40**(3) (Providence, R.I., AMS, 1998).

[15] **J. I. Hall, G. P. Nagy:** *On Moufang* 3*-nets and groups with triality*, Acta Sci. Math. (Szeged) **67** (2001), 675 – 685.

[16] **E. I. Khukhro:** *Nilpotent groups and their automorphisms*, De Gruyter Expositions in Mathematics, W. de Gruyter, Berlin, 1993.

[17] **M. W. Liebeck:** *The classification of finite simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **102** (1987), 33 – 47.

[18] **P. O. Mikheev:** *Moufang loops and their enveloping groups*, Webs and quasigroups (1993), 33 – 3.

[19] **G. P. Nagy:** *Burnside problems for Moufang and Bol loops of small exponent*, Acta Sci. Szeged **67**(3-4) (2001), 687 – 696.

[20] **G. P. Nagy, M. Valsecchi:** *Splitting automorphisms and Moufang loops.* Manuscript, 2003.

[21] **G. P. Nagy, P. Vojtěchovský:** *Automorphism Groups of Simple Moufang Loops over Perfect Fields*, to appear in Math. Proc. Cambridge Philos. Soc.

[22] **T. A. Springer, F. D. Veldkamp:** *Octonions, Jordan Algebrs and Exceptional Groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[23] **L. J. Paige:** *A class of simple Moufang loops*, Proc. Amer. Math. Soc. **7** (1956), 471 – 482.

[24] **J. D. Phillips:** *Moufang loop multiplication groups with triality*, Rocky Mountain J. of Math. **29/4** (1999), 1483 – 1490.

[25] **H. O. Pflugfelder:** *Quasigroups and Loops: Introduction*, Heldermann Verlag, Berlin, 1990.

[26] **J. D. H. Smith:** *A left loop on the* 15*-sphere*, J. Algebra **176** (1995), 128 – 138.

[27] **D. E. Taylor:**, *The Geometry of the Classical Groups*, Heldermann Verlag, Berlin, 1992.

[28] **J. Tits:** *Sur la trialité et les algèbres d'octaves*, Acad. Roy. Belg. Bull. Cl. Sci. **44**(5) (1958), 332 – 350.

[29] **P. Vojtěchovský:** *Finite simple Moufang loops.* PhD Thesis, Iowa State University, 2001.

[30] **P. Vojtěchovský:** *Generators of nonassociative simple Moufang loops over finite prime fields*, J. Algebra **241** (2001), 186 – 192.

[31] **P. Vojtěchovský:** *Generators for finite simple Moufang loops*, J. Group Theory **6** (2003), 169 – 174.

Received April 29, 2003

Gábor P. Nagy
Bolyai Institute
University of Szeged
Aradi vértanúk tere 1
H-6720 Szeged
Hungary
e-mail: nagyg@math.u-szeged.hu

Petr Vojtěchovský
Department of Mathematics
University of Denver
2360 S Gaylord St
Denver, Colorado 80208
U.S.A.
e-mail: petr@math.du.edu

Quasigroups and Related Systems **10** (2003), 115 – 134

Quasigroup permutation representations

Jonathan D. H. Smith

Abstract

The paper surveys the current state of the theory of permutation representations of finite quasigroups. A permutation representation of a quasigroup includes a Markov chain for each element of the quasigroup, and yields an iterated function system in the sense of fractal geometry. If the quasigroup is associative, the concept specializes to the usual notion of a permutation representation of a group, the transition matrices of the Markov chains becoming permutation matrices in this case. The class of all permutation representations of a given fixed quasigroup forms a covariety of coalgebras. Burnside's Lemma extends to quasigroup permutation representations. The theory leads to a new approach to the study of Lagrangean properties of loops.

1. Introduction

One of the major programs in the study of quasigroups and loops has been the extension to them of various aspects of the representation theory of groups. For summaries of character theory, see [11], [19]. For a summary of module theory, see [18]. The purpose of the present paper is to survey the current state of the theory of permutation representations of finite quasigroups. The theory began with the papers [20], [21] introducing a concept of homogeneous space for finite quasigroups. Given a subquasigroup P of a finite quasigroup Q, the elements of the corresponding homogeneous space $P\backslash Q$ are the orbits on Q of the group of permutations generated by the left multiplications by elements of P. Each element of Q yields a Markov chain action on the homogeneous space $P\backslash Q$ as a set of states. The full structure is an instance of an iterated function system (IFS) in the sense of fractal geometry [1]. If P is a subgroup of a group Q, then the concept just specializes

2000 Mathematics Subject Classification: 20N05
Keywords: loop, quasigroup, permutation representation, coalgebra, Burnside lemma, Lagrange property, iterated function system, IFS

to the usual concept of a homogeneous space or transitive permutation representation for groups, the transition matrices of the Markov chain actions becoming deterministic permutation matrices in this case. Now arbitrary Q-sets for a group Q are just built up by taking disjoint unions of homogeneous spaces. Moreover, the class of (finite) Q-sets is closed under direct products. The class of all Q-sets admits a syntactical characterization as a variety of universal algebras, the axioms essentially characterizing a Q-set (X, Q) as a set X with a group homomorphism from Q to the group $X!$ of permutations of the set X.

For a quasigroup Q, the situation is not so simple. The first step is to establish a general framework, the concrete category $\mathbf{IFS}_Q$ of iterated function systems over the quasigroup Q. An object of this category, a so-called Q-IFS, is just a set X that is the state space of a family of Markov chain actions indexed by the underlying set of the quasigroup Q. Each homogeneous space $P\backslash Q$ is certainly a Q-IFS in this sense. The category $\mathbf{IFS}_Q$ has sums or coproducts given by disjoint unions, and products given by direct products. The transition matrices in the disjoint union are the direct sums of the transition matrices of the summands, while the transition matrices in the direct product are the tensor or Kronecker products of the transition matrices of the factors. If Q is a group, then the category of Q-sets is a full subcategory of $\mathbf{IFS}_Q$, and one may readily recognize when a Q-IFS is a Q-set (Proposition 5.3). For a finite quasigroup Q, each Q-IFS is equivalent to a certain coalgebra (Theorem 7.4). The class of Q-sets or permutation representations for Q is then defined to be the covariety of coalgebras generated by the homomorphic images of homogeneous spaces. Each Q-set is a sum of orbits or images of homogeneous spaces (Theorem 10.2), the number of orbits being counted by Burnside's Lemma (Theorem 11.2). The paper concludes with an application of the theory of quasigroup permutation representations to the study of Lagrangean properties of loops. For concepts and conventions of quasigroup theory and universal algebra that are not otherwise explained here, readers are referred to [23].

