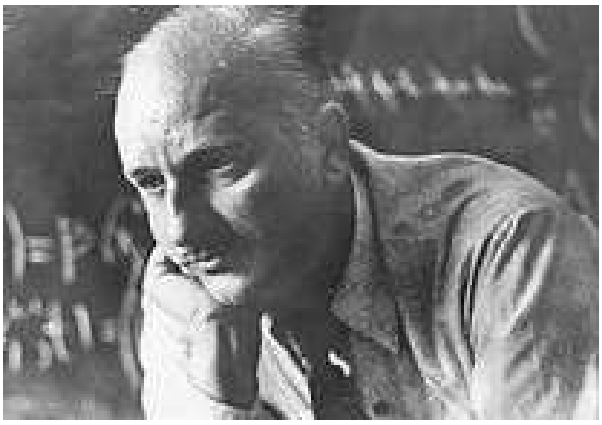
BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 3–6
ISSN 1024–7696

Valentin Belousov (20.02.1925 – 23.07.1988)



The present issue of the journal "Buletinul Academiei de Stiinte a Republicii Moldova, Matematica" is devoted to the 90th anniversary of Valentin D. Belousov.

In 2015 the mathematical community celebrated the 90th anniversary of Valentin Belousov. Since the late 70s of XX century V. Belousov became one of the world's leading specialists in the theory of quasigroups and loops. He created a successful school in this direction in the former Soviet Union. Belousov's major contribution in mathematics refers as well to the theory of functional equations, algebraic nets and combinatorial analysis.

Valentin Belousov was born on February 20, 1925, in Balti, a town in the north of the Republic of Moldova. His father, Daniil A. Belousov graduated from a military school in Tiflis and, before the October Revolution in Russia, was an officer in the Russian tsarist army. After the revolution he immigrated to Moldova, which returned to Romania during 1918–1944. In Balti Belousov parents worked at a post office, but his father worked also, for a period, at an oil factory. Valentin Belousov spent his early childhood with his grandparents in Soroca town. He graduated from primary and secondary schools and from "Ion Creanga" Lyceum (1944) in Balti. On March 1944, during the Second World War, the Balti Oil Factory and its workers were evacuated to another district of Romania, where Belousov family lived till November 1944. Valentin Belousov applied for studies (passed examinations) at the Polytechnical University of Bucharest, being the second in the list of admitted students. After Bessarabia retrocession in August 1944, Belousov family returned to Balti, that time part of the Soviet Union, and in December 1944 he started his studies at the Pedagogical Institute in Chisinau (1944-1947). Still a student, Belousov was involved in teaching at the preparatory department of this institute (1947–1948). In

1948, for personal reasons, he leaved Chisinau for the village Sofia, near Balti, where he worked as a teacher and a manager, responsible for studies, at the secondary school. Here he began his research on functional equations on quasigroups. As Belousov mentioned, he has chosen quasigroups as his area of research due to the book "The theory of Generalized Groups"(Harkov-Kiev, 1937), by Sushkevich, which he found accidentally, in a second-hand market. In 1950 he began his work at the Pedagogical Institute of Balti. During 1954–1955 V. Belousov was delegated for an internship, for qualification courses, at "M. V. Lomonosov" State University in Moscow, where he became later a PhD student (1955–1956), under the supervision of Prof. Alexandr Kurosh. In 1958 Belousov defended his PhD dissertation "Research in the theory of quasigroups and loops" at "M. V. Lomonosov" State University. After doctoral studies he continued his activity at Balti Pedagogical Institute, in the position of a lecturer (1957–1960), and head of the Chair of Mathematics (1961–1962). During October 1960 – July 1961 he was delegated for an internship to the University of Wisconsin, Madison State, USA, to Prof. R. H. Bruck. In 1966 he successfully defended his second doctoral thesis "Systems of quasigroups with identities" at "M. V. Lomonosov" State University in Moscow.

In 1962 V. Belousov began his activity at the Institute of Mathematics of the Academy of Sciences of Moldova. Since 1963 he led the Department of algebra and mathematical logics and after, the Department of theory of quasigroups and combinatorial analysis (until 1986), the first and the only research department in this area in the former Soviet Union. The last two years of life he worked as a principal researcher at the same institute.

A considerable part of his scientific results, obtained until 1979, was included in the monographs: Foundations of the theory of quasigroups and loops (Moscow, 1967), Algebraic nets and quasigroups (Chisinau, 1971), n-Ary Quasigroups (Chisinau, 1972), Configurations in the algebraic nets (Chisinau, 1979).

He has drawn much attention to different classes of binary quasigroups and loops, significantly developed the theory of distributive quasigroups, described the transitive distributive quasigroups (1969), and established connections between the left distributive quasigroups and Bol loops. In particular, he proved the famous theorem (Belousov Theorem, 1960): any distributive quasigroup is isotopic to a Moufang loop. This theorem plays an important role in the theory of distributive quasigroups.

V. Belousov developed the theory of quasigroups with inverse properties: F-quasigroups (1961, 1966), CI-quasigroups (1969), I-quasigroups (1987), IP-quasigroups, Bol loops and generalized Bol loops, and others. Some classes of quasigroups and loops have been introduced by him: P-quasigroups, S-loops, M-loops, linear quasigroups over groups. Many of these results are included in his monograph "Foundations of the theory of quasigroups and loops".

He dedicated a series of papers to the theory of quasigroups with balanced identities. In particular, he proved that quasigroups with irreducible balanced identities and quasigroups with partly irreducible balanced identities are isotopic to some groups (1966, 1985). In 1966 Belousov found identities, in the e-quasigroup, which

represent the necessary and sufficient conditions when a quasigroup is isotopic to a group, and respectively, to an abelian group.

Belousov studied systems of quasigroups with different generalized identities (generalized lows of associativity, mediality, transitivity, distributivity and generalized Stein identity (S-systems)). The main part of his second doctoral dissertation is devoted to systems of quasigroups with generalized identities.

A special contribution was brought to the theory of functional equations on quasigroups, such as functional equations of generalized associativity, distributivity, mediality, the functional Moufang equation, etc. Connected with the functional equation of generalized associativity, Belousov proved a theorem that bears his name (Belousov's theorem "about four quasigroups"): if four quasigroup operations satisfy the generalized associative law, then they are isotopic to the same group (1958–1961). This theorem has many applications. In 1960 he published the solution of the functional equation of generalized mediality on binary quasigroups and in 1976 on quasigroups of arity greater than two. In 1970–1973 Belousov gave the general solution of the functional equation of generalized associativity on quasigroup operations of arity not less than two. In 1976 he gave a complete solution for the balanced functional equation of genus 2 for quasigroups of any arity. At present, balanced equations with a special condition on subwords, are called Belousov equations.

V. Belousov investigated connections between the functional equation of generalized associativity and some special partial algebras, which were called positional algebras of quasigroups. These algebras are called today Belousov's algebras. The identities in positional algebras are functional equations of genus 1 (in positional algebras on quasigroup operations) or of genus 2 (in the positional algebras on quasigroups with substitutions). In 1971 Belousov proved that any positional algebra can be imbedded in a positional algebra with substitutions, and in 1972 the functional equation of generalized associativity of genus 2 was reduced to a functional equation of genus 1. The theory of positional algebras is included in the monograph "n-Ary quasigroups".

A large number of papers are devoted to the study of n-ary and infinite-ary quasigroups. In fact, V. Belousov created the theory of n-quasigroups, which generalizes many results that occur in binary case, but it does also reflect the specific properties of n-ary quasigroups. The monograph "n-Ary quasigroups" includes the study of a series of classes of n-ary quasigroups, such as IP-quasigroups, TS-quasigroups, Menger quasigroups, Dicker quasigroups, (i, j)-associative quasigroups.

V. Belousov granted special attention to the geometrical aspects of the theory of binary and n-ary quasigroups. He developed the general theory of algebraic nets, studied many closing conditions and configurations in algebraic nets, developed methods of investigation of the algebraic configurations (1959–1979). Its main results on algebraic nets are contained in the monographs "Algebraic nets and quasigroups" and "Configurations in the algebraic nets".

The research related to the combinatorial aspects of the theory of quasigroups is devoted to the problem of extending finite quasigroups, orthogonal binary and n-ary operations, orthogonal systems of operations (quasigroups), and the orthogonality

of parastrophes of quasigroups (1968–1983). In particular, V. Belousov obtained a classification of identities of length 5 with two variables (minimal identities) in 1983.

Valentin Belousov created a successful school in the theory of quasigroups and loops in the former Soviet Union. Many of his results, ideas and techniques have been developed and generalized by his disciples and many specialists in the theory of quasigroups and loops. Twenty three PhD theses have been defended under Belousov's supervision by: I. Florya (1966), M. Sandic (1966), A. Basarab (1968), E. Sokolov (1969), G. Belyavskaya (1970), A. Ceban (1972), V. Dementieva (1972), M. Chitoroaga (1972), B. Turcan (1972), V. Onoi (1973), Iu. Movsisyan (1974), T. Yakubov (1975), N. Sandu (1979), Iu. Sharkov (1981), V. Beglaryan (1982), S. Murathudjaev (1982), P. Gorinchioi (1982), F. Sohatskii (1986), I. Leah (1986), W. Dudek (1990), V. Shcherbakov (1991), V. Izbash (1992), L. Ursu (1993).

V. Belousov was a member of editorial boards of the mathematical journals "Aecuationes Mathematicae" and "Buletinul Academiei de Stiinte a Moldovei". He also was one of the editors of the known series of collected works "Matematiceskie issledovanija" published by the Academy of Sciences of Moldova.

During his life V. Belousov was actively involved in teaching: in 1964–1966 as an associate professor and a head of the Chair of Mathematics at the Polytechnical Institute in Chisinau (he initiated the foundation of this chair), also as a professor (1966-1988) and a head of the Department of Higher Algebra (until 1977) at the Chisinau State University (at present Moldova State University). In 1968 he was elected a corresponding member of the Academy of Pedagogical Sciences of the former Soviet Union. He participated in various community activities as a deputy of Supreme Council of the republic, member of Balti City Council, led the Student Scientific Society "Viitorul", and was one of the main organizers of the national mathematical Olympiads. During the life for his important scientific achievements and active social life Professor Belousov was awarded the State Prize of MSSR (1982) and many honorary titles and state awards. He died on July 23 1988, of cirrhosis, at the State Chancellery hospital in Chisinau.

His wife, Elizaveta (1925–1991) was a philologist and a teacher at Moldova State University. His son Alexander (1948–1998) was a physicist (PhD in Physics) and his daughter Tatiana is a doctor neuropathologist.

Those who knew Valentin Belousov, characterize him as a brilliant mathematician with an excellent mathematical intuition, having an extensive knowledge in different areas, very generous, positive and friendly, a scientist who devoted his life to mathematics.

M. Choban, V. Izbash, V. Shcherbacov, P. Syrbu

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 7–23
ISSN 1024–7696

Belousov's Theorem and the quantum Yang-Baxter equation

Jonathan D. H. Smith

Abstract. Quantum quasigroups are self-dual objects that provide a general framework for the nonassociative extension of quantum group techniques. Within this context, the classical theorem of Belousov on the isotopy of distributive quasigroups and commutative Moufang loops is reinterpreted to yield solutions of the quantum Yang-Baxter equation. A new concept of principal bimagma isotopy is introduced.

Mathematics subject classification: 20N05, 16T25.
Keywords and phrases: Belousov theorem, quasigroup, loop, quantum Yang-Baxter equation, quantum quasigroup, distributive, isotopy.

1 Introduction

In the 1960s, Belousov published his now classic theorem on the isotopy of distributive quasigroups and commutative Moufang loops [1, Teorema 1], [2, Teorema 8.1]. The theorem states that for each element e of a given distributive quasigroup $(Q, \cdot)$, the operation $x + y = xR(e)^{-1} \cdot yL(e)^{-1}$ defines a commutative Moufang loop on Q, with identity element e. In the following decade, Belousov's Theorem became a key step in showing how a purely group-theoretic result of Fischer [6], on the nilpotence of the derived subgroup G' of a group G generated by a class of involutions whose products have order 3, could be proved entirely by quasigroup-theoretical methods [8]. The current paper sets out to explore further new aspects of Belousov's Theorem, showing how it leads to solutions of the quantum Yang-Baxter equation within the theory of quantum quasigroups.

The self-dual concept of a quantum quasigroup was introduced recently as a far-reaching unification of Hopf algebras and quasigroups [11]. Let $(\mathbf{V}, \otimes, \mathbf{1})$ be a symmetric monoidal category (§2). For example, one might take a category of vector spaces under the usual tensor product, or the category of sets under the cartesian product. Consider a *bimagma* (A, ∇, Δ), an object of $\mathbf{V}$ equipped with morphisms providing a *magma* structure $\nabla\colon A \otimes A \to A$ and a *comagma* structure $\Delta\colon A \to A \otimes A$ such that Δ is a magma homomorphism. Then the definition of a *quantum quasigroup* requires the invertibility of two dual endomorphisms of the tensor square of the bimagma object: the *left composite*

$$\mathsf{G}\colon A \otimes A \xrightarrow{\Delta \otimes 1_A} A \otimes A \otimes A \xrightarrow{1_A \otimes \nabla} A \otimes A$$

and the *right composite*

$$\supset\colon A \otimes A \xrightarrow{\Delta \otimes 1_A} A \otimes A \otimes A \xrightarrow{1_A \otimes \nabla} A \otimes A \ .$$

The quantum Yang-Baxter equation (QYBE) is

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12} \tag{1.1}$$

[3, §2.2C], [12]. It applies to an endomorphism

$$R\colon A \otimes A \to A \otimes A$$

of the tensor square of an object A in a symmetric, monoidal category. For a given integer $n > 1$, the notation R^{ij}, for $1 \leq i < j \leq n$, means applying R to the i-th and j-th factors in the n-th tensor power of A. Since the left and right composite morphisms are also endomorphisms of tensor squares, it is natural to seek conditions under which they satisfy the QYBE. Then, as anticipated by B. B. Venkov working in the category of sets with cartesian product [5, §9], the QYBE corresponds generally to various distributivity conditions on the products $\nabla\colon A \otimes A \to A$ appearing in the left and right composites. If the left (or right) composite of a bimagma satisfies the QYBE, then the bimagma is said to possess the property of left (or right) *quantum distributivity*.

The plan of the paper is as follows. Section 2 presents the requisite background on symmetric monoidal categories and bimagmas; Section 3 gives the background on quasigroups and quantum quasigroups. Section 4 then examines quantum distributivity of bimagmas, in particular furnishing both necessary and sufficient conditions (Theorem 4.5, Corollary 4.6) that correspond to sufficient conditions for quantum distributivity established earlier [12]. The formal similarity of the identities (4.4) and (4.7) of these results, namely

$$x(yz) = (x^R y)(x^L z) \quad \text{and} \quad (zy)x = (zx^R)(yx^L)\,,$$

with identities that appear in connection with the proof of Belousov's Theorem [2, (8.7), (8.8)], was the first indication that Belousov's Theorem might prove relevant to quantum distributivity and solution of the QYBE.

Section 5 reformulates the well-known concept of principal isotopy in terms of magmas in a symmetric monoidal category (Definition 5.1). The new concept specializes to the classical concept in the symmetric monoidal category of sets with the cartesian product (Remark 5.2). Definition 5.3 then introduces the concept of *principal bimagma isotopy*, which combines the principal isotopy of magmas with a new *enneagon condition* on the comagma side. Corollary 5.6 notes that in the category of sets with the cartesian product, any classical principal isotopy, whose components are commuting automorphisms of the domain magma of the isotopy, may be enriched to a principal bimagma isotopy simply by defining a suitable comultiplication on the underlying set of the classical principal isotopy.

Section 6 investigates preservation of quantum distributivity under principal isotopy of magmas and bimagmas. The main results (Theorem 6.1, Corollary 6.2, Theorem 6.4) include a number of apparently restrictive conditions within their hypotheses, but these conditions are both modeled on, and implemented by, the prototype of Belousov's Theorem. Indeed, the culminating Theorem 7.2 shows how the isotopy in Belousov's Theorem from a classically distributive quasigroup to a commutative Moufang loop yields a quantum distributive quantum quasigroup with the commutative Moufang loop as its magma reduct. Thus the commutative Moufang loop yields new solutions to the quantum Yang-Baxter equation that are not apparent from the classical distributivity of the original quasigroup.

For algebraic concepts and conventions that are not otherwise discussed in this paper, readers are referred to [13]. In particular, algebraic notation is used throughout the paper, with functions to the right of, or as superfixes to, their arguments. Thus compositions are read from left to right. These conventions serve to minimize the proliferation of brackets.

2 Structures in symmetric monoidal categories

The general setting for the structures studied in this paper is a symmetric monoidal category (or "symmetric tensor category" — compare [14, Ch. 11]) $(\mathbf{V}, \otimes, \mathbf{1})$. The standard example is provided by the category $\underline{\underline{K}}$ of vector spaces over a field K, under the usual tensor product. More general concrete examples are provided by varieties $\mathbf{V}$ of entropic (universal) algebras, algebras on which each (fundamental and derived) operation is a homomorphism (compare [4, 7]). These include the categories **Set** of sets and **FinSet** of finite sets (under the cartesian product), the category of pointed sets, the category $\underline{\underline{S}}$ of unital (right) modules over a commutative, unital ring S, the category of commutative monoids, and the category of semilattices.

In a monoidal category $(\mathbf{V}, \otimes, \mathbf{1})$, there is an object $\mathbf{1}$ known as the *unit object*. For example, the unit object of $\underline{\underline{K}}$ is the vector space K, while the unit object of **Set** under the cartesian product is a terminal object $\top$, a singleton. For objects A and B in a monoidal category, a *tensor product* object $A \otimes B$ is defined. For example, if U and V are vector spaces over K with respective bases X and Y, then $U \otimes V$ is the vector space with basis $X \times Y$, written as $\{x \otimes y \mid x \in X,\ y \in Y\}$. There are natural isomorphisms with components

$$\alpha_{A,B;C} \colon (A \otimes B) \otimes C \to A \otimes (B \otimes C)\,,\ \rho_A \colon A \otimes \mathbf{1} \to A\,,\ \lambda_A \colon \mathbf{1} \otimes A \to A$$

satisfying certain *coherence* conditions guaranteeing that one may as well regard these isomorphisms as identities [14, p.67]. Thus the bracketing of repeated tensor products is suppressed in this paper. In the vector space example, adding a third space W with basis Z, one has

$$\alpha_{U,V;W} \colon (x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$$

for $z \in Z$, along with $\rho_U : x \otimes 1 \mapsto x$ and $\lambda_U : 1 \otimes x \mapsto x$ for $x \in X$.

A monoidal category $(\mathbf{V}, \otimes, \mathbf{1})$ is said to be *symmetric* if there is a given natural isomorphism with *twist* components $\tau_{A,B} : A \otimes B \to B \otimes A$ such that $\tau_{A,B}\tau_{B,A} = 1_{A\otimes B}$ [14, pp.67–8]. One uses $\tau_{U,V} : x \otimes y \mapsto y \otimes x$ with $x \in X$ and $y \in Y$ in the vector space example.

Definition 2.1. Let $\mathbf{V}$ be a symmetric monoidal category.

(a.1) A *magma* in $\mathbf{V}$ is a $\mathbf{V}$-object A with a $\mathbf{V}$-morphism

$$\nabla : A \otimes A \to A$$

known as *multiplication*.

(a.2) Let A and B be magmas in $\mathbf{V}$. Then a *magma homomorphism* $f : A \to B$ is a $\mathbf{V}$-morphism such that the diagram

$$\begin{array}{ccc} A & \xleftarrow{\nabla} & A \otimes A \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f\otimes f} \\ B & \xleftarrow[\nabla]{} & B \otimes B \end{array}$$

commutes.

(b.1) A *comagma* in $\mathbf{V}$ is a $\mathbf{V}$-object A with a $\mathbf{V}$-morphism

$$\Delta : A \to A \otimes A$$

known as *comultiplication*.

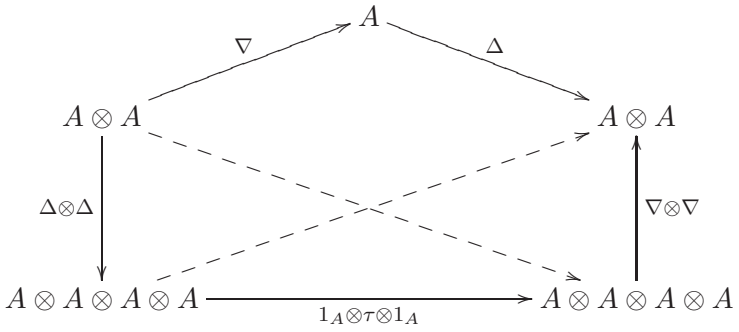
(b.2) Let A and B be comagmas in $\mathbf{V}$. A *comagma homomorphism* $f : A \to B$ is a $\mathbf{V}$-morphism such that the diagram

$$\begin{array}{ccc} B & \xrightarrow{\Delta} & B \otimes B \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle f\otimes f} \\ A & \xrightarrow[\Delta]{} & A \otimes A \end{array}$$

commutes.

(c) A *bimagma* (A, ∇, Δ) in $\mathbf{V}$ is a magma (A, ∇) and comagma (A, Δ) in $\mathbf{V}$ such that the following *bimagma diagram* commutes:

(2.1)



Remark 2.2. (a) The arrow across the bottom of the bimagma diagram (2.1) makes use of the twist isomorphism $\tau_{A,A}$ or $\tau\colon A \otimes A \to A \otimes A$.

(b) Commuting of the bimagma diagram (2.1) in a bimagma (A, ∇, Δ) means that

$$\Delta\colon (A, \nabla) \to \big(A \otimes A, (1_A \otimes \tau \otimes 1_A)(\nabla \otimes \nabla)\big)$$

is a magma homomorphism (commuting of the upper left-hand solid and dotted quadrilateral), or equivalently, that

$$\nabla\colon \big(A \otimes A, (\Delta \otimes \Delta)(1_A \otimes \tau \otimes 1_A)\big) \to (A, \Delta)$$

is a comagma homomorphism (commuting of the upper right-hand solid and dotted quadrilateral).

(c) If $\mathbf{V}$ is an entropic variety of universal algebras, the comultiplication of a comagma in $\mathbf{V}$ may be written as

$$\Delta\colon A \to A \otimes A; a \mapsto \big((a^{L_1} \otimes a^{R_1}) \dots (a^{L_{n_a}} \otimes a^{R_{n_a}})\big) w_a \tag{2.2}$$

in a universal-algebraic version of the well-known *Sweedler notation*. In (2.2), the *tensor rank* of the image of a (or any such general element of $A \otimes A$) is the smallest arity n_a of the derived word w_a expressing the image (or general element) in terms of elements of the generating set $\{b \otimes c \mid b, c \in A\}$ for $A \otimes A$. A more compact but rather less explicit version of Sweedler notation, generally appropriate within any concrete monoidal category $\mathbf{V}$, is $a\Delta = a^L \otimes a^R$, with the understanding that the tensor rank of the image is not implied to be 1.

(d) Magma multiplications on an object A of a concrete monoidal category are often denoted by juxtaposition, namely $(a \otimes b)\nabla = ab$, or with $a \cdot b$ as an infix notation, for elements a, b of A.

(e) With the notations of (c) and (d), commuting of the bimagma diagram (2.1) in a concrete bimagma (A, ∇, Δ) amounts to

$$a^L b^L \otimes a^R b^R = (ab)^L \otimes (ab)^R \tag{2.3}$$

for a, b in A.

3 Quantum quasigroups

While one- or two-sided quasigroups may be defined either equationally or combinatorially, it is actually the combinatorial definition of these structures which is "quantized" into the definition of quantum quasigroups, so here it suffices to recall the classical combinatorial definitions. Thus a *quasigroup* $(Q, \cdot)$ is defined as a set Q that is equipped with a binary *multiplication* operation denoted by $\cdot$ or simple juxtaposition of the two arguments, where specification of any two of x, y, z in the equation $x \cdot y = z$ determines the third uniquely. Such a binary

multiplication $Q \times Q \to Q; (x, y) \mapsto xy$ will often be written as a magma structure $\nabla\colon Q \otimes Q \to Q; x \otimes y \mapsto xy$ in notation for the symmetric monoidal category $(\mathbf{Set}, \times, \top)$ of sets under the cartesian product. In particular, note that tensor products of elements just correspond here to tuples. For example, $x \otimes y \otimes z$ is the ordered triple (x, y, z).

A *left quasigroup* $(Q, \cdot)$ is a set Q with a multiplication such that in the equation $a \cdot x = b$, specification of a and b determines x uniquely. The definition of *right quasigroups* is chirally dual: In the equation $x \cdot a = b$, specification of a and b determines x uniquely. If Q is a set, the right projection product $xy = y$ yields a left quasigroup structure on Q, while the left projection product $xy = x$ yields a right quasigroup structure.

Definition 3.1. Let (A, ∇, Δ) be a bimagma in a symmetric monoidal category $(\mathbf{V}, \otimes, \mathbf{1})$.

(a) On (A, ∇, Δ), the endomorphism

$$\mathsf{G}\colon A \otimes A \xrightarrow{\Delta \otimes 1_A} A \otimes A \otimes A \xrightarrow{1_A \otimes \nabla} A \otimes A \tag{3.1}$$

of $A \otimes A$ is known as the *left composite* morphism.

(b) On (A, ∇, Δ), the endomorphism

$$\mathfrak{d}\colon A \otimes A \xrightarrow{1_A \otimes \Delta} A \otimes A \otimes A \xrightarrow{\nabla \otimes 1_A} A \otimes A \tag{3.2}$$

of $A \otimes A$ is known as the *right composite* morphism.

Definition 3.2. Consider a symmetric monoidal category $(\mathbf{V}, \otimes, \mathbf{1})$.

(a) A *left quantum quasigroup* (A, ∇, Δ) in $\mathbf{V}$ is a bimagma in $\mathbf{V}$ for which the left composite morphism G is invertible.

(b) A *right quantum quasigroup* (A, ∇, Δ) in $\mathbf{V}$ is a bimagma in $\mathbf{V}$ for which the right composite morphism $\mathfrak{d}$ is invertible.

(c) A *quantum quasigroup* (A, ∇, Δ) in $\mathbf{V}$ is a bimagma in $\mathbf{V}$ where both G and $\mathfrak{d}$ are invertible.

Since these basic definitions are expressed entirely within the structure of a symmetric, monoidal category, their concepts are maintained under the so-called symmetric, monoidal functors which preserve that structure. A typical example of such a functor is given by the free monoid functor from sets under cartesian products to the category of modules over a commutative ring, with the usual tensor product.

Proposition 3.3. *Suppose that* $(\mathbf{V}, \otimes, \mathbf{1_V})$ *and* $(\mathbf{W}, \otimes, \mathbf{1_W})$ *are symmetric monoidal categories. Let* $F\colon \mathbf{V} \to \mathbf{W}$ *be a symmetric monoidal functor. If* (A, ∇, Δ) *is a left, right, or two-sided quantum quasigroup in* $(\mathbf{V}, \otimes, \mathbf{1_V})$*, the structure* (AF, ∇^F, Δ^F) *is a respective left, right, or two-sided quantum quasigroup in* $(\mathbf{W}, \otimes, \mathbf{1_W})$.

Theorem 3.4. *Consider the symmetric, monoidal category* $(\mathbf{FinSet}, \times, \top)$ *of finite sets under the cartesian product.*

(a) *Left quantum quasigroups* $(Q, \nabla, \Delta\colon x \mapsto x^L \otimes x^R)$ *in* $(\mathbf{FinSet}, \times, \top)$ *are equivalent to triples* (A, L, R) *that consist of a left quasigroup* (Q, ∇) *with an automorphism* L *and endomorphism* R *[10].*

(b) *The quantum quasigroups* $(Q, \nabla, \Delta\colon x \mapsto x^L \otimes x^R)$ *in* $(\mathbf{FinSet}, \times, \top)$ *are equivalent to triples* (Q, L, R) *consisting of a quasigroup* (Q, ∇) *equipped with automorphisms* L *and* R *[11].*

Corollary 3.5. *[10] Given a left quasigroup* $(Q, \cdot)$ *with an automorphism* L *and endomorphism* R*, define* $\nabla\colon Q \otimes Q \to Q; x \otimes y \mapsto xy$ *as a multiplication and* $\Delta\colon Q \to Q \otimes Q; x \mapsto x^L \otimes x^R$ *as a comultiplication. Then* (Q, ∇, Δ) *is a left quantum quasigroup in* $(\mathbf{Set}, \times, \top)$*.*

Corollary 3.6. *[11] Suppose that* $(Q, \cdot)$ *is a quasigroup equipped with two automorphisms* L *and* R*. Define* $\nabla\colon Q \otimes Q \to Q; x \otimes y \mapsto xy$ *as a multiplication and* $\Delta\colon Q \to Q \otimes Q; x \mapsto x^L \otimes x^R$ *as a comultiplication. Then* (Q, ∇, Δ) *is a quantum quasigroup in* $(\mathbf{Set}, \times, \top)$*.*

4 Quantum distributivity

Definition 4.1 ([12])**.** Suppose that (A, ∇, Δ) is a bimagma in a symmetric, monoidal category.

(a) The bimagma (A, ∇, Δ) is said to satisfy the condition of *quantum left distributivity* if the left composite G of (A, ∇, Δ) satisfies the quantum Yang-Baxter equation (1.1).

(b) The bimagma (A, ∇, Δ) is said to satisfy the condition of *quantum right distributivity* if the right composite $\eth$ of (A, ∇, Δ) satisfies the quantum Yang-Baxter equation (1.1).

(c) The bimagma (A, ∇, Δ) satisfies the condition of *quantum distributivity* if it has both the left and right quantum distributivity properties.

Since the quantum distributivity concepts of Definition 4.1 are written entirely in the language of symmetric monoidal categories, one immediately obtains the following analogue of Proposition 3.3.

Proposition 4.2. *Suppose that* $(\mathbf{V}, \otimes, \mathbf{1_V})$ *and* $(\mathbf{W}, \otimes, \mathbf{1_W})$ *are symmetric monoidal categories. Let* $F\colon \mathbf{V} \to \mathbf{W}$ *be a symmetric monoidal functor. If* (A, ∇, Δ) *is a left, right, or two-sided distributive bimagma in* $(\mathbf{V}, \otimes, \mathbf{1_V})$*, then the structure* (AF, ∇^F, Δ^F) *becomes a respective left, right, or two-sided quantum distributive bimagma in* $(\mathbf{W}, \otimes, \mathbf{1_W})$*.*

The explicit results of this paper are predominantly concerned with obtaining quantum distributivity, and therefore solutions of the QYBE, in the symmetric monoidal category $(\mathbf{Set}, \otimes, \top)$ of sets with the cartesian product. On the other hand, one is generally interested in solving the QYBE within the symmetric monoidal category $(\underline{\underline{K}}, \otimes, K)$ of unital modules over a commutative, unital ring K. To this end, one may apply Proposition 4.2, with the symmetric, monoidal free monoid functor $F\colon \mathbf{Set} \to \underline{\underline{K}}$, to the quantum distributive structures in $(\mathbf{Set}, \otimes, \top)$ that are exhibited in the paper.

The terminology of Definition 4.1 is justified by the following result.

Proposition 4.3 ([5, 12])**.** *Let (Q, ∇) be a magma in the category of sets with the cartesian product. Define $\Delta\colon Q \to Q \otimes Q; x \mapsto x \otimes x$. Then the bimagma (Q, ∇, Δ) is quantum left distributive if and only if the magma (Q, ∇) is left distributive, in the classical sense that the identity*

$$x(yz) = (xy)(xz) \tag{4.1}$$

is satsified.

Proposition 4.4 ([12], Prop. 6.4)**.** *Let (Q, ∇, Δ) be a bimagma in $(\mathbf{Set}, \times, \top)$, equipped with the comultiplication $\Delta\colon Q \to Q \otimes Q; x \mapsto x^L \otimes x^R$.*

(a) *The bimagma (Q, ∇, Δ) is quantum left distributive if $LR = RL$ and the identity*

$$x^R(y^R z) = (x^{RR} y^R)(x^{RL} z) \tag{4.2}$$

is satisfied.

(b) *The bimagma (Q, ∇, Δ) is quantum right distributive if $LR = RL$ and the identity*

$$(zy^L)x^L = (zx^{LR})(y^L x^{LL}) \tag{4.3}$$

is satisfied.

Theorem 4.5. *Let (Q, ∇, Δ) be a bimagma in $(\mathbf{Set}, \times, \top)$, with comultiplication $\Delta\colon Q \to Q \otimes Q; x \mapsto x^L \otimes x^R$. Suppose that the following conditions are satisfied:*

(a) *The magma (Q, ∇) is a right quasigroup;*

(b) *The second comultiplication component $R\colon Q \to Q$ is surjective.*

Then the bimagma (Q, ∇, Δ) is quantum left distributive if and only if $LR = RL$ and the identity

$$x(yz) = (x^R y)(x^L z) \tag{4.4}$$

is satisfied.

Proof. Note that the identity (4.4) implies the identity (4.2). Then the sufficiency of (4.4), together with the commutation condition, follows by Proposition 4.4(a).

Conversely, suppose that (Q, ∇, Δ) is quantum left distributive. Consider an element $x \otimes y \otimes z$ of $Q \otimes Q \otimes Q$. Then

$$\begin{aligned} x^{LL} \otimes x^{LR} y^L \otimes x^R (y^R z) & \qquad (4.5) \\ &= \big(x^L \otimes y^L \otimes x^R (y^R z)\big) \mathsf{G}^{12} \\ &= (x \otimes y^L \otimes y^R z) \mathsf{G}^{13} \mathsf{G}^{12} \\ &= (x \otimes y \otimes z) \mathsf{G}^{23} \mathsf{G}^{13} \mathsf{G}^{12} \\ &= (x \otimes y \otimes z) \mathsf{G}^{12} \mathsf{G}^{13} \mathsf{G}^{23} \\ &= (x^L \otimes x^R y \otimes z) \mathsf{G}^{13} \mathsf{G}^{23} \\ &= (x^{LL} \otimes x^R y \otimes x^{LR} z) \mathsf{G}^{23} \\ &= x^{LL} \otimes (x^R y)^L \otimes (x^R y)^R (x^{LR} z)\,. \qquad (4.6) \end{aligned}$$

Since (Q, ∇, Δ) is a bimagma, (2.3) implies that the maps L and R are endomorphisms of the right quasigroup (Q, ∇). Since the respective middle factors of (4.5) and (4.6) agree, one has $x^{LR} y^L = x^{RL} y^L$. Canceling y^L in the right quasigroup (Q, ∇) then yields $x^{LR} = x^{RL}$, so the commutation condition $LR = RL$ holds. Since the respective final factors of (4.5) and (4.6) agree, the identity (4.2) is satisfied. The surjectivity of $R\colon Q \to Q$ then implies that (4.4) is satisfied. □

The chiral dual of Theorem 4.5 is formulated as follows.