2. Relative multiplication groups

Quasigroups are construed as sets $(Q, \cdot, /, \backslash)$ equipped with three binary operations of multiplication, *right division* $/$ and *left division* $\backslash$, satisfying the identities:

$$\text{(IL)}\quad y\backslash(y\cdot x) = x; \qquad \text{(SL)}\quad y\cdot(y\backslash x) = x;$$

$$\text{(IR)}\quad x = (x\cdot y)/y; \qquad \text{(SR)}\quad x = (x/y)\cdot y.$$

A subset P of a quasigroup Q is a *subquasigroup* of Q if it is closed under the three binary operations. More generally, the equational definition of quasigroups means that they form a variety in the sense of universal algebra, and are thus susceptible to study by the concepts and methods of universal algebra [23].

For each element q of a quasigroup Q, the *right multiplication*

$$R(q) : Q \to Q; x \mapsto x \cdot q$$

and *left multiplication*

$$L(q) : Q \to Q; x \mapsto q \cdot x$$

are elements of the group $Q!$ of bijections from the set Q to itself. For a subquasigroup P of a quasigroup Q, the *relative left multiplication group* of P in Q is the subgroup $\mathrm{LMlt}_Q(P)$ of $Q!$ generated by

$$L(P) = \{L(p) : Q \to Q \mid p \in P\}. \qquad (2.1)$$

Relative right multiplication groups are defined similarly. A *loop* is a (non-empty) quasigroup Q with an *identity* element, an element e such that $R(e) = L(e) = 1$ in $Q!$. Loops form the non-empty members of the variety of quasigroups satisfying the identity $x/x = y\backslash y$. They may also be construed as algebras $(Q, \cdot, /, \backslash, e)$ such that $(Q, \cdot, /, \backslash)$ is a quasigroup and e is a nullary operation satisfying the identities $e \cdot x = x = x \cdot e$.

3. Quasigroup homogeneous spaces

The construction of a quasigroup homogeneous space for a finite quasigroup [20] [21] is analogous to the permutation representation of a group Q (with subgroup P) on the homogeneous space

$$P \setminus Q = \{Px \mid x \in Q\} \qquad (3.1)$$

by the actions

$$R_{P\setminus Q}(q) : P \setminus Q \to P \setminus Q\,;\, Px \mapsto Pxq \qquad (3.2)$$

for elements q of Q. Let P be a subquasigroup of a finite quasigroup Q. Let L be the relative left multiplication group of P in Q. Let $P \setminus Q$ be the set of orbits of the permutation group L on the set Q. If Q is a group, and P is nonempty, then this notation is consistent with (3.1). Let A be the incidence matrix of the membership relation between the set Q and the set $P \setminus Q$ of subsets of Q. Let A^+ be the pseudoinverse of the matrix A, i.e. the unique matrix A^+ satisfying:

$$\begin{array}{ll} (a) & AA^+A = A \\ (b) & A^+AA^+ = A^+ \\ (c) & (A^+A)^* = A^+A \\ (d) & (AA^+)^* = AA^+ \end{array}$$

[13]. For each element q of Q, right multiplication in Q by q yields a permutation of Q. Let $R_Q(q)$ be the corresponding permutation matrix. Define a new matrix

$$R_{P\setminus Q}(q) = A^+R_Q(q)A\,. \tag{3.3}$$

[In the group case, the matrix (3.3) is just the permutation matrix given by the permutation (3.2).] Then in the homogeneous space of the quasigroup Q, each quasigroup element q yields a Markov chain on the state space $P \setminus Q$ with transition matrix $R_{P\setminus Q}(q)$ given by (3.3). For the intuition behind (3.3), see the discussion of the example in the following section.

Remark 3.1. The set of convex combinations of the states from $P\setminus Q$ forms a complete metric space, and the actions (3.3) of the quasigroup elements form an iterated function system or IFS in the sense of fractal geometry [1]. For present purposes, this remark is relevant only as motivation for the nomenclature of Section 5 below.

4. An example

Consider the quasigroup Q whose multiplication table is the following Latin square:

1	3	2	5	6	4
3	2	1	6	4	5
2	1	3	4	5	6
4	5	6	1	2	3
5	6	4	2	3	1
6	4	5	3	1	2

.

Let P be the singleton subquasigroup $\{1\}$. Note that $\mathrm{LMlt}_Q P$ is the cyclic subgroup of $Q!$ generated by $(23)(456)$. Thus

$$P \setminus Q = \{\{1\}, \{2, 3\}, \{4, 5, 6\}\},$$

yielding

$$A_P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad A_P^+ = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix} ,$$

whence (3.3) gives

$$R_{P\backslash Q}(5) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix} . \tag{4.1}$$

The bottom row of (4.1), determining the image of the orbit $\{4,5,6\}$ under the action of the quasigroup element 5, may be understood as follows. From the multiplication table, one has $4 \cdot 5 = 2$, $5 \cdot 5 = 3$, and $6 \cdot 5 = 1$. Thus a uniformly chosen random element of $\{4,5,6\}$ is multiplied by the quasigroup element 5 to an element of the orbit $\{1\}$ with probability 1/3, and to an element of the orbit $\{2,3\}$ with probability 2/3.

5. The IFS category

Let Q be a finite quasigroup. Define a Q-IFS (X,Q) as a finite set X together with an *action map*

$$R : Q \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}X); q \mapsto R_X(q) \tag{5.1}$$

from Q to the set of endomorphisms of the complex vector space with basis X (identified with their matrices with respect to the basis X), such that each *action matrix* $R_X(q)$ is stochastic. (Recall that a square complex matrix is said to be *stochastic* if its entries are non-negative real numbers, and if each row sum is 1.)

Definition 5.2. Let (X,Q) be a Q-IFS. Then for Q non-empty, the *Markov matrix* of (X,Q) is the arithmetic mean

$$M_{(X,Q)} = \frac{1}{|Q|} \sum_{q \in Q} R_X(q) \tag{5.2}$$

of the action matrices of the elements of Q.

Note that the Markov matrix of a Q-IFS is stochastic. If P is a subquasigroup of a finite non-empty quasigroup Q, then the homogeneous space $P \setminus Q$ is a Q-IFS with the action map specified by (3.3). Each row of the Markov matrix of the Q-IFS $P \setminus Q$ takes the form

$$(|P_1|/|Q|, \dots, |P_r|/|Q|), \tag{5.3}$$

where $P_1, \dots, P_r$ are the orbits of the relative left multiplication group of P in Q. (Compare [22, Prop. 8.1], where this result was formulated for a loop Q. The proof given there applies to an arbitrary non-empty quasigroup Q.)

A *morphism*

$$\phi : (X, Q) \to (Y, Q) \tag{5.4}$$

from a Q-IFS (X, Q) to a Q-IFS (Y, Q) is a function $\phi : X \to Y$, whose graph has incidence matrix F, such that

$$R_X(q)F = FR_Y(q) \tag{5.5}$$

for each element q of Q. It is readily checked that the class of morphisms (5.4), for a fixed quasigroup Q, forms a concrete category $\mathbf{IFS}_Q$.

Proposition 5.3. *Let Q be a finite group.*

- (a) *The category of finite Q-sets forms the full subcategory of $\mathbf{IFS}_Q$ consisting of those objects for which the action map* (5.1) *is a monoid homomorphism.*
- (b) *A Q-IFS (X, Q) is a Q-set if and only if it is isomorphic to a Q-set (Y, Q) in $\mathbf{IFS}_Q$.*

Proof. For (a), suppose that the action map (5.1) of a Q-IFS (X, Q) is a monoid homomorphism. Let A be in the image of (5.1). Then A is a stochastic matrix with $A^r = I$ for some positive integer r. It follows that A is a permutation matrix (cf. §XV.7 of [4]). Part (b) follows from part (a): if the morphism $\phi : (X, Q) \to (Y, Q)$ is an isomorphism whose graph has incidence matrix F, then the action map of (X, Q) is the composite of the action map of (Y, Q) with the monoid isomorphism $R_Y(q) \mapsto FR_Y(q)F^{-1}$ given by (5.5). □

For a fixed finite quasigroup Q, the category $\mathbf{IFS}_Q$ has finite products and coproducts. Consider objects (X, Q) and (Y, Q) of $\mathbf{IFS}_Q$. Their *sum* or *disjoint union* $(X + Y, Q)$ consists of the disjoint union $X + Y$ of the sets X and Y together with the action map

$$q \mapsto R_X(q) \oplus R_Y(q) \tag{5.6}$$

sending each element q of Q to the direct sum of the matrices $R_X(q)$ and $R_Y(q)$. One obtains an object of $\mathbf{IFS}_Q$, since the direct sum of stochastic matrices is stochastic. The *direct product* $(X \times Y, Q)$ of (X, Q) and (Y, Q) is the direct product $X \times Y$ of the sets X and Y together with the action map

$$q \mapsto R_X(q) \otimes R_Y(q)$$

sending each element q of Q to the tensor (or Kronecker) product of the matrices $R_X(q)$ and $R_Y(q)$. Again, one obtains an object of $\mathbf{IFS}_Q$, since the tensor product of stochastic matrices is stochastic. It is straightforward to check that the disjoint union, equipped with the appropriate insertions, yields a coproduct in $\mathbf{IFS}_Q$, and that the direct product, equipped with the appropriate projections, yields a product in $\mathbf{IFS}_Q$.

6. Coalgebras and covarieties

For a given finite quasigroup Q, the permutation representations of Q are axiomatized as a certain covariety of coalgebras. This section thus summarises the basic coalgebraic concepts required. For more details, readers may consult [7], [8] or [17]. Crudely speaking, coalgebras are just the duals of algebras: coalgebras in a category $\mathcal{C}$ are algebras in the dual category $\mathcal{C}^{\mathrm{op}}$.

Let $F : \mathbf{Set} \to \mathbf{Set}$ be an endofunctor on the category of sets and functions. Then an *F-coalgebra*, or simply a *coalgebra* if the endofunctor is implicit in the context, is a set X equipped with a function α_X or $\alpha : X \to XF$. This function is known as the *structure map* of the coalgebra X. (Of course, for complete precision, one may always denote a coalgebra by its structure map.) A function $f : X \to Y$ between coalgebras is a *homomorphism* if $f\alpha_Y = \alpha_X f^F$. A subset S of a coalgebra X is a *subcoalgebra* if it is itself a coalgebra such that the embedding of S in X is a homomorphism. A coalgebra Y is a *homomorphic image* of a coalgebra X if there is a surjective homomorphism $f : X \to Y$.

Let $(X_i \mid i \in I)$ be a family of coalgebras. Then the *sum* of this family is the disjoint union of the sets of the family, equipped with a coalgebra structure map α given as follows. Let $\iota_i : X_i \to X$ insert X_i as a summand in the disjoint union X of the family. For each i in I, let α_i be the structure map of X_i. Then the restriction of α to the subset X_i of X is given by $\alpha_i \iota_i^F$. (More generally, the forgetful functor from coalgebras to sets creates colimits — cf. Proposition 1.1 of [2].)