Corollary 4.6. *Let (Q, ∇, Δ) be a bimagma in $(\mathbf{Set}, \times, \top)$, with comultiplication $\Delta\colon Q \to Q \otimes Q; x \mapsto x^L \otimes x^R$. Suppose that the following conditions are satisfied:*

(a) *The magma (Q, ∇) is a left quasigroup;*

(b) *The first comultiplication component $L\colon Q \to Q$ is surjective.*

Then the bimagma (Q, ∇, Δ) is quantum right distributive if and only if $LR = RL$ and the identity

$$(zy)x = (zx^R)(yx^L) \qquad (4.7)$$

is satisfied.

Extracting details from the necessity proof in Theorem 4.5 yields the following.

Corollary 4.7. *Let (Q, ∇, Δ) be a bimagma in $(\mathbf{Set}, \times, \top)$, with comultiplication $\Delta\colon Q \to Q \otimes Q; x \mapsto x^L \otimes x^R$ satisfying $LR = RL$.*

(a) *Suppose that the second comultiplication component $R\colon Q \to Q$ is surjective. Then the identity (4.4) is satisfied if the bimagma (Q, ∇, Δ) is quantum left distributive.*

(b) *Suppose that the first comultiplication component $L\colon Q \to Q$ is surjective. Then the identity (4.7) is satisfied if the bimagma (Q, ∇, Δ) is quantum right distributive.*

5 Principal isotopy

Definition 5.1. Consider a symmetric monoidal category $(\mathbf{V}, \otimes, \mathbf{1})$. Let (A, ∇_i) be a magma in $(\mathbf{V}, \otimes, \mathbf{1})$, for $i = 1, 2$. Then an automorphism ϕ of the object $A \otimes A$ of $\mathbf{V}$ is a *principal magma isotopy*

$$\phi \colon (A, \nabla_1) \rightsquigarrow (A, \nabla_2)$$

in $(\mathbf{V}, \otimes, \mathbf{1})$ if the diagram

$$\begin{array}{ccccc} & & Q & & \\ & \overset{\nabla_2}{\nearrow} & & \overset{\nabla_1}{\nwarrow} & \\ A \otimes A & & \xrightarrow[\phi]{} & & A \otimes A \end{array} \tag{5.1}$$

commutes in $\mathbf{V}$.

Remark 5.2. Suppose that $(Q, \nabla_i \colon x \otimes y \mapsto x \circ_i y)$ are magmas on an object Q of $(\mathbf{Set}, \times, \top)$ for $i = 1, 2$. Then if $f \otimes g \colon (Q, \nabla_1) \rightsquigarrow (Q, \nabla_2)$ is a principal isotopy in $(\mathbf{Set}, \times, \top)$ for automorphisms f, g of Q, one has

$$x \circ_2 y = x^f \circ_1 y^g \tag{5.2}$$

for $x, y \in Q$, as usual for a classical principal isotopy [2, p.13], [9, p.5].

Definition 5.3. Consider a symmetric monoidal category $(\mathbf{V}, \otimes, \mathbf{1})$. Let (A, ∇_i, Δ_i) be a bimagma in $(\mathbf{V}, \otimes, \mathbf{1})$, for $i = 1, 2$. Then an automorphism ϕ of the object $A \otimes A$ of $\mathbf{V}$ is a *principal bimagma isotopy*

$$\phi \colon (A, \nabla_1, \Delta_1) \rightsquigarrow (A, \nabla_2, \Delta_2)$$

in $(\mathbf{V}, \otimes, \mathbf{1})$ if the *decagon diagram*

$$\begin{array}{ccccccc} & & & A & & & \\ & & \overset{\nabla_2}{\nearrow} & & \overset{\nabla_1}{\nwarrow} & & \\ & A^{\otimes 2} & & \xrightarrow[\phi]{} & & A^{\otimes 2} & \\ {\scriptstyle \Delta_2 \otimes \Delta_2}\downarrow & & & & & & \downarrow{\scriptstyle \Delta_1 \otimes \Delta_1} \\ A^{\otimes 4} & & & A^{\otimes 4} & & & A^{\otimes 4} \\ {\scriptstyle \tau \otimes \tau}\downarrow & & {\scriptstyle \tau \otimes \tau}\nearrow & & {\scriptstyle 1_A \otimes \tau \otimes 1_A}\searrow & & \uparrow{\scriptstyle 1_A \otimes \tau \otimes 1_A} \\ A^{\otimes 4} & \xrightarrow[\phi^{\otimes 2}]{} & A^{\otimes 4} & & A^{\otimes 4} & \xrightarrow[\phi^{\otimes 2}]{} & A^{\otimes 4} \end{array} \tag{5.3}$$

commutes in $\mathbf{V}$. Here, the superfix $^{\otimes r}$ is used for the r-th tensor power of an object or morphism in $\mathbf{V}$. The lower part of the decagon diagram is called the *nonagon diagram* or *enneagon diagram*.

Remark 5.4. Note that the upper triangle in the decagon diagram is just the diagram (5.1). Thus a principal bimagma isotopy

$$\phi\colon (A, \nabla_1, \Delta_1) \rightsquigarrow (A, \nabla_2, \Delta_2)$$

includes a principal magma isotopy $\phi\colon (A, \nabla_1) \rightsquigarrow (A, \nabla_2)$.

Proposition 5.5. *Suppose that $(Q, \nabla_i, \Delta_i\colon x \mapsto xL_i \otimes xR_i)$, for $i = 1, 2$, are bimagmas in $(\mathbf{Set}, \times, \top)$, with permutations $f\colon Q \to Q$ and $g\colon Q \to Q$. Then the validity of the equations*

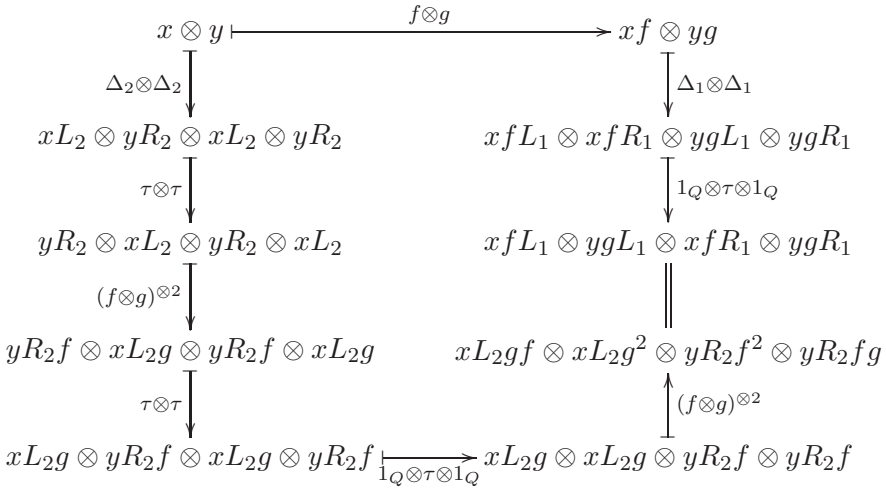
$$L_2gf = fL_1\,, \quad L_2g^2 = gL_1\,, \quad R_2f^2 = fR_1\,, \quad R_2fg = gR_1 \tag{5.4}$$

is equivalent to the commuting of the enneagon diagram (5.3) *for a principal bimagma isotopy*

$$f \otimes g\colon (Q, \nabla_1, \Delta_1) \rightsquigarrow (Q, \nabla_2, \Delta_2)$$

composed from $f\colon Q \to Q$ and $g\colon Q \to Q$.

Proof. For an element x of Q, the commuting of the enneagon diagram (5.3) gives



which is equivalent to the equations

$$L_2gf = fL_1\,, \quad L_2g^2 = gL_1\,, \quad R_2f^2 = fR_1\,, \quad R_2fg = gR_1$$

holding in the endomorphism monoid of the set Q. □

Corollary 5.6. *Consider a magma $(Q, \nabla_1\colon x \otimes y \mapsto x \cdot y)$ in $(\mathbf{Set}, \times, \top)$, with commuting automorphisms f and g.*

(a) *There is a bimagma*

$$(Q, \nabla_1\colon x \otimes y \mapsto x \cdot y, \Delta_1\colon x \mapsto x \otimes x)$$

in $(\mathbf{Set}, \times, \top)$.

(b) *There is a bimagma*

$$(Q, \nabla_2 \colon x \otimes y \mapsto xf \cdot yg, \Delta_2 \colon x \mapsto xg^{-1} \otimes xf^{-1})$$

in $(\mathbf{Set}, \times, \top)$.

(c) *There is a principal bimagma isotopy*

$$f \otimes g \colon (Q, \nabla_1, \Delta_1) \rightsquigarrow (Q, \nabla_2, \Delta_2)\,.$$

Proof. (a) Trivially, (2.3) holds for $L = R = 1$.

(b) Applying (2.3) to (Q, ∇_2, Δ_2), note that

$$\begin{aligned}(xg^{-1} \otimes yg^{-1})\nabla_2 \otimes (xf^{-1} \otimes yf^{-1})\nabla_2 \\ &= (xg^{-1}f \cdot yg^{-1}g) \otimes (xf^{-1}f \cdot yf^{-1}g) \\ &= (xf \cdot yg)g^{-1} \otimes (xf \cdot yg)f^{-1} \\ &= (x \otimes y)\nabla_2 g^{-1} \otimes (x \otimes y)\nabla_2 f^{-1}\end{aligned}$$

for x, y in Q, so that (Q, ∇_2, Δ_2) is a bimagma.

(c) With $L_1 = R_1 = 1_Q$ and $L_2 = g^{-1}$, $R_2 = f^{-1}$, the equations (5.4) hold. □

Remark 5.7. In Corollary 5.6(b), duality interchanges and inverts the respective components f, g of the magma isotopy to yield the corresponding components g^{-1}, f^{-1} of the comultiplication.

6 Isotopy of quantum distributive structures

This section investigates the preservation of quantum distributivity under principal isotopy. The conditions assembled in the hypotheses of its theorems are seen to appear naturally in the following section, within the context of Belousov's Theorem.

Theorem 6.1. *Suppose that* $(Q, \nabla_i \colon x \otimes y \mapsto x \circ_i y, \Delta_i \colon x \mapsto x^{L_i} \otimes x^{R_i})$ *are bimagmas on an object* Q *of* $(\mathbf{Set}, \times, \top)$ *for* $i = 1, 2$*, such that the following conditions are satisfied:*

(a) *The comultiplication component* $R_1 \colon Q \to Q$ *is surjective;*

(b) *The comultiplication components* L_i *and* R_i *commute for* $i = 1, 2$*;*

(c) *The bimagma* (Q, ∇_1, Δ_1) *is quantum left distributive;*

(d) *There is a principal magma isotopy*

$$f \otimes g \colon (Q, \nabla_1) \rightsquigarrow (Q, \nabla_2)$$

whose components f, g *are commuting automorphisms of* (Q, ∇_1)*;*

(e) *The equations* $L_2gf = fL_1$ *and* $R_2f^2 = fR_1$ *hold.*

Then (Q, ∇_2, Δ_2) *is quantum left distributive.*

Proof. By the conditions (a)–(c), Corollary 4.7 implies that the identity (4.4) holds in (Q, ∇_1, Δ_1). For $x, y, z \in Q$, one then has

$$\begin{aligned} x \circ_2 (y \circ_2 z) &= x^f \circ_1 (y \circ_2 z)^g = x^f \circ_1 (y^f \circ_1 z^g)^g \\ &= x^f \circ_1 (y^{fg} \circ_1 z^{g^2}) \\ &= (x^{fR_1} \circ_1 y^{fg}) \circ_1 (x^{fL_1} \circ_1 z^{g^2}) \end{aligned} \tag{6.1}$$

and

$$\begin{aligned} (x^{R_2} \circ_2 y) \circ_2 (x^{L_2} \circ_2 z) &= (x^{R_2 f} \circ_1 y^g) \circ_2 (x^{L_2 f} \circ_1 z^g) \\ &= (x^{R_2 f} \circ_1 y^g)^f \circ_1 (x^{L_2 f} \circ_1 z^g)^g \\ &= (x^{R_2 f^2} \circ_1 y^{gf}) \circ_1 (x^{L_2 fg} \circ_1 z^{g^2}) \end{aligned} \tag{6.2}$$

by (5.2), the identity (4.4) in (Q, ∇_1, Δ_1), and condition (d) saying that the principal isotopy components f and g are automorphisms of (Q, ∇_1). Now the commutation condition in (d) and the equations of (e) imply the equality of (6.1) and (6.2). Thus the identities (4.4) and (4.2) hold in (Q, ∇_2, Δ_2). By the condition (b) for $i = 2$, Proposition 4.4 implies that (Q, ∇_2, Δ_2) is quantum left distributive. □

The chiral dual of Theorem 6.1 may be formulated as follows.

Corollary 6.2. *Suppose that* $(Q, \nabla_i \colon x \otimes y \mapsto x \circ_i y, \Delta_i \colon x \mapsto x^{L_i} \otimes x^{R_i})$ *are bimagmas on an object* Q *of* $(\mathbf{Set}, \times, \top)$ *for* $i = 1, 2$*, such that the following conditions are satisfied:*

(a) *The comultiplication component* $L_1 \colon Q \to Q$ *is surjective;*

(b) *The comultiplication components* L_i *and* R_i *commute for* $i = 1, 2$*;*

(c) *The bimagma* (Q, ∇_1, Δ_1) *is quantum right distributive;*

(d) *There is a principal magma isotopy*

$$f \otimes g \colon (Q, \nabla_1) \rightsquigarrow (Q, \nabla_2)$$

whose components f, g *are commuting automorphisms of* (Q, ∇_1)*;*

(e) *The equations* $L_2g^2 = gL_1$ *and* $R_2fg = gR_1$ *hold.*

Then (Q, ∇_2, Δ_2) *is quantum right distributive.*

Remark 6.3. The equations of Theorem 6.1(e) may be written as

$$\Delta_2(g \otimes f)(f \otimes f) = f\Delta_1$$

within the symmetric monoidal category $(\mathbf{Set}, \times, \top)$. Similarly, the chirally dual equations of Corollary 6.2(e) may be written as

$$\Delta_2(g \otimes f)(g \otimes g) = g\Delta_1$$

within $(\mathbf{Set}, \times, \top)$. According to Proposition 5.5, the enneagon diagram elegantly captures the conjunction of all four equations, using the isotopy $f \otimes g$. On the other hand, there does not appear to be an equally elegant or natural way to capture the respective pairs of individual equations that appear in the theorem and corollary separately.

The diverse conditions of Theorem 6.1 and Corollary 6.2 are simplified and unified in the context of quantum quasigroups within the symmetric monoidal category of finite sets and cartesian products.

Theorem 6.4. *Suppose that* $(Q, \nabla_i \colon x \otimes y \mapsto x \circ_i y, \Delta_i \colon x \mapsto x^{L_i} \otimes x^{R_i})$ *are quantum quasigroups on an object* Q *of* $(\mathbf{FinSet}, \times, \top)$ *for* $i = 1, 2$*, such that the following conditions are satisfied:*

(a) *The comultiplication components* L_i *and* R_i *commute for* $i = 1, 2$*;*

(b) *The quantum quasigroup* (Q, ∇_1, Δ_1) *is quantum distributive;*

(c) *There is a principal bimagma isotopy*

$$f \otimes g \colon (Q, \nabla_1, \Delta_1) \rightsquigarrow (Q, \nabla_2, \Delta_2)$$

whose components f, g *are commuting automorphisms of* (Q, ∇_1)*.*

Then (Q, ∇_2, Δ_2) *is quantum distributive.*

Proof. The bimagmas (Q, ∇_i, Δ_i), for $i = 1, 2$, satisfy the conditions (a)–(e) of Theorem 6.1 and Corollary 6.2:

(a) The mappings R_1 and L_1 are bijective, by Theorem 3.4(b);

(b) This is condition (a) of the current theorem;

(c) This is condition (b) of the current theorem;

(d) By Remark 5.4, this is part of condition (c) of the current theorem;

(e) The equations

$$L_2 g f = f L_1 \,, \quad L_2 g^2 = g L_1 \,, \quad R_2 f^2 = f R_1 \,, \quad R_2 f g = g R_1$$

hold by Proposition 5.5, given condition (c) of the current theorem.

Then by Theorem 6.1, (Q, ∇_2, Δ_2) is quantum left distributive. By Corollary 6.2, it is quantum right distributive. □

7 Belousov's Theorem and quantum distributivity

If e is an element of a magma $(Q,\cdot)$, one has the *left multiplication*

$$L(e)\colon Q \to Q; x \mapsto e \cdot x$$

and *right multiplication*

$$R(e)\colon Q \to Q; x \mapsto x \cdot e\,.$$

If $(Q,\cdot)$ is a left quasigroup, $L(e)$ is bijective. Similarly, if $(Q,\cdot)$ is a right quasigroup, $R(e)$ is bijective.

Lemma 7.1. *Let e be an element of a distributive quasigroup $(Q,\cdot)$.*

(a) *The left and right multiplications $L(e)$ and $R(e)$ are automorphisms of $(Q,\cdot)$ [2, p.131];*

(b) *The element e is idempotent: $ee = e$ [2, p.131];*

(c) *The multiplications $L(e)$ and $R(e)$ commute [2, (8.3)].*

Proof. (a) By distributivity, one has

$$e(xy) = (ex)(ey) \quad \text{and } (xy)e = (xe)(ye)$$

for elements x, y of Q.

(b) Note that $e(ee) = (ee)(ee)$, so $e = ee$.

(c) Let x be an element of Q. Then $xL(e)R(e) = (ex)e = (ee)(xe) = e(xe) = xR(e)L(e)$ by respective application of (a) and (b). □

Theorem 7.2. *Suppose that (Q,∇_1) is a distributive quasigroup with an element e. Set $f = R(e)^{-1}$ and $g = L(e)^{-1}$. Let (Q,∇_2) be the commutative Moufang loop with multiplication*

$$\nabla_2\colon Q \otimes Q \to Q; x \otimes y \mapsto (xf \otimes yg)\nabla_1 \tag{7.1}$$

given by Belousov's Theorem [1, Teorema 1], [2, Teorema 8.1]. Then with the comultiplication

$$\Delta_2\colon Q \to Q \otimes Q; x \mapsto x^{L(e)} \otimes x^{R(e)}\,, \tag{7.2}$$

there is a quantum distributive quantum quasigroup (Q,∇_2,Δ_2) in the symmetric monoidal category $(\mathbf{Set},\times,\top)$.

Proof. Lemma 7.1(a) implies that the respective components $L(e)$ and $R(e)$ of the comultiplication (7.2) are automorphisms of (Q,∇_1). Lemma 7.1(c) yields

$$(x \otimes y)\nabla_2 L(e) = (xf \otimes yg)\nabla_1 L(e) = \big(xfL(e) \otimes ygL(e)\big)\nabla_1$$

$$= \big(xL(e)f \otimes yL(e)g\big)\nabla_1 = (xL(e) \otimes yL(e))\nabla_2$$

and

$$\begin{aligned}(x \otimes y)\nabla_2 R(e) &= (xf \otimes yg)\nabla_1 R(e) = \big(xfR(e) \otimes ygR(e)\big)\nabla_1 \\ &= \big(xR(e)f \otimes yR(e)g\big)\nabla_1 = (xR(e) \otimes yR(e))\nabla_2\,,\end{aligned}$$

so that $L(e)$ and $R(e)$ are automorphisms of (Q, ∇_2). Corollary 3.6 then implies that (Q, ∇_2, Δ_2) is a quantum quasigroup in $(\mathbf{Set}, \times, \top)$.

Define $\Delta_1 \colon Q \to Q \otimes Q; x \mapsto x \otimes x$. Corollary 3.6 implies that (Q, ∇_1, Δ_1) is a quantum quasigroup in $(\mathbf{Set}, \times, \top)$. Then the bimagmas (Q, ∇_i, Δ_i), for $i = 1, 2$, satisfy the conditions (a)–(e) of Theorem 6.1 and Corollary 6.2:

(a) The identity mapping $R_1 = L_1 = 1_Q$ is surjective;

(b) Note $R_2L_2 = R(e)L(e) = L(e)R(e) = L_2R_2$ by Lemma 7.1(c), while of course $R_1L_1 = L_1R_1 = 1_Q$;

(c) Apply Proposition 4.3 and its chiral dual;

(d) The definition (7.1) yields a principal magma isotopy $f \otimes g$; by Lemma 7.1(c), its components commute;

(e) The equations

$$\begin{aligned}L_2gf = f = fL_1\,, \quad R_2f^2 = f = fR_1\,,\\ L_2g^2 = g = gL_1\,, \quad R_2fg = g = gR_1\end{aligned}$$

hold since $L_2 = g^{-1}$, $R_2 = f^{-1}$, and $L_1 = R_1 = 1_Q$.

By Theorem 6.1, (Q, ∇_2, Δ_2) is quantum left distributive, while by Corollary 6.2, it is quantum right distributive. □

Corollary 7.3. *In the context of Theorem 7.2, with*

$$\Delta_1 \colon Q \to Q \otimes Q; x \mapsto x \otimes x\,,$$

there is a principal bimagma isotopy

$$f \otimes g \colon (Q, \nabla_1, \Delta_1) \rightsquigarrow (Q, \nabla_2, \Delta_2)\,.$$

Proof. Apply Corollary 5.6. □

Remark 7.4. The left composite morphism of (Q, ∇_1, Δ_1) is

$$x \otimes y \mapsto x \otimes xy\,,$$

while the left composite morphism of (Q, ∇_2, Δ_2) is

$$x \otimes y \mapsto xe \otimes x \cdot yL(e)^{-1}\,.$$

These two distinct automorphisms of $Q \otimes Q$ give solutions of the QYBE in $(\mathbf{Set}, \times, \top)$. For each commutative, unital ring S, Proposition 4.2 shows that applying the free S-module functor then yields solutions of the QYBE in the module category $(\underline{\underline{S}}, \otimes, S)$.

References

[1] Belousov V. D. *On the structure of distributive quasigroups.* Mat. Sbornik, 1960, **50**, 267–298 (in Russian).

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

[3] Chari V., Pressley A. *A Guide to Quantum Groups.* Cambridge University Press, Cambridge, 1994.

[4] Davey B. A., Davis G. *Tensor products and entropic varieties.* Algebra Universalis, 1985, **21**, 68–88.

[5] Drinfeld V. G. "On some unsolved problems in quantum group theory", p. 1–8 in *Quantum Groups* (P. P. Kulish, ed.), Springer Lecture Notes in Mathematics 1510, Springer-Verlag, Berlin, 1992.

[6] Fischer B. *Distributive Quasigruppen endlicher Ordnung.* Math. Z., 1964, **83**, 267–303.

[7] Romanowska A. B., Smith J. D. H. *On Hopf algebras in entropic Jónsson-Tarski varieties.* Bull. Korean Math. Soc., 2015, **52**, 1587–1606. DOI: 10.4134/BKMS.2015.52.5.1587.

[8] Smith J. D. H. *Finite distributive quasigroups.* Math. Proc. Camb. Phil. Soc., 1976, **80**, 37–41.

[9] Smith J. D. H. *An Introduction to Quasigroups and Their Representations.* Chapman and Hall/CRC, Boca Raton, FL, 2007.

[10] Smith J. D. H. *One-sided quantum quasigroups and loops.* Demonstr. Math., 2015, **48**, 620–636. DOI: 10.1515/dema-2015-0043.

[11] Smith J. D. H. *Quantum quasigroups and loops.* J. Alg., 2016, **456**, 46–75. DOI: 10.1016/j.jalgebra.2016.02.014.

[12] Smith J. D. H. *Quantum idempotence, distributivity, and the Yang-Baxter equation.* Preprint, 2015.

[13] Smith J. D. H., Romanowska A. B. *Post-Modern Algebra.* Wiley, New York, NY, 1999.

[14] Street R. *Quantum Groups.* Cambridge University Press, Cambridge, 2007.

Jonathan D. H. Smith
Dept. of Math., Iowa State Univ.
Ames, IA 50011, U.S.A.

E-mail: *jdhsmith@iastate.edu*

Received August 23, 2015

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 24–40
ISSN 1024–7696

Central and medial quasigroups of small order

David Stanovský, Petr Vojtěchovský

Abstract. We enumerate central and medial quasigroups of order less than 128 up to isomorphism, with the exception of those quasigroups that are isotopic to $C_4 \times C_2^4$, C_2^6, C_3^4 or C_5^3. We give an explicit formula for the number of quasigroups that are affine over a finite cyclic group.

Mathematics subject classification: 20N05, 05A15.
Keywords and phrases: Medial quasigroup, entropic quasigroup, central quasigroup, T-quasigroup, abelian quasigroup, quasigroup affine over abelian group, abelian algebra, affine algebra, classification of quasigroups, enumeration of quasigroups.

This paper was written on the occasion of the 90th anniversary of Valentin Danilovich Belousov's birthday. Prof. Belousov pioneered enumerative results for quasigroups in his book "Fundametals of the theory of quasigroups and loops" and his work has been a frequent source of inspiration for the Prague algebraic school.

1 Introduction

Given an abelian group $(G, +)$, automorphisms φ, ψ of $(G, +)$, and an element $c \in G$, define a new operation $*$ on G by

$$x * y = \varphi(x) + \psi(y) + c.$$

The resulting quasigroup $(G, *)$ is said to be *affine over* $(G, +)$, and it will be denoted by $\mathcal{Q}(G, +, \varphi, \psi, c)$. Quasigroups that are affine over an abelian group are called *central quasigroups* or *T-quasigroups*. We will use the terms "quasigroup affine over an abelian group" and "central quasigroup" interchangeably. Central quasigroups are precisely the abelian quasigroups in the sense of universal algebra [15].

A quasigroup $(Q, \cdot)$ is called *medial* if it satisfies the medial law

$$(x \cdot y) \cdot (u \cdot v) = (x \cdot u) \cdot (y \cdot v).$$

Medial quasigroups are also known as *entropic* quasigroups. The fundamental Toyoda-Bruck theorem [13, Theorem 3.1] states that, up to isomorphism, medial quasigroups are precisely central quasigroups $\mathcal{Q}(G, +, \varphi, \psi, c)$ with commuting automorphisms φ, ψ.

Research partially supported by the GAČR grant 13-01832S (Stanovský), the Simons Foundation Collaboration Grant 210176 (Vojtěchovský) and the University of Denver PROF grant (Vojtěchovský).

The classification of central (or medial) quasigroups up to isotopy is trivial in the sense that it coincides with the classification of abelian groups up to isomorphism. Indeed:

- If $(G, *) = \mathcal{Q}(G, +, \varphi, \psi, c)$ is a central quasigroup then $(G, *)$ is isotopic to $(G, +)$ via the isotopism $(x \mapsto \varphi(x),\ x \mapsto \psi(x) + c,\ x \mapsto x)$.

- If two central quasigroups $Q_i = \mathcal{Q}(G_i, +_i, \varphi_i, \psi_i, c_i)$ are isotopic then the underlying groups $(G_i, +_i)$ are isotopic. But isotopic groups are necessarily isomorphic, cf. [10, Proposition 1.4].

Classifying and enumerating central and medial quasigroups up to isomorphism is nontrivial, however, and that is the topic of the present paper.

There are not many results in the literature concerning enumeration and classification of central and medial quasigroups.

Simple idempotent medial quasigroups were classified by Smith in [9, Theorem 6.1]. Sokhatsky and Syvakivskij [12] classified n-ary quasigroups affine over cyclic groups and obtained a formula for the number of those of prime order. Kirnasovsky [5] carried out a computer enumeration of central quasigroups up to order 15, and obtained more classification results in his PhD thesis [6]. Idempotent medial quasigroups of order p^k, $k \leq 4$, were classified by Hou [4, Table 1].

At the time of writing this paper, the On-line Encyclopedia of Integer Sequences [8] gives the number of medial quasigroups of order ≤ 8 up to isomorphism as the sequence A226193, and there appears to be no entry for the number of central quasigroups up to isomorphism.

Drápal [1] and Sokhatsky [11] obtained a general isomorphism theorem for quasigroups isotopic to groups, cf. [1, Theorem 2.10] and [11, Corollary 28], and for central quasigroups in particular, cf. [1, Theorem 3.2], or its restatement, Theorem 2.5. Drápal applied the machinery to calculate isomorphism classes of quasigroups of order 4 (by hand), and Kirnasovsky used Sokhatsky's theory for the calculations mentioned above. In the present paper, we use a similar approach to obtain stronger enumeration results, taking advantages of the computer system `GAP` [2].

We refer the reader to [10] for general theory of quasigroups, to [1] for a more extensive list of references on central quasigroups, to [11] for results on quasigroups isotopic to groups, to [13] for results on quasigroups affine over various kinds of loops, and to [14, 15] for a broader context on affine representation of general algebraic structures. The article [3] gives a gentle introduction into automorphism groups of finite abelian groups and points to original sources on that topic.

The paper is organized as follows.

In Section 2, we formulate an isomorphism theorem for central quasigroups, Theorem 2.4, which is less general than [1, Theorem 2.10] or [11, Corollary 28], and equivalent to but less technical than [1, Theorem 3.2]. We also present the enumeration algorithm in detail.

In Section 3, we establish our own version of [12, Theorem 2] and [1, Theorem 3.5] for cyclic p-groups, Theorem 3.1, providing an explicit formula for the number of isomorphism classes. We were informed that the same result was obtained by Kirnasovsky in his unpublished PhD thesis [6]. Since the automorphism groups of cyclic groups are commutative, Theorem 3.1 also yields the number of medial quasigroups up to isomorphism over finite cyclic groups, and of prime order in particular.

Finally, the results of the enumeration are presented in the Appendix.

2 Isomorphism theorem and enumeration algorithm

2.1 Elementary properties of the counting functions cq and mq

For an abelian group G, let $cq(G)$ (resp. $mq(G)$) denote the number of all central (resp. medial) quasigroups over G up to isomorphism. For $n \geq 1$, let $cq(n)$ (resp. $mq(n)$) denote the number of all central (resp. medial) quasigroups of order n up to isomorphism.

Let us establish two fundamental properties of the counting functions.

First, by the remarks in the introduction,

$$cq(n) = \sum_{|G|=n} cq(G) \quad \text{and} \quad mq(n) = \sum_{|G|=n} mq(G),$$

where the summations run over all abelian groups of order n up to isomorphism.

Second, Proposition 2.1 shows that the classification of central and medial quasigroups can be reduced to prime power orders. As far as enumeration is concerned, Proposition 2.1 implies that the functions cq, $mq : \mathbb{N}^+ \to \mathbb{N}^+$ are multiplicative in the number-theoretic sense.

Proposition 2.1. *Let $G = H \times K$ be an abelian group such that $\gcd(|H|, |K|) = 1$. Up to isomorphism, any quasigroup affine over G can be expressed in a unique way as a direct product of a quasigroup affine over H and a quasigroup affine over K. In particular,*

$$cq(G) = cq(H) \cdot cq(K) \quad \textit{and} \quad mq(G) = mq(H) \cdot mq(K).$$

Proof. Any automorphism of G decomposes uniquely as a direct product of an automorphism of H and an automorphism of K, cf. [3, Lemma 2.1]. The rest is easy. □

2.2 The isomorphism problem for central quasigroups

Let us now consider the isomorphism problem for quasigroups affine over a fixed abelian group $(G, +)$.

Consider any group A. (Later we will take $A = \mathrm{Aut}(G, +)$.) Then A acts on itself by conjugation, and A also acts on $A \times A$ by a simultaneous conjugation in both coordinates, i.e., $(\alpha, \beta)^\gamma = (\alpha^\gamma, \beta^\gamma)$.

Lemma 2.2. *Let A be a group. Let X be a complete set of orbit representatives of the conjugation action of A on itself. For $\xi \in X$, let Y_ξ be a complete set of orbit representatives of the conjugation action of the centralizer $C_A(\xi)$ on A. Then*

$$\{(\xi, \upsilon) : \xi \in X,\, \upsilon \in Y_\xi\}$$

is a complete set of orbit representatives of the conjugation action of A on $A \times A$.

Proof. For every $(\alpha, \beta) \in A \times A$ there is a unique $\xi \in X$ and some $\gamma \in A$ such that (α, β) and (ξ, γ) are in the same orbit. For a fixed $\xi \in X$ and some β, $\gamma \in A$, we have (ξ, β) in the same orbit as (ξ, γ) if and only if there is $\delta \in C_A(\xi)$ such that $\beta^\delta = \gamma$. □

Lemma 2.3. *Let $(G, +)$ be an abelian group, $A = \mathrm{Aut}(G, +)$ and α, $\beta \in A$. Then $C_A(\alpha) \cap C_A(\beta)$ acts naturally on $G/\mathrm{Im}(1 - \alpha - \beta)$.*

Proof. Let $U = \mathrm{Im}(1 - \alpha - \beta)$. It suffices to show that for every $\gamma \in C_A(\alpha) \cap C_A(\beta)$ the mapping $u + U \mapsto \gamma(u) + U$ is well-defined. Now, if $u + U = v + U$ then $u = v + w - \alpha(w) - \beta(w)$ for some $w \in G$ and we have $\gamma(u) = \gamma(v) + \gamma(w) - \gamma\alpha(w) - \gamma\beta(w) = \gamma(v) + \gamma(w) - \alpha\gamma(w) - \beta\gamma(w) = \gamma(v) + (1 - \alpha - \beta)(\gamma(w)) \in \gamma(v) + U$. □

We will now state a theorem that solves the isomorphism problem for central and medial quasigroups over $(G, +)$. Instead of showing how it follows from the more general [1, Theorem 2.10], we show that it is equivalent to [1, Theorem 3.2], which we restate as Theorem 2.5 here.