A *covariety* of coalgebras is a class of coalgebras closed under the operations H of taking homomorphic images, S of taking subalgebras, and Σ of taking sums. (Note that homomorphic images are dual to subalgebras, while sums are dual to products.) If $\mathcal{K}$ is a class of F-coalgebras, then the smallest covariety containing $\mathcal{K}$ is given by $\mathrm{SH}\Sigma(\mathcal{K})$ (cf. [7, Th. 7.5] or [8, Th. 3.3]). This result is dual to the well-known characterization of the variety generated by a class of algebras (cf. e.g. Exercise 2.3A of [23, Ch. IV] or [16, Prop. 1.5.12]).

7. Actions as coalgebras

For a finite set Q, the Q-IFS are realised as coalgebras for the Q-th power of the endofunctor B sending a set to (the underlying set of) the free barycentric algebra it generates. Thus it is first necessary to recall some basic facts about barycentric algebras. For more details, readers may consult [15] or [16]. Let I° denote the open unit interval $]0,1[$. For p in I°, define $p' = 1-p$.

Definition 7.1. A *barycentric algebra* A or (A, I°) is an algebra of type $I^\circ \times \{2\}$, equipped with a binary operation

$$\underline{p} : A \times A \to A; \quad (x,y) \mapsto xy\,\underline{p}$$

for each p in I°, satisfying the identities

$$xx\,\underline{p} = x \tag{7.1}$$

of *idempotence* for each p in I°, the identities

$$xy\,\underline{p} = yx\,\underline{p'} \tag{7.2}$$

of *skew-commutativity* for each p in I°, and the identities

$$xy\,\underline{p}\;z\,\underline{q} = x\;yz\,\underline{q/(p'q')'}\;\underline{(p'q')'} \tag{7.3}$$

of *skew-associativity* for each p, q in I°. The variety of all barycentric algebras, construed as a category with the homomorphisms as morphisms, is denoted by $\mathbf{B}$. The corresponding free algebra functor is $B : \mathbf{Set} \to \mathbf{B}$.

A convex set C forms a barycentric algebra (C, I°), with $xy\,\underline{p} = (1-p)x + py$ for x, y in C and p in I°. A semilattice $(S, \cdot)$ becomes a barycentric algebra on setting $xy\,\underline{p} = x \cdot y$ for x, y in S and p in I°.

For the following result, see [12], [15, §2.1], [16, §5.8]. The equivalence of the final two structures in the theorem corresponds to the identification of the barycentric coordinates in a simplex with the weights in finite probability distributions.

Theorem 7.2. *Let X be a finite set. The following structures are equivalent:*

(a) *The free barycentric algebra XB on X;*

(b) *The simplex spanned by X;*

(c) *The set of all probability distributions on X.*

Definition 7.3. Let Q be a finite set. The functor $B^Q : \mathbf{Set} \to \mathbf{Set}$ sends a set X to the set XB^Q of functions from Q to the free barycentric algebra XB over X. For a function $f : X \to Y$, its image under the functor B^Q is the function $fB^Q : XB^Q \to YB^Q$ defined by

$$fB^Q : (Q \to XB; q \mapsto w) \mapsto (Q \to YB; q \mapsto wf^B).$$

Theorem 7.4. *Let Q be a finite set. Then the category $\mathbf{IFS}_Q$ is isomorphic with the category of finite B^Q-coalgebras.*

Proof. Given a Q-IFS (X, Q) with action map R as in (5.1), define a B^Q-coalgebra $L_X : X \to XB^Q$ with structure map

$$L_X : X \to XB^Q; x \mapsto (Q \to XB; q \mapsto xR_X(q)). \tag{7.4}$$

(Note the use of Theorem 7.2 interpreting the vector $xR_X(q)$, lying in the simplex spanned by X, as an element of XB.) Given a Q-IFS morphism $\phi : (X, Q) \to (Y, Q)$ as in (5.4), with incidence matrix F, one has

$$xL_X.\phi B^Q : Q \to YB; q \mapsto xR_X(q)F \tag{7.5}$$

for each x in X, by Definition 7.3. On the other hand, one also has

$$x\phi L_Y : Q \to YB; q \mapsto xFR_Y(q). \tag{7.6}$$

By (5.5), it follows that the maps (7.5) and (7.6) agree. Thus $\phi : X \to Y$ is a coalgebra homomorphism. These constructions yield a functor from $\mathbf{IFS}_Q$ to the category of finite B^Q-coalgebras.

Conversely, given a finite B^Q-coalgebra with structure map $L_X : X \to XB^Q$, define a Q-IFS (X, Q) with action map

$$R_X : Q \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}X); q \mapsto (x \mapsto qL_X(x)), \tag{7.7}$$

well-defined by Theorem 7.2. Let $\phi : X \to Y$ be a coalgebra homomorphism with incidence matrix F. Then the maps (7.5) and (7.6) agree for all x in the basis X of $\mathbb{C}X$, whence (5.5) holds and $\phi : (X, Q) \to (Y, Q)$ becomes a Q-IFS morphism. In this way one obtains mutually inverse functors between the two categories. □

Corollary 7.5. *Each homogeneous space over a finite quasigroup Q yields a B^Q-coalgebra.*

Example 7.6. Consider the structure map of the coalgebra corresponding to the homogeneous space presented in Section 4. In accordance with (4.1), the image of the state $\{4, 5, 6\}$ sends the element 5 of Q to the convex combination weighting the state $\{1\}$ with 1/3 and the state $\{2, 3\}$ with 2/3.

Corollary 7.7. *Let Q be a finite group. Then the category of finite Q-sets embeds faithfully as a full subcategory of the category of B^Q-coalgebras.*

Proof. Apply Theorem 7.4 and Proposition 5.3. □

8. Irreducibility

Definition 8.1. Let Q be a finite set. Let Y be a B^Q-coalgebra with structure map $L : Y \to YB^Q$. For elements y, y' of Y, the element y' is said to be *reachable* from y in Y if there is an element q of Q such that y' appears in the support of the distribution $qL(y)$ on Y. The *reachability graph* of Y is the directed graph of the reachability relation on Y. The coalgebra Y is said to be *irreducible* if its reachability graph is strongly connected.

Proposition 8.2. *If $P \backslash Q$ is a homogeneous space over a finite quasigroup Q, realised as a B^Q-coalgebra according to Corollary 7.5, then $P \backslash Q$ is irreducible.*

Proof. Let H be the relative left multiplication group of P in Q. For an arbitrary pair x, x' of elements of Q, consider the corresponding elements xH and $x'H$ of $P \backslash Q$. For $q = x \backslash x'$ in Q, the element $x'H$ then appears in the support of $qL(xH)$. □

Corollary 8.3. *Let Q be a finite quasigroup. Suppose that Y is a B^Q-coalgebra that is a homomorphic image of a homogeneous space S over Q. Then Y is irreducible.*

Proof. Since S and Y are finite, one may use the correspondence of Theorem 7.4. Let $\phi : S \to Y$ be the homomorphism, with incidence matrix F. Consider elements y and y' of Y. Suppose x and x' are elements of S with $x\phi = y$ and $x'\phi = y'$. By Proposition 8.2, there is an element q of Q with x' in the support of the distribution $xR_S(q)$. Then $yR_Y(q) = xFR_Y(q) = xR_S(q)F$, so the support of $yR_Y(q)$, as the image of the support of $xR_S(q)$ under ϕ, contains $x'\phi = y'$. □

9. Regular representations

For a quasigroup Q, the *regular* homogeneous space or permutation representation is the homogeneous space (Q, Q) or $(\varnothing \setminus Q, Q)$. Recall that the relative left multiplication group of the empty subquasigroup is trivial. If Q is a loop with identity element e, then the regular homogeneous space may also be described as $(\{e\} \setminus Q, Q)$. (This definition was used in [22, §7].) A finite, non-empty quasigroup Q may be recovered from its regular representation. For example, the multiplication table of Q may be realised as the formal sum $\Sigma_{q\in Q} qR_{\varnothing\setminus Q}(q)$ of multiples of the action matrices of $\varnothing \setminus Q$.

For a group Q, each homogeneous space $(P \setminus Q, Q)$ is obtained as a homomorphic image of the regular permutation representation. The following considerations show that the corresponding property does not hold for general quasigroups.

Definition 9.1. Let Q be a finite set. A Q-IFS (X, Q) is said to be *crisp* if, for each q in Q, the action matrix $R_X(q)$ is a 0-1-matrix. A B^Q-coalgebra $L : X \to XB^Q$ is said to be *crisp* if its structure map corestricts to $L : X \to X^Q$.

Note that crisp Q-IFS and finite crisp B^Q-coalgebras correspond under the isomorphism of Theorem 7.4.

Proposition 9.2. *Homomorphic images of finite crisp B^Q-coalgebras are crisp.*

Proof. Using Theorem 7.4, it is simpler to work in the category $\mathbf{IFS}_Q$. Let $\phi : X \to Y$ be a surjective $\mathbf{IFS}_Q$-morphism with incidence matrix F and crisp domain. For an element y of Y, suppose that x is an element of X

with $x\phi = y$. Then for each element q of Q, one has $yR_Y(q) = x\phi R_Y(q) = xFR_Y(q) = xR_X(q)F$, using (5.5) for the last step. Since X is crisp, there is an element x' of X with $xR_X(q) = x'$. Then $yR_Y(q) = x'F = y'$ for the element $y' = x'\phi$ of Y. Thus Y is also crisp. □

For each finite quasigroup Q, the regular permutation representation is crisp. On the other hand, the homogeneous space exhibited in Section is not crisp. Proposition 9.2 shows that such spaces are not homomorphic images of the regular representation.

10. The covariety of Q-sets

Definition 10.1. Let Q be a finite quasigroup. Then the *category* $\underline{\underline{Q}}$ *of* *Q-sets* or of *permutation representations* of Q is defined to be the covariety of B^Q-coalgebras generated by the (finite) set of homogeneous spaces over Q.

For a finite quasigroup Q, the terms "Q-set" or "permutation representation of Q" are used for objects of the category of Q-sets, and also for those Q-IFS which correspond to finite Q-sets via Theorem 7.4. (For a finite loop Q, these terms were used in a different, essentially broader sense — at least for the finite case — in [22, Defn. 5.2]. If necessary, one may refer to "loop Q-sets" in that context, and to "proper Q-sets" or "quasigroup Q-sets" in the present context.)

Theorem 10.2. *For a finite quasigroup Q, the Q-sets are precisely the sums of homomorphic images of homogeneous spaces.*

Proof. Let $\mathcal{H}$ be the set of homogeneous spaces over Q. By [9, Prop. 2.4], the covariety generated by $\mathcal{H}$ is $\mathrm{HS}\Sigma(\mathcal{H})$. By [9, Prop. 2.5], the operators S and Σ commute. By Proposition 8.2, the homogeneous spaces do not contain any proper, non-empty subcoalgebras. Thus the covariety generated by $\mathcal{H}$ becomes $\mathrm{H}\Sigma(\mathcal{H})$. By [9, Prop. 2.4(iii)], one has $\Sigma\mathrm{H}(\mathcal{H}) \subseteq \mathrm{H}\Sigma(\mathcal{H})$. It thus remains to be shown that each homomorphic image of a sum of homogeneous spaces is a sum of homomorphic images of homogeneous spaces.