Theorem 2.4 (Isomorphism problem for central quasigroups)**.** *Let $(G, +)$ be an abelian group, let φ_1, ψ_1, φ_2, $\psi_2 \in \mathrm{Aut}(G, +)$, and let c_1, $c_2 \in G$. Then the following statements are equivalent:*

(i) the central quasigroups $\mathcal{Q}(G, +, \varphi_1, \psi_1, c_1)$ and $\mathcal{Q}(G, +, \varphi_2, \psi_2, c_2)$ are isomorphic;

(ii) there is an automorphism γ of $(G, +)$ and an element $u \in \mathrm{Im}(1 - \varphi_1 - \psi_1)$ such that

$$\varphi_2 = \gamma\varphi_1\gamma^{-1}, \quad \psi_2 = \gamma\psi_1\gamma^{-1}, \quad c_2 = \gamma(c_1 + u).$$

Theorem 2.5 ([1, Theorem 3.2])**.** *Let $(G, +)$ be an abelian group and denote $A = \mathrm{Aut}(G, +)$. The isomorphism classes of central quasigroups (resp. medial quasigroups) over $(G, +)$ are in one-to-one correspondence with the elements of the set*

$$\{(\varphi, \psi, c) : \varphi \in X,\, \psi \in Y_\varphi,\, c \in G_{\varphi,\psi}\},$$

where

- *X is a complete set of orbit representatives of the conjugation action of A on itself;*
- *Y_φ is a complete set of orbit representatives of the conjugation action of $C_A(\varphi)$ on A (resp. on $C_A(\varphi)$), for every $\varphi \in X$;*
- *$G_{\varphi,\psi}$ is a complete set of orbit representatives of the natural action of $C_A(\varphi) \cap C_A(\psi)$ on $G/\mathrm{Im}(1-\varphi-\psi)$.*

Here is a proof of the equivalence of Theorems 2.4 and 2.5: By Lemma 2.2, we can assume that we are investigating the equivalence of two triples (φ, ψ, c_1) and (φ, ψ, c_2) for some $\varphi \in X$, $\psi \in Y_\varphi$ and $c_1, c_2 \in G$. Let $U = \mathrm{Im}(1-\varphi-\psi)$. The following conditions are then equivalent for any $\gamma \in \mathrm{Aut}(G,+)$, using Lemma 2.3: $c_2 = \gamma(c_1 + u)$ for some $u \in U$, $c_2 \in \gamma(c_1 + U) = \gamma(c_1) + U$, $c_2 + U = \gamma(c_1) + U = \gamma(c_1 + U)$. This finishes the proof.

2.3 The algorithm

Theorem 2.5 together with the results of Subsection 2.1 gives rise to the following algorithm that enumerates central and medial quasigroups of order n. In the algorithm we denote by `R(H,X)` a complete set of representatives of the (clear from context) action of `H` on `X`.

Algorithm 2.6.
Input: positive integer n
Output: $cq(n)$ and $mq(n)$

```
cqn := 0; mqn := 0;
for G in the set of abelian groups of order n up to isomorphism do
    cqG := 0; mqG := 0;
    A := automorphism group of G;
    for f in R(A,A) do
        for g in R(C_A(f),A) do
            for c in R( Intersection(C_A(f),C_A(g)), G/Im(1-f-g) ) do
                cqG := cqG + 1;
                if f*g=g*f then mqG := mqG + 1; fi;
            od;
        od;
    od;
    cqn := cqn + cqG; mqn := mqn + mqG;
od;
return cqn, mqn;
```

The algorithm was implemented in the `GAP` system [2] in a straightforward fashion, taking advantage of some functionality of the `LOOPS` [7] package. The code is available from the second author at `www.math.du.edu/~petr`.

In small situations it is possible to directly calculate the orbits of the conjugation action of $A = \mathrm{Aut}(G,+)$ on $A \times A$. For larger groups, it is safer (due to memory constraints) to work with one conjugacy class of A at a time, as in Algorithm 2.5.

Among the cases we managed to calculate, the elementary abelian group C_2^5 took the most effort, about 4 hours on a standard personal computer. It might not be difficult to calculate some of the missing entries for $mq(G)$. However, $cq(C_2^6)$, for instance, appears out of reach without further theoretical advances or more substantial computational resources.

The outcome of the calculation can be found in the Appendix.

3 Quasigroups affine over cyclic groups

Let G be a cyclic group. Since $\mathrm{Aut}(G)$ is commutative, every quasigroup affine over G is medial.

Theorem 3.1 ([6, p. 70])**.** *Let p be a prime and k a positive integer. Then*

$$cq(C_{p^k}) = mq(C_{p^k}) = p^{2k} + p^{2k-2} - p^{k-1} - \sum_{i=k-1}^{2k-1} p^i.$$

Proof. Let $G = C_{p^k}$ and $A = \mathrm{Aut}(G)$. We will identify A with the $p^k - p^{k-1}$ elements of $G^* = \{a \in G : \ p \nmid a\}$. We will follow Algorithm 2.6. Since A is commutative, the conjugation action is trivial and we have to consider every $(\varphi, \psi) \in A \times A$. For a fixed $(\varphi, \psi) \in A \times A$, we must consider a complete set of orbit representatives $G_{\varphi,\psi}$ of the action of $A = C_A(\varphi) \cap C_A(\psi)$ on $G/\mathrm{Im}(1 - \varphi - \psi)$. Now, $\mathrm{Im}(1 - \varphi - \psi)$ is equal to p^iG if and only if $p^i \mid 1 - \varphi - \psi$ and $p^{i+1} \nmid 1 - \varphi - \psi$.

Case $i = 0$, i. e.,

$$\varphi + \psi \not\equiv 1 \pmod{p}.$$

In this case, we can take $G_{\varphi,\psi} = \{0\}$. How many such pairs (φ, ψ) exist? First, let us count those with $\varphi \equiv 1 \pmod{p}$. Then $\psi \in G^*$ can be chosen arbitrarily, hence we have $p^{k-1}(p^k - p^{k-1})$ such pairs. Next, let us count those with $\varphi \not\equiv 1 \pmod{p}$. Then $\psi \in G^*$ must satisfy $\psi \not\equiv 1 - \varphi \pmod{p}$, hence we have $(p^k - 2p^{k-1})(p^k - 2p^{k-1})$ such pairs. Since $|G_{\varphi,\psi}| = 1$, this case contributes to $cq(G)$ by

$$p^{k-1}(p^k - p^{k-1}) + (p^k - 2p^{k-1})^2.$$

Cases $i = 1, \ldots, k-1$, i. e.,

$$\varphi + \psi \equiv 1 \pmod{p^i} \quad \text{and} \quad \varphi + \psi \not\equiv 1 \pmod{p^{i+1}}.$$

In this case, we can take $G_{\varphi,\psi} = \{0, p^0, \ldots, p^{i-1}\}$. How many such pairs (φ, ψ) exist? For $\varphi \equiv 1 \pmod{p}$, any solution ψ to the congruence above is divisible by p, hence there is no such solution $\psi \in G^*$. For $\varphi \not\equiv 1 \pmod{p}$, we have precisely $p^{k-i} - p^{k-i-1}$

solutions to the conditions in G^*. Since $|G_{\varphi,\psi}| = i+1$, this case contributes to $cq(G)$ by

$$(p^k - 2p^{k-1})(p^{k-i} - p^{k-i-1})(i+1).$$

Case $i = k$, i. e.,

$$\varphi + \psi = 1.$$

In this case, we can take $G_{\varphi,\psi} = \{0, p^0, \ldots, p^{k-1}\}$. How many such pairs (φ, ψ) exist? Since ψ is uniquely determined by φ and neither of φ, ψ shall be divisible by p, we have precisely $p^k - 2p^{k-1}$ such pairs. Since $|G_{\varphi,\psi}| = k+1$, this case contributes to $cq(G)$ by

$$(p^k - 2p^{k-1})(k+1).$$

Summarized, the cases $i = 1, \ldots, k$ contribute to $cq(G)$ the total of

$$(p^k - 2p^{k-1}) \left(\left(\sum_{i=1}^{k-1} (p^{k-i} - p^{k-i-1}) \cdot (i+1) \right) + (k+1) \right),$$

which, after rearrangement, gives

$$(p^k - 2p^{k-1})(2p^{k-1} + p^{k-2} + p^{k-3} + \cdots + p + 1).$$

The total sum is then

$$\begin{aligned} cq(G) &= p^{2k-1} - p^{2k-2} + (p^k - 2p^{k-1})((p^k - 2p^{k-1}) \\ &\quad + (2p^{k-1} + p^{k-2} + p^{k-3} + \cdots + p + 1)) \\ &= p^{2k-1} - p^{2k-2} + (p^k - 2p^{k-1})(p^k + p^{k-2} + p^{k-3} + \cdots + p + 1) \\ &= p^{2k} - p^{2k-1} - p^{2k-3} - \cdots - p^k - 2p^{k-1}, \end{aligned}$$

which can be expressed as in the statement of the theorem. □

Corollary 3.2. *For any $k \geq 1$ we have $cq(C_{2^k}) = mq(C_{2^k}) = 2^{2k-2}$.*

Corollary 3.3. *For any prime p we have $cq(p) = mq(p) = p^2 - p - 1$.*

Corollary 3.3 is a special case of [12, Corollary 2] for binary quasigroups.

As a counterpart to Theorem 3.1, we ask:

Problem 3.4. For a prime p and $k > 1$, find explicit formulas for $cq(C_p^k)$ and $mq(C_p^k)$.

Appendix: Central and medial quasigroups of order less than 128

The following table contains the results of our enumeration of central and medial quasigroups of order less than 128.

If a row in the table starts with n/k then: column "G" gives the catalog number n/k corresponding to the abelian group `SmallGroup(n,k)` of `GAP`; column "structure" gives a structural description of the group G from which a decomposition of G into p-primary components is readily seen and hence Proposition 2.1 can be routinely applied; column "$|A|$" gives the cardinality of the group $A = \mathrm{Aut}(G)$; column "$|X|$" gives the number of conjugacy classes of A; column "$|O|$" gives the number of orbits of the conjugation action of A on $A \times A$ (with action $(f,g)^h = (f^h, g^h)$), which is a lower bound on the number of quasigroups affine over G; column "cq" gives the number of quasigroups affine over G up to isomorphism; column "$|O_c|$" gives the number of orbits in O with a representative (f,g) such that $fg = gf$, which is a lower bound on the number of medial quasigroups over G; column "mq" gives the number of medial quasigroups over G up to isomorphism; and column "ref" gives a reference to a numbered result within this paper if the entries in the row follow from the cited result and possibly also from previously listed table entries.

If a row in the table starts with **n** then: column "G" gives the order n; column "cq" gives the number of central quasigroups of order n up to isomorphism; and column "mq" gives the number of medial quasigroups of order n up to isomorphism.

Entries that we were not able to establish are denoted by "?" or "**?**".

All entries corresponding to prime-power orders were explicitly calculated by Algorithm 2.6 although the cyclic cases follow from Theorem 3.1. Many of the entries corresponding to the remaining orders were also initially obtained by Algorithm 2.6 (to test the algorithm) but in the final version they were calculated directly from earlier entries using Proposition 2.1.

To reduce the number of transcription and arithmetical errors, the entries and the LaTeX source of the table were computer generated.

G	structure	$\lvert A\rvert$	$\lvert X\rvert$	$\lvert O\rvert$	cq	$\lvert O_c\rvert$	mq	ref
1/1	C_1	1	1	1	1	1	1	
1					**1**		**1**	
2/1	C_2	1	1	1	1	1	1	3.1
2					**1**		**1**	
3/1	C_3	2	2	4	5	4	5	3.1
3					**5**		**5**	
4/1	C_4	2	2	4	4	4	4	3.1
4/2	C_2^2	6	3	11	15	8	9	
4					**19**		**13**	
5/1	C_5	4	4	16	19	16	19	3.1
5					**19**		**19**	
6/2	$C_2 \times C_3$	2	2	4	5	4	5	2.1
6					**5**		**5**	
7/1	C_7	6	6	36	41	36	41	3.1
7					**41**		**41**	

G	structure	$\lvert A\rvert$	$\lvert X\rvert$	$\lvert O\rvert$	cq	$\lvert O_c\rvert$	mq	ref
8/1	C_8	4	4	16	16	16	16	3.1
8/2	$C_4\times C_2$	8	5	28	28	22	22	
8/5	C_2^3	168	6	197	341	32	35	
8					**385**		**73**	
9/1	C_9	6	6	36	48	36	48	3.1
9/2	C_3^2	48	8	136	183	56	68	
9					**231**		**116**	
10/2	$C_2\times C_5$	4	4	16	19	16	19	2.1
10					**19**		**19**	
11/1	C_{11}	10	10	100	109	100	109	3.1
11					**109**		**109**	
12/2	$C_4\times C_3$	4	4	16	20	16	20	2.1
12/5	$C_2^2\times C_3$	12	6	44	75	32	45	2.1
12					**95**		**65**	
13/1	C_{13}	12	12	144	155	144	155	3.1
13					**155**		**155**	
14/2	$C_2\times C_7$	6	6	36	41	36	41	2.1
14					**41**		**41**	
15/1	$C_3\times C_5$	8	8	64	95	64	95	2.1
15					**95**		**95**	
16/1	C_{16}	8	8	64	64	64	64	3.1
16/2	C_4^2	96	14	400	624	168	188	
16/5	$C_8\times C_2$	16	10	112	112	88	88	
16/10	$C_4\times C_2^2$	192	13	564	820	146	150	
16/14	C_2^4	20160	14	20747	39767	160	179	
16					**41387**		**669**	
17/1	C_{17}	16	16	256	271	256	271	3.1
17					**271**		**271**	
18/2	$C_2\times C_9$	6	6	36	48	36	48	2.1
18/5	$C_2\times C_3^2$	48	8	136	183	56	68	2.1
18					**231**		**116**	
19/1	C_{19}	18	18	324	341	324	341	3.1
19					**341**		**341**	
20/2	$C_4\times C_5$	8	8	64	76	64	76	2.1
20/5	$C_2^2\times C_5$	24	12	176	285	128	171	2.1
20					**361**		**247**	
21/2	$C_3\times C_7$	12	12	144	205	144	205	2.1
21					**205**		**205**	
22/2	$C_2\times C_{11}$	10	10	100	109	100	109	2.1
22					**109**		**109**	
23/1	C_{23}	22	22	484	505	484	505	3.1
23					**505**		**505**	

G	structure	$\lvert A\rvert$	$\lvert X\rvert$	$\lvert O\rvert$	cq	$\lvert O_c\rvert$	mq	ref
24/2	$C_8\times C_3$	8	8	64	80	64	80	2.1
24/9	$C_4\times C_2\times C_3$	16	10	112	140	88	110	2.1
24/15	$C_2^3\times C_3$	336	12	788	1705	128	175	2.1
24					**1925**		**365**	
25/1	C_{25}	20	20	400	490	400	490	3.1
25/2	C_5^2	480	24	2336	2847	512	594	
25					**3337**		**1084**	
26/2	$C_2\times C_{13}$	12	12	144	155	144	155	2.1
26					**155**		**155**	
27/1	C_{27}	18	18	324	441	324	441	3.1
27/2	$C_9\times C_3$	108	20	864	1356	336	528	
27/5	C_3^3	11232	24	23236	34321	484	605	
27					**36118**		**1574**	
28/2	$C_4\times C_7$	12	12	144	164	144	164	2.1
28/4	$C_2^2\times C_7$	36	18	396	615	288	369	2.1
28					**779**		**533**	
29/1	C_{29}	28	28	784	811	784	811	3.1
29					**811**		**811**	
30/4	$C_2\times C_3\times C_5$	8	8	64	95	64	95	2.1
30					**95**		**95**	
31/1	C_{31}	30	30	900	929	900	929	3.1
31					**929**		**929**	
32/1	C_{32}	16	16	256	256	256	256	3.1
32/3	$C_8\times C_4$	128	26	1216	1216	592	592	
32/16	$C_{16}\times C_2$	32	20	448	448	352	352	
32/21	$C_4^2\times C_2$	1536	30	6224	9808	884	904	
32/36	$C_8\times C_2^2$	384	26	2256	3280	584	600	
32/45	$C_4\times C_2^3$	21504	30	48412	87580	804	834	
32/51	C_2^5	9999360	27	10024077	19721077	590	655	
32					**19823665**		**4193**	
33/1	$C_3\times C_{11}$	20	20	400	545	400	545	2.1
33					**545**		**545**	
34/2	$C_2\times C_{17}$	16	16	256	271	256	271	2.1
34					**271**		**271**	
35/1	$C_5\times C_7$	24	24	576	779	576	779	2.1
35					**779**		**779**	
36/2	$C_4\times C_9$	12	12	144	192	144	192	2.1
36/5	$C_2^2\times C_9$	36	18	396	720	288	432	2.1
36/8	$C_4\times C_3^2$	96	16	544	732	224	272	2.1
36/14	$C_2^2\times C_3^2$	288	24	1496	2745	448	612	2.1
36					**4389**		**1508**	
37/1	C_{37}	36	36	1296	1331	1296	1331	3.1
37					**1331**		**1331**	

G	structure	$\lvert A\rvert$	$\lvert X\rvert$	$\lvert O\rvert$	cq	$\lvert O_c\rvert$	mq	ref
38/2	$C_2\times C_{19}$	18	18	324	341	324	341	2.1
38					**341**		**341**	
39/2	$C_3\times C_{13}$	24	24	576	775	576	775	2.1
39					**775**		**775**	
40/2	$C_8\times C_5$	16	16	256	304	256	304	2.1
40/9	$C_4\times C_2\times C_5$	32	20	448	532	352	418	2.1
40/14	$C_2^3\times C_5$	672	24	3152	6479	512	665	2.1
40					**7315**		**1387**	
41/1	C_{41}	40	40	1600	1639	1600	1639	3.1
41					**1639**		**1639**	
42/6	$C_2\times C_3\times C_7$	12	12	144	205	144	205	2.1
42					**205**		**205**	
43/1	C_{43}	42	42	1764	1805	1764	1805	3.1
43					**1805**		**1805**	
44/2	$C_4\times C_{11}$	20	20	400	436	400	436	2.1
44/4	$C_2^2\times C_{11}$	60	30	1100	1635	800	981	2.1
44					**2071**		**1417**	
45/1	$C_9\times C_5$	24	24	576	912	576	912	2.1
45/2	$C_3^2\times C_5$	192	32	2176	3477	896	1292	2.1
45					**4389**		**2204**	
46/2	$C_2\times C_{23}$	22	22	484	505	484	505	2.1
46					**505**		**505**	
47/1	C_{47}	46	46	2116	2161	2116	2161	3.1
47					**2161**		**2161**	
48/2	$C_{16}\times C_3$	16	16	256	320	256	320	2.1
48/20	$C_4^2\times C_3$	192	28	1600	3120	672	940	2.1
48/23	$C_8\times C_2\times C_3$	32	20	448	560	352	440	2.1
48/44	$C_4\times C_2^2\times C_3$	384	26	2256	4100	584	750	2.1
48/52	$C_2^4\times C_3$	40320	28	82988	198835	640	895	2.1
48					**206935**		**3345**	
49/1	C_{49}	42	42	1764	2044	1764	2044	3.1
49/2	C_7^2	2016	48	13896	16055	2088	2344	
49					**18099**		**4388**	
50/2	$C_2\times C_{25}$	20	20	400	490	400	490	2.1
50/5	$C_2\times C_5^2$	480	24	2336	2847	512	594	2.1
50					**3337**		**1084**	
51/1	$C_3\times C_{17}$	32	32	1024	1355	1024	1355	2.1
51					**1355**		**1355**	
52/2	$C_4\times C_{13}$	24	24	576	620	576	620	2.1
52/5	$C_2^2\times C_{13}$	72	36	1584	2325	1152	1395	2.1
52					**2945**		**2015**	
53/1	C_{53}	52	52	2704	2755	2704	2755	3.1
53					**2755**		**2755**	

G	structure	$\lvert A\rvert$	$\lvert X\rvert$	$\lvert O\rvert$	cq	$\lvert O_c\rvert$	mq	ref
54/2	$C_2\times C_{27}$	18	18	324	441	324	441	2.1
54/9	$C_2\times C_9\times C_3$	108	20	864	1356	336	528	2.1
54/15	$C_2\times C_3^3$	11232	24	23236	34321	484	605	2.1
54					**36118**		**1574**	
55/2	$C_5\times C_{11}$	40	40	1600	2071	1600	2071	2.1
55					**2071**		**2071**	
56/2	$C_8\times C_7$	24	24	576	656	576	656	2.1
56/8	$C_4\times C_2\times C_7$	48	30	1008	1148	792	902	2.1
56/13	$C_2^3\times C_7$	1008	36	7092	13981	1152	1435	2.1
56					**15785**		**2993**	
57/2	$C_3\times C_{19}$	36	36	1296	1705	1296	1705	2.1
57					**1705**		**1705**	
58/2	$C_2\times C_{29}$	28	28	784	811	784	811	2.1
58					**811**		**811**	
59/1	C_{59}	58	58	3364	3421	3364	3421	3.1
59					**3421**		**3421**	
60/4	$C_4\times C_3\times C_5$	16	16	256	380	256	380	2.1
60/13	$C_2^2\times C_3\times C_5$	48	24	704	1425	512	855	2.1
60					**1805**		**1235**	
61/1	C_{61}	60	60	3600	3659	3600	3659	3.1
61					**3659**		**3659**	
62/2	$C_2\times C_{31}$	30	30	900	929	900	929	2.1
62					**929**		**929**	
63/2	$C_9\times C_7$	36	36	1296	1968	1296	1968	2.1
63/4	$C_3^2\times C_7$	288	48	4896	7503	2016	2788	2.1
63					**9471**		**4756**	
64/1	C_{64}	32	32	1024	1024	1024	1024	3.1
64/2	C_8^2	1536	60	13568	22784	3072	3408	
64/26	$C_{16}\times C_4$	256	52	4864	4864	2368	2368	
64/50	$C_{32}\times C_2$	64	40	1792	1792	1408	1408	
64/55	C_4^3	86016	60	206144	441664	4448	4672	
64/83	$C_8\times C_4\times C_2$	2048	104	31168	31168	7240	7240	
64/183	$C_{16}\times C_2^2$	768	52	9024	13120	2336	2400	
64/192	$C_4^2\times C_2^2$	147456	100	550480	1239472	9108	9656	
64/246	$C_8\times C_2^3$	43008	60	193648	350320	3216	3336	
64/260	$C_4\times C_2^4$	10321920	69	?	?	?	?	
64/267	C_2^6	20158709760	60	?	?	?	?	
64					**?**		**?**	
65/1	$C_5\times C_{13}$	48	48	2304	2945	2304	2945	2.1
65					**2945**		**2945**	
66/4	$C_2\times C_3\times C_{11}$	20	20	400	545	400	545	2.1
66					**545**		**545**	
67/1	C_{67}	66	66	4356	4421	4356	4421	3.1
67					**4421**		**4421**	

G	structure	$\lvert A\rvert$	$\lvert X\rvert$	$\lvert O\rvert$	cq	$\lvert O_c\rvert$	mq	ref
68/2	$C_4\times C_{17}$	32	32	1024	1084	1024	1084	2.1
68/5	$C_2^2\times C_{17}$	96	48	2816	4065	2048	2439	2.1
68					**5149**		**3523**	
69/1	$C_3\times C_{23}$	44	44	1936	2525	1936	2525	2.1
69					**2525**		**2525**	
70/4	$C_2\times C_5\times C_7$	24	24	576	779	576	779	2.1
70					**779**		**779**	
71/1	C_{71}	70	70	4900	4969	4900	4969	3.1
71					**4969**		**4969**	
72/2	$C_8\times C_9$	24	24	576	768	576	768	2.1
72/9	$C_4\times C_2\times C_9$	48	30	1008	1344	792	1056	2.1
72/14	$C_8\times C_3^2$	192	32	2176	2928	896	1088	2.1
72/18	$C_2^3\times C_9$	1008	36	7092	16368	1152	1680	2.1
72/36	$C_4\times C_2\times C_3^2$	384	40	3808	5124	1232	1496	2.1
72/50	$C_2^3\times C_3^2$	8064	48	26792	62403	1792	2380	2.1
72					**88935**		**8468**	
73/1	C_{73}	72	72	5184	5255	5184	5255	3.1
73					**5255**		**5255**	
74/2	$C_2\times C_{37}$	36	36	1296	1331	1296	1331	2.1
74					**1331**		**1331**	
75/1	$C_3\times C_{25}$	40	40	1600	2450	1600	2450	2.1
75/3	$C_3\times C_5^2$	960	48	9344	14235	2048	2970	2.1
75					**16685**		**5420**	
76/2	$C_4\times C_{19}$	36	36	1296	1364	1296	1364	2.1
76/4	$C_2^2\times C_{19}$	108	54	3564	5115	2592	3069	2.1
76					**6479**		**4433**	
77/1	$C_7\times C_{11}$	60	60	3600	4469	3600	4469	2.1
77					**4469**		**4469**	
78/6	$C_2\times C_3\times C_{13}$	24	24	576	775	576	775	2.1
78					**775**		**775**	
79/1	C_{79}	78	78	6084	6161	6084	6161	3.1
79					**6161**		**6161**	
80/2	$C_{16}\times C_5$	32	32	1024	1216	1024	1216	2.1
80/20	$C_4^2\times C_5$	384	56	6400	11856	2688	3572	2.1
80/23	$C_8\times C_2\times C_5$	64	40	1792	2128	1408	1672	2.1
80/45	$C_4\times C_2^2\times C_5$	768	52	9024	15580	2336	2850	2.1
80/52	$C_2^4\times C_5$	80640	56	331952	755573	2560	3401	2.1
80					**786353**		**12711**	
81/1	C_{81}	54	54	2916	3996	2916	3996	3.1
81/2	C_9^2	3888	78	35316	54405	5616	8055	
81/5	$C_{27}\times C_3$	324	60	7776	12897	3024	5157	
81/11	$C_9\times C_3^2$	23328	74	152892	270441	4176	7167	
81/15	C_3^4	24261120	78	?	?	?	?	
81					**?**		**?**	

G	structure	$\lvert A\rvert$	$\lvert X\rvert$	$\lvert O\rvert$	cq	$\lvert O_c\rvert$	mq	ref
82/2	$C_2\times C_{41}$	40	40	1600	1639	1600	1639	2.1
82					**1639**		**1639**	
83/1	C_{83}	82	82	6724	6805	6724	6805	3.1
83					**6805**		**6805**	
84/6	$C_4\times C_3\times C_7$	24	24	576	820	576	820	2.1
84/15	$C_2^2\times C_3\times C_7$	72	36	1584	3075	1152	1845	2.1
84					**3895**		**2665**	
85/1	$C_5\times C_{17}$	64	64	4096	5149	4096	5149	2.1
85					**5149**		**5149**	
86/2	$C_2\times C_{43}$	42	42	1764	1805	1764	1805	2.1
86					**1805**		**1805**	
87/1	$C_3\times C_{29}$	56	56	3136	4055	3136	4055	2.1
87					**4055**		**4055**	
88/2	$C_8\times C_{11}$	40	40	1600	1744	1600	1744	2.1
88/8	$C_4\times C_2\times C_{11}$	80	50	2800	3052	2200	2398	2.1
88/12	$C_2^3\times C_{11}$	1680	60	19700	37169	3200	3815	2.1
88					**41965**		**7957**	
89/1	C_{89}	88	88	7744	7831	7744	7831	3.1
89					**7831**		**7831**	
90/4	$C_2\times C_9\times C_5$	24	24	576	912	576	912	2.1
90/10	$C_2\times C_3^2\times C_5$	192	32	2176	3477	896	1292	2.1
90					**4389**		**2204**	
91/1	$C_7\times C_{13}$	72	72	5184	6355	5184	6355	2.1
91					**6355**		**6355**	
92/2	$C_4\times C_{23}$	44	44	1936	2020	1936	2020	2.1
92/4	$C_2^2\times C_{23}$	132	66	5324	7575	3872	4545	2.1
92					**9595**		**6565**	
93/2	$C_3\times C_{31}$	60	60	3600	4645	3600	4645	2.1
93					**4645**		**4645**	
94/2	$C_2\times C_{47}$	46	46	2116	2161	2116	2161	2.1
94					**2161**		**2161**	
95/1	$C_5\times C_{19}$	72	72	5184	6479	5184	6479	2.1
95					**6479**		**6479**	
96/2	$C_{32}\times C_3$	32	32	1024	1280	1024	1280	2.1
96/46	$C_8\times C_4\times C_3$	256	52	4864	6080	2368	2960	2.1
96/59	$C_{16}\times C_2\times C_3$	64	40	1792	2240	1408	1760	2.1
96/161	$C_4^2\times C_2\times C_3$	3072	60	24896	49040	3536	4520	2.1
96/176	$C_8\times C_2^2\times C_3$	768	52	9024	16400	2336	3000	2.1
96/220	$C_4\times C_2^3\times C_3$	43008	60	193648	437900	3216	4170	2.1
96/231	$C_2^5\times C_3$	19998720	54	40096308	98605385	2360	3275	2.1
96					**99118325**		**20965**	
97/1	C_{97}	96	96	9216	9311	9216	9311	3.1
97					**9311**		**9311**	

G	structure	$\lvert A\rvert$	$\lvert X\rvert$	$\lvert O\rvert$	cq	$\lvert O_c\rvert$	mq	ref
98/2	$C_2\times C_{49}$	42	42	1764	2044	1764	2044	2.1
98/5	$C_2\times C_7^2$	2016	48	13896	16055	2088	2344	2.1
98					**18099**		**4388**	
99/1	$C_9\times C_{11}$	60	60	3600	5232	3600	5232	2.1
99/2	$C_3^2\times C_{11}$	480	80	13600	19947	5600	7412	2.1
99					**25179**		**12644**	
100/2	$C_4\times C_{25}$	40	40	1600	1960	1600	1960	2.1
100/5	$C_2^2\times C_{25}$	120	60	4400	7350	3200	4410	2.1
100/8	$C_4\times C_5^2$	960	48	9344	11388	2048	2376	2.1
100/16	$C_2^2\times C_5^2$	2880	72	25696	42705	4096	5346	2.1
100					**63403**		**14092**	
101/1	C_{101}	100	100	10000	10099	10000	10099	3.1
101					**10099**		**10099**	
102/4	$C_2\times C_3\times C_{17}$	32	32	1024	1355	1024	1355	2.1
102					**1355**		**1355**	
103/1	C_{103}	102	102	10404	10505	10404	10505	3.1
103					**10505**		**10505**	
104/2	$C_8\times C_{13}$	48	48	2304	2480	2304	2480	2.1
104/9	$C_4\times C_2\times C_{13}$	96	60	4032	4340	3168	3410	2.1
104/14	$C_2^3\times C_{13}$	2016	72	28368	52855	4608	5425	2.1
104					**59675**		**11315**	
105/2	$C_3\times C_5\times C_7$	48	48	2304	3895	2304	3895	2.1
105					**3895**		**3895**	
106/2	$C_2\times C_{53}$	52	52	2704	2755	2704	2755	2.1
106					**2755**		**2755**	
107/1	C_{107}	106	106	11236	11341	11236	11341	3.1
107					**11341**		**11341**	
108/2	$C_4\times C_{27}$	36	36	1296	1764	1296	1764	2.1
108/5	$C_2^2\times C_{27}$	108	54	3564	6615	2592	3969	2.1
108/12	$C_4\times C_9\times C_3$	216	40	3456	5424	1344	2112	2.1
108/29	$C_2^2\times C_9\times C_3$	648	60	9504	20340	2688	4752	2.1
108/35	$C_4\times C_3^3$	22464	48	92944	137284	1936	2420	2.1
108/45	$C_2^2\times C_3^3$	67392	72	255596	514815	3872	5445	2.1
108					**686242**		**20462**	
109/1	C_{109}	108	108	11664	11771	11664	11771	3.1
109					**11771**		**11771**	
110/6	$C_2\times C_5\times C_{11}$	40	40	1600	2071	1600	2071	2.1
110					**2071**		**2071**	
111/2	$C_3\times C_{37}$	72	72	5184	6655	5184	6655	2.1
111					**6655**		**6655**	

G	structure	$\lvert A\rvert$	$\lvert X\rvert$	$\lvert O\rvert$	cq	$\lvert O_c\rvert$	mq	ref
112/2	$C_{16}\times C_7$	48	48	2304	2624	2304	2624	2.1
112/19	$C_4^2\times C_7$	576	84	14400	25584	6048	7708	2.1
112/22	$C_8\times C_2\times C_7$	96	60	4032	4592	3168	3608	2.1
112/37	$C_4\times C_2^2\times C_7$	1152	78	20304	33620	5256	6150	2.1
112/43	$C_2^4\times C_7$	120960	84	746892	1630447	5760	7339	2.1
112					**1696867**		**27429**	
113/1	C_{113}	112	112	12544	12655	12544	12655	3.1
113					**12655**		**12655**	
114/6	$C_2\times C_3\times C_{19}$	36	36	1296	1705	1296	1705	2.1
114					**1705**		**1705**	
115/1	$C_5\times C_{23}$	88	88	7744	9595	7744	9595	2.1
115					**9595**		**9595**	
116/2	$C_4\times C_{29}$	56	56	3136	3244	3136	3244	2.1
116/5	$C_2^2\times C_{29}$	168	84	8624	12165	6272	7299	2.1
116					**15409**		**10543**	
117/2	$C_9\times C_{13}$	72	72	5184	7440	5184	7440	2.1
117/4	$C_3^2\times C_{13}$	576	96	19584	28365	8064	10540	2.1
117					**35805**		**17980**	
118/2	$C_2\times C_{59}$	58	58	3364	3421	3364	3421	2.1
118					**3421**		**3421**	
119/1	$C_7\times C_{17}$	96	96	9216	11111	9216	11111	2.1
119					**11111**		**11111**	
120/4	$C_8\times C_3\times C_5$	32	32	1024	1520	1024	1520	2.1
120/31	$C_4\times C_2\times C_3\times C_5$	64	40	1792	2660	1408	2090	2.1
120/47	$C_2^3\times C_3\times C_5$	1344	48	12608	32395	2048	3325	2.1
120					**36575**		**6935**	
121/1	C_{121}	110	110	12100	13288	12100	13288	3.1
121/2	C_{11}^2	13200	120	144200	158199	13400	14508	
121					**171487**		**27796**	
122/2	$C_2\times C_{61}$	60	60	3600	3659	3600	3659	2.1
122					**3659**		**3659**	
123/1	$C_3\times C_{41}$	80	80	6400	8195	6400	8195	2.1
123					**8195**		**8195**	
124/2	$C_4\times C_{31}$	60	60	3600	3716	3600	3716	2.1
124/4	$C_2^2\times C_{31}$	180	90	9900	13935	7200	8361	2.1
124					**17651**		**12077**	
125/1	C_{125}	100	100	10000	12325	10000	12325	3.1
125/2	$C_{25}\times C_5$	2000	104	47200	66580	9280	13270	
125/5	C_5^3	1488000	120	?	?	?	?	
125					**?**		**?**	
126/6	$C_2\times C_9\times C_7$	36	36	1296	1968	1296	1968	2.1
126/16	$C_2\times C_3^2\times C_7$	288	48	4896	7503	2016	2788	2.1
126					**9471**		**4756**	
127/1	C_{127}	126	126	15876	16001	15876	16001	3.1
127					**16001**		**16001**	

References

[1] Drápal A. *Group isotopes and a holomorphic action*. Result. Math., 2009, **54**, No. 3–4, 253–272.