Let Y be a Q-set, with structure map L_Y, that is a homomorphic image of a sum X of homogeneous spaces under a homomorphism ϕ. It will first be shown that each element y of Y lies in a subcoalgebra Y_y of Y that is a homomorphic image of a homogeneous space. Since y lies in the image Y of X under ϕ, there is an element x of X such that $x\phi = y$. Since X is a sum of homogeneous spaces, the element x lies in such a space S. Consider the restriction of ϕ to S. Let Y_y be the image of this restriction. Then Y_y is a subcoalgebra of Y that is a homomorphic image of a homogeneous space (cf. [7, Lemma 4.5]).

Now suppose that for elements y and z of Y, the corresponding images Y_y and Y_z of homogeneous spaces intersect non-trivially, say with a common element t. By Corollary 8.3, there is an element q of Q such that z lies in the support of $qL_Y(t)$. On the other hand, since t lies in the subcoalgebra Y_y, the support of the distribution $qL_Y(t)$ lies entirely in Y_y. Thus z is an element of Y_y, and for each q in Q, the support of the distribution $qL_Y(z)$ lies entirely in Y_y. It follows that Y_z is entirely contained in Y_y. Similarly, one finds that Y_y is contained in Y_z, and so the two images agree. Thus Y is a sum of such images. □

Corollary 10.3. *A finite quasigroup Q has only finitely many isomorphism classes of irreducible Q-sets.*

Proof. By Theorem 10.2, the irreducible Q-sets are precisely the homomorphic images of homogeneous spaces. Since Q is finite, it has only finitely many homogeneous spaces. The (First) Isomorphism Theorem for coalgebras (cf. [7, Th. 4.15]) then shows that each of these homogeneous spaces has only finitely many isomorphism classes of homomorphic images. □

Corollary 10.4. *For a finite group Q, the quasigroup Q-sets coincide with the group Q-sets.*

Proof. For a group Q, each homomorphic image of a homogeneous space is isomorphic to a homogeneous space, and each group Q-set is isomorphic to a sum of homogeneous spaces. □

In considering the final corollary of Theorem 10.2, recall that the intersection of a family of subcoalgebras of a coalgebra is not necessarily itself a subcoalgebra (cf. [7, Cor. 4.9]).

Corollary 10.5. *Let y be an element of a Q-set Y over a finite quasigroup Q. Then the intersection of the subcoalgebras of Y containing y is itself a subcoalgebra of Y.*

Proof. In the notation of the proof of Theorem 10.2, this intersection is the subcoalgebra Y_y. □

11. Burnside's Lemma

Definition 11.1. For a Q-set Y over a finite quasigroup Q, the irreducible summands of Y given by Theorem 10.2 are called the *orbits* of Y. For an element y of Y, the smallest subcoalgebra of Y containing y (guaranteed to exist by Corollary 10.5) is called the *orbit* of the element y.

Burnside's Lemma concerns itself with finite permutation representations. In the quasigroup case, its formulation (and proof) rely on the identification given by Theorem 7.4. Recall that the classical Burnside Lemma for a finite group Q (cf. e.g. Theorem 3.1.2 in [23, Ch. I]) states that the number of orbits in a finite Q-set X is equal to the average number of points of X fixed by elements q of Q. The number of points fixed by such an element q is equal to the trace of the permutation matrix of q on X. In the IFS terminology of §3, this permutation matrix is the action matrix $R_X(q)$ of q on the corresponding Q-IFS (X, Q). Thus the following theorem does specialise to the classical Burnside Lemma in the associative case.

Theorem 11.2. Burnside's Lemma for quasigroups
Let X be a finite Q-set over a finite, non-empty quasigroup Q. Then the trace of the Markov matrix of X is equal to the number of orbits of X.

Proof. Consider the Q-IFS (X, Q). By Theorem 7.4, Theorem 10.2 and (5.6), its Markov matrix decomposes as a direct sum of the Markov matrices of its orbits. Thus it suffices to show that the trace of the Markov matrix of a homomorphic image of a homogeneous space is equal to 1.

Consider a Q-set $Y = \{y_1, \dots, y_m\}$ which is the image of a homogeneous space $P \backslash Q$ under a surjective homomorphism $\phi : P \backslash Q \to Y$ with incidence matrix F. Let F^+ be the pseudoinverse of F. Note that each row sum of F^+ is 1. Suppose that the Markov matrix Π of $P \setminus Q$ is given by (5.3). By (5.5), one has

$$R_Y(q) = F^+ R_{P \backslash Q}(q) F$$

for each q in Q. Thus the trace of the Markov matrix of Y is given by

$$\begin{aligned} tr(F^+ \Pi F) &= \sum_{i=1}^{m} \sum_{j=1}^{r} \sum_{k=1}^{r} F^+_{ij} \Pi_{jk} F_{ki} \\ &= |Q|^{-1} \sum_{i=1}^{m} (\sum_{j=1}^{r} F^+_{ij}) (\sum_{k=1}^{r} |P_k| F_{ki}) \\ &= |Q|^{-1} \sum_{k=1}^{r} |P_k| = 1, \end{aligned}$$

the penultimate equality following since for each $1 \leq k \leq r$, there is exactly one index i (corresponding to $P_k\phi = y_i$) such that $F_{ki} = 1$, the other terms of this type vanishing. □

Remark 11.3. Burnside's Lemma may fail for a Q-IFS which does not correspond to a Q-set. For example, the square $P \setminus Q \times P \setminus Q$ of the homogeneous space $P \setminus Q$ of Section 4 (in the category of Q-IFS) has a 9×9 Markov matrix of trace 1.875, which is not even integral.