[2] The GAP Group, GAP – Groups, Algorithms and Programming, Version 4.5.5; 2012. `http://www.gap-system.org`

[3] Hillar C. J., Rhea D. L. *Automorphisms of finite abelian groups*. Amer. Math. Monthly, 2007, **114**, 917–923.

[4] Hou X., *Finite modules over* $\mathbb{Z}[t, t^{-1}]$. J. Knot Theory Ramifications, 2012, **21**, No. 8, 1250079, 28 pp.

[5] Kirnasovsky O. U. *Linear isotopes of small order groups*. Quasigroups and Related Systems, 1995, **2**, No. 1, 51–82.

[6] Kirnasovsky O. U. *Binary and n-ary isotopes of groups: fundamental algebraic properties and characterizations*, PhD thesis, Kiev 2001 (Ukrainian).

[7] Nagy G. P., Vojtěchovský P. `LOOPS`: Computing with quasigroups and loops in GAP, version 3.0.0, `www.math.du.edu/loops`.

[8] OEIS Foundation Inc. (2011), The On-Line Encyclopedia of Integer Sequences, `http://oeis.org`.

[9] Smith J. D. H. *Finite equationally complete entropic quasigroups*, Contributions to general algebra (Proc. Klagenfurt Conf. 1978), 345–356 (1979).

[10] Smith J. D. H. *An introduction to quasigroups and their representations*, Chapman & Hall/CRC, 2007.

[11] Sokhatsky F. *On isotopes of groups, I, II, III.* Ukrainian Math. J., 1995, 47/10, 1585–1598; 1995, 47/12, 1935–1948; 1996, 48/2, 283–293.

[12] Sokhatsky F., Syvakivskij P. *On linear isotopes of cyclic groups*. Quasigroups and Related Systems, 1994, **1**, No. 1, 66–76.

[13] Stanovský D. *A guide to self-distributive quasigroups, or latin quandles*, Quasigroups and Related Systems, 2015, **23**, No. 1, 91–128.

[14] Stronkowski M., Stanovský D. *Embedding general algebras into modules*. Proc. Amer. Math. Soc., 2010, **138**, No. 8, 2687–2699.

[15] Szendrei Á. *Modules in general algebra*. Contributions to general algebra **10** (Proc. Klagenfurt Conf. 1997), 41–53 (1998).

Received November 11, 2015

David Stanovský
Department of Algebra
Charles University
Sokolovská 83
186 75 Praha 8, CZECH REPUBLIC
E-mail: *stanovsk@karlin.mff.cuni.cz*

Petr Vojtěchovský
Department of Mathematics
University of Denver
2280 S Vine St
Denver, Colorado 80208, U.S.A.
E-mail: *petr@math.du.edu*

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 41–63
ISSN 1024–7696

Algebras with Parastrophically Uncancellable Quasigroup Equations

Amir Ehsani, Aleksandar Krapež, Yuri Movsisyan

Abstract. We consider 48 parastrophically uncancellable quadratic functional equations with four object variables and two quasigroup operations in two classes: balanced non–Belousov (consists of 16 equations) and non–balanced non–gemini (consists of 32 equations). A linear representation of a group (Abelian group) for a pair of quasigroup operations satisfying one of these parastrophically uncancellable quadratic equations is obtained. As a consequence of these results, a linear representation for every operation of a binary algebra satisfying one of these hyperidentities is obtained.

Mathematics subject classification: 20N05; 39B52; 08A05.
Keywords and phrases: Quadratic equation, Gemini equation, Level equation, Balanced equation, Belousov equation, Medial–like equation, Parastrophically uncancellable equation, Quasigroup operation, Algebra of quasigroup operations, Hyperidentity.

Dedicated to V. D. Belousov and G. B. Belyavskaya

1 Introduction

A binary quasigroup is usually defined to be a groupoid $(B; f)$ such that for any $a, b \in B$ there are unique solutions x and y to the following equations:

$$f(a, x) = b \quad \text{and} \quad f(y, a) = b.$$

The basic properties of quasigroups were given in books [3, 8, 9, 24]. We remind the reader of those properties we shall use in the paper.

If $(B; f)$ is quasigroup we say that f is a quasigroup operation. A loop is a quasigroup with unit (e) such that

$$f(e, x) = f(x, e) = x.$$

Groups are associative quasigroups, i. e. they satisfy:

$$f(f(x, y), z) = f(x, f(y, z))$$

and they necessarily contain a unit. A quasigroup is commutative if

$$f(x, y) = f(y, x). \tag{1.1}$$

Commutative groups are also known as Abelian groups.

A triple (α, β, γ) of bijections from a set B onto a set C is called an isotopy of a groupoid $(B; f)$ onto a groupoid $(C; g)$ provided

$$\gamma f(x, y) = g(\alpha x, \beta y)$$

for all $x, y \in B$. $(C; g)$ is then called an isotope of $(B; f)$, and groupoids $(B; f)$ and $(C; g)$ are said to be isotopic to each other. An isotopy of $(B; f)$ onto $(B; f)$ is called an autotopy of $(B; f)$. Let α and β be permutations of B and let ι denote the identity map on B. Then (α, β, ι) is a principal isotopy of a groupoid $(B; f)$ onto a groupoid $(B; g)$ means that (α, β, ι) is an isotopy of $(B; f)$ onto $(B; g)$. Isotopy is a generalization of isomorphism. Isotopic image of a quasigroup is again a quasigroup. A loop isotopic to a group is isomorphic to it. Every quasigroup is isotopic to some loop, i. e., it is a loop isotope.

If $(B; +)$ is a group, then the bijection $\alpha : B \to B$ is called a *holomorphism* of $(B; +)$ if

$$\alpha(x + y^{-1} + z) = \alpha x + (\alpha y)^{-1} + \alpha z. \tag{1.2}$$

The set of all holomorphisms of $(B; +)$ is denoted by $Hol(B; +)$. It is a group under the composition of mappings: $(\alpha \cdot \beta)x = \beta(\alpha x)$, for every $x \in B$. Note that this concept is equivalent to the concept of quasiautomorphism of groups, by [3].

A binary quasigroup $(B; f)$ is linear over a group (Abelian group) if

$$f(x, y) = \varphi x + a + \psi y,$$

where $(B; +)$ is a group (Abelian group), φ and ψ are automorphisms of $(B; +)$ and $a \in B$ is a fixed element. A quasigroup linear over an Abelian group is also called a T-quasigroup.

Quasigroups are important algebraic (combinatorial, geometric) structures which arise in various areas of mathematics and other disciplines. We mention just a few of their applications: in combinatorics (as latin squares, see [9]), in geometry (as nets/webs, see [4]), in statistics (see [11]), in special theory of relativity (see [27]), in coding theory and cryptography [25].

2 Preliminaries

We use (object) variables x, y, z, u, v, w (perhaps with indices) and operation symbols (i. e. functional variables) f, g, h (also with indices). We assume that all operation symbols represent quasigroup operations.

The set of all variables which appear in a term t is called the *content* of t and is denoted by $var(t)$. A variable x is *linear variable* in a term t when it occurs just once in t. A variable x is *quadratic variable* in a term t when it occurs twice in t. The sets of all linear and quadratic variables of term t are denoted by $var_1(t)$ and $var_2(t)$, respectively.

A *functional equation* is an equality $s = t$, where s and t are terms with symbols of unknown operations occurring in at least one of them.

Definition 1. A functional equation $s = t$ is *quadratic* if every (object) variable occurs exactly twice in $s = t$. It is *balanced* if every (object) variable appears exactly once in s and once in t.

Definition 2. A variable x from a quadratic equation $s = t$ is *linear* if x occurrs once in s and once in t; it is *left (right) quadratic* if it occurrs twice in $s\,(t)$ and *quadratic* if it is either left or right quadratic.

Definition 3. A balanced equation $s = t$ is *Belousov* if for every subterm p of s (t) there is a subterm q of t (s) such that p and q have exactly the same variables.

Definition 4. A quadratic quasigroup equation is *gemini* iff it is a theorem of TS-loops (= Steiner loops), i. e., consequence of the identities of the variety of TS-loops.

Definition 5. Functional equation $s = t$ is *generalized* if every operation symbol from $s = t$ occurrs there just once.

Definition 6. Let x be a variable occurring in a quadratic equation $s = t$. The function Lh (Rh) of the *left (right) height of the variable x in the equation $s = t$ is given by:*

– *If $x \notin var(t)$, then* $\mathrm{Lh}(x,t)$ $(\mathrm{Rh}(x,t))$ *is not defined,*

– $Lh(x,x) = 0$ $(Rh(x,x) = 0)$,

– *If $t = f(t_1,t_2)$ and both occurrences of x are in t_1 then* $\mathrm{Lh}(x,t) = 1 + \mathrm{Lh}(x,t_1)$ $(\mathrm{Rh}(x,t) = 1 + \mathrm{Rh}(x,t_1))$,

– *If $t = f(t_1,t_2)$ and both occurrences of x are in t_2 then* $\mathrm{Lh}(x,t) = 1 + \mathrm{Lh}(x,t_2)$ $(\mathrm{Rh}(x,t) = 1 + \mathrm{Rh}(x,t_2))$,

– *If $t = f(t_1,t_2)$ and x occurrs in both t_1 and t_2 then* $\mathrm{Lh}(x,t) = 1 + \mathrm{Lh}(x,t_1)$ $(\mathrm{Rh}(x,t) = 1 + \mathrm{Rh}(x,t_2))$,

– $$\mathrm{Lh}(x, s = t) = \begin{cases} \mathrm{Lh}(x,s) & \text{if } x \in var(s), \\ \mathrm{Lh}(x,t) & \text{otherwise,} \end{cases}$$

– $$\mathrm{Rh}(x, s = t) = \begin{cases} \mathrm{Rh}(x,t) & \text{if } x \in var(t), \\ \mathrm{Rh}(x,s) & \text{otherwise.} \end{cases}$$

Definition 7. Let $s = t$ be a quadratic equation. It is a *level equation iff* $\mathrm{Lh}(x, s = t) = \mathrm{Rh}(y, s = t)$ *for all variables x, y of $s = t$.*

Example 1. The following are various functional equations:

(commutativity)	$f(x,y) = f(y,x),$	(2.1)
(associativity)	$f(f(x,y),z) = f(x,f(y,z)),$	(2.2)
(mediality)	$f(f(x,y),f(u,v)) = f(f(x,u),f(y,v)),$	(2.3)
(paramediality)	$f(f(x,y),f(u,v)) = f(f(v,y),f(u,x)),$	(2.4)
(distributivity)	$f(x,f(y,z)) = f(f(x,y),f(x,z)),$	(2.5)
(transitivity)	$f(f(x,y),f(y,z)) = f(x,z),$	(2.6)
(intermediality)	$f(f(x,y),f(y,u)) = f(f(x,v),f(v,u)),$	(2.7)
(extramediality)	$f(f(x,y),f(u,x)) = f(f(v,y),f(u,v)),$	(2.8)
(4-palindromic identity)	$f(f(x,y),f(u,v)) = f(f(v,u),f(y,x)),$	(2.9)
(idempotency)	$f(x,x) = x,$	(2.10)
(trivial)	$f(x,y) = f(x,y),$	(2.11)
	$f(x,f(y,z)) = f(f(z,y),x).$	(2.12)

Associativity, (para)mediality, 4-palindromic, trivial identity and (2.12) are balanced, transitivity, intermediality and extramediality are quadratic but not balanced and idempotency and (left) distributivity are not even quadratic. Commutativity, trivial, 4-palindromic and (2.12) are gemini functional equations and since they are balanced, they are Belousov equations as well. The equations (2.2) – (2.8) are non-gemini and non-Belousov. Commutativity, mediality, paramediality, intermediality, extramediality, 4–palindromic and trivial identity are level equations.

Every quasigroup satisfying (para)medial identity is called *(para)medial quasigroup*. Every quasigroup satisfying 4-palindromic identity is called 4-*palindromic quasigroup*.

Theorem 1 (Toyoda [26])**.** *If $(B;f)$ is a medial quasigroup then there exists an Abelian group $(B;+)$ such that $f(x,y) = \varphi(x) + c + \psi(y)$, where $\varphi, \psi \in Aut(B;+)$, $\varphi\psi = \psi\varphi$ and $c \in B$.*

Theorem 2 (Němec, Kepka [23])**.** *If $(B;f)$ is a paramedial quasigroup then there exists an Abelian group $(B;+)$ such that $f(x,y) = \varphi(x) + c + \psi(y)$, where $\varphi, \psi \in Aut(B;+)$, $\varphi\varphi = \psi\psi$ and $c \in B$.*

More generaly, considering the following equations with two functional variables, we can define the notion of (para)medial pair of operations:

$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(x,u),f_1(y,v)), \tag{2.13}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(v,y),f_1(u,x)). \tag{2.14}$$

Definition 8. A pair (f_1, f_2) of binary operations is called *(para)medial pair of operations* if the algebra $(B; f_1, f_2)$ satisfies the equation (2.13) ((2.14)).

Definition 9. A binary algebra $\mathbf{B} = (B; F)$ is called *(para)medial algebra* if every pair of operations of the algebra $\mathbf{B}$ is (para)medial (or, the algebra $\mathbf{B}$ satisfies (para)medial hyperidentity).

The following theorem generalizes above results by Toyoda and Němec, Kepka:

Theorem 3 (Nazari, Movsisyan [22], Ehsani, Movsisyan [10])**.** *Let the set B form a quasigroup under the binary operations f_1 and f_2. If the pair of binary operations (f_1, f_2) is (para)medial, then there exists a binary operation $'+'$ under which B forms an Abelian group and for arbitrary elements $x, y \in B$ we have:*

$$f_i(x, y) = \varphi_i(x) + \psi_i(y) + c_i,$$

where c_is are fixed elements of B, and $\varphi_i, \psi_i \in Aut(B; +)$ for $i = 1, 2$, such that:

$\varphi_1\psi_2 = \psi_2\varphi_1$, $\varphi_2\psi_1 = \psi_1\varphi_2$, $\psi_1\psi_2 = \psi_2\psi_1$ *and* $\varphi_1\varphi_2 = \varphi_2\varphi_1$ *should be satisfied by the medial pair of operations,*

$\varphi_1\varphi_2 = \psi_2\psi_1$, $\varphi_2\varphi_1 = \psi_1\psi_2$, $\varphi_1\psi_2 = \varphi_2\psi_1$ *and* $\psi_1\varphi_2 = \psi_2\varphi_1$ *should be satisfied by the paramedial pair of operations.*

The group $(B; +)$, is unique up to isomorphisms.

The following results will be frequently utilized.

Theorem 4 (Aczél, Belousov, Hosszú [1], see also [2])**.** *Let the set B form a quasigroup under six operations $A_i(x, y)$ (for $i = 1, \ldots, 6$). If these operations satisfy the following equation:*

$$A_1(A_2(x, y), A_3(u, v)) = A_4(A_5(x, u), A_6(y, v)), \tag{2.15}$$

for all elements x, y, u and v of the set B then there exists an operation $'+'$ under which B forms an abelian group isotopic to all these six quasigroups. And there exist eight permutations α, β, γ, δ, ϵ, ψ, φ, χ of B such that:

$$\begin{aligned}
A_1(x, y) &= \delta x + \varphi y,\\
A_2(x, y) &= \delta^{-1}(\alpha x + \beta y),\\
A_3(x, y) &= \varphi^{-1}(\chi x + \gamma y),\\
A_4(x, y) &= \psi x + \epsilon y,\\
A_5(x, y) &= \psi^{-1}(\alpha x + \chi y),\\
A_6(x, y) &= \epsilon^{-1}(\beta x + \gamma y).
\end{aligned}$$

Theorem 5 (Krapež [14])**.** *If the set B forms a quasigroup under four operations $A_i(x, y)$ (for $i = 1, \ldots, 4$) and if these operations satisfy the equation of generalized transitivity:*

$$A_1(A_2(x, y), A_3(y, z)) = A_4(x, z),$$

for all elements $x, y, z \in B$, then there exists an operation $'+'$ under which B forms a group isotopic to all these quasigroups and there exist permutaions α, β, γ, δ, ϵ, ψ, φ, χ of B such that

$$\begin{aligned} A_1(x,y) &= \alpha x + \beta y, \\ A_2(x,y) &= \alpha^{-1}(\alpha\gamma x + \alpha\delta y), \\ A_3(x,y) &= \beta^{-1}(\beta\epsilon x + \beta\psi y), \\ A_4(x,y) &= \varphi x + \chi y. \end{aligned}$$

Theorem 6 (Krapež [13], Belousov [5])**.** *A quasigroup satisfying a balanced but not Belousov equation is isotopic to a group.*

Theorem 7 (Krapež, Taylor [16])**.** *A quasigroup satisfying a quadratic but not gemini equation is isotopic to a group.*

3 Parastrophically uncancellable quadratic equations with two function variables

We consider parastrophically uncancellable quadratic quasigroup equations of the form:

$$f_1(f_2(x_1,x_2),f_2(x_3,x_4)) = f_2(f_1(x_5,x_6),f_1(x_7,x_8)) \tag{Eq}$$

where $x_i \in \{x,y,u,v\}$, for $i = 1,\ldots,8$. Therefore, the equation (Eq) is quadratic level quasigroup equation with four (object) variables each appearing twice in the equation and with two function variables each appearing three times in the equation. There are 48 such equations and we attempt to solve them all.

There is a correspondence between generalized quadratic quasigroup equations and connected cubic graphs, namely Krstić graphs. Two such equations are parastrophically equivalent iff they have the same (i.e. isomorphic) Krstić graphs. Furthermore, an equation is parastrophically uncancellable iff the corresponding Krstić graph is 3–connected. For more detailed account of this correspondence see [16, 17] and [18].

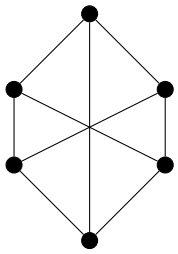
For everyone of the 48 equations (Eq) there is a corresponding generalized equation:

$$f_1(f_3(x_1,x_2),f_4(x_3,x_4)) = f_2(f_5(x_5,x_6),f_6(x_7,x_8)) \tag{GEq}$$

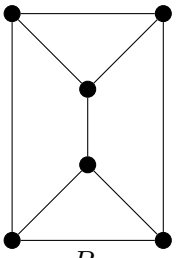
(where $x_i \in \{x,y,u,v\}$, for $i = 1,\ldots,8$) with the appropriate Krstić graph. This Krstić graph *will be assumed* to be the Krstić graph of (Eq) as well. All these equations can be partitioned into two classes, depending on their Krstić graphs, as follows:

– 16 balanced (and non-Belousov) equations with the Krstić graph $K_{3,3}$,

– 32 non–balanced non-gemini equations with the Krstić graph P_3.



$K_{3,3}$



P_3

To characterize a pair of quasigroup operations which satisfies a non–Belousov balanced functional equation, we need the notion of Lbranch (Rbranch) and the following properties of holomorphisms which were proved for Muofang loops in [19].

Definition 10. Let t be a term and x a variable. We define:

- If $x \notin var(t)$, then $\mathrm{Lbranch}(x,t)$ $(\mathrm{Rbranch}(x,t))$ is not defined,
- $\mathrm{Lbranch}(x,x) = \Lambda$ $(\mathrm{Rbranch}(x,x) = \Lambda)$ (Λ is the empty word),
- If $t = f_i(t_1,t_2)$ and both occurrences of x are in t_1, then $\mathrm{Lbranch}(x,t) = \alpha_i\,\mathrm{Lbranch}(x,t_1)$ $(\mathrm{Rbranch}(x,t) = \alpha_i\,\mathrm{Rbranch}(x,t_1))$,
- If $t = f_i(t_1,t_2)$ and both occurrences of x are in t_2, then $\mathrm{Lbranch}(x,t) = \beta_i\,\mathrm{Lbranch}(x,t_2)$ $(\mathrm{Rbranch}(x,t) = \beta_i\,\mathrm{Rbranch}(x,t_2))$,
- If $t = f_i(t_1,t_2)$ and x occurrs in both t_1 and t_2, then $\mathrm{Lbranch}(x,t) = \alpha_i\,\mathrm{Lbranch}(x,t_1)$ $(\mathrm{Rbranch}(x,t) = \beta_i\,\mathrm{Rbranch}(x,t_2))$,
- $\mathrm{Lbranch}(x, s=t) = \begin{cases} \mathrm{Lbranch}(x,s) & \text{if } x \in var(s), \\ \mathrm{Lbranch}(x,t) & \text{otherwise} \end{cases}$
- $\mathrm{Rbranch}(x, s=t) = \begin{cases} \mathrm{Rbranch}(x,t) & \text{if } x \in var(t), \\ \mathrm{Rbranch}(x,s) & \text{otherwise} \end{cases}$

Lemma 1. *Let the identity:*

$$\alpha_1(x+y) = \alpha_2(x) + \alpha_3(y)$$

be satisfied for bijections $\alpha_1, \alpha_2, \alpha_3$ on the group $(B;+)$. Then $\alpha_1, \alpha_2, \alpha_3 \in Hol(B;+)$.

Lemma 2. *Every holomorphism α of the group $(B;+)$ has the following forms:*

$$\alpha x = \varphi_1 x + k_1, \qquad \alpha x = k_2 + \varphi_2 x,$$

where $\varphi_1, \varphi_2 \in Aut(B;+)$ and $k_1, k_2 \in B$.

4 Equations with Krstić graph $K_{3,3}$

The class of non–gemini balanced (and therefore non–Belousov) quadratic functional equations consists of the following 16 equations with four object variables x, y, u, v and two quasigroup operations f_1, f_2:

$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(x,u),f_1(y,v)) \tag{4.1}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(x,u),f_1(v,y)) \tag{4.2}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(x,v),f_1(y,u)) \tag{4.3}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(x,v),f_1(u,y)) \tag{4.4}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(y,u),f_1(x,v)) \tag{4.5}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(y,u),f_1(v,x)) \tag{4.6}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(y,v),f_1(x,u)) \tag{4.7}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(y,v),f_1(u,x)) \tag{4.8}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(u,x),f_1(y,v)) \tag{4.9}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(u,x),f_1(v,y)) \tag{4.10}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(u,y),f_1(x,v)) \tag{4.11}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(u,y),f_1(v,x)) \tag{4.12}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(v,x),f_1(y,u)) \tag{4.13}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(v,x),f_1(u,y)) \tag{4.14}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(v,y),f_1(x,u)) \tag{4.15}$$
$$f_1(f_2(x,y),f_2(u,v)) = f_2(f_1(v,y),f_1(u,x)) \tag{4.16}$$

The following result generalizes, on the one hand Theorem 3, and on the other, the results from and immediately after Example 7 in [12].

Theorem 8. *Let the balanced non–Belousov quasigroup equations* (4.j) (j = 1,. . . ,16) *have the Krstić graph* $K_{3,3}$. *A general solution of any of* (4.j) *is given by:*

$$f_i(x,y) = \alpha_i x + c_i + \beta_i y \quad (i = 1,2) \tag{4.17}$$

where:

- $(B;+)$ *is an arbitrary Abelian group,*
- c_1, c_2 *are arbitrary elements of* B *such that* $f_1(c_2,c_2) = f_2(c_1,c_1)$,
- α_i, β_i $(i = 1,2)$ *are arbitrary automorphisms of* $+$ *such that:*

$$\mathrm{Lbranch}(z,(4.j)) = \mathrm{Rbranch}(z,(4.j)) \tag{4.18}$$

for all variables z *of the equation* (4.j).

The group $(B;+)$ *is unique up to isomorphism.*

Proof. (1) To show that the pair (f_1, f_2) of operations is a solution of (4.j), just replace $f_i(x, y)$ in (4.j) using (4.17) and all conditions (4.18).

(2) An equation (4.j) is an instance of the appropriate generalized equation (GEq) with the Krstić graph $K_{3,3}$. Therefore, all operations of (GEq) are isotopic to an Abelian group $+$ and the main operations f_1, f_2 can be chosen to be principally isotopic to it (see [17]):

$$f_i(x, y) = \lambda_i x + \varrho_i y \quad (i = 1, 2).$$

Replace this in (Eq) to get:

$$\lambda_1 f_2(x_1, x_2) + \varrho_1 f_2(x_3, x_4) = \lambda_2 f_1(x_5, x_6) + \varrho_2 f_1(x_7, x_8). \tag{4.19}$$

Since variables x_1, x_2 are separated on the right hand side of equation (4.19), replacing x_3 and x_4 by 0, we get:

$$\lambda_1(\lambda_2 x_1 + \varrho_2 x_2) + d = \sigma x_1 + \tau x_2$$

for $d = \varrho_1(\lambda_2 0 + \varrho_2 0)$ and appropriate σ, τ depending on n. Therefore:

$$\lambda_1(z + w) = \sigma\lambda_2^{-1} z + T\tau\varrho_2^{-1} w$$

(where $Tx = x - d$) and $\lambda_1 \in Hol(B; +)$.

Analogously we get $\varrho_1, \lambda_2, \varrho_2 \in Hol(B; +)$.

Using Lemma 2 we easily get (4.17) for $i = 1, 2$ where α_i, β_i are automorphisms of $(B; +)$.

Replace f_1 and f_2 in (4.j):

$$\alpha_1(\alpha_2 x_1 + c_2 + \beta_2 x_2) + c_1 + \beta_1(\alpha_2 x_3 + c_2 + \beta_2 x_4) =$$

$$= \alpha_2(\alpha_1 x_5 + c_1 + \beta_1 x_6) + c_2 + \beta_2(\alpha_1 x_7 + c_1 + \beta_1 x_8).$$

Replacing $x_1 = x_2 = x_3 = x_4 = 0$, we get:

$$\alpha_1 c_2 + c_1 + \beta_1 c_2 = \alpha_2 c_1 + c_2 + \beta_2 c_1,$$

i. e. $f_1(c_2, c_2) = f_2(c_1, c_1)$.

For $x_2 = x_3 = x_4 = 0$, we get:

$$\mathrm{Lbranch}(x_1, (4.\mathrm{j})) = \alpha_1\alpha_2 \mathrm{x}_1 = \gamma\delta \mathrm{x}_1 = \mathrm{Rbranch}(\mathrm{x}_1, (4.\mathrm{j}))$$

for some $\gamma, \delta \in \{\alpha_1, \beta_1, \alpha_2, \beta_2\}$ depending on j.

Analogously:

$$\mathrm{Lbranch}(x_i, (4.\mathrm{j})) = \mathrm{Rbranch}(\mathrm{x_i}, (4.\mathrm{j}))$$

for $i = 2, 3, 4$.

The uniqueness of the group $(B; +)$ follows from the Albert Theorem (see [6]): If two groups are isotopic, then they are isomorphic. □

5 Equations with Krstić graph P_3

There exist 32 parastrophically uncancellable non-gemini and non-balanced quadratic functional equations with four object variables and two operations:

$$f_1(f_2(x,y),f_2(x,u)) = f_2(f_1(y,v),f_1(u,v)) \tag{5.1}$$
$$f_1(f_2(x,y),f_2(x,u)) = f_2(f_1(y,v),f_1(v,u)) \tag{5.2}$$
$$f_1(f_2(x,y),f_2(x,u)) = f_2(f_1(u,v),f_1(y,v)) \tag{5.3}$$
$$f_1(f_2(x,y),f_2(x,u)) = f_2(f_1(u,v),f_1(v,y)) \tag{5.4}$$
$$f_1(f_2(x,y),f_2(x,u)) = f_2(f_1(v,y),f_1(u,v)) \tag{5.5}$$
$$f_1(f_2(x,y),f_2(x,u)) = f_2(f_1(v,y),f_1(v,u)) \tag{5.6}$$
$$f_1(f_2(x,y),f_2(x,u)) = f_2(f_1(v,u),f_1(y,v)) \tag{5.7}$$
$$f_1(f_2(x,y),f_2(x,u)) = f_2(f_1(v,u),f_1(v,y)) \tag{5.8}$$
$$f_1(f_2(x,y),f_2(y,u)) = f_2(f_1(x,v),f_1(u,v)) \tag{5.9}$$
$$f_1(f_2(x,y),f_2(y,u)) = f_2(f_1(x,v),f_1(v,u)) \tag{5.10}$$
$$f_1(f_2(x,y),f_2(y,u)) = f_2(f_1(u,v),f_1(x,v)) \tag{5.11}$$
$$f_1(f_2(x,y),f_2(y,u)) = f_2(f_1(u,v),f_1(v,x)) \tag{5.12}$$
$$f_1(f_2(x,y),f_2(y,u)) = f_2(f_1(v,x),f_1(u,v)) \tag{5.13}$$
$$f_1(f_2(x,y),f_2(y,u)) = f_2(f_1(v,x),f_1(v,u)) \tag{5.14}$$
$$f_1(f_2(x,y),f_2(y,u)) = f_2(f_1(v,u),f_1(x,v)) \tag{5.15}$$
$$f_1(f_2(x,y),f_2(y,u)) = f_2(f_1(v,u),f_1(v,x)) \tag{5.16}$$
$$f_1(f_2(x,y),f_2(u,x)) = f_2(f_1(y,v),f_1(u,v)) \tag{5.17}$$
$$f_1(f_2(x,y),f_2(u,x)) = f_2(f_1(y,v),f_1(v,u)) \tag{5.18}$$
$$f_1(f_2(x,y),f_2(u,x)) = f_2(f_1(u,v),f_1(y,v)) \tag{5.19}$$
$$f_1(f_2(x,y),f_2(u,x)) = f_2(f_1(u,v),f_1(v,y)) \tag{5.20}$$
$$f_1(f_2(x,y),f_2(u,x)) = f_2(f_1(v,y),f_1(u,v)) \tag{5.21}$$
$$f_1(f_2(x,y),f_2(u,x)) = f_2(f_1(v,y),f_1(v,u)) \tag{5.22}$$
$$f_1(f_2(x,y),f_2(u,x)) = f_2(f_1(v,u),f_1(y,v)) \tag{5.23}$$
$$f_1(f_2(x,y),f_2(u,x)) = f_2(f_1(v,u),f_1(v,y)) \tag{5.24}$$
$$f_1(f_2(x,y),f_2(u,y)) = f_2(f_1(x,v),f_1(u,v)) \tag{5.25}$$
$$f_1(f_2(x,y),f_2(u,y)) = f_2(f_1(x,v),f_1(v,u)) \tag{5.26}$$
$$f_1(f_2(x,y),f_2(u,y)) = f_2(f_1(u,v),f_1(x,v)) \tag{5.27}$$
$$f_1(f_2(x,y),f_2(u,y)) = f_2(f_1(u,v),f_1(v,x)) \tag{5.28}$$
$$f_1(f_2(x,y),f_2(u,y)) = f_2(f_1(v,x),f_1(u,v)) \tag{5.29}$$
$$f_1(f_2(x,y),f_2(u,y)) = f_2(f_1(v,x),f_1(v,u)) \tag{5.30}$$
$$f_1(f_2(x,y),f_2(u,y)) = f_2(f_1(v,u),f_1(x,v)) \tag{5.31}$$
$$f_1(f_2(x,y),f_2(u,y)) = f_2(f_1(v,u),f_1(v,x)) \tag{5.32}$$

The next theorem gives a general solution of the equation (5.10) which generalizes the *intermedial equation* (see equation (4.36) and Theorem 8.4 of [15] for the original definition of intermedial equation).

Lemma 3. *A general solution of the equation* (5.10) *is given by:*

$$f_i(x,y) = \alpha_i x + c_i + \beta_i y \quad (i = 1,2) \tag{5.33}$$

where:

- $(B;+)$ *is an arbitrary group,*
- c_1, c_2 *are arbitrary elements of* B *such that* $f_1(c_2,c_2) = f_2(c_1,c_1)$*,*
- α_i, β_i $(i = 1,2)$ *are arbitrary automorphisms of* $+$ *such that:*

$$\mathrm{Lbranch}(z,(5.10)) = \mathrm{Rbranch}(z,(5.10)) \tag{5.34}$$

for $z \in \{x,u\}$ *and*

$$\mathrm{Lbranch}(w_i,(5.10))w_i + c_i + \mathrm{Rbranch}(w_i,(5.10))w_i = c_i \tag{5.35}$$

for $i \in \{1,2\}, w_1 = y$ *and* $w_2 = v$*.*

The group $(B;+)$ *is unique up to isomorphism.*

Proof. (1) To show that the pair (f_1,f_2) of operations is a solution of (5.10), just replace $f_i(x,y)$ in (5.10) using (5.33) and all conditions (5.34), (5.35).

(2) The equation (5.10) is an instance of the generalized intermedial equation:

$$f_1(h_1(x,y),h_2(y,u)) = f_2(h_3(x,v),h_4(v,u)). \tag{GI}$$

Choose $v = a$ for some $a \in B$ and define $\gamma x = h_1(x,a), \delta u = h_2(a,u)$ and $g(x,u) = f_2(\gamma x, \delta u)$. We get:

$$f_1(h_1(x,y),h_2(y,u)) = g(x,u) \tag{GT}$$

which is the generalized transitivity equation. By Theorem 5 all operations of this equation are isotopic to a group $+$ and the main operations f_1, g can be chosen to be principally isotopic to it:

$$f_1(x,y) = \lambda_1 x + \varrho_1 y, \qquad g(x,y) = \lambda_3 x + \varrho_3 y.$$

It follows that $f_2(x,y) = \lambda_3\gamma^{-1}x + \varrho_3\delta^{-1}y = \lambda_2 x + \varrho_2 y$ for appropriate λ_2, ϱ_2. Replacing this in (5.10) we get:

$$\lambda_1(\lambda_2 x + \varrho_2 y) + \varrho_1(\lambda_2 y + \varrho_2 u) = \lambda_2(\lambda_1 x + \varrho_1 v) + \varrho_2(\lambda_1 v + \varrho_1 u). \tag{5.36}$$

If we choose $\varrho_2 u = \varrho_1 v = 0$ and define $d = \varrho_2(\lambda_1\varrho_1^{-1}0 + \varrho_1\varrho_2^{-1}0)$ we get:

$$\lambda_1(\lambda_2 x + \varrho_2 y) + \varrho_1\lambda_2 y = \lambda_2\lambda_1 x + d$$

which implies that $\lambda_1 \in Hol(B;+)$.

Analogously we get $\varrho_1, \lambda_2, \varrho_2 \in Hol(B;+)$.

Using Lemma 2 we easily get (5.33) for $i = 1, 2$ where α_i, β_i are automorphisms of $(B;+)$.

Replace f_1 and f_2 in (5.10):

$$\alpha_1(\alpha_2 x + c_2 + \beta_2 y) + c_1 + \beta_1(\alpha_2 y + c_2 + \beta_2 u) =$$

$$= \alpha_2(\alpha_1 x + c_1 + \beta_1 v) + c_2 + \beta_2(\alpha_1 v + c_1 + \beta_1 u).$$

Putting $x = y = u = v = 0$, we get:

$$\alpha_1 c_2 + c_1 + \beta_1 c_2 = \alpha_2 c_1 + c_2 + \beta_2 c_1,$$

i. e. $f_1(c_2, c_2) = f_2(c_1, c_1)$.

For $y = u = v = 0$ we get:

$$\mathrm{Lbranch}(x, (5.10)) = \alpha_1\alpha_2 = \alpha_2\alpha_1 = \mathrm{Rbranch}(x, (5.10)).$$

Analogously:

$$\mathrm{Lbranch}(u, (5.10)) = \mathrm{Rbranch}(u, (5.10)),$$

$$\mathrm{Lbranch}(y, (5.10))y + c_1 + \mathrm{Rbranch}(u, (5.10))y = \alpha_1\beta_2 y + c_1 + \beta_1\alpha_2 y = c_1,$$

$$\mathrm{Lbranch}(v, (5.10))v + c_2 + \mathrm{Rbranch}(v, (5.10))v = \alpha_2\beta_1 v + c_2 + \beta_2\alpha_1 v = c_2.$$

The uniqueness of the group $(B;+)$ follows from the Albert Theorem. □

Lemma 4. *A general solution of the equation* (5.j) (j = 1, 2, 5, 6, 9, 13, 14, 17, 18, 21, 22, 25, 26, 29, 30) *is given by:*

$$f_i(x, y) = \alpha_i x + c_i + \beta_i y \quad (i = 1, 2) \tag{5.37}$$

where:

- $(B;+)$ *is an arbitrary Abelian group,*
- c_1, c_2 *are arbitrary elements of* B *such that* $f_1(c_2, c_2) = f_2(c_1, c_1)$,
- α_i, β_i $(i = 1, 2)$ *are arbitrary automorphisms of* $+$ *such that:*

$$\mathrm{Lbranch}(z, (5.\mathrm{j})) = \mathrm{Rbranch}(z, (5, \mathrm{j})) \tag{5.38}$$

for all linear variables z *of* (5.j) *and*

$$\mathrm{Lbranch}(w, (5.\mathrm{j}))w + \mathrm{Rbranch}(w, (5.\mathrm{j}))w = 0 \tag{5.39}$$

for all quadratic variables w *from the equation.*

The group $(B;+)$ *is unique up to isomorphism.*

Proof. (1) To show that the pair (f_1, f_2) of operations is a solution of (5.j), just replace $f_i(x, y)$ in (5.j) using (5.37) and all conditions (5.38), (5.39).

(2) The crucial property of all 15 equations (5.j) is that, by applying duality to some of non–main operations of the generalized version of (5.j), they may be transformed into equation (GI):

$$f_1(h_1(x, y), h_2(y, u)) = f_2(h_3(x, v), h_4(v, u))$$

which, by the proof of Lemma 3, has a solution:

$$f_i(x, y) = \alpha_i x + c_i + \beta_i y \quad (i = 1, 2)$$

where $(B; +)$ is a group and α_i, β_i are automorphisms of $+$.

Replacing f_1, f_2 in (5.j), we get:

$$\begin{aligned} &\alpha_1(\alpha_2 x_1 + c_2 + \beta_2 x_2) + c_1 + \beta_1(\alpha_2 x_3 + c_2 + \beta_2 x_4) = \\ &= \alpha_2(\alpha_1 x_5 + c_1 + \beta_1 x_6) + c_2 + \beta_2(\alpha_1 x_7 + c_1 + \beta_1 x_8). \end{aligned} \tag{5.40}$$

Just as in the proof of Lemma 3, we conclude that $f_1(c_2, c_2) = f_2(c_1, c_1)$. Let us define $c = f_1(c_2, c_2)$.

To prove the properties from the statement of the lemma, we need to discuss the arrangement $x_1 \dots x_4 = x_5 \dots x_8$ of variables in the equation (5.40). It is easy to see:

- The order of first (i. e. left) appearances of variables is always $xyuv$.
- $x_1 = x$.
- Since P_3 has no loops, $x_2 = y$.
- Either x or y is quadratic, but not both.
- Variable u is always linear.
- Variable v is always quadratic.
- Arrangement $xyyu = xvvu$ is not allowed.

There are two possibilities: x is either linear or quadratic.

a) Variable x is linear (and y is quadratic).
Again, there are two possibilities: Either $x_3 = y$ or $x_3 = u$.

a1) $x_3 = y$ (and $x_4 = u$).
Yet again, there are two possibilities: Either $x_5 = x$ or $x_5 = v$.

a11) The arrangement of variables is $xyyu = xvuv$.
We have equation (5.9). Replacing $x = y = 0$ in (5.40), we get:

$$c + \beta_1\beta_2 u = \alpha_2 c_1 + \alpha_2\beta_1 v + c_2 + \beta_2\alpha_1 u + \beta_2 c_1 + \beta_2\beta_1 v. \tag{5.41}$$

For $v = 0$ we get:

$$\beta_2 c_1 + \beta_1\beta_2 u = \beta_2\alpha_1 u + \beta_2 c_1 \tag{5.42}$$

and for $u = 0$:

$$c - \beta_2\beta_1 v = \alpha_2 c_1 + \alpha_2\beta_1 v + c_2 + \beta_2 c_1. \tag{5.43}$$

Applying (5.42) and (5.43) to (5.41), we conclude:

$$c + \beta_1\beta_2 u - \beta_2\beta_1 v = c - \beta_2\beta_1 v + \beta_1\beta_2 u$$

which is, after cancellation from the left, equivalent to commutativity of $+$. Therefore $(B; +)$ is an Abelian group.

a12) The arrangement of variables is $xyyu = vx(uv \text{ or } vu)$.
Replacement $y = u = 0$ leads to:

$$\alpha_1\alpha_2 x + c = \alpha_2\alpha_1 v + \alpha_2 c_1 + \alpha_2\beta_1 x + c_2 + t(v) \tag{5.44}$$

where

$$t(v) = \begin{cases} \beta_2\alpha_1 v + \beta_2 c_1 & \text{if } \ x_7 = v, \\ \beta_2 c_1 + \beta_2\beta_1 v & \text{if } \ x_7 = u. \end{cases}$$

Note that in both cases $t(0) = \beta_2 c_1$. Putting $x = 0$, we get:

$$t(v) = -c_2 - \alpha_2 c_1 - \alpha_2\alpha_1 v + c \tag{5.45}$$

while replacement $v = 0$ leads to:

$$\alpha_1\alpha_2 x + \alpha_2 c_1 = \alpha_2 c_1 + \alpha_2\beta_1 x. \tag{5.46}$$

Using (5.45) and (5.46) in (5.44), we conclude:

$$\alpha_1\alpha_2 x + c = \alpha_2\alpha_1 v + \alpha_1\alpha_2 x - \alpha_2\alpha_1 v + c$$

which implies that the group $(B; +)$ is Abelian.

a2) $x_3 = u$ (and $x_4 = y$).
The arrangement of variables is $xyuy = (xv \text{ or } vx)(uv \text{ or } vu)$. Replacement $x = v = 0$ in (5.j) yields:

$$\alpha_1 c_2 + \alpha_1\beta_2 y + c_1 + \beta_1\alpha_2 u + \beta_1 c_2 + \beta_1\beta_2 y = t(u) \tag{5.47}$$

where

$$t(u) = \begin{cases} \alpha_2 c_1 + c_2 + \beta_2\alpha_1 u + \beta_2 c_1 & \text{if } \ x_7 = u, \\ c + \beta_2\beta_1 u & \text{if } \ x_7 = v. \end{cases}$$

Note that in both cases $t(0) = c$. Putting $y = 0$ in (5.47), we get:

$$\alpha_1 c_2 + c_1 + \beta_1\alpha_2 u + \beta_1 c_2 = t(u) \tag{5.48}$$

while replacement $u = 0$ yields:

$$\alpha_1 c_2 + \alpha_1\beta_2 y + c_1 = c - \beta_1\beta_2 y - \beta_1 c_2. \tag{5.49}$$

Feeding (5.48) and (5.49) in (5.47), we get:

$$c - \beta_1\beta_2 y - \beta_1 c_2 + \beta_1\alpha_2 u + \beta_1 c_2 = \alpha_1 c_2 + c_1 + \beta_1\alpha_2 u + \beta_1 c_2 - \beta_1\beta_2 y$$

which implies commutativity of $+$.

b) Variable x is quadratic (and y is linear).
The arrangement of variables is $xy(xu \text{ or } ux) = (yv \text{ or } vy)(uv \text{ or } vu)$. Let $u = v = 0$. We have:

$$\alpha_1\alpha_2 x + \alpha_1 c_2 + \alpha_1\beta_2 y + c_1 + s(x) = t(y) \tag{5.50}$$

where:

$$s(x) = \begin{cases} \beta_1\alpha_2 x + \beta_1 c_2 & \text{if } \ x_3 = x, \\ \beta_1 c_2 + \beta_1\beta_2 x & \text{if } \ x_3 = u, \end{cases}$$

$$t(y) = \begin{cases} \alpha_2\alpha_1 y + c & \text{if } \ x_5 = y, \\ \alpha_2 c_1 + \alpha_2\beta_1 y + c_2 + \beta_2 c_1 & \text{if } \ x_5 = v. \end{cases}$$

Note that $s(0) = \beta_1 c_2$ and $t(0) = c$. Specifying $x = 0$, we get:

$$\alpha_1 c_2 + \alpha_1\beta_2 y + c_1 + \beta_1 c_2 = t(y) \tag{5.51}$$

while $y = 0$ yields:

$$c_1 + s(x) = -\alpha_1 c_2 - \alpha_1\alpha_2 x + c. \tag{5.52}$$

Feeding (5.51) and (5.52) into (5.50), we get:

$$\alpha_1\alpha_2 x + \alpha_1 c_2 + \alpha_1\beta_2 y - \alpha_1 c_2 - \alpha_1\alpha_2 x + \alpha_1 c_2 = \alpha_1 c_2 + \alpha_1\beta_2 y$$

which implies that the group $(B; +)$ is Abelian.

Because of commutativity of $+$ and the condition for c, the equation (5.j) reduces to:

$$\begin{aligned} &\alpha_1\alpha_2 x_1 + \alpha_1\beta_2 x_2 + \beta_1\alpha_2 x_3 + \beta_1\beta_2 x_4 = \\ &= \alpha_2\alpha_1 x_5 + \alpha_2\beta_1 x_6 + \beta_2\alpha_1 x_7 + \beta_2\beta_1 x_8), \end{aligned}$$

which is equivalent to the system:

$$\mathrm{Lbranch}(z, (5.\mathrm{j})) = \mathrm{Rbranch}(\mathrm{z}, (5, \mathrm{j}))$$

$$\mathrm{Lbranch}(w, (5.\mathrm{j}))\mathrm{w} + \mathrm{Rbranch}(\mathrm{w}, (5.\mathrm{j}))\mathrm{w} = 0$$

for all linear variables z and all quadratic variables w.

The uniqueness of the group $(B; +)$ follows from the Albert Theorem. □

Lemma 5. *A general solution of the equation* (5.23) *is given by:*

$$\begin{cases} f_1(x,y) = \alpha_1 x + c_1 + \beta_1 y \\ f_2(x,y) = \beta_2 y + c_2 + \alpha_2 x \end{cases} \tag{23}$$

where:

- $(B;+)$ *is an arbitrary group,*
- c_1, c_2 *are arbitrary elements of* B *such that* $f_1(c_2,c_2) = f_2(c_1,c_1)$*,*
- α_i, β_i $(i=1,2)$ *are arbitrary automorphisms of* $+$ *such that:*

$$\mathrm{Lbranch}(z,(5.23)) = \mathrm{Rbranch}(z,(5.23)) \tag{5.53}$$

for $z \in \{y,u\}$*,*

$$\mathrm{Lbranch}(x,(5.23))x + c_1 + \mathrm{Rbranch}(x,(5.23))x = c_1 \tag{5.54}$$

,

$$\mathrm{Rbranch}(v,(5.23))v + c_2 + \mathrm{Lbranch}(v,(5.23))v = c_2. \tag{5.55}$$

The group $(B;+)$ *is unique up to isomorphism.*

Proof. (1) To show that the pair (f_1,f_2) of operations is a solution of (5.23), just replace $f_i(x,y)$ in (5.23) using (23) and all conditions (5.53)–(5.55).

(2) Define new quasigroup f_3 to be the dual quasigroup of f_2, i. e. $f_3(x,y) = f_2(y,x)$. The equation (5.23) transforms into equation (5.10) with a general solution given by Lemma 3:

$$\begin{cases} f_1(x,y) = \alpha_1 x + c_1 + \beta_1 y \\ f_3(x,y) = \alpha_3 x + c_3 + \beta_3 y \end{cases} \tag{23*}$$

where:

- $(B;+)$ is an arbitrary group,
- c_1, c_3 are arbitrary elements of B such that $f_1(c_3,c_3) = f_3(c_1,c_1)$,
- α_i, β_i $(i=1,3)$ are arbitrary automorphisms of $+$ such that:

$$\alpha_1\alpha_3 = \alpha_3\alpha_1$$

$$\beta_1\beta_3 = \beta_3\beta_1$$

$$\alpha_1\beta_3 x + c_1 + \beta_1\beta_3 x = c_1$$

$$\alpha_3\beta_1 v + c_3 + \beta_3\alpha_1 v = c_3.$$

Define: $\alpha_2 = \beta_3, \beta_2 = \alpha_3$ and $c_2 = c_3$ and replace in (23*) to get:
$f_2(x,y) = f_3(y,x) = \alpha_3 y + c_2 + \beta_3 x = \beta_2 y + c_2 + \alpha_2 x$, and

$$\alpha_1\beta_2 = \beta_2\alpha_1$$

$$\beta_1\alpha_2 = \alpha_2\beta_1$$

$$\alpha_1\alpha_2 x + c_1 + \beta_1\alpha_2 x = c_1$$

$$\beta_2\beta_1 v + c_2 + \alpha_2\alpha_1 v = c_2,$$

which is:

$$\mathrm{Lbranch}(z,(5.23)) = \mathrm{Rbranch}(z,(5.23))$$

for $z \in \{y,u\}$, and

$$\mathrm{Lbranch}(x,(5.23))x + c_1 + \mathrm{Rbranch}(x,(5.23))x = c_1,$$

$$\mathrm{Rbranch}(v,(5.23))v + c_2 + \mathrm{Lbranch}(v,(5.23))v = c_2.$$

Trivially, $f_1(c_2,c_2) = f_2(c_1,c_1)$.
The uniqueness of the group $(B;+)$ follows from the Albert Theorem. □

Lemma 6. *A general solution of the equation* (5.k) (k = 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 24, 27, 28, 31, 32) *is given by:*

$$f_i(x,y) = \alpha_i x + c_i + \beta_i y \quad (i = 1,2) \tag{5.56}$$

where:

- $(B;+)$ *is an arbitrary Abelian group,*
- c_1, c_2 *are arbitrary elements of* B *such that* $f_1(c_2,c_2) = f_2(c_1,c_1)$,
- α_i, β_i $(i = 1,2)$ *are arbitrary automorphisms of* $+$ *such that:*

$$\mathrm{Lbranch}(z,(5.\mathrm{k})) = \mathrm{Rbranch}(z,(5,\mathrm{k})) \tag{5.57}$$

for all linear variables z *of* (5.j) *and*

$$\mathrm{Lbranch}(w,(5.\mathrm{k}))w + \mathrm{Rbranch}(w,(5.\mathrm{k}))w = 0 \tag{5.58}$$

for all quadratic variables w *from the equation.*

The group $(B;+)$ *is unique up to isomorphism.*

Proof. (1) To show that the pair (f_1, f_2) of operations is a solution of (5.k), just replace $f_i(x, y)$ in (5.k) using (5.56) and all conditions (5.57), (5.58).

(2) Let us prove that the solution given in the lemma is general in the case $k = 3$.

The equation (5.3) has arrangement of variables equal to $xyxu = uvyv$. Let us replace the operation f_2 in (5.3) by the dual operation $f_3(x, y) = f_2^*(x, y) = f_2(y, x)$. We get the equation

$$f_1(f_3(y, x), f_3(u, x)) = f_3(f_1(y, v), f_1(u, v))$$

with the arrangement of variables equal to $yxux = yvuv$. Normalizing (i.e. applying the permutation (xy) to variables) we get the equation (5.25) with a general solution given in Lemma 4:

$$f_i(x, y) = \alpha_i x + c_i + \beta_i y \quad (i = 1, 3) \tag{5.59}$$

where:

- $(B; +)$ is an arbitrary group,
- c_1, c_3 are arbitrary elements of B such that $f_1(c_3, c_3) = f_3(c_1, c_1)$,
- α_i, β_i $(i = 1, 3)$ are arbitrary automorphisms of $+$ such that:

  $$\mathrm{Lbranch}(z, (5.25)) = \mathrm{Rbranch}(z, (5.25)) \tag{5.60}$$

  for all linear variables z of (5.25) and

  $$\mathrm{Lbranch}(w, (5.25))w + \mathrm{Rbranch}(w, (5.25))w = 0 \tag{5.61}$$

  for all quadratic variables w from the equation.

Conditions (5.60) and (5.61) evaluate to:

$$\alpha_1\alpha_3 = \alpha_3\alpha_1$$

$$\beta_1\alpha_3 = \beta_3\alpha_1$$

$$\alpha_1\beta_3 x + \beta_1\beta_3 x = 0$$

$$\alpha_3\beta_1 v + \beta_3\beta_1 v = 0.$$

Define: $\alpha_2 = \beta_3, \beta_2 = \alpha_3, c_2 = c_3$ and replace in (5.59) to get:
$f_2(x, y) = f_3(y, x) = \alpha_3 y + c_3 + \beta_3 x = \beta_2 y + c_2 + \alpha_2 x = \alpha_2 x + c_2 + \beta_2 y$, and

$$\alpha_1\beta_2 = \beta_2\alpha_1$$

$$\beta_1\beta_2 = \alpha_2\alpha_1$$

$$\alpha_1\alpha_2 x + \beta_1\alpha_2 x = 0$$

$$\beta_2\beta_1 v + \alpha_2\beta_1 v = 0,$$

which is:

$$\mathrm{Lbranch}(z,(5,3)) = \mathrm{Rbranch}(z,(5,3))$$

for $z \in \{y,u\}$, and

$$\mathrm{Lbranch}(w,(5.3))w + \mathrm{Rbranch}(x,(5.3))w = 0,$$

for $w \in \{x,v\}$.

Trivially, $f_1(c_2,c_2) = f_2(c_1,c_1)$.

Analogously, we can transform (5.4) into (5.29), (5.7) into (5.26), (5.8) into (5.30), (5.11) into (5.17), (5.12) into (5.21), (5.15) into (5.18), (5.16) into (5.22), (5.19) into (5.9), (5.20) into (5.13), (5.24) into (5.14), (5.27) into (5.1), (5.28) into (5.5), (5.31) into (5.2), (5.32) into (5.6) and prove appropriate relationships between $\alpha_i, \beta_i, c_i\,(i = 1,2)$ for these equations, using results given in Lemma 4. □

Definition 11. Let $\partial : B \longrightarrow B$ be the natural antiautomorphism of the group $(B;+)$ with itself so that $\partial(x+y) = y+x$.

It is easy to see that for all natural numbers n, $\partial(x_1 + x_2 + \cdots + x_n) = x_n + x_{n-1} + \cdots x_1$. In particular $\partial(x+y+z) = z+y+x$. Also, for all even (odd) j and all terms t: $\partial^j(t) = t$ $(\partial^j(t) = \partial(t))$.

We may now combine Lemmas 3 and 5 into:

Theorem 9. *A general solution of the equation* (5.j) (j = 10,23) *is given by:*

$$\begin{cases} f_1(x,y) = \alpha_1 x + c_1 + \beta_1 y \\ f_2(x,y) = \partial^{\mathrm{j}}(\alpha_2 x + c_2 + \beta_2 y) \end{cases}$$

where:

- $(B;+)$ *is an arbitrary group,*
- c_1, c_2 *are arbitrary elements of* B *such that* $f_1(c_2,c_2) = f_2(c_1,c_1)$,
- α_i, β_i $(i = 1,2)$ *are arbitrary automorphisms of* $+$ *such that:*

  $$\mathrm{Lbranch}(z,(5.\mathrm{j})) = \mathrm{Rbranch}(z,(5.\mathrm{j}))$$

  for all linear variables z *of the equation* (5.j) *and*

  $$\mathrm{Lbranch}(w_i,(5.\mathrm{j}))w_i + c_i + \mathrm{Rbranch}(w_i,(5.\mathrm{j}))w_i = c_i$$

  for $i \in \{1,2\}$, *where* w_1 *is the left quadratic variable while* w_2 *is the right quadratic variable of* (5.j).

The group $(B;+)$ *is unique up to isomorphism.*

Likewise, Theorem 8 and Lemmas 4 and 6 can be combined into:

Theorem 10. *A general solution of the equation* $(m.\mathrm{j_m})$ $(m = 4, 5;\ 1 \leq \mathrm{j}_4 \leq 16;\ 1 \leq \mathrm{j}_5 \leq 32;\ \mathrm{j}_5 \neq 10, 23)$ *is given by:*

$$f_i(x, y) = \alpha_i x + c_i + \beta_i y \quad (i = 1, 2)$$

where:

- $(B; +)$ *is an arbitrary Abelian group,*
- c_1, c_2 *are arbitrary elements of* B *such that* $f_1(c_2, c_2) = f_2(c_1, c_1)$*,*
- α_i, β_i $(i = 1, 2)$ *are arbitrary automorphisms of* $+$ *such that:*

$$\mathrm{Lbranch}(z, (m.\mathrm{j_m})) = \mathrm{Rbranch}(\mathrm{z}, (\mathrm{m.j_m}))$$

for all linear variables z *of* $(m.\mathrm{j_m})$ *and*

$$\mathrm{Lbranch}(w, (m.\mathrm{j_m}))\mathrm{w} + \mathrm{Rbranch}(\mathrm{w}, (\mathrm{m.j_m}))\mathrm{w} = 0$$

for all quadratic variables w *from the equation.*

The group $(B; +)$ *is unique up to isomorphism.*

6 Algebras with Parastrophically Uncancellable Quadratic Hyperidentities

By [20, 21], a hyperidentity (or $\forall(\forall)$-identity) is a second-order formula of the following form:

$$\forall f_1, \ldots, f_k \forall x_1, \ldots, x_n \qquad (w_1 = w_2),$$

where w_1, w_2 are words (terms) in the alphabet of function variables $f_1, \ldots, f_k$ and object variables $x_1, \ldots, x_n$. However hyperidentities are usually presented without universal quantifiers: $w_1 = w_2$. The hyperidentity $w_1 = w_2$ is said to be satisfied in the algebra $(B; F)$ if this equality holds whenever every function variable f_i is replaced by an arbitrary operation of the corresponding arity from F and every object variable x_i is replaced by an arbitrary element of B.

Now, as a consequence of the results of the previous section, we can establish the following representation of a binary algebra satisfying one of the non-gemini hyperidentities.

Theorem 11. *Let* $(B; F)$ *be a binary algebra with quasigroup operations which satisfy one of the non–gemini hyperidentities* $(m.\mathrm{j_m})$ $(m = 4, 5;\ 1 \leq \mathrm{j}_4 \leq 16;\ 1 \leq \mathrm{j}_5 \leq 32)$*. Then there exists an Abelian group* $(B; +)$ *such that every operation* $f_i \in F$ *is represented by:*

$$f_i(x, y) = \alpha_i(x) + c_i + \beta_i(y),$$

where:

- c_i $(i = 1, \ldots, |F|)$ *are arbitrary elements of* B *such that* $f_l(c_k, c_k) = f_k(c_l, c_l)$ *for* $1 \leqslant l, k \leqslant |F|$,
- α_i, β_i $(i = 1, \ldots, |F|)$ *are arbitrary automorphisms of* $+$ *such that:*

$$\mathrm{Lbranch}(z, (m.\mathrm{j_m})) = \mathrm{Rbranch}(\mathrm{z}, (\mathrm{m}.\mathrm{j_m}))$$

for all linear variables z *of* $(m.\mathrm{j_m})$ *and*

$$\mathrm{Lbranch}(w, (m.\mathrm{j_m}))\mathrm{w} + \mathrm{Rbranch}(\mathrm{w}, (\mathrm{m}.\mathrm{j_m}))\mathrm{w} = 0$$

for all quadratic variables w *from the equation.*

Proof. Let us consider the pair (f_1, f_1) of operations satisfying equation $(m.\mathrm{j_m})$ (for $m = 4$ or 5; j_4 is some of $1, 2, \ldots, 16$ while j_5 is some of $1, 2, \ldots, 32$). Then

$$f_1(x, y) = \alpha_1(x) + c_1 + \beta_1(y)$$

where $+$ is a group and α_1, β_1 its automorphisms. In the case of equation (5.10) ((5.23)) the group $+$ is commutative by Theorem 1 (Theorem 2). In all other cases $+$ is commutative by Theorem 10.

For any $i \in F$, $i \neq 1$, the pair (f_1, f_i) also satisfies $(m.\mathrm{j_m})$, hence both are principally isotopic to a group (perhaps other than $+$). Anyway, f_i is also principally isotopic to $+$ and by Theorem 9 or 10

$$f_i(x, y) = \alpha_i(x) + c_i + \beta_i(y)$$

where $c_i \in B$ and $\alpha_i, \beta_i \in Aut(B; +)$ such that

$$\mathrm{Lbranch}(z, (m.\mathrm{j_m})) = \mathrm{Rbranch}(\mathrm{z}, (\mathrm{m}.\mathrm{j_m}))$$

for all linear variables z of $(m.j_m)$ and

$$\mathrm{Lbranch}(w, (m.\mathrm{j_m}))\mathrm{w} + \mathrm{Rbranch}(\mathrm{w}, (\mathrm{m}.\mathrm{j_m}))\mathrm{w} = 0$$

for all quadratic variables w from the equation.

The rest of the proof is easy. □

Acknowledgement

The work of A. Krapež is supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia, grants ON 174008 and ON 174026.

The work of Yu. Movsisyan is supported by the 'Center of Mathematical Research' of the state Committee of Science of the Republic of Armenia.

References

[1] Aczél J., Belousov V. D., Hosszú M. *Generalized associativity and bisymmetry on quasigroups* . Acta Math. Sci. Hung., 1960, **11**, 127-136.

[2] Belousov V. D. *Systems of quasigroups with generalized identities.* Usp. Mat. Nauk., 1965, **20**, 75–144 (in Russian). English translation: Russian Mathematical Surveys., **20**, 1965, 73–143.

[3] Belousov V. D. *Foundations of the theory of quasigroups and loops.* Moscow, Nauka, 1967 (in Russian).

[4] Belousov V. D. *Configurations in algebraic nets.* Kishinev, Shtiinca, 1979 (in Russian).

[5] Belousov V. D. *Quasigroups with completely reducible balanced identities.* Mat. Issled., 1985, **83**, 11–25 (in Russian).

[6] Bruck R. H. *Some results in the theory of quasigroups.* Trans. American Math. Soc., 1944, **55**, 19–52.

[7] Burris S., Sankappanavar H. P. *A course in Universal Algebra.* Graduate Texts in Mathematics, vol. 78, Springer-Verlag, Berlin-Heidelberg-New York, 1981.

[8] Chein O., Pflugfelder H. O., Smith J. D. H. *Quasigroups and Loops: Theory and Applications.* Sigma Series in Pure Math. 9, Heldermann Verlag, Berlin, 1990.

[9] Dénes J., Keedwell A. D. *Latin squares and their applications.* Acadmiai Kiadó, Budapest, 1974.

[10] Ehsani A., Movsisyan Yu. M. *Linear representation of medial-like algebras.* Comm. Algebra, 2013, **41, No. 9**, 3429–3444.

[11] Fisher R. A. *The design of experiments (8th edition).* Oliver & Boyd, Edinburgh, 1966.

[12] Förg-Rob W., Krapež A. *Equations which preserve the height of variables.* Aequat. Math., 2005, **70**, 63–76.

[13] Krapež A. *On solving a system of balanced functional equations on quasigroups III.* Publ. Inst. Math., Nouv. Sér., 1979, **26(40)**, 145–156.

[14] Krapež A. *Functional equations of generalized associativity, bisymmetry, transitivity and distributivity.* Publications de L'Institut Mathematique, 1981, **30(44)**, 81–87.

[15] Krapež A. *Quadratic level quasigroup equations with four variables I.* Publ. Inst. Math., Nouv. Sér., 2007, **81(95)**, 53–67.

[16] Krapež A., Taylor M. A. *Gemini functional equations on quasigroups.* Publ. Math. (Debrecen), 1995, **47/3-4**, 283–292.

[17] Krapež A., Živković D. *Parastrophically equivalent quasigroup equations.* Publ. Inst. Math., Nouv. Sér., 2010, **87(101)**, 39–58.

[18] Krstić S. *Quadratic quasigroup identities.* PhD thesis (in Serbocroatian), University of Belgrade, 1985.
`http//elibrary.matf.bg.ac.rs/handle/123456789/182/phdSavaKrstic.pdf`, (accessed May 5, 2015).

[19] Movsisyan Yu. M. *Introduction to the theory of algebras with hyperidentities*. Yerevan State Univ. Press, Yerevan, 1986 (in Russian).

[20] Movsisyan Yu. M. *Hyperidentities in algebras and varieties*. Russian Math. Surveys, 1998, **53(1)**, 57–108.

[21] Movsisyan Yu. M. *Hyperidentities and hypervarieties*. Sci. Math. Jap., 2001, **54**, 595–640.

[22] Nazari E., Movsisyan Yu. M. *Transitive modes*. Demonstratio Math., 2011, **44**, No. 3, 511–522.

[23] Němec P., Kepka T. *T-quasigroups I*. Acta Univ. Carolin. Math. Phys., 1971, **12**, No. 1, 39–49.

[24] Pflugfelder H. O. *Quasigroups and Loops: Introduction*. Sigma Series in Pure Mathematics, Heldermann Verlag, Berlin, 1990.

[25] Shcherbacov V. A. *Quasigroups in cryptology*. Comp. Sci. J. Moldova, 2009, **17**, No. 2(50), 193–228.

[26] Toyoda K. *On Axioms of linear functions*. Proc. Imp. Acad. Tokyo Conf., 1941, **17**, 211–237.

[27] Ungar A. *Beyond the Einstein Addition Law and its Gyroscopic Thomas Precession – The Theory of Gyrogroups and Gyrovector Spaces*. Kluwer Academic Publishers, Dordrecht, Boston, London, 2001.

Received Novemmber 20, 2015

Amir Ehsani
Department of Mathematics, Mahshahr Branch
Islamic Azad University, Mahshahr, Iran
E-mail: *a.ehsani@mhriau.ac.ir*

Aleksandar Krapež
Mathematical Institute of the Serbian Academy
of Sciences and Arts, Knez Mihailova 36
11001 Belgrade, Serbia
E-mail: *sasa@mi.sanu.ac.rs*

Yuri Movsisyan
Department of Mathematics and Mechanics
Yerevan State University, Alex Manoogian 1
Yerevan 0025, Armenia.
E-mail: *yurimovsisyan@yahoo.com*

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 64–69
ISSN 1024–7696

Linear groups that are the multiplicative groups of neofields

Anthony B. Evans

Abstract. A neofield N is a set with two binary operations, addition and multiplication, for which N is a loop under addition with identity 0, the nonzero elements of N form a group under multiplication, and both left and right distributive laws hold. Which finite groups can be the multiplicative groups of neofields? It is known that any finite abelian group can be the multiplicative group of a neofield, but few classes of finite nonabelian groups have been shown to be multiplicative groups of neofields. We will show that each of the groups $GL(n,q)$, $PGL(n,q)$, $SL(n,q)$, and $PSL(n,q)$, q even, $q \neq 2$, can be the multiplicative group of a neofield.