12. Lagrangean properties of loops

For a group Q, Lagrange's Theorem states that the order of a subgroup always divides the order of Q. For a general loop Q, the order of a subloop need not divide $|Q|$. In [14], a subloop P of Q is called "Lagrange-like" in Q if $|P|$ does divide $|Q|$. The loop Q is said to satisfy the *weak Lagrange property* if each subloop is Lagrange-like. It is said to satisfy the *strong Lagrange property* if each of its subloops satisfies the weak Lagrange property. Nonassociative loops satisfying the strong Lagrange property were discussed in [3], [5], [6]. Recalling that Lagrange's Theorem for a group Q relies on the uniformity of the sizes of the elements of a homogeneous space $P \setminus Q$, this section formulates Lagrangean properties for loops in homogeneous space terms. Let P be a subloop of a finite loop Q. The *type* of the homogeneous space $P \setminus Q$ is the partition of $|P \setminus Q|$ given by the sizes of the orbits of the relative left multiplication group of P in Q. Note that the type of a homogeneous space is determined by its Markov matrix, according to (5.3). The type of a homogeneous space $P \setminus Q$ is said to be *uniform* if all the parts of the partition are equal. A subloop P of Q is said to be (*right*) *Lagrangean* in Q if the type of $P \setminus Q$ is uniform, i.e. if the relative left multiplication group of P in Q acts semitransitively (in the sense of [10, Defn. II.1.14b]). Note that a Lagrangean subloop P is Lagrange-like in Pflugfelder's sense, since P is one of the states of $P \setminus Q$. On the other hand, the subloop P of the loop Q of Example 12.6 below is Lagrange-like in Q, but not right Lagrangean in Q.

The Lagrangean property is more robust than Lagrange-likeness. It may happen that a subloop P of a loop Q is Lagrange-like in Q, but not in a subloop of Q that contains P. For example, suppose that a loop Q has a subloop P that is not Lagrange-like in Q. Then $P \times \{e\}$ is Lagrange-like in the loop $Q \times P$, but not in the subloop $Q \times \{e\}$. The following proposition shows that the Lagrangean property does not exhibit such pathology.

Proposition 12.1. *Let P be a Lagrangean subloop in a finite loop Q. Then P is Lagrangean in each subloop S of Q that contains P.*

Proof. Since P is a subloop of the loop S, the action of the relative left multiplication group $\mathrm{LMlt}_S P$ of P in S is just a restriction to S of the action of the relative left multiplication group $\mathrm{LMlt}_Q P$ of P in Q. Thus the uniformity of the sizes of the orbits of $\mathrm{LMlt}_Q P$ implies the uniformity of the sizes of the orbits of $\mathrm{LMlt}_S P$. □

Definition 12.2. A finite loop Q is said *to satisfy the* (*right*) *Lagrange property* if each subloop of Q is (right) Lagrangean in Q.

Example 12.3. The only proper, non-trivial subloop of the loop T with multiplication table

1	2	3	4	5	6
2	1	6	5	4	3
3	6	5	1	2	4
4	5	1	6	3	2
5	3	4	2	6	1
6	4	2	3	1	5

is the subloop $\{1, 2\}$, which is Lagrangean in T. Thus T is a non-associative loop satisfying the right Lagrange property.

In contrast with the global properties based on Lagrange-likeness, Proposition 12.1 shows that one does not need to make a distinction between "weak" and "strong" versions of the Lagrangean property of Definition 12.2.

Corollary 12.4. *Suppose that a finite loop Q satisfies the right Lagrange property. Then each subloop of Q also satisfies the right Lagrange property.*

Proof. Let P be a subloop of a subloop Q' of Q. Then by Proposition 12.1, P is Lagrangean in Q'. □

Corollary 12.5. *If a finite loop Q satisfies the right Lagrange property, then it also satisfies the strong Lagrange property.*

Proof. Let P be a subloop of a subloop Q' of Q. By Corollary 12.4, Q' satisfies the right Lagrange property, so that P is Lagrangean in Q'. It then follows that P is Lagrange-like in Q'. Thus each subloop Q' of Q satisfies the weak Lagrange property, i.e. Q itself satisfies the strong Lagrange property. □

Example 12.6. The converse of Corollary 12.5 is false: the strong Lagrange property is too weak to imply the right Lagrange property. Consider the loop Q whose multiplication table is the following Latin square:

1	2	3	4	5	6
2	1	4	5	6	3
3	4	5	6	1	2
4	3	6	1	2	5
5	6	1	2	3	4
6	5	2	3	4	1

.

The proper, non-trivial subquasigroups of Q are $P = \{1, 2\}$, $P' = \{1, 4\}$, and $P'' = \{1, 6\}$, each Lagrange-like in Q, and without mutual containments. Thus Q does satisfy the strong Lagrange property. On $P \setminus Q$, the action matrices (3.3) of the elements of P are the identity I_2, while the action matrices of the remaining elements of Q are

$$A = \begin{bmatrix} 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}.$$

The type of $P \setminus Q$ is $2 + 4$, so that P is not Lagrangean in Q, and Q does not satisfy the right Lagrange property.

Corollary 12.4 shows that the right Lagrange property is inherited by subloops. The property is also inherited by homomorphic images.

Proposition 12.7. *Suppose that a finite loop Q satisfies the right Lagrange property. Then each homomorphic image of Q also satisfies the right Lagrange property.*

Proof. Suppose that $\overline{Q}$ is a quotient of Q by a projection

$$Q \to \overline{Q}; q \mapsto \overline{q}. \tag{12.1}$$

Let $\overline{P}$ be a subloop of $\overline{Q}$ whose preimage under (12.1) is the subloop P of Q. The projection (12.1) induces a group epimorphism

$$\mathrm{LMlt}_Q P \to \mathrm{LMlt}_{\overline{Q}} \overline{P}; l \mapsto \overline{l}$$

acting on the set (2.1) of generators of its domain by $L(p) \mapsto L(\overline{p})$. Set $L = \mathrm{LMlt}_Q P$ and $\overline{L} = \mathrm{LMlt}_{\overline{Q}} \overline{P}$. Now for q in Q, one has

$$\overline{q}\overline{L} = \overline{qL}. \tag{12.2}$$

To see this, consider an element $\overline{q}\overline{l}$ of the left hand side of (12.2), where the element l of $\mathrm{LMlt}_Q P$ is given by

$$l = L(p_1)\dots L(p_r)$$

with elements $p_1, \dots, p_r$ of P. Then

$$\overline{q}\overline{l} = \overline{q}L(\overline{p_1})\dots L(\overline{p_r}) = \overline{qL(p_1)\dots L(p_r)} \in \overline{qL},$$

the second equality holding since (12.1) is a loop homomorphism. Conversely, the typical element of the right hand side of (12.2) is of the form

$$\overline{qL(p_1)\dots L(p_r)}$$

with q in Q and elements $p_1, \dots, p_r$ of P. Such an element may be rewritten in the form

$$\overline{q}L(\overline{p_1})\dots L(\overline{p_r}),$$

exhibiting it as an element of the left hand side of (12.2).