Mathematics subject classification: 20N05, 12K99.
Keywords and phrases: neofield, linear group, orthomorphism, near orthomorphism.

1 Introduction

Neofields were introduced by Paige [7] in 1949. A *neofield* is a set N with two binary operations, addition and multiplication, satisfying the following:

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

For a neofield N we will use 1 to denote the multiplicative identity. If N is a neofield, then the additive loop of N is completely determined by its multiplicative group and its *presentation function* $T\colon x \mapsto 1 + x$, as

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

In fact, N is completely determined by its multiplicative group and its presentation function as an easy argument shows that $a0 = 0a = 0$ for all $a \in N$.

The question that will concern us is, Which finite groups can be multiplicative groups of neofields? For abelian groups, this question was answered by Paige [7].

His answer illustrates a divide between neofields in which $1+1=0$ and neofields in which $1+1\neq 0$. In fact Johnson [4] showed that a finite group cannot be both the multiplicative group of a neofield in which $1+1=0$ and the multiplicative group of a neofield in which $1+1\neq 0$.

Theorem 1 (Paige, 1949)**.** *Any finite abelian group G can be the multiplicative group of a neofield. G can be the multiplicative group of a neofield in which $1+1=0$ if and only if G does not contain a unique element of order two; and G can be the multiplicative group of a neofield in which $1+1\neq 0$ if and only if G contains a unique element of order two.*

Thus, the question of which finite groups can be multiplicative groups of neofields reduces to the question, Which finite nonabelian groups can be multiplicative groups of neofields? Johnson [4] answered this question for dihedral groups.

Theorem 2 (Johnson, 1986)**.** *No dihedral group can be the multiplicative group of a neofield.*

In a list of unsolved problems Keedwell [5] posed a closely related problem, For which finite orders do there exist nonabelian groups that can be multiplicative groups of neofields?

For a group G, a bijection $\theta\colon G\to G$ is an *orthomorphism* of G if the mapping $\delta\colon x\mapsto x^{-1}\theta(x)$ is a bijection: θ is *normalized* if $\theta(1)=1$. A *near orthomorphism* of G is a bijection $\theta\colon G\setminus\{h\}\to G\setminus\{1\}$, $h\neq 1$, for which the mapping $\delta\colon g\mapsto g^{-1}\theta(g)$ is a bijection $\theta\colon G\setminus\{h\}\to G\setminus\{k\}$, for some $k\in G$, $k\neq h^{-1}$. A near orthomorphism θ is *normalized* if $k=1$, in which case h is the *exdomain element* of θ.

Orthomorphisms and near orthomorphisms of G that commute with all inner automorphisms of G, i. e., $\theta(g^{-1}xg)=g^{-1}\theta(x)g$ for all $g\in G$, are particularly useful in the construction of neofields. Orthomorphisms are used to construct neofields in which $1+1=0$, and near orthomorphisms to construct neofields in which $1+1\neq 0$.

Theorem 3. *Let G be a finite group. There exists a neofield, with multiplicative group G, in which $1+1=0$ if and only if G admits normalized orthomorphisms that commute with all inner automorphisms of G.*

There exists a neofield, with multiplicative group G, in which $1+1\neq 0$ if and only if G admits normalized near orthomorphisms that commute with all inner automorphisms of G.

Proof. If θ is a normalized orthomorphism of G that commutes with all inner automorphisms of G and $0\notin G$, then the function $T\colon G\cup\{0\}\to G\cup\{0\}$ defined by

$$T(x)=\begin{cases}1 & \text{if } x=0,\\ 0 & \text{if } x=1,\\ \theta(x) & \text{if } x\neq 0,1,\end{cases}$$

is the presentation function of a neofield, with multiplicative group G, in which $1+1=0$.

If T is the presentation function of a neofield, with multiplicative group G, in which $1 + 1 = 0$, then the mapping $\theta\colon G \to G$ defined by

$$\theta(x) = \begin{cases} 1 & \text{if } x = 1, \\ T(x) & \text{otherwise,} \end{cases}$$

is a normalized orthomorphism of G that commutes with all inner automorphisms of G.

A similar proof establishes the relationship between neofields, with multiplicative group G, in which $1+1 \neq 0$ and normalized near orthomorphisms of G that commute with all inner automorphisms of G. □

As an example.

Corollary 1. *Any group of odd order can be the multiplicative group of a neofield in which* $1 + 1 = 0$.

Proof. If G is a group of odd order, then the mapping $x \mapsto x^2$ is a normalized orthomorphism of G that commutes with all inner automorphisms of G. The result then follows from Theorem 3. □

In this paper we will show that, if G is one of $GL(n, q)$, $SL(n, q)$, $PGL(n, q)$ or $PSL(n, q)$, q even, $q \neq 2$, then G can be the multiplicative group of a neofield in which $1 + 1 = 0$. We will do this by constructing normalized orthomorphisms of G that commute with all inner automorphisms of G. We will adapt techniques that were used in [3] to construct sets of mutually orthogonal latin squares based on $GL(n, q)$, q even, $q \neq 2$: a remark in this paper claimed that the orthomorphisms constructed yield neofields with multipicative group $GL(n, q)$, q even, $q \neq 2$, in which $1 + 1 = 0$. For more information on neofields and orthomorphisms consult [1] and [2].

2 The even-odd decomposition

Throughout this paper G will denote a finite group, U the set of 2–elements of G, and S the set of odd–order elements of G. Note that $U \cap S = \{1\}$. We will make extensive use of the even-odd decomposition, described in the following lemma.

Lemma 1 (even-odd decomposition)**.** *Each $g \in G$ can be uniquely written as a product $g = us$, where $us = su$, $u \in U$, and $s \in S$.*

Proof. See [6], Lemma 2.2.4 with $p = 2$, for instance. □

For this paper we need to define orthomorphisms of U and S. We call a bijection $\theta\colon U \to U$ an *orthomorphism* of U if the mapping $x \mapsto x^{-1}\theta(x)$ is also a bijection $U \to U$: θ is *normalized* if $\theta(1) = 1$. Orthomorphisms of S are defined similarly. We are interested in normalized orthomorphisms of U and S that commute with all inner automorphisms of G.

We first present a method for constructing orthomorphisms of G from orthomorphisms of U and S, using even-odd decompositions. Given two mappings $\theta\colon U \to U$ and $\phi\colon S \to S$, we will define the *product of θ and ϕ* (with respect to U and S), written $\theta \times_J \phi$, by $\theta \times_J \phi(g) = \theta(u)\phi(s)$, where $g = us$ is the even-odd decomposition of g. A product construction of orthomorphisms is described in the following lemma. Note that $C_U(s)$ denotes the centralizer of s in U and $C_S(u)$ the centralizer of u in S.

Lemma 2. *Let θ be an orthomorphism of U that acts on $C_U(s)$ for each $s \in S$, and let ϕ be an orthomorphism of S that acts on $C_S(u)$ for each $u \in U$. Then $\theta \times_J \phi$ is an orthomorphism of G.*

Proof. See Lemma 2 in [3]. □

Theorem 4. *Let θ be a normalized orthomorphism of U that acts on $C_U(s)$ for each $s \in S$, and let ϕ be a normalized orthomorphism of S that acts on $C_S(u)$ for each $u \in U$. If θ and ϕ commute with all inner automorphisms of G, then there exists a neofield in which $1 + 1 = 0$, with multiplicative group G.*

Proof. By Lemma 2, $\theta \times_J \phi$ is a normalized orthomorphism of G. Further $\theta \times_J \phi$ commutes with all inner automorphisms of G, as, if $g = us$, $u \in U$, $s \in S$, is the even-odd decomposition of g and $h \in G$, then $h^{-1}gh = (h^{-1}uh)(h^{-1}sh)$ is the even-odd decomposition of $h^{-1}gh$. □

Corollary 2. *If there exists a normalized orthomorphism of U that acts on $C_U(s)$ for each $s \in S$, and commutes with all inner automorphisms of G, then there exists a neofield in which $1 + 1 = 0$ with multiplicative group G.*

Proof. The mapping $x \mapsto x^2$ is a normalized orthomorphism of S that acts on $C_S(u)$ for each $u \in U$ and commutes with all inner automorphisms of G. □

3 The construction

For G one of $GL(n,q)$, $SL(n,q)$, $PGL(n,q)$, or $PSL(n,q)$, q even, $q \neq 2$, we will construct normalized orthomorphisms of U that commute with inner automorphisms of G. It will then follow from Corollary 2 that each of these groups can be the multiplicative group of a neofield in which $1 + 1 = 0$.

Let $M_n(q)$ denote the set of $n \times n$ matrices over $GF(q)$, q a power of 2. For each $a \in GF(q)^*$, the multiplicative group of $GF(q)$, we define the mapping

$$\theta_a\colon M_n(q) \to M_n(q) \text{ by } \theta_a(A) = I + a(I + A).$$

Suppose that G is a subgroup of $GL(n,q)$, q a power of 2. Note that, if $A^m = I$, m a power of 2, then $\theta_a(A)^m = I$ and so θ_a maps 2-elements to 2-elements. Thus, if $\theta_a(U) \subseteq G$, then $\theta_a(U) \subseteq U$. The next lemmas establish some properties of this class of mappings.

Lemma 3. *Suppose that G is a subgroup of $GL(n,q)$, q even, $q \neq 2$. If $a \in GF(q)$, $a \neq 0,1$, and $\theta_a(U) \subseteq G$, then $\theta_a \mid_U$ is an orthomorphism of U which acts on $C_U(B)$ for each $B \in S$.*

Proof. See Lemma 4 in [3]. □

Lemma 4. *Suppose that G is a subgroup of $GL(n,q)$, q even, $q \neq 2$. If $a \in GF(q)$, $a \neq 0,1$, and $\theta_a(U) \subseteq G$, then $\theta_a \mid_U$ commutes with all inner automorphisms of G.*

Proof. Routine. □

For the linear groups $GL(n,q)$ and $SL(n,q)$, q even, $q \neq 2$, we give a simple proof that each of these groups can be the multiplicative group of a neofield in which $1+1=0$.

Theorem 5. *If G is one of $GL(n,q)$ or $SL(n,q)$, q even, $q \neq 2$, then G can be the multiplicative group of a neofield in which $1+1=0$.*

Proof. Suppose $G = GL(n,q)$, q even, $q \neq 2$, and $a \in GF(q)^*$, $a \neq 1$. By Lemmas 3 and 4, θ_a is an orthomorphism of U that commutes with inner automorphisms of G and, hence, by Corollary 2, $GL(n,q)$ can be the multiplicative group of a neofield in which $1+1=0$.

As det is a homomorphism from $GL(n,q)$ to $GF(q)^*$, a group of odd order, every element of U has determinant 1. Thus $U \subseteq SL(n,q)$. It follows that $SL(n,q)$ can be the multiplicative group of a neofield in which $1+1=0$. □

In order to extend the result of Theorem 5 to $PGL(n,q)$ and $PSL(n,q)$, q even, $q \neq 2$, we need to describe the relationship between the sets of 2-elements and odd-order elements of $PGL(n,q)$ and $PSL(n,q)$, and those of $GL(n,q)$ and $SL(n,q)$.

Lemma 5. *Let G be one of $GL(n,q)$ or $SL(n,q)$, set $P = \{cI \mid c \in GF(q)^*, cI \in G\}$, let U^* be the set of 2-elements of G/P and let S^* be the set of odd-order elements of G/P. Then $U^* = UP$ and $S^* = SP$. Further, the mapping $A \mapsto AP$ is a bijection $U \to U^*$ and, if $A \in U$ and $B \in S$, then AP commutes with BP if and only if A commutes with B.*

Proof. Clearly $UP \subseteq U^*$. For $XP \in U^*$, $X \in G$, let $X = AB$, $A \in U$, $B \in S$, be the even-odd decomposition of X. Let m be a power of 2 for which $A^m = I$ and $(XP)^m = P$ and let s be an odd positive integer for which $B^s = I$. Then $B^m P = (XP)^m = P$, and so $B^m \in P$. As $\gcd(m,s) = 1$, there exists a positive integer r for which $B^{mr} = B$. Then $B = B^{mr} \in P^r \subseteq P$. It follows that $U^* \subseteq UP$ and hence $U^* = UP$. A similar proof shows that $S^* = SP$

For $A, B \in U$, if $AP = BP$, then $A = cB$ for some $c \in GF(q)^*$. There exists m, a power of 2, for which $A^m = B^m = I$. Thus $I = c^m I$, and so $c^m = 1$. As the multiplicative order of c is odd, $c = 1$. Hence, if $A, B \in U$, then $AP = BP$ if and only if $A = B$. It follows that the mapping $A \mapsto AP$ is a bijection $U \to U^*$.

Clearly, if $A \in U$ commutes with $B \in S$, then AP commutes with BP. If AP commutes with BP, $A \in U$ and $B \in S$, then $ABP = BAP$. Hence $AB = cBA$ for

some $c \in GF(q)^*$, and so $A = c(BAB^{-1})$. Let m be a power of 2 for which $A^m = I$. Then $I = c^m I$, from which it follows that $c^m = 1$, and, as c is of odd multiplicative order, it must be that $c = 1$. Hence A and B commute. □

For the linear groups $PGL(n, q)$ and $PSL(n, q)$, q even, $q \neq 2$, we can now give a proof that each of these groups can be the multiplicative group of a neofield in which $1 + 1 = 0$.

Theorem 6. *If G is one of $PGL(n, q)$ or $PSL(n, q)$, q even, $q \neq 2$, then G can be the multiplicative group of a neofield in which $1 + 1 = 0$.*

Proof. Let G be one of $GL(n, q)$ or $SL(n, q)$, set $P = \{cI \mid c \in GF(q)^*, cI \in G\}$, let U^* be the set of 2-elements of G/P, and let S^* be the set of odd-order elements of G/P. By Lemma 5, $U^* = UP$ and, if $A, A' \in U$, then $AP = A'P$ if and only if $A = A'$. It follows that, for any mapping $\theta\colon U \to U$, if we define $\theta^*\colon U^* \to U^*$ by $\theta^*(AP) = \theta(A)P$, $A \in U$, then θ^* is well-defined, and is a bijection if and only if θ is a bijection. Thus, if θ is an orthomorphism of U, then, as the mapping $AP \mapsto (AP)^{-1}\theta^*(AP) = A^{-1}\theta(A)P$ is a bijection, θ^* is an orthomorphism of U^*. Hence, if $a \in GF(q)^*$, $a \neq 1$, then θ_a^* is an orthomorphism of U^*. As θ_a commutes with inner automorphisms of G, θ_a^* commutes with inner automorphisms of G/P. The result then follows from Corollary 2. □

References

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

[2] Evans A. B. *Orthomorphism graphs of groups.* Lecture Notes in Mathematics, **1535**, Springer-Verlag, Berlin, Heidelberg, 1992.

[3] Evans A. B. *Mutually orthogonal latin squares based on general linear groups.* Des. Codes Cryptogr., 2014, **71**, 479–492.

[4] Johnson C. P. *Complete mappings, neofields, and dihedral groups.* J. Miss. Acad. Sci., 1986, **XXXI**, 147–152.

[5] Keedwell A. D. *Sequenceable groups, generalized complete mappings, neofields and block designs.* Combinatorial mathematics, X (Adelaide, 1982), 49–71, Lecture Notes in Math., **1036**, Springer, Berlin, 1983.

[6] Michler G. *Theory of finite simple groups.* Cambridge University Press, Cambridge, 2006.

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

Anthony B. Evans
Wright State University
E-mail: *anthony.evans@wright.edu*

Received November 23, 2015

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 70–77
ISSN 1024–7696

On isotopies of some classes of Moufang loops

A. Grishkov, M. Rasskazova, L. Sabinina

Abstract. In this note we discuss questions concerning loop isotopes of automorphic Moufang loops and related questions.

Mathematics subject classification: 20N05.
Keywords and phrases: LF-quasigroups, Moufang loops, automorphic loops, isotopy.

1 Introduction

Isotopies between various kinds of F-quasigroups and Moufang loops are just one aspect of the rich and fruitful field of investigations of Valentin Danilovich Belousov to whose memory this note is dedicated. We will report about some of these results and questions which have been of interest for recent research, particularly on automorphic Moufang loops. Whereas that are algebraic things we would like to mention the importance of this matter to homogenous spaces if one applies these results to smooth quasigroups ([18,21,22] and more). Section 3 and Section 4 contain essential parts of the article. In Section 3 we speak of the existence of an isotopy between quasigroups and loops from different varieties. In Section 4 we treat the problem of isotopical invariance of some varieties of loops.

2 Preliminaries and definitions

In this section we will give definitions and facts from the theory of quasigroups and loops which are necessary to make this note self-contained.

Let us consider a set with a binary operation $(Q, \cdot)$. If it does not lead to misunderstandings we will often write xy instead of $x \cdot y$.

The mapping $L_a : Q \to Q,\ L_a x = ax$ is called a *left multiplication*, analogously the mapping $R_a : Q \to Q,\ R_a y = ya$ is called a *right multiplication* for all elements $a \in Q$. With these notations $(Q, \cdot)$ is called a *quasigroup* if all mappings $L_a,\ R_b, a, b \in Q$ are bijections. Thus one can define $x\backslash y = L_x^{-1} y$ and $y/x = R_x^{-1} y$ for $x, y \in Q$.

If additionally there exists a neutral element $1 \in Q$ such that $L_1 = Id_Q = R_1$, then the quasigroup $(Q, \cdot, 1)$ is called a *loop*.

In these notes we will focus on the following varieties of quasigroups and loops:

Left distributive (LD)-quasigroups are defined by

$$x(yz) = (xy)(xz).$$

Right distributive (RD)-quasigroups are defined by the mirror identity of the LD-identity:

$$(zy)x = (zx)(yx).$$

Distributive quasigroups are left and right distributive at the same time.

V. D. Belousov has studied generalizations of left distributive, right distributive and distributive quasigroups, namely:

Left F (LF)-quasigroups:

$$x(yz) = (xy)(x\backslash x \cdot z).$$

Right F (RF)-quasigroups:

$$(zy)x = (z \cdot x/x)(yx).$$

F-quasigroups are left and right F-quasigroups at the same time.

Diassociative loops are defined in the following way: every pair of elements $x, y \in Q$ generates a subgroup of Q. It is known that no finite number of identities defines the variety of diassociative loops.

Moufang loops are defined by any of the following equivalent identities:

$$((xy)x)z = x(y(xz)),$$

$$((xy)z)y = x(y(zy)),$$

$$(xy)(zx) = (x(yz))x.$$

It is known that Moufang loops are diassociative. It is also known that a quasigroup in which any of the Moufang identities holds is a Moufang loop.

Commutative Moufang loops (CML) can be defined by one identity:

$$x^2(yz) = (xy)(xz).$$

We will use the concept of an *isotopy* for quasigroups and loops.

Let $(Q, \cdot)$ be a quasigroup. Let $T = (\alpha, \beta, \gamma)$ be a triple of permutations of the set Q. Then the quasigroup $(Q, \circ_T)$ is called isotopic to $(Q, \cdot)$ where

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

Obviously isotopy is an equivalence relation. A *principal isotope* of $(Q, \cdot)$ is given by the triple $T = (R_f^{-1}, L_g^{-1}, Id)$ for $f, g \in Q$.
It is easy to see that every principal isotope of a quasigroup is a loop with the neutral element gf.

The mappings L_a and R_a for all $a \in Q$ generate Mlt(Q), the *multiplication group* of Q. If a quasigroup Q is isotopic to a loop L, then the multiplication groups Mlt(Q) and Mlt(L) are isomorphic.

For a quasigroup $(Q,\cdot)$ we will speak of the group $\mathrm{Inn}(Q)$, the *inner mapping group* of $(Q,\cdot)$, generated by the following three types of generators:

$$\ell_{x,y} = L_{xy}^{-1} \circ L_x \circ L_y, \qquad r_{x,y} = R_{xy}^{-1} \circ R_y \circ R_x,$$

$$T_x = L_x^{-1} \circ R_x$$

for all $x, y \in Q$. If $(Q,\cdot,1)$ is a loop, the group $\mathrm{Inn}(Q)$ is just the stabilizer of the neutral element 1, that is

$$\mathrm{Inn}(Q) = \{\phi \in \mathrm{Mlt(Q)} \mid \phi(1) = 1\}.$$

We will call a quasigroup Q *left automorphic* or an A_l-quasigroup if the mappings $\ell_{x,y}$ are automorphisms of Q for all $x, y \in Q$, analogously *right automorphic* or an A_r-quasigroup if the mappings $r_{x,y}$ are automorphisms of Q for all $x, y \in Q$ and *T-automorphic* or an A_T-quasigroup if the mappings T_x are automorphisms of Q for all $x \in Q$.

A quasigroup Q is called *automorphic* or an A-quasigroup if $\mathrm{Inn}(Q)$ is a subgroup of the group of all automorphisms of Q.

A subquasigroup of a given quasigroup Q is *normal* if and only if it is invariant under the group $\mathrm{Inn}(Q)$. In the case of loops a *normal* subloop is just the kernel of a loop homomorphism.

In any automorphic quasigroup all characteristic subquasigroups are normal. In a quasigroup Q we define the *commutator subquasigroup* $[Q,Q]$ as the normal closure of the subquasigroup generated by all elements of the form $(yx)\backslash(xy) = [x,y]$, where $x, y \in Q$ and the *associator subquasigroup* (Q,Q,Q) as the normal closure of the subquasigroup generated by all elements of the form $(x(yz))\backslash(xy)z) = (x,y,z)$ for all $x, y, z \in Q$.

For all $a, b \in Q$ the subgroups

$$N_l(Q) = \{x \in Q \mid (x,a,b) = 1\}, \quad N_r(Q) = \{y \in Q \mid (a,b,y) = 1\},$$

$$N_m(Q) = \{z \in Q \mid (a,z,b) = 1\}$$

are called the *left nucleus*, the *right nucleus* and the *middle nucleus* respectively and $N(Q) = N_l(Q) \cap N_r(Q) \cap N_m(Q)$ is called just the *nucleus* of Q.
The subgroup $C(Q) = \{z \in N(Q) \mid xz = zx \text{ for all } x \in Q\}$ is called the *center* of the quasigroup Q. In a Moufang loop M all nuclei coincide and the nucleus and the center are normal subgroups. Moreover the set $K(M) = \{x \in M : xy = yx \text{ for all } y \in M\}$ is a normal subloop which is called the *commutant* of M (see [11]).

3 Some important isotopies

For the variety of groups the following fact is true: if a group is isotopic to a loop, then it is isomorphic to this isotope. It is known that any isotope of a Moufang loop is a Moufang loop. In other words, the variety of Moufang loops is isotopically invariant.

V. D. Belousov [1,2] proved that any distributive quasigroup Q is isotopic to some commutative Moufang loop. He also gave a sufficient condition when a commutative Moufang loop M is an isotope of some distributive quasigroup. This is the case if the mapping $x \to x^2$ is a bijection in M. One can show a bit more:

Proposition 1. *Any commutative Moufang loop M is an isotope of some F-quasigroup.*

Proof. Let us consider a loop M such that the identity

$$x^2(yz) = (xy)(xz)$$

holds. The isotope defined by $x \circ y = x^{-1}y$ is an F-quasigroup. (See [20].) □

Belousov was interested in isotopes of LF- and F-quasigroups. In 2007 Kepka, Kinyon, Phillips [6], solving a Belousov problem, showed that any F-quasigroup is isotopic to some automorphic Moufang loop M, such that M is the product of the nucleus $N(M)$ and the commutant $K(M)$.

For LF-quasigroups Belousov has proved that loop isotopes of LF-quasigroups belong to the class of so-called left M-loops, and showed that a loop isotope of any left M-loop is a left M-loop again. Note that an identity which defines an M-loop contains a mapping $\phi : M \to M$ (see [3]).

Developing further the ideas of Belousov, V. Shcherbacov studied the isotopy of an LF-quasigroup. He used Belousov's result that for an LF-quasigroup Q the mapping $e : Q \to Q$ defined by $e(x) = x\backslash x$ is an endomorphism (see [3]). The main statement of his paper [23] is the following. For an LF- quasigroup Q there exists an isotopic loop which is a product of a normal subgroup N and a subloop S such that S is isotopic to an LD-quasigroup. He claimed that this product is a direct product.

At the same time in [18] in a geometric context a different isotope was constructed, using another result of Belousov. He had observed that every LF-quasigroup is isotopic to an LF-quasigroup with a left neutral element ([3] and see also [21]). This fact allows the use of kernels in the homomorphism theory. It was shown that an LF-quasigroup Q is isotopic to a semidirect product of a normal factor N_1 which is a nuclear extension of a group by a group and a loop S_1 which is an isotope of an LD-quasigroup. Inspired by Shcherbacov's paper, in [19] the authors showed that in the above construction N_1 is just a group. The authors realized that N_1 is the left nucleus of the LF-quasigroup Q. Thus the endomorphism e restricted to $e(Q)$ is an automorphism.

However, they could not verify that S_1 is normal. From an example of Gagola [9] one learns that in the finite case it is not always possible to get an isotope which is a direct product. It should be mentioned that in the geometric situation one treats smooth quasigroups. Isotopy of smooth quasigroups is important since isotopic smooth quasigroups define equivalent geometries. For this case the question of the existence of a direct decomposition is still open.

4 Automorphic Moufang loops, a theory in progress

The concept of automorphic loops goes back to a paper of R. Bruck and L. Paige [5]. In this paper they observed that diassociative automorphic loops have similar properties as Moufang loops, but the conjecture that these two varieties of loops are identical was proved only many years later in [7]. In their paper Kinyon, Kunen and Phillips wrote: "We also do not know whether every loop isotope of a Moufang A-loop is a (Moufang) A-loop." We will return to this question later. The variety of left automorphic Moufang loops is defined by Moufang identity and by the additional identity

$$([x, y], z, t) = 1.$$

Note that the variety of left automorphic Moufang loops coincides with the variety of right automorphic Moufang loops. The variety of T-automorphic Moufang loops is defined by the Moufang identity and by the additional identity (see [4])

$$(x^3, y, z) = 1.$$

The papers [7] and [6] gave a strong impulse to study the variety of automorphic loops and in particular the variety of automorphic Moufang loops. For instance in the paper [17] it was shown that in the variety of automorphic Moufang loops the Restricted Burnside Problem has a positive answer. Some particular properties of finite automorphic Moufang loops like the consequences of Sylow's theorems for Moufang loops were treated in [12].

Recently the structure of automorphic Moufang loops was described in the papers [13] and [14]. In [13] the structure of a free automorphic Moufang loop L_n of rank n was described. Take a free group F_n of rank n with a base $x_1, \ldots, x_n$ and a free commutative Moufang loop C_n of the same rank with a base $y_1, \ldots, y_n$. Then the elements $(x_1, y_1), \ldots, (x_n, y_n)$ of the direct product $F_n \times C_n$ form a base of L_n. Using this approach one can see that for every Moufang loop M the factor loop $A = M/([M, M] \cap (M, M, M))$ is an automorphic Moufang loop. It is clear that for the loop A one has $[A, A] \cap (A, A, A) = 1$. But of course not every automorphic Moufang loop B has the property that $([B, B] \cap (B, B, B)) = 1$. In [14] we have shown that for every automorphic Moufang loop B there is a minimal automorphic Moufang loop B_1 and an epimorphism $\eta : B_1 \to B$ such that $([B_1, B_1] \cap (B_1, B_1, B_1)) = 1$.

In [7] results of Hala Pflugfelder from [15] are mentioned. There M_k-loops are introduced and the following results are proved. The variety $\mathcal{M}_k$ is defined by the

generalized Moufang M_k-idenity:

$$x(yz)x^k = (xy)(zx^k)$$

for every $k \in \mathbb{N}$.

H. Pflugfelder proved that M_k-loops are isotopically invariant for every $k \in \mathbb{N}$ and that M_k-loops are Moufang loops. It was also proved that the variety $\mathcal{M}_k$ can be defined by the Moufang identity and by $(x^{k-1}, y, z) = 1$. It is easy to see that for Moufang loops the M_4-identity is equivalent to the property A_T. Thus we see that Moufang A_T-loops are isotopically invariant.

In fact using the same reasoning one can describe the isotopy of the class of code loops. Code loops are left (and right) automorphic Moufang loops, but not A_T-loops. For code loops the identity $(x^2, y, z) = 1$ holds. This means that code loops belong to the isotopically invariant variety $\mathcal{M}_3$. By [16, Theorem IV.4.11, page 105], a loop isotopic to a code loop C is isomorphic to C.

The variety of commutative Moufang loops is not isotopically invariant (see [16]). However, every isotope of a commutative Moufang loop satisfies the following identities:

$$(x^3, y, z) = 1, \quad [x^3, y] = 1,$$

$$[[x, y], y] = 1$$

(see [4, Lemma 5.1, page 122 and Lemma 5.7, page 128]).

Returning to the initial question of this section whether every isotope of any automomorphic Moufang loop is automorphic we are convinced that the answer is negative in general. We have in mind an isotope of a free commutative Moufang loop of exponent 3 and of rank 5. Such an isotope was used by G. Nagy in [8].

Gagola's result gives us sufficient conditions when every isotope of an automomorphic Moufang loop is automorphic. In [10] the following result was obtained. Let M be a Moufang loop, and let H be a subloops generated by all cubes of elements of M. If one of conditions

(a) $H = M$,

(b) $[M : H] = 3$

holds, then $Inn(M) = \langle T_x \rangle$.

Suppose now additionally that M is an automorphic Moufang loop. Then note that the case (a) is trivial since M is a group. In the case (b) one sees that $M/N(M) \cong \mathbb{Z}_3$ or $M = N(M)$, where $N(M)$ is the nucleus of M. Thus in both cases any isotope of M is automorphic.

Hence we have the

Conjecture. *Any isotope of an automorphic Moufang loop is automorphic if and only if the identity*

$$((x, y, z), u, v) = 1$$

holds.

Acknowledgements. The first author thanks FAPESP, CNPQ and Russian grant RFFI 13-01-00239. The second author thanks the Russian Foundation for Basic Research (grant no. 2014/319, project no. 258). The third author thanks FAPESP grant processo 2015/07245-4 for support.

References

[1] Belousov V. D. *The structure of distributive quasigroups.* Mat. Sb., 1960, **50(92)**, 267–298.

[2] Belousov V. D. *Foundations of the theory of quasigroups and loops.* Moscow, Nauka, 1967 (in Russian).

[3] Belousov V. D. *Elements of Quasigroups Theory: A Special Course.* Kishinev State University Press, Kishinev, 1981 (in Russian).

[4] Bruck R. H. *A Survey of Binary Systems.* Springer-Verlag, 1966.

[5] Bruck R. H., Paige L. J. *Loops whose inner mappings are automorphisms.* Ann. of Math., 1956, (2) **63**, 308–323.

[6] Kepka T., Kinyon M., Phillips J. D. *The structure of F-quasigroups.* J. Algebra, 2007, **317**, No. 2, 435–461.

[7] Kinyon M., Kunen K., Phillips J. D. *Every diassociative A-loop is Moufang.* Proc. Amer. Math. Soc., 2002, **130**, No. 3, 619–624.

[8] Nagy G. P. *Burnside problems for Moufang and Bol loops of small exponent.* Acta Sci. Math. (Szeged), 2001, **67**, 687–696.

[9] Gagola S. M. *Nonsplitting F-quasigroups.* Comment. Math. Univ. Carolin., 2012, **53**, No. 3, 375–381.

[10] Gagola S. M. *When are inner mapping groups generated by conjugation maps?* Arch. Math. (Basel), 2013, **101**, No. 3, 207–212.

[11] Gagola S. M. *A Moufang's loop commutant.* Proc. Cambridge Phil. Soc., 2012, **152**, No. 2, 193–206.

[12] Grishkov A., Merlini Giuliani M. L., Rasskazova M., Sabinina L. *Half-isomorphisms of finite automorphic Moufang loops.* Comm. Algebra (in print).

[13] Grishkov A., Plaumann P., Sabinina L. *Structure of free automorphic Moufang loops.* Proc. Amer. Math. Soc., 2012, **140**, No. 7, 2209–2214.

[14] Grishkov A., Rasskazova M., Sabinina L. *On the structure of automorphic Moufang loops.* Publ. Math. Debrecen (in print).

[15] Orlik-Pflugfelder H. , *A special class of Moufang loops.* Proc. Amer. Math. Soc., 1970, **26**, 583-586.

[16] Pflugfelder H. *Quasigroups and Loops: Introduction.* Sigma Series in Pure Mathematics, **7**, Heldermann, Berlin, 1990.

[17] Plaumann P., Sabinina L. *On nuclearly nilpotent loops of finite exponent.* Comm. Algebra, 2008, **36**, No. 4, 1346–1353.

[18] Plaumann P., Sabinina L., Sbitneva L. *A decomposition of LF-quasigroups. Algebras, representations and applications*, Contemp. Math., **483**, Amer. Math. Soc., Providence, RI, 2009, 221–227.

[19] Plaumann P., Sabinina L., Sbitneva L. *Some Varieties of Quasigroups, Loops and their Parastrophes.* Communications in Mathematics and Applications, 2012, **3**, No. 1, 75–85.

[20] Sabinina L. *On smooth left square distributive quasigroup. Lecture Notes in Pure and Appl. Math.*, **211**, Dekker, New York, 2000, 345–348.

[21] Sabinin L. V., Sabinina L. *On the theory of left F-quasigroups.* Algebras Groups Geom., 1995, **12**, No. 2, 127–137.

[22] Sabinina L. *Trans-symmetric spaces.* Adv. Appl. Clifford Algebras, 1994, **4**, S1, 509–514.

[23] Shcherbacov V. A. *On the structure of left and right F-, SM-, and E-quasigroups,* J. Gen. Lie Theory Appl., 2009, **3 (3)**, 197–259.

Received November 30, 2015

Alexander Grishkov
Instituto de Matemática e Estatística
Universidade de São Paulo
Rua de Matão 1010
São Paulo, 05508-090
Brazil
E-mail: *grishkov@ime.usp.br*

Marina Rasskazova
Omsk State Institute of Service
Pevtsova street 13
Omsk, 644099
Russia
E-mail: *marinarasskazova@yandex.ru*

Liudmila Sabinina
Universidad Autónoma del Estado de Morelos
Av. Universidad 1001
Cuernavaca, 62209
México
E-mail: *liudmila@uaem.mx*

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 78–82
ISSN 1024–7696

Doubly transitive sets of even permutations

Gábor P. Nagy

Abstract. In this paper we investigate doubly transitive sets of permutations which consist of even permutations.

Mathematics subject classification: 20N05, 51E05.
Keywords and phrases: Sharply transitive set, finite projective plane, alternating group.

Dedicated to the 90th anniversary of Prof. V. D. Belousov

1 Introduction

Let S be a set of permutations of some fixed set Ω of n symbols. We say that S is *sharply t–transitive* if for any two tuples $(x_1, \dots, x_t)$, $(y_1, \dots, y_t)$ of distinct symbols, there is a unique element $s \in S$ with $x_1^s = y_1, \dots, x_t^s = y_t$. It is well known that sharply 1– and 2–transitive sets of permutations correspond to Latin squares and affine planes, respectively, cf.[3]. One of the main motivation for the study of finite sharply 2–transitive sets is the famous Prime Power Conjecture for projective planes. (Both parts of the PPC are *folklore,* and it is surprisingly hard to find them in printed literature. The second part of the PPC is mentioned in [4, p. 276].)

Problem 1. (Prime Power Conjecture (PPC) for projective planes)

(1) *Finite projective planes have prime power order.*

(2) *Finite projective planes of prime order are desarguesian.*

The classical construction of a sharply 2–transitive set is the group

$$AGL(1, F) = \{x \mapsto ax + b \mid a \in F^*, b \in F\}$$

of affine linear transformations of the field F. The corresponding projective plane is the desarguesian plane $PG(2, F)$ over F. A wider class of sharply 2–transitive sets is based on the concept of *quasifields.* The set Q endowed with two binary operations $+, \cdot$ is called a (right) quasifield if

(Q1) $(Q, +)$ is an abelian group with neutral element $0 \in Q$,

(Q2) any two of the elements $x, y, z \in Q \setminus \{0\}$ determine the third when $x \cdot y = z$,

Research supported by OTKA Grant No. NN.114614.

(Q3) the right distributive law $(x+y)z = xz + yz$ holds, and,

(Q4) for each $a, b, c \in Q$ with $a \neq b$, there is a unique $x \in Q$ satisfying $xa = xb + c$.

The connection between affine and projective planes and their coordinatizing algebraic structures as plenary ternary rings and mutually orthogonal latin squares are given in [2, Chapter VIII], [4, Chapter 8]. One finds details on the concept of quasifields and translation planes in [4, Section 8.4], and, using the language of sharply transitive sets in [7, 12]. Notice that for the structures considered in [1], two-sided distributivity is assumed; such objects are now called *nearfields*.

It is immediate to show that for a quasifield Q, the set

$$\Lambda(Q) = \{v \mapsto u \cdot v + w \mid u \in H^*, w \in H\}$$

of $Q \to Q$ maps forms a sharply 2–transitive set on Q.

Let $\Omega^{(t)}$ denote the set of t–tuples of distinct symbols of Ω. The permutation group $G \leq \mathrm{Sym}(\Omega)$ has a natural action on $\Omega^{(t)}$, let $G^{(t)}$ denote the corresponding permutation group. It is immediate that the existence of a sharply t–transitive set in G is equivalent with the existence of a sharply 1–transitive set in $G^{(t)}$. In the 1970's, P. Lorimer started the systematic investigation of the question of existence of sharply 2–transitive sets in finite 2–transitive permutation groups. This program was continued by Th. Grundhöfer, M. E. O'Nan, P. Müller, see [6] and the references therein. Some of the 2–transitive permutation groups needed rather elaborated methods from character theory in order to show that they do not contain sharply 2–transitive sets of permutations.

In the paper [10], the authors presented a combinatorial method to show that a given permutation group cannot contain sharply 1–transitive sets. An important implication of this method was the following

Proposition 1 ([10, Theorem 3])**.** *If $n \equiv 2, 3 \pmod 4$ then the alternating group A_n does not contain a sharply 2–transitive set of permutations.*

Recently, Gyula Károlyi [9] asked the question concerning the existence of a sharply 2–transitive set of A_n in the remaining cases, that is, when $n \equiv 0, 1 \pmod 4$. The main result of this paper gives a partial answer to this problem. In particular, we show that for infinitely many integers $n \equiv 0, 1 \pmod 4$, A_n does contain a sharply 2–transitive set.

Theorem 1. *(1) If $n = 2^m$ with $m \geq 2$, or $n = p^{2m}$ with odd prime p, then A_n contains a sharply 2–transitive set of permutations.*

(2) Let p be an odd prime, $n = p^{2m+1}$. If A_n contains a sharply 2–transitive set of permutations, then $p \equiv 1 \pmod 4$ and the corresponding projective plane is nondesarguesian.

The formulation of the theorem shows that no attempts are made to attack the Prime Power Conjecture. We notice that the existence of a sharply 2–transitive set in A_p with a prime p would deliver a nondesarguesian plane of prime order, hence a counterexample to part (b) of Problem 1.

2 Proof of the theorem

In this section, $\mathrm{Alt}(X)$ denotes the group of even permutations of the finite set X. Furthermore, H^* denotes the set of nonzero elements of the quasifield H.

Lemma 1. *Let $q = p^m$ be a prime power. $AGL(1,q) \leq A_q$ if and only if $p = 2$ and $m \geq 2$.*

Proof. Clearly, the only nontrivial element of $AGL(1,2)$ is the transposition $(0,1)$ which is odd. Let us assume $q > 2$. Let g be a primitive element in $\mathbb{F}_q$. $AGL(1,q)$ is generated by an elementary abelian p–group N of order q and the permutation $\gamma : x \mapsto gx$. While the elements of N consist of q/p cycles of length p, the permutation γ acts on $\mathbb{F}_q^*$ as a cycle of length $q-1$. Hence, $N \leq A_q$ and $\gamma \in A_q$ if and only if $2 \mid q-1$. □

We recall the construction of Hall quasifields from [8, Section IX.2.]. Let F be a field and $f(s) = s^2 - as - b$ an irreducible polynomial over F. Let H be the two-dimensional right vector space over F, with basis elements 1 and λ so that H consists of all elements of the form $x + \lambda y$ as x and y vary over F. The multiplication on H is defined by

$$x \circ (z + \lambda t) = xz + \lambda(xt) \tag{1}$$

and

$$(x + \lambda y) \circ (z + \lambda t) = xz - y^{-1}tf(x) + \lambda(yz - xt + at) \tag{2}$$

for $y \neq 0$. As the right hand sides of (1) and (2) are linear in z, t, one can write the left translation maps $L_u : v \mapsto uv$ in the F-basis $\{1, \lambda\}$ as matrices:

$$L_x = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}, \qquad L_{x+\lambda y} = \begin{pmatrix} x & -y^{-1}f(x) \\ y & -x + a \end{pmatrix}.$$

The determinants are $\det(L_x) = x^2$ and $\det(L_{x+\lambda y}) = -b$.

Lemma 2. *Let p be an odd prime, $r = p^m$, and $\varepsilon \in \mathbb{F}_r$ a nonsquare. Define the Hall quasifield $H = (H, +, \circ)$ with irreducible polynomial $f(s) = s^2 - as - b$, where*

$$a = \frac{\varepsilon + 1}{2}, \qquad b = -\left(\frac{\varepsilon - 1}{4}\right)^2.$$

Then the set

$$\Lambda(H) = \{v \mapsto u \circ v + w \mid u \in H^*, w \in H\}$$

of $H \to H$ maps forms a sharply 2–transitive set in $\mathrm{Alt}(H)$.

Proof. Since the discriminant of f is $a^2 + 4b = \varepsilon$ and is a non-square, the polynomial f is irreducible. Hence, the Hall quasifields is well defined and $\Lambda(H)$ is a sharply 2–transitive set of permutations. Each element of $\Lambda(H)$ is the composition of a translation $v \mapsto v + w$ and an H-multiplication L_u. Since the former is an even

permutation, it suffices to show that the H-multiplication L_u is in $\mathrm{Alt}(H^*)$. By the choice of the parameters, all H-multiplications are contained in the subgroup

$$S = \{A \in GL(2,r) \mid \det(A) \text{ is a square in } \mathbb{F}_r\}$$

of index 2 of $GL(2,r)$. Since $GL(2,r)/GL(2,r)'$ is cyclic, $GL(2,r)$ has a unique subgroup of index 2. As the subgroup $GL(2,r) \cap \mathrm{Alt}(H^*)$ has index at most 2 in $GL(2,q)$, it must contain S. This proves the lemma. □

Lemma 2 implies the first part, while Lemma 1 and Proposition 1 imply the second part of Theorem 1.

We finish the paper with a

Conjecture 1. *Let $p \equiv 1 \pmod 4$ be a prime and m a positive integer. The linear group*

$$S = \{A \in GL(2m+1,p) \mid \det(A) \textit{ is a square in } \mathbb{F}_p\}$$

does not contain sharply transitive sets.

Using the command `OneLoopTableInGroup` of the LOOPS package [11] of the computer algebra system GAP4 [5], the conjecture can be verified for $p = 5$, $m = 1$.

References

[1] Belousov V. D. *On the definition of the concept of a quasi-field.* Bul. Akad. Stiince RSS Moldoven., 1964, **6**, 3–10.

[2] Belousov V. D. *Algebraic nets and quasigroups.* Kishinev, Ştiinţa, 1971 (in Russian).

[3] Dembowski P. *Finite geometries.* Ser. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Berlin, Springer-Verlag, 1968.

[4] Dénes J., Keedwell A. D. *Latin squares and their applications.* Academic Press, New York–London, 1974.

[5] *GAP – Groups, Algorithms, and Programming, Version 4.7.9*, (http://www. gap-system.org), The GAP Group, 2015.

[6] Grundhöfer T., Müller P. *Sharply 2-transitive sets of permutations and groups of affine projectivities.* Beiträge zur Algebra und Geometrie. Contributions to Algebra and Geometry, 2009, **50**, No. 1, 143–154.

[7] Hall M. *Projective planes.* Trans. Amer. Math. Soc., 1943, **54**, 229–277.

[8] Hughes D. R., Piper F. C. *Projective planes.* New York, Springer-Verlag, 1973, Graduate Texts in Mathematics, Vol. 6.

[9] Károlyi G. Private communication, 2015.

[10] Müller P., Nagy G. P. *On the non-existence of sharply transitive sets of permutations in certain finite permutation groups.* Advances in Mathematics of Communications, 2011, **5**, No. 2, 303–308.

[11] Nagy G. P., Vojtechovsky P. *LOOPS, computing with quasigroups and loops in GAP, Version 3.1.0* (http://www.math.du.edu/loops). Refereed GAP package, 2015.

[12] Nagy G. P. *Semifields in loop theory and in finite geometry.* Quasigroups and Related Systems, 2011, **1 9**, No. 1, 109–122.

Gábor P. Nagy
Bolyai Institute
University of Szeged
Aradi vértanúk tere 1
H-6720 Szeged, Hungary

MTA-ELTE Geometric and Algebraic Combinatorics
Research Group
Pázmány P. sétány 1/c
H-1117 Budapest, Hungary

E-mail: *nagyg@math.u-szeged.hu*

Received January 12, 2016

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 83–90
ISSN 1024–7696

Triality and Universal Multiplication Groups of Moufang Loops

J. D. Phillips

Abstract. We investigate the triality status of combinatorial and universal multiplication groups of various classes of Moufang loops. We also investigate whether some of these are, qua Doro, the largest and smallest groups with triality associated with a given Moufang loop.

Mathematics subject classification: 20N05.
Keywords and phrases: Moufang loop, group with triality, universal multiplication group.

1 Moufang Loops and Universal Multiplication Groups

A *loop* is a set with a single binary operation such that in $x \cdot y = z$, knowledge of any two of x, y, and z specifies the third uniquely, and with a unique two-sided identity element, denoted by 1. A *Moufang loop* is a loop satisfying the identity $x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z$. We use the notation x^{-1} to denote the unique 2-sided inverse of x.

The *commutant*, $\mathrm{C}(M)$, of a Moufang loop M is the set of those elements which commute with each element in the loop. That is, $\mathrm{C}(M) = \{c : \forall x \in M, cx = xc\}$; it is a subloop. Define the *left nucleus* of a Moufang loop, M, by $\mathrm{N}_\lambda(M) = \{a : a \cdot (x \cdot y) = (a \cdot x) \cdot y, \forall x, y \in M\}$. The *middle nucleus*, $\mathrm{N}_\mu(M)$, and the *right nucleus*, $\mathrm{N}_\rho(M)$, are defined analogously. The *nucleus*, $\mathrm{N}(M)$, is then defined by $\mathrm{N}(M) = \mathrm{N}_\lambda(M) \cap \mathrm{N}_\mu(M) \cap \mathrm{N}_\rho(M)$. (In fact, each of these four subsets coincides with the other three [2].) $\mathrm{N}(M)$ is a normal subloop of M [2]. The *center*, $\mathrm{Z}(M)$, of M is defined as $\mathrm{Z}(M) = \mathrm{C}(M) \cap \mathrm{N}(M)$; it is a normal subloop.

We use the standard notation for the right and left translations: $xR(y) = yL(x) = x \cdot y$. The *(combinatorial) multiplication group*, $\mathrm{Mlt}(M)$, of a loop M is the subgroup of the group of all bijections on M generated by right and left translations. Clearly, $\mathrm{Mlt}(M)$ acts as a permutation group on M.

Let M be a Moufang loop, and let $\mathbf{M}$ be an arbitrary variety of Moufang loops containing M. We also use $\mathbf{M}$ to denote the category whose objects are the Moufang loops in $\mathbf{M}$ and whose morphisms are loop homomorphisms. As an algebraic category, $\mathbf{M}$ is complete and co-complete [6, 13.12, 13.14]. In $\mathbf{M}$, form the coproduct of M with $< x >$, the free $\mathbf{M}$-algebra on one generator. Denote this coproduct by $M[x]$ (the variety, $\mathbf{M}$, though not explicitly noted in our coproduct notation, will be clear from context). Since M may be indentified with its image in $M[x]$ [8, p. 33], we

can consider the subgroup of $\mathrm{Mlt}(M[x])$ generated by right and left multiplications by elements of M. This subgroup is the *universal multiplication group*, $U(M;\mathbf{M})$, of M in $\mathbf{M}$.

The assignment of $U(M;\mathbf{M})$ to M gives a functor from the category $\mathbf{M}$ to the category $\mathbf{GP}$ of all groups [8, p. 34]. Note that $U(M;\mathbf{M})$ is "variety dependent" in the sense that for a given Moufang loop M and two varieties $\mathbf{M}_1$ and $\mathbf{M}_2$ containing M, it is not necessarily the case that $U(M;\mathbf{M}_1) \cong U(M;\mathbf{M}_2)$ [8, p. 36]. But if $\mathbf{M}_1 \subseteq \mathbf{M}_2$, then there is a natural group epimorphism $F : U(M;\mathbf{M}_2) \to U(M;\mathbf{M}_1)$ [8, p. 55]. This can be summarized informally as "the smaller the variety, the smaller the universal multiplication group."

For any variety, $\mathbf{M}$ of Moufang loops containing M, there is a natural group epimorphism $F : U(M;\mathbf{M}) \to \mathrm{Mlt}M$ [8, p. 55]. This can summarized informally as "a universal multiplication group can be no smaller than the combinatorial multiplication group."

2 Groups with Triality

If M is a Moufang loop, there exists an involutary automorphism, σ on $\mathrm{Mlt}M$, defined on generators by $R(x)^\sigma = L(x^{-1})$ and $L(x)^\sigma = R(x^{-1})$ [4]. If $\mathrm{N}(M) = 1$, Glauberman [4] showed that there exists an automorphism ρ on $\mathrm{Mlt}M$, defined on generators by $L(x)^\rho = R(x), R(x)^\rho = P(x)$ and $P(x)^\rho = L(x)$. Here and throughout, $P(x) = R(x^{-1})L(x^{-1})$; and so note that $P(x)R(x)L(x) = 1$. Also, clearly $\rho^3 = 1$. So it is easy to see that if both σ and ρ are nontrivial, then together they generate S_3.

Inspired by Glauberman, Doro [3] defined a *group with triality* to be a group, G with two automorphisms, σ and ρ, such that $\sigma^2 = 1$, $\rho^3 = 1$, $< \sigma, \rho >= S_3$ and satisfying the identity $g^{-1}g^\sigma g^{-\rho}g^{\sigma\rho}g^{-\rho^2}g^{\rho\sigma} = 1$, $\forall g \in G$ (this identity is a kind of encoding of $P(x)R(x)L(x) = 1$, the details are in [3]). Groups with triality were crucial in Liebeck's classification of all finite simple Moufang loops [5].

Given a group with triality, G, Doro [3] constructs a Moufang loop, M so that $\mathrm{Mlt}M$ is a homomorphic image of G. Conversely, given a Moufang loop, M, Doro constructs a group with triality, G, such that the construction in the previous sentence yields M, and such that $\mathrm{Mlt}M$ is a homomorphic image of G. Note that for a given Moufang loop, M, there may be more than one group with triality which gives M via Doro's construction. But, for a given M, Doro [3] shows that there is a largest group with triality, denoted by $\mathrm{G}(M)$, that gives M, in the sense that any other group with triality that gives M is itself a homomorphic image of $\mathrm{G}(M)$. Doro [3] also shows that there is a smallest group with triality, denoted by $\mathrm{G}_0(M)$, that gives M, in the sense that $\mathrm{G}_0(M)$ is a homomorphic image of any other group with triality that gives M. And Doro shows that, given any group with triality, G, if M is the Moufang loop constructed from G, then $\mathrm{Mlt}M$ is a homomorphic image of G. Thus, given any group with triality, G, with associated Moufang loop M, there is a sequence of group epimoprhisms, from $\mathrm{G}(M)$ to G to $\mathrm{G}_0(M)$ to $\mathrm{Mlt}M$.

Given a Moufang loop, M, to determine whether any of its multiplication

groups is with triality, it suffices to determine which, if any, of these groups admit the automorphism ρ. This means that if we define ρ on generators (i.e., on the $R(x)$'s and $L(x)$'s, as above), we must decide if ρ extends to the entire group. Thus, it suffices to determine if $Q_1(x_1)Q_2(x_2)\dots Q_n(x_n) = 1$ implies that $Q_1(x_1)^\rho Q_2(x_2)^\rho \dots Q_n(x_n)^\rho = 1$ (here, each $Q_i(x_i)$ is either $R(x_i)$ or $L(x_i)$). This task is greatly simplified by the following result from Glauberman [4]: if $Q_1(x_1)Q_2(x_2)\dots Q_n(x_n) = 1$ then $Q_1(x_1)^\rho Q_2(x_2)^\rho \dots Q_n(x_n)^\rho = R(c)$ for some $c \in \mathrm{N}(M)$. Thus, the multiplication group admits ρ, and hence is with triality, precisely if this nuclear element c equals 1. We use this fact freely in the balance of the paper.

3 Results

In this section, M always represents a Moufang loop (perhaps with more structure, as noted in those instances). The first five results in this section focus on Moufang loop multiplication groups with triality. In [7], the triality status of $\mathrm{Mlt}M$ is established for all M except for those of the following form:

$$1 < \mathrm{N}(M) \leq \mathrm{C}(M) < M \text{ and } \mathrm{C}(M)^3 = 1.$$

We note that the center of a loop and the center of its combinatorial multiplication group are isomorphic via the mapping $z \mapsto R(z)$ [1]. Thus, we use $\mathrm{Z}(M)$ and $\mathrm{Z}(\mathrm{Mlt}M)$ interchangeably, as in the next theorem.

Theorem 3.1. *If* $\mathrm{N}(M) \leq \mathrm{C}(M)$ *then* $\mathrm{Mlt}M/\mathrm{Z}(M)$ *is with triality.*

Proof. Elements in $\mathrm{Mlt}M/\mathrm{Z}(M)$ have the form $Q_1(x_1)Q_2(x_2)\dots Q_n(x_n)\mathrm{Z}(M)$. So, if $Q_1(x_1)Q_2(x_2)\dots Q_n(x_n)\mathrm{Z}(M) = 1\mathrm{Z}(M)$, then there exists an element z in the center, such that $Q_1(x_1)Q_2(x_2)\dots Q_n(x_n) = R(z)$. Rearranging gives $Q_1(x_1)Q_2(x_2)\dots\ Q_n(x_n)R(z^{-1}) = 1$. Thus, applying ρ we have $Q_1(x_1)^\rho Q_2(x_2)^\rho \dots$ $Q_n(x_n)^\rho R(z^{-1})^\rho = R(c)$, for some element c in the center. Rearranging gives $Q_1(x_1)^\rho Q_2(x_2)^\rho \dots Q_n(x_n)^\rho = R(z^{-2}c)$, where obviously $z^{-2}c$ is in the center. Thus,

$$Q_1(x_1)^\rho Q_2(x_2)^\rho \dots Q_n(x_n)^\rho \mathrm{Z}(M) = 1\mathrm{Z}(M).$$

Hence ρ is well defined on $\mathrm{Mlt}M/\mathrm{Z}(M)$, and so $\mathrm{Mlt}M/\mathrm{Z}(M)$ is with triality. □

Theorem 3.2. *If* $\mathrm{Mlt}M$ *is a group with triality, then so too is* $U(M;\boldsymbol{M})$*, where* $\boldsymbol{M}$ *is any variety of Moufang loops containing* M*.*

Proof. Define ρ on the generators of $U(M;\mathbf{M})$. We show that ρ extends to all of $U(M;\mathbf{M})$. Assume $Q_1(x_1)Q_2(x_2)\dots Q_n(x_n) = 1$ in $U(M;\mathbf{M})$. Then $Q_1(x_1)^\rho Q_2(x_2)^\rho \dots Q_n(x_n)^\rho = R(c)$ for some $c \in \mathrm{N}(M[x])$. But $Q_1(x_1)Q_2(x_2)\dots$ $Q_n(x_n) = 1$ in $\mathrm{Mlt}M$, also. And since $\mathrm{Mlt}M$ is with triality, we have $Q_1(x_1)^\rho Q_2(x_2)^\rho \dots Q_n(x_n)^\rho = 1$ in $\mathrm{Mlt}M$. This means that $c = 1 \cdot c = 1Q_1(x_1)^\rho Q_2(x_2)^\rho \dots Q_n(x_n)^\rho = 1$. Hence, ρ is well defined, and so $U(M;\mathbf{M})$ is a group with triality. □

Before proving our next theorem we need two technical lemmas. (For the balance of the paper, if G is a group with triality, we let S be the subset of elements of G fixed by ρ, and we let I be the subset of elements fixed by σ.)

Lemma 3.3. *If* G *is a group with triality and D is the S_3 group of triality automorphisms acting on* G*, then* $\mathrm{C}_G(GD) \cong (I \cap S \cap \mathrm{Z}(\mathrm{G}(M)))$.

Proof.

$$\begin{aligned} \mathrm{C}_G(GD) &= \{(g,1) : \forall h \in G, \forall \theta \in D, (g,1)(h,\theta) = (h,\theta)(g,1)\} \\ &= \{(g,1) : \forall h \in G, \forall \theta \in D, (gh,\theta) = (hg^{\theta^{-1}},\theta)\}. \end{aligned}$$

Taking $h = 1$ and $\theta = \sigma$ ($\theta = \rho^2$, $\theta = 1$, respectively) yields

$$\mathrm{C}_G(GD) \subset I \quad (\subset S, G), \text{respectively}).$$

The converse is now trivial. □

Lemma 3.4. *If M is a Moufang loop such that* Mlt$M$ *is with triality, then* $\mathrm{C}_{\mathrm{Mlt}M}(\mathrm{Mlt}MD) = 1$.

Proof. From the proof of the preceeding lemma, $\mathrm{C}_{\mathrm{Mlt}M}(\mathrm{Mlt}MD) = I \cap S \cap \mathrm{Z}(\mathrm{Mlt}M)$. Now, if $h \in \mathrm{Z}(\mathrm{Mlt}M)$, then $h = R(c)$ for some $c \in \mathrm{Z}(M)$ [1, Thm. 11]. But h is also in I, so $c = 1$, and hence $h = 1$. Thus, $I \cap S \cap \mathrm{Z}(\mathrm{Mlt}M) = 1$. □

Our next theorem is a generalization of [3, Corollary 5]. It is offered here because the proof in [3] is incorrect.

Theorem 3.5. *If M is a Moufang loop such that* Mlt$M$ *is with triality, then* $\mathrm{Mlt}M = \mathrm{G}_0(M)$.

Proof. $\mathrm{G}_0(M) \cong \mathrm{Mlt}M/\mathrm{C}_{\mathrm{Mlt}M}(\mathrm{Mlt}MD) \cong \mathrm{Mlt}M$. The first isomorphism is [3, Cor. 1, p. 384]. The second isomorphism is by the previous lemma. □

We turn our attention now to cyclic groups. We begin with a technical lemma.

Lemma 3.6. *If M is a cyclic group, then $M \cap \mathrm{C}(M[x]) = 1$. (Here, the coproduct $M[x]$ is any category of Moufang loops containing all groups.)*

Proof. M embeds in some group G so that $\mathrm{Z}(G) \cap M = 1$. (If M is infinite, take G free on two or more generators; if the order of M is n, take $G =< x, y : x^n = 1 >$.) Say $f : M \to G$ is such an embedding. Then, given $y \in M$, there is a $g \in G$ such that $f(y)g \neq gf(y)$. Let $h :< x > \to G$ be determined by $x \mapsto g$. Thus, there is a unique $F : M[x] \to G$ such that the coproduct diagram commutes. So, if $xy = yx$, then $f(y)g = f(y)h(x) = F(y)F(x) = F(yx) = F(xy) = F(x)F(y) = h(x)f(y) = gf(y)$. Hence, $yx \neq xy$ and $y \notin \mathrm{C}(M[x])$. And thus, $M \cap \mathrm{C}(M[x]) = 1$. □

We are now able to describe the universal multiplication groups of cyclic groups.

Theorem 3.7. *If M is a cyclic group and $\boldsymbol{M}$ is any variety of Moufang loops containing M and all groups, then $U(M;\boldsymbol{M}) \cong M \times M$ and $U(M;\boldsymbol{M})$ is with triality.*

Proof. Let $R(M) =< R(x) : x \in M >_{U(M;\mathbf{M})}$, i. e., the subgroup of $U(M;\mathbf{M})$ generated by the set of all right translations by elements in M. Similarly, let $L(M) =< L(x) : x \in M >_{U(M;\mathbf{M})}$. Since M is cyclic, $M[x]$ is generated by two elements, and so by Moufang's Theorem [2], $M[x]$ is a group. Thus, both $R(M)$ and $L(M)$ are normal in $U(M;\mathbf{M})$. Thus, by the preceding lemma, $R(M) \cap L(M) = 1$, and since $U(M;\mathbf{M}) =< R(M), L(M) >$, we have $U(M;\mathbf{M}) \cong R(M) \times L(M) \cong M \times M$.

Now, define ρ on $U(M;\mathbf{M})$ as follows: $(R(w)L(y))^\rho = R(w^{-1}y)L(y^{-1})$. Next, we compute,

$$\begin{aligned}
([R(w_1)L(y_1)][R(w_2)L(y_2)])^\rho &= (R(w_1w_2)L(y_1y_2))^\rho \\
&= R(w_2^{-1}w_1^{-1}y_1y_2)L(w_2^{-1}w_1^{-1}) \\
&= R(w_1^{-1}y_1w_2^{-1}y_2)L(w_2^{-1}w_1^{-1}) \\
&= R(w_1^{-1}y_1)L(w_1^{-1})R(w_2^{-1}y_2)L(w_2^{-1}) \\
&= [R(w_1)L(y_1)]^\rho[R(w_2)L(y_2)]^\rho.
\end{aligned}$$

Thus, ρ is a well-defined homomorphism, and so $U(M;\mathbf{M})$ is with triality. (As an alternate proof, note that the proof of the following theorem shows that $U(M;\mathbf{M}) \cong \mathrm{G}(M)$, and hence, is with triality.) □

We are also able to describe $\mathrm{G}(M)$, the largest group with triality associated with an arbitrary cyclic group, M.

Theorem 3.8. *If M is a cyclic group, then $\mathrm{G}(M) \cong M \times M$.*

Proof. Let $M =< a >$. Two trivial induction arguments show that for every pair of positive integers m and n, we have $R(a^m)R(a^n) = R(a^{m+n})$ and $L(a^m)L(a^n) = L(a^{m+n})$.

Next, we use induction on $m+n$ to show that $R(a^m)L(a^n) = L(a^n)R(a^m)$. The cases $m+n = 1$ and either $m = 0$ or $n = 0$ are both trivial. The nontrivial instance of $m + n = 2$ is proved by noting that $R(a)L(a) = R(a)P(1)L(a) = P(a^{-1}) = L(a)P(1)R(a) = L(a)R(a)$. So assume that the statement is true for all $m+n < k$. Now consider the case $m+n = k$:

$$\begin{aligned}
R(a^m)L(a^n) &= R(a)R(a^{m-1})L(a^{n-1})L(a) \\
&= R(a)L(a^{n-1})R(a^{m-1})L(a) \\
&= L(a^{n-1})R(a)L(a)R(a^{m-1}) \\
&= L(a^{n-1})L(a)R(a)R(a^{m-1}) \\
&= L(a^n)R(a^m).
\end{aligned}$$

Thus, we have shown that $R(a^m)L(a^n) = L(a^n)R(a^m)$, and hence, the following map is onto: $F : M \times M \to \mathrm{G}(M); (a^m, a^n) \mapsto R(a^m)L(a^n)$. By the computations above, F is a homomorphism. Finally, $U(M;\mathbf{M}) \cong M \times M$ is a homomorphic image of $\mathrm{G}(M)$, and so F is one-to-one. □

For a finite cyclic group M we have a complete description of $\mathrm{G}_0(M)$, the smallest group with triality associated with M.

Theorem 3.9. *If M is a finite cyclic group of order n then $\mathrm{G}_0(M) \cong M \times M$ if 3 does not divide n, and $\mathrm{G}_0(M) \cong (M \times M)/C_3$ if 3 divides n (cf. [3, Prop. 1]).*

Proof. Let $< x >= M$. Doro shows that $\mathrm{G}_0(M) \cong \mathrm{C}_{\mathrm{G}(M)}(\mathrm{G}(M)D)$ [3, p. 384]. Thus, by Lemma 3.3, $\mathrm{G}_0(M) \cong \mathrm{G}(M)/(I \cap S \cap \mathrm{Z}(\mathrm{G}(M)))$.

In $\mathrm{G}(M)$, $R(x^k)L(x^m)$ is in I if and only if $R(x^{k+m})L(x^{k+m}) = 1$. But since, as above, $\mathrm{G}(M)$ is really just $U(M;\mathbf{M})$ and since $U(M;\mathbf{Gp})$ is a homomorphic image of $U(M;\mathbf{M})$, the proof of [8, Thm 235] assures us that $|x|$ divides $m+k$. But clearly we are assuming that $|x|$ is greater than or equal to both m and k. Thus, $|x| = m+k$.

On the other hand, in $\mathrm{G}(M), R(x^k)L(x^m)$ is in S if and only if $|x|$ divides $3k$. So if 3 does not divide n (and note that $n = |x|$), we must have that $|x|$ divides k. And since $|x| = m + k$, this means that $m = 0$ and $n = k$. Thus, $R(x^k)L(x^m) = 1$ and so $I \cap S = 1$. Thus, $(I \cap S \cap \mathrm{Z}(\mathrm{G}(M))) = 1$. And hence, $\mathrm{G}_0(M) \cong \mathrm{G}(M)/(I \cap S \cap \mathrm{Z}(\mathrm{G}(M))) \cong \mathrm{G}(M) \cong M \times M$. This proves the first part of the theorem.

If 3 does divide n, say $n = 3s$, then it is easy to check that $I \cap S = \{1, R(x^s)L(x^{n-s}), R(x^{2s})L(x^{n-2s})\} = C_3$. And since $\mathrm{Z}(\mathrm{G}(M)) = \mathrm{G}(M)$ we have $I \cap S = (I \cap S \cap \mathrm{Z}(\mathrm{G}(M)))$. And hence, $\mathrm{G}_0(M) \cong \mathrm{G}(M)/(I \cap S \cap \mathrm{Z}(\mathrm{G}(M))) \cong (M \times M)/C_3$. □

And we can describe the smallest group with triality associated with the infinite cyclic group.

Theorem 3.10. *If M is the infinite cyclic group, then $\mathrm{G}_0(M) \cong M \times M$.*

Proof. In $\mathrm{G}(M), R(x^k)L(x^m)$ is in I if and only if $R(x^{k+m})L(x^{k+m}) = 1$. But as we have shown, $\mathrm{G}(M)$ is really just $U(M;\mathbf{M})$, and since $U(M;\mathbf{Gp})$ is a homomorphic image of $U(M;\mathbf{M})$, the proof of [8, Thm. 235] assures us that $|x|$ divides $m + k$. Thus $x = 1$ and hence, $I = 1$. Thus, $\mathrm{G}_0(M) = \mathrm{G}(M)/(I \cap S \cap \mathrm{Z}(\mathrm{G}(M))) \cong \mathrm{G}(M) \cong M \times M$. □

We have thus shown that if M is a finite cyclic group whose order is divisible by 3, then there are precisely two groups with triality giving rise to M, namely $M \times M$ and $(M \times M)/C_3$. If M is any other type of cyclic group (i.e., either infinite or of finite order coprime with 3), then there is precisely one group with triality giving rise to M, namely $M \times M$.

Next, in the corollary to the following theorem, we determine the triality status of the universal multiplication groups of finitely generated abelian groups.