Since the homogeneous space $P \backslash Q$ has uniform type, it follows that for each element q of Q the injection

$$R(q) : P \to qL; p \mapsto pq$$

bijects. In other words, $qL = \{pq \mid p \in P\}$. Then by (12.2), one has

$$\overline{q}\overline{L} = \overline{qL} = \{\overline{pq} \mid p \in P\} = \{\overline{p} \cdot \overline{q} \mid \overline{p} \in \overline{P}\},$$

so that each state of $\overline{P} \backslash \overline{Q}$ has cardinality $|\overline{P}|$. Thus $\overline{P}$ is Lagrangean in $\overline{Q}$, as required. □

In view of Corollary 12.4 and Proposition 12.7, it is natural to pose the following:

Problem 12.8. Suppose that loops Q_1 and Q_2 satisfy the right Lagrange property. Does the product $Q_1 \times Q_2$ also satisfy this property?

The asymmetry inherent in Definition 12.2 means that one should also consider matters from the other side. Thus a subloop P of a loop Q is said to be (*left*) *Lagrangean* in Q if the relative right multiplication group of P in Q acts semitransitively. A loop Q is said to satisfy the *left Lagrange property* if each subloop P of Q is left Lagrangean in Q. It is said to satisfy the *bilateral Lagrange property* if it satisfies both left and right Lagrange properties. Note that the subloop P of the loop Q of Example 12.6 is left Lagrangean in Q, although it is not right Lagrangean in Q.

Finally, Chein's paper [3] suggests the following:

Problem 12.9. Which loops satisfying Pflugfelder's M_k-laws possess the right, left, or bilateral Lagrange properties?

References

[1] **M. F. Barnsley**: *Fractals Everywhere*, Academic Press, San Diego, CA, 1988.

[2] **M. Barr**: *Terminal coalgebras in well-founded set theory*, Theoret. Comput. Sci. **1**14 (1993), 299 – 315.

[3] **O. Chein**: *Lagrange's Theorem for M_k-loops*, Arch. Math. **24** (1973), 121 – 122.

[4] **W. Feller**: *An Introduction to Probability Theory and its Applications*, 2nd. Ed., Vol. I, Wiley, New York, NY, 1957.

[5] **G. Glauberman**: *On loops of odd order II*, J. Alg. **8** (1968), 393 – 414.

[6] **G. Glauberman and C. R. B. Wright**: *Nilpotence of finite Moufang 2-loops*, J. Alg. **8** (1968), 415 – 417.

[7] **H.-P. Gumm**: *Elements of the general theory of coalgebras*, LUATCS'99, Rand Afrikaans University, Johannesburg, 1999.

[8] **H.-P. Gumm**: *Birkhoff's variety theorem for coalgebras*, Contributions to General Algebra **13** (2001), 159 – 173.

[9] **H.-P. Gumm and T. Schröder**: *Covarieties and complete covarieties*, pp. 43 – 56 in "Coalgebraic Methods in Computer Science," (eds. B. Jacobs et al.), Electronic Notes in Theoretical Computer Science, vol. 11, Elsevier Science, 1998.

[10] **B. Huppert**: *Endliche Gruppen I*, Springer, Berlin, 1967.

[11] **K. W. Johnson**: *Some historical aspects of the representation theory of groups and its extension to quasigroups*, pp. 101 – 117 in "Universal Algebra and Quasigroup Theory," (eds. A. Romanowska and J.D.H. Smith), Heldermann, Berlin, 1992.

[12] **W. D. Neumann**: *On the quasivariety of convex subsets of affine spaces*, Arch. Math. **21** (1970), 11 – 16.

[13] **R. Penrose**: *A generalised inverse for matrices*, Proc. Camb. Phil. Soc. **51** (1955), 406 – 413.

[14] **H. O. Pflugfelder**: *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.

[15] **A. B. Romanowska and J. D. H. Smith**: *Modal Theory*, Heldermann, Berlin, 1985.

[16] **A. B. Romanowska and J. D. H. Smith**: *Modes*, World Scientific, Singapore, 2002.

[17] **J. J. M. M. Rutten**: *Universal coalgebra: a theory of systems*, Theoret. Comput. Sci. **249** (2000), 3 – 80.

[18] **J. D. H. Smith**: *Representation Theory of Infinite Groups and Finite Quasigroups*, Université de Montréal, Montreal, 1986.

[19] **J. D. H. Smith**: *Combinatorial characters of quasigroups*, pp. 163 – 187 in "Coding Theory and Design Theory, Part I: Coding Theory," (ed. D. Ray-Chaudhuri), Springer, New York, NY, 1990.

[20] **J. D. H. Smith**: *Quasigroup actions: Markov chains, pseudoinverses, and linear representations*, Southeast Asian Bull. Math. **23** (1999), 719 – 729.

[21] **J. D. H. Smith**: *Quasigroup homogeneous spaces and linear representations*, J. Alg. **241** (2001), 193 – 203.

[22] **J. D. H. Smith**: *Permutation representations of loops*, J. Alg., to appear.

[23] **J. D. H. Smith and A. B. Romanowska**: *Post-Modern Algebra*, Wiley, New York, NY, 1999.

Department of Mathematics
Iowa State University
Ames
Iowa 50011
U.S.A.
e-mail: jdhsmith@math.iastate.edu
http://www.math.iastate.edu/jdhsmith/

Received March 10, 2003