Theorem 3.11. *If $A = \prod_{i \in I} A_i$ and if each $U(A_i; \boldsymbol{V})$ is a group with triality, then so too is $U(A; \boldsymbol{V})$ where $\boldsymbol{V}$ is any variety of Moufang loops containing each A_i.*

Proof. We will use vector notation, $\underline{x}$ to denote elements of A. So, $Q_1(\underline{x_1})Q_2(\underline{x_2}) \ldots Q_n(\underline{x_n}) = 1$, implies that $Q_1(\underline{x_1})^\rho Q_2(\underline{x_2})^\rho \ldots Q_n(\underline{x_n})^\rho = R(\underline{c})$ for some $\underline{c} \in \mathrm{N}(A)$.

Now, in each $U(A_i;\mathbf{V})$ we have $Q_1(x_1)Q_2(x_2)\dots Q_n(x_n) = 1$. But since each $U(A_i;\mathbf{V})$ is with triality, we have $Q_1(x_1)^\rho Q_2(x_2)^\rho \dots Q_n(x_n)^\rho = 1$. Thus,

$$\begin{aligned} \underline{c} &= \underline{1}R(\underline{c}) \\ &= \underline{1}Q_1(\underline{x_1})^\rho Q_2(\underline{x_2})^\rho \dots Q_n(\underline{x_n})^\rho \\ &= \underline{1Q_1(x_1)^\rho Q_2(x_2)^\rho \dots Q_n(x_n)^\rho} \\ &= \underline{1}. \end{aligned}$$

Thus, A is a group with triality. □

Corollary 3.12. *If A is a finitely generated abelian group, then $U(A;\boldsymbol{V})$ is a group with triality.*

Finally, we offer two theorems about other classes of Moufang loops.

Theorem 3.13. *If M is a commutative Moufang loop of exponent three, if $\boldsymbol{V}$ is any variety of commutative Moufang loops of exponent three containing M, and if $\mathrm{Z}(U(M;\boldsymbol{V}))\cap I = 1$, then $U(M;\boldsymbol{V}) \cong \mathrm{Mlt}M$.*

Proof. $U(M;\mathbf{V})$ is a group with triality with $\rho = 1$. Let $G = U(M;\mathbf{V})$. By [3, Thm. 1] $G/\mathrm{core}_G(I) \cong \mathrm{Mlt}M$. Now, let k be in $\mathrm{core}_G(I)$. Thus, for every g in G, we have $k = g^{-1}g^\sigma k(g^{-1})^\sigma g$. Taking $g = R(x)$, for any x in M, we get $k = P(x^{-1})kP(x)$. But $M[x]$ is a commutative Moufang loop of exponent three, so $R(x) = L(x) = P(x)$. And since x was arbitrary, k is in $\mathrm{Z}(G)$. Thus, k is in $\mathrm{Z}(G)\cap I = 1$, and so $k = 1$. Thus, $\mathrm{core}_G(I) = 1$, and so $U(M;\mathbf{V}) \cong \mathrm{Mlt}M$. □

We note that if M is an infinitely generated free commutative Moufang loop of exponent three, and if $\mathbf{V}$ is any variety of commutative Moufang loops of exponent three containing M, then $\mathrm{Z}(U(M;\mathbf{V}))\cap I = 1$. Hence, we have the following corollary.

Corollary 3.14. *With M and $\boldsymbol{V}$ as in the previous theorem, $U(M;\boldsymbol{V}) \cong \mathrm{Mlt}M$.*

Theorem 3.15. *If M is a Moufang loop that is not commutative of exponent 2, then $M[x]$ is not commutative. (Here, the coproduct $M[x]$ is in the variety of all Moufang loops.)*

Proof. If M is not commutative, then there is nothing to show. So assume that M is commutative. Let $J : M \to M;\ x \mapsto x^{-1}$. Form the semidirect product $M < J >$. Select $y \in M$ such that $y^{-1} \neq y$. Let $1_M : M \to M < J >$; $y \mapsto (y, 1)$. Let $h :< x >\to M < J >$ be determined by sending $x \mapsto (1, J)$. Then there exists a unique $F : M[x] \to M < J >$ such that the coproduct diagram commutes.

Thus, if $yx = xy$ then $(y, J) = (y, 1)(1, J) = F(y)F(x) = F(yx) = F(xy) = F(x)F(y) = (1, J)(y, 1) = (y^{-1}, J)$, and thus, $y = y^{-1}$, a contradiction. Thus, $yx \neq xy$, and $M[x]$ is not commutative. □

References

[1] Albert A. A. *Quasigroups I.* Trans. Amer. Math. Soc., 1943, **54**, 507–520.

[2] Bruck R. H. *A Survey of Binary Systems.* Springer-Verlag, 1971.

[3] Doro S. *Simple Moufang Loops.* Math. Proc. Camb. Phil. Soc., 1978, **83**, 377–392.

[4] Glauberman G. *On Loops of Odd Order II.* Journal of Algebra, 1968, **8**, 383–414.

[5] Liebeck M. *The Classification of Finite Simple Moufang Loops.* Math. Proc. Camb. Phil. Soc., 1987, **102**, No. 1, 33–47.

[6] Herrlick H., Strecker G. E. *Category Theory.* Allyn and Bacon, 1973.

[7] Phillips J. D. *Moufang loop multiplication groups with triality.* Rocky Mountain Journal of Mathematics, 1999, **29**, No. 4, 1483–1490.

[8] Smith J. D. H. *A Course in the Theory of Groups and Finite Quasigroups.* Les Presses de l'Université de Montréal, 1986.

J. D. Phillips
Department of Mathematics & Computer Science
Northern Michigan University
Marquette, MI 49855, USA
E-mail: *jophilli@nmu.edu*

Received January 20, 2016

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 91–117
ISSN 1024–7696

On paratopies of orthogonal systems of ternary quasigroups. I

P. Syrbu, D. Ceban

Abstract. A paratopy of an orthogonal system $\Sigma = \{A_1, A_2, \ldots, A_n\}$ of n-ary quasigroups, defined on a nonempty set Q, is a mapping $\theta : Q^n \mapsto Q^n$ such that $\Sigma\theta = \Sigma$, where $\Sigma\theta = \{A_1\theta, A_2\theta, \ldots, A_n\theta\}$. The paratopies of the orthogonal systems, consisting of two binary quasigroups and two binary selectors, have been described by Belousov in [1]. He proved that there exist 9 such systems, admitting at least one non-trivial paratopy and that the existence of paratopies implies (in many cases) the parastrophic-orthogonality of a quasigroup from Σ. A generalization of this result (ternary case) is considered in the present paper. We prove that there exist 153 orthogonal systems, consisting of three ternary quasigroups and three ternary selectors, which admit at least one non-trivial paratopy. The existence of paratopies implies (in many cases) some identities. One of them was considered earlier by T. Evans, who proved that it implies the self-orthogonality of the corresponding ternary quasigroup. The present paper contains the first part of our investigation. We give the necessary and sufficient conditions when a triple θ, consisting of three ternary quasigroup operations or of a ternary selector and two ternary quasigroup operations, defines a paratopy of Σ.

Mathematics subject classification: 20N15, 20N05.
Keywords and phrases: Ternary quasigroup, orthoghonal system, strongly orthogonal system, paratopy, self-orthogonal quasigroup.

Let Q be a nonempty set and let n be a positive integer. We will use below (x_1^n) to denote the n-tuple $(x_1, x_2, \ldots, x_n) \in Q^n$ and $i = \overline{1,n}$ for "$i = 1, 2, \ldots, n$". An n-ary groupoid (Q, A) is called an n-ary quasigroup if in the equality $A(x_1, x_2, \ldots, x_n) = x_{n+1}$ any element of the set $\{x_1, x_2, \ldots, x_{n+1}\}$ is uniquely determined by the remaining n elements. If (Q, A) is an n-ary quasigroup and $\sigma \in S_n$, then the operation ${}^{\sigma}A$ defined by the equivalence: ${}^{\sigma}A(x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma n}) = x_{\sigma(n+1)} \Leftrightarrow A(x_1, x_2, \ldots, x_n) = x_{n+1}$, for every $x_1, x_2, \ldots, x_n, x_{n+1} \in Q$, is called a σ-parastrophe (or, simply, a parastrophe) of (Q, A). Following [3], we will denote the transposition $(i, n+1)$, where $i \in \{1, 2, \ldots n\}$, by π_i, so ${}^{(i,n+1)}A = {}^{\pi_i}A$. A σ-parastrophe of an n-ary quasigroup (Q, A) is called a principal parastrophe if $\sigma(n+1) = n+1$. The n-ary operations $A_1, A_2, \ldots, A_n$, defined on Q, are called orthogonal if, for every $a_1, a_2, \ldots, a_n \in Q$, the system of equations $\{A_i(x_1, x_2, \ldots, x_n) = a_i\}_{i=\overline{1,n}}$ has a unique solution [4]. A system of n-ary operations $A_1, A_2, \ldots, A_s$, defined on a set Q, where $s \geq n$, is called orthogonal if every n operations of this system are orthogonal. For every mapping $\theta : Q^n \to Q^n$ there exist, and are unique, n n-ary operations $A_1, A_2, \ldots, A_n$, defined on Q, such that

$\theta((x_1^n)) = (A_1(x_1^n), A_2(x_1^n), \ldots, A_n(x_1^n))$, for every $(x_1^n) \in Q^n$. Moreover, the mapping θ is a bijection if and only if the operations $A_1, A_2, \ldots, A_n$ are orthogonal [4, 6]. The operations $E_1, E_2, \ldots, E_n$, defined on Q, where $E_i(x_1, x_2, \ldots, x_n) = x_i$, for every $x_1, x_2, \ldots, x_n \in Q$, are called the n-ary selectors on Q. Remark that a system of n-ary operations $\{A_1, A_2, \ldots, A_s\}$, defined on Q, where $s \geq 1$, is called strongly orthogonal if the system $\{A_1, A_2, \ldots, A_s, E_1, E_2, \ldots, E_n\}$ is orthogonal [4]. An n-ary operation A is a quasigroup operation if and only if the system $\{A, E_1, E_2, \ldots, E_n\}$ is orthogonal, consequently in a strongly orthogonal system all non-selectors are quasigroup operations. n-Ary quasigroups for which there exist n orthogonal parastrophes (principal parastrophes) are called parastrophic-orthogonal (resp. self-orthogonal) quasigroups. It is known that quasigroups with minimal identities are parastrophic orthogonal [2, 7–9]. If $\Sigma = \{A_1, A_2, \ldots, A_n\}$ is an orthogonal system, then we will denote the system $\{A_1\theta, A_2\theta, \ldots, A_n\theta\}$ by $\Sigma\theta$. A bijection $\theta : Q^n \to Q^n$ is called a paratopy of the system Σ if $\Sigma\theta = \Sigma$.

Let $\Sigma = \{F, E, A, B\}$ be an orthogonal system, where A and B are binary quasigroups defined on a nonempty set Q, F and E are the binary selectors on Q: $F(x, y) = x, E(x, y) = y, \forall x, y \in Q$, and let $\theta : Q^2 \to Q^2$, $\theta = (C, D)$, be a mapping, where C and D are binary operations on Q and $\theta(x, y) = (C(x, y), D(x, y))$, for every $x, y \in Q$. If θ is a paratopy of Σ, i.e. if $\Sigma\theta = \Sigma$, then $\Sigma = \Sigma\theta = \{A\theta, B\theta, F\theta, E\theta\} = \{A\theta, B\theta, C, D\}$, so $C, D \in \Sigma$. Belousov described in [1] all orthogonal systems, consisting of two binary quasigroups and two binary selectors, which have at least one paratopy. Necessary and sufficient conditions when a pair of operations of $\Sigma = \{F, E, A, B\}$ is a paratopy of Σ are given in the following theorem.

Theorem 1 [1]. *Let $\Sigma = \{F, E, A, B\}$ be an orthogonal system of binary operations, defined on a nonempty set Q, where F and E are the binary selectors. Then:*
1. $\theta = (F, E)$ is a paratopy of Σ;
2. $\theta = (E, F)$ is a paratopy of Σ if and only if $B =^s A$, where $s = (12)$;
3. $\theta = (F, A)$ is a paratopy of Σ if and only if $B =^r A$, where $r = (23)$, and (Q, A) satisfies the identity $A(x, A(x, A(x, y))) = y$;
4. $\theta = (A, F)$ is a paratopy of Σ if and only if one of the following conditions holds:
a. $B =^{rl} A$, where $l = (13)$, and (Q, A) satisfies the identity $A(A(y, x), A(x, y)) = x$,
b. $A =^{lr} B(F, B)$ and (Q, B) satisfies the identity ${}^rB({}^rB({}^rB(x, y), y), y) = x$;
5. $\theta = (E, A)$ is a paratopy of Σ if and only if one of the following conditions holds:
a. $B =^{lr} A$ and (Q, A) satisfies the identity $A(A(x, y), x) = A(y, A(x, y))$,
b. $A =^{rl} B(B, E)$ and (Q, B) satisfies the identity ${}^rB({}^rB({}^rB(x, y), y), y) = x$;
6. $\theta = (A, E)$ is a paratopy of Σ if and only if $B =^l A$ and (Q, A) satisfies the identity $A(x, A(x, A(x, y))) = y$;
7. $\theta = (A, B)$ is a paratopy of Σ if and only if one of the following conditions holds:
a. $B =^s A$ and (Q, A) satisfies the identity $A(A(y, x), A(x, y)) = x$,
b. $B =^{rl} A(F, A)$.

A generalization of this result for the ternary case is given in the present paper. Let A_1, A_2, A_3 be ternary quasigroups defined on a nonempty set Q and

let E_1, E_2, E_3 be the ternary selectors: $E_i(x_1, x_2, x_3) = x_i, \forall x_1, x_2, x_3 \in Q, i = \overline{1,3}$. We consider the orthogonal system $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ and denote the set $\{A_1\theta, A_2\theta, A_3\theta, E_1\theta, E_2\theta, E_3\theta\}$ by $\Sigma\theta$. Let $\theta : Q^3 \to Q^3$, $\theta = (B_1, B_2, B_3)$, be a mapping, where B_1, B_2, B_3 are ternary operations on Q and $\theta(x_1^3) = (B_1(x_1^3), B_2(x_1^3), B_3(x_1^3))$, for every $(x_1^3) \in Q^3$. If θ is a paratopy of Σ, then $\Sigma = \Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, E_1\theta, E_2\theta, E_3\theta\} = \{A_1\theta, A_2\theta, A_3\theta, B_1, B_2, B_3\}$, so $\{B_1, B_2, B_3\} \subset \Sigma$, i.e. all paratopies of Σ are triples of operations from Σ. We study the necessary and sufficient conditions when a triple of operations of Σ defines a paratopy of Σ. So as the ternary selectors E_1, E_2, E_3 are fixed, we consider the tuples containing all possible distributions of the ternary selectors in their positions. We prove that, similarly to the binary case, a triple of operations of Σ defines a paratopy of Σ if and only if two quasigroup operations of Σ can be expressed by the third quasigroup operation (using parastrophy and/or superposition) and, in most of cases, the corresponding quasigroup satisfies an identity. Moreover, some of the obtained identities involve the self-orthogonality of the corresponding ternary quasigroup or of its binary retracts.

The present paper includes the first part of our investigation. We consider the triples with three ternary quasigroup operations of Σ and those with a ternary selector and two ternary quasigroup operations (there are 9 possible cases for the triples containing a selector, as E_i occurs in each of three positions and $i = 1, 2, 3$). We prove that there exist 48 orthogonal systems consisting of three ternary quasigroups and ternary selectors E_1, E_2, E_3, that admit at least one paratopy, which components are three ternary quasigroup operations or a ternary selector and two ternary quasigroup operations.

Lemma 1. *The triple (A_1, A_2, A_3) of ternary quasigroups, defined on a nonempty set Q, is a paratopy of the orthogonal system $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ if and only if one of the following statements holds:*
1. $A_2 =^{(132)} A_1$, $A_3 =^{(123)} A_1$ *and* $A_1(A_1,^{(132)} A_1,^{(123)} A_1) = E_2$;
2. $A_2 =^{(132)} A_1$, $A_3 =^{(123)} A_1$ *and* $A_1(A_1,^{(132)} A_1,^{(123)} A_1) = E_3$;
3. $A_1 =^{(12)} A_2$, $A_3 =^{\pi_3} A_2(^{(12)}A_2, A_2, E_1)$ *and* $A_3 =^{(12)} A_3$;
4. $A_2 =^{(23)} A_3$, $A_1 =^{\pi_1} A_3(E_2,^{(23)} A_3, A_3)$ *and* $A_1 =^{(23)} A_1$;
5. $A_3 =^{(13)} A_1$, $A_2 =^{\pi_2} A_1(A_1, E_3,^{(13)} A_1)$ *and* $A_2 =^{(13)} A_2$;
6. $A_3 =^{\pi_3} A_1(A_1, A_2, E_1) =^{\pi_3} A_2(A_1, A_2, E_2)$.

Proof. Let $\theta = (A_1, A_2, A_3)$ be a paratopy of the system Σ. Using $E_1\theta = A_1, E_2\theta = A_2$ and $E_3\theta = A_3$, we obtain $\Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, A_1, A_2, A_3\}$, hence $\{A_1\theta, A_2\theta, A_3\theta\} = \{E_1, E_2, E_3\}$, i. e. there are six possible cases.

1. If $A_1\theta = E_2, A_2\theta = E_3, A_3\theta = E_1$, then $\theta^2 = (E_2, E_3, E_1)$, $\theta^3 = (A_2, A_3, A_1)$, $\theta^4 = (E_3, E_1, E_2)$, $\theta^5 = (A_3, A_1, A_2)$, $\theta^6 = \varepsilon$. From $A_1\theta = E_2$ it follows $A_1\theta^4 = A_3$, i. e. $A_1(E_3, E_1, E_2) = A_3$, so

$$A_3 =^{(123)} A_1. \tag{1.1}$$

Also $A_1\theta = E_2$ implies $A_1\theta^2 = A_2$ and $A_1(E_2, E_3, E_1) = A_2$, hence

$$A_2 =^{(132)} A_1. \tag{1.2}$$

Using (1.1) and (1.2) in $A_1\theta = E_2$, we get

$$A_1(A_1, {}^{(132)}A_1, {}^{(123)}A_1) = E_2. \tag{1.3}$$

Conversely, if (1.1), (1.2) and (1.3) hold, then using (1.1) and (1.2) in (1.3), we obtain $A_1\theta = E_2$, so $A_1(A_1(x_1^3), A_2(x_1^3), A_3(x_1^3)) = E_2(x_1^3)$, $\forall x_1, x_2, x_3 \in Q$, which implies ${}^{(132)}A_1(A_3(x_1^3), A_1(x_1^3), A_2(x_1^3)) = E_2(x_1^3)$. Using (1.2) in the last equality, we get $A_2({}^{(123)}A_1(x_1^3), {}^{(123)}A_2(x_1^3), {}^{(123)}A_3(x_1^3)) = E_2(x_1^3)$, hence

$$A_2(A_1(x_3, x_1, x_2), A_2(x_3, x_1, x_2), A_3(x_3, x_1, x_2)) = E_3(x_3, x_1, x_2),$$

i. e. $A_2\theta = E_3$. From $A_1\theta = E_2$ it follows $A_1(A_1(x_1^3), A_2(x_1^3), A_3(x_1^3)) = E_2(x_1^3)$, which implies ${}^{(123)}A_1(A_2(x_1^3), A_3(x_1^3), A_1(x_1^3)) = E_2(x_1^3)$. Using (1.1) in the last equality, we get $A_3({}^{(132)}A_1(x_1^3), {}^{(132)}A_2(x_1^3), {}^{(132)}A_3(x_1^3)) = E_2(x_1^3)$ hence, for $\forall x_1, x_2, x_3 \in Q$, $A_3(A_1(x_2, x_3, x_1), A_2(x_2, x_3, x_1), A_3(x_2, x_3, x_1)) = E_1(x_2, x_3, x_1)$, i. e. $A_3\theta = E_1$.

2. Let $A_1\theta = E_3, A_2\theta = E_1, A_3\theta = E_2$, then $\theta^2 = (E_3, E_1, E_2)$, $\theta^3 = (A_3, A_1, A_2)$, $\theta^4 = (E_2, E_3, E_1)$, $\theta^5 = (A_2, A_3, A_1)$, $\theta^6 = \varepsilon$. From $A_1\theta = E_3$ it follows $A_1\theta^2 = A_3$, i.e. $A_1(E_3, E_1, E_2) = A_3$, so

$$A_3 = {}^{(123)}A_1. \tag{1.4}$$

Also $A_1\theta = E_3$ implies $A_1\theta^4 = A_2$, i.e. $A_1(E_2, E_3, E_1) = A_2$, hence

$$A_2 = {}^{(132)}A_1. \tag{1.5}$$

Using (1.4) and (1.5) in $A_1\theta = E_3$, we get

$$A_1(A_1, {}^{(132)}A_1, {}^{(123)}A_1) = E_3. \tag{1.6}$$

Conversely, if (1.4), (1.5) and (1.6) hold, then using (1.4) and (1.5) in (1.6), we obtain $A_1\theta = E_3$. Now, the equality $A_1\theta = E_3$ implies $A_1(A_1(x_1^3), A_2(x_1^3), A_3(x_1^3)) = E_3(x_1^3)$, so ${}^{(123)}A_1(A_2(x_1^3), A_3(x_1^3), A_1(x_1^3)) = E_3(x_1^3)$. Using (1.4) in the last equality, we get $A_3({}^{(132)}A_1(x_1^3), {}^{(132)}A_2(x_1^3), {}^{(132)}A_3(x_1^3)) = E_3(x_1^3)$, hence

$$A_3(A_1(x_2, x_3, x_1), A_2(x_2, x_3, x_1), A_3(x_2, x_3, x_1)) = E_2(x_2, x_3, x_1),$$

$\forall x_1, x_2, x_3 \in Q$, i. e. $A_3\theta = E_2$. From $A_1\theta = E_3$ follows $A_1(A_1(x_1^3), A_2(x_1^3), A_3(x_1^3)) = E_3(x_1^3)$, which implies ${}^{(132)}A_1(A_3(x_1^3), A_1(x_1^3), A_2(x_1^3)) = E_2(x_1^3)$. Using (1.5) in the last equality, we get $A_2({}^{(123)}A_1(x_1^3), {}^{(123)}A_2(x_1^3), {}^{(123)}A_3(x_1^3)) = E_3(x_1^3)$, hence

$$A_2(A_1(x_3, x_1, x_2), A_2(x_3, x_1, x_2), A_3(x_3, x_1, x_2)) = E_1(x_3, x_1, x_2),$$

$\forall x_1, x_2, x_3 \in Q$, i.e. $A_2\theta = E_1$.

3. Let $A_1\theta = E_2$, $A_2\theta = E_1$, $A_3\theta = E_3$, then $\theta^2 = (E_2, E_1, E_3)$, $\theta^3 = (A_2, A_1, A_3)$, $\theta^4 = \varepsilon$. From $A_2\theta = E_1$ it follows $A_2\theta^2 = A_1$, i.e. $A_2(E_2, E_1, E_3) = A_1$, so

$$A_1 = {}^{(12)}A_2. \tag{1.7}$$

Also $A_2\theta = E_1$ and (1.7) imply

$$A_3 = {}^{\pi_3}A_2({}^{(12)}A_2, A_2, E_1). \tag{1.8}$$

From $A_2\theta = E_3$ it follows $A_3\theta^2 = A_3$, i. e. $A_3(E_2, E_1, E_3) = A_3$, so

$$A_3 =^{(12)} A_3. \tag{1.9}$$

Conversely, if (1.7), (1.8) and (1.9) hold, then from (1.7) and (1.8) it follows $A_2\theta = E_1$, so $A_2(A_1(x_1^3), A_2(x_1^3), A_3(x_1^3)) = E_1(x_1^3)$, and ${}^{(12)}A_2(A_2(x_1^3), A_1(x_1^3), A_3(x_1^3)) = E_1(x_1^3)$. Using (1.7) in the last equality, we get

$$A_1({}^{(12)}A_2(x_2, x_1, x_3), {}^{(12)}A_1(x_2, x_1, x_3), {}^{(12)}A_3(x_2, x_1, x_3)) = E_2(x_2, x_1, x_3),$$

hence $A_1(A_1(x_2, x_1, x_3), A_2(x_2, x_1, x_3), A_3(x_2, x_1, x_3)) = E_2(x_2, x_1, x_3)$, $\forall x_1, x_2, x_3 \in Q$, i.e. $A_1\theta = E_2$. Also, from $A_2\theta = E_1$ it follows $A_2(A_1\theta, A_2\theta, A_3\theta) = A_1$, so $A_2(E_2, E_1, A_3\theta) = A_1$. Using (1.7) in the last equality, we get ${}^{(12)}A_1(E_2, E_1, A_3\theta) = A_1$, hence $A_1(E_1, E_2, A_3\theta) = A_1$, which implies $A_3\theta = E_3$.

4. Let $A_1\theta = E_1, A_2\theta = E_3, A_3\theta = E_2$, then $\theta^2 = (E_1, E_3, E_2)$, $\theta^3 = (A_1, A_3, A_2)$, $\theta^4 = \varepsilon$. From $A_3\theta = E_2$ it follows $A_3\theta^2 = A_2$, i.e. $A_3(E_1, E_3, E_2) = A_2$, so

$$A_2 =^{(23)} A_3. \tag{1.10}$$

Also $A_3\theta = E_2$ and (1.10) imply

$$A_1 =^{\pi_1} A_3(E_2, {}^{(23)}A_3, A_3). \tag{1.11}$$

From $A_1\theta = E_1$ it follows $A_1\theta^2 = A_1$, i. e. $A_1(E_1, E_3, E_2) = A_1$, so

$$A_1 =^{(23)} A_1. \tag{1.12}$$

Conversely, if (1.10), (1.11) and (1.12) hold, then from (1.10) and (1.11) it follows $A_3\theta = E_2$. Now, the equality $A_3\theta = E_2$ implies $A_3(A_1(x_1^3), A_2(x_1^3), A_3(x_1^3)) = E_2(x_1^3)$, so ${}^{(23)}A_3(A_1(x_1^3), A_3(x_1^3), A_2(x_1^3)) = E_2(x_1^3)$. Using (1.10) in the last equality, we get $A_2({}^{(23)}A_1(x_1, x_3, x_2), {}^{(23)}A_3(x_1, x_3, x_2), {}^{(23)}A_2(x_1, x_3, x_2)) = E_3(x_1, x_3, x_2)$, hence $A_2(A_1(x_1, x_3, x_2), A_2(x_1, x_3, x_2), A_3(x_1, x_3, x_2)) = E_3(x_1, x_3, x_2)$, $\forall x_1, x_2, x_3 \in Q$, i.e. $A_2\theta = E_3$. Also from $A_3\theta = E_2$ it follows $A_3(A_1\theta, A_2\theta, A_3\theta) = A_2$, so $A_3(A_1\theta, E_3, E_2) = A_1$. Using (1.10) in the last equality, we get ${}^{(23)}A_2(A_1\theta, E_3, E_2) = A_1$, hence $A_2(A_1\theta, E_2, E_3) = A_2$, which implies $A_1\theta = E_1$.

5. Let $A_1\theta = E_3, A_2\theta = E_2, A_3\theta = E_1$, then $\theta^2 = (E_3, E_2, E_1)$, $\theta^3 = (A_3, A_2, A_1)$, $\theta^4 = \varepsilon$. From $A_1\theta = E_3$ it follows $A_1\theta^2 = A_3$, i.e. $A_1(E_3, E_2, E_1) = A_3$, so

$$A_3 =^{(13)} A_1. \tag{1.13}$$

Also $A_1\theta = E_3$ and (1.13) imply

$$A_2 =^{\pi_2} A_1(A_1, E_3, {}^{(13)}A_1). \tag{1.14}$$

From $A_2\theta = E_2$ it follows $A_2\theta^2 = A_2$ i.e. $A_2(E_3, E_2, E_1) = A_2$, hence

$$A_2 =^{(13)} A_2. \tag{1.15}$$

Conversely, if (1.13), (1.14) and (1.15) hold, then $A_1\theta = E_3$. Now using $A_1\theta = E_3$, we get $A_1(A_1(x_1^3), A_2(x_1^3), A_3(x_1^3)) = E_3(x_1^3)$, so ${}^{(13)}A_1(A_3(x_1^3), A_2(x_1^3), A_1(x_1^3)) = E_3(x_1^3)$. Using (1.13) in the last equality, we get

$$A_3({}^{(13)}A_3(x_3,x_2,x_1),{}^{(13)}A_2(x_3,x_2,x_1),{}^{(13)}A_1(x_3,x_2,x_1)) = E_1(x_3,x_2,x_1),$$

for $\forall x_1,x_2,x_3 \in Q$, hence

$$A_3(A_1(x_3,x_2,x_1),A_2(x_3,x_2,x_1),A_3(x_3,x_2,x_1)) = E_1(x_3,x_2,x_1),$$

i. e. $A_3\theta = E_1$. Also from $A_1\theta = E_3$ it follows $A_1(A_1\theta,A_2\theta,A_3\theta) = A_3$, so $A_1(E_3,A_2\theta,E_1) = A_3$. Using (1.13) in the last equality, we get ${}^{(13)}A_3(E_3,A_2\theta,E_1) = A_3$, hence $A_3(E_1,A_2\theta,E_3) = A_3$, which implies $A_2\theta = E_2$.

6. Let $A_1\theta = E_1, A_2\theta = E_2, A_3\theta = E_3$, then $\theta^2 = \varepsilon$. From $A_1\theta = E_1$ it follows

$$A_3 = {}^{\pi_3}A_1(A_1,A_2,E_1), \tag{1.16}$$

and from $A_2\theta = E_2$ it follows

$$A_3 = {}^{\pi_3}A_2(A_1,A_2,E_2). \tag{1.17}$$

Conversely, if (1.16) and (1.17) hold, then from (1.16) we get $A_1\theta = E_1$, and (1.17) implies $A_2\theta = E_2$. Now (1.16) implies $A_3\theta = {}^{\pi_3}A_1(E_1,E_2,A_1)$, so $A_3\theta = E_3$. □

Remark. It was proved by T. Evans in [5] that, if a ternary quasigroup (Q,A) satisfies the identity $A(A,{}^{(132)}A,{}^{(123)}A) = E_i$, for some $i \in \{1,2,3\}$, then the triple of principal parastrophes $\{A,{}^{(132)}A,{}^{(123)}A\}$ is orthogonal, so (Q,A) is self-orthogonal of type $(\varepsilon,(132),(123))$, where ε is the unit of the symmetric group S_3.

Lemma 2. *The triple (E_1,A_1,A_2) is a paratopy of the system $\Sigma = \{A_1,A_2,A_3,E_1,E_2,E_3\}$ if and only if one of the following statements holds:*

1. $A_2 = {}^{(23)}A_1$, $A_3(E_1,A_1,{}^{(23)}A_1) = A_3$ *and* $A_1(E_1,A_1,{}^{(23)}A_1) = E_3$;

2. $A_2 = {}^{\pi_3}A_1(E_1,A_1,E_2)$, $A_3(E_1,A_1,{}^{\pi_3}A_1(E_1,A_1,E_2)) = A_3$;

3. $A_1 = {}^{\pi_2}A_2(E_1,E_2,A_2)$, $A_3 = {}^{\pi_3}A_2(E_1,A_2,E_3)$ *and* $A_2(E_1,E_3,{}^{\pi_2}A_2(E_1,E_2,A_2)) = {}^{\pi_3}A_2(E_1,A_2,E_3)$;

4. $A_2 = {}^{\pi_3}A_1(E_1,A_1,E_3)$, $A_3 = {}^{\pi_2}A_1(E_1,E_2,A_1)$ *and* $A_1(E_1,{}^{\pi_3}A_1(E_1,A_1,E_3),E_2) = {}^{\pi_2}A_1(E_1,E_2,A_1)$.

Proof. Let the tuple (E_1,A_1,A_2) be a paratopy of the system Σ. Using $E_1\theta = E_1, E_2\theta = A_1, E_3\theta = A_2$, we obtain $\Sigma = \Sigma\theta = \{A_1\theta,A_2\theta,A_3\theta,A_1,A_2,E_1\}$, i. e. $\{A_1\theta,A_2\theta,A_3\theta\} = \{E_2,E_3,A_3\}$.

1. If $A_1\theta = E_3, A_2\theta = E_2, A_3\theta = A_3$, then $\theta^2 = (E_1,E_3,E_2)$, $\theta^3 = (E_1,A_2,A_1)$, $\theta^4 = \varepsilon$. From $A_1\theta = E_3$ it follows $A_1\theta^2 = A_2$, so

$$A_2 = {}^{(23)}A_1. \tag{2.1}$$

Using (2.1) in $A_3\theta = A_3$, we get

$$A_3(E_1,A_1,{}^{(23)}A_1) = A_3. \tag{2.2}$$

From $A_1\theta = E_3$ and (2.1) it follows

$$A_1(E_1,A_1,{}^{(23)}A_1) = E_3. \tag{2.3}$$

Conversely, if (2.1), (2.2) and (2.3) hold, then (2.1) and (2.3) imply

$$A_1(E_1,A_1,A_2) = E_3, \tag{2.4}$$

so $A_1\theta = E_3$. From (2.1) it follows

$$E_2 =^{\pi_3} A_1(E_1, E_3, A_2). \tag{2.5}$$

The equality (2.4) implies $A_2 =^{\pi_3} A_1(E_1, A_1, E_3)$, hence $A_2\theta =^{\pi_3} A_1(E_1, E_3, A_2)$. Using (2.5) in the last equality, we obtain $A_2\theta = E_2$. From (2.2) and (2.1) it follows $A_3\theta = A_3$.

2. If $A_1\theta = E_3, A_2\theta = A_3, A_3\theta = E_2$, then $\theta^2 = (E_1, E_3, A_3)$, $\theta^3 = (E_1, A_2, E_2)$, $\theta^4 = (E_1, A_3, A_1)$, $\theta^5 = \varepsilon$. From $A_1\theta = E_3$ it follows

$$A_2 =^{\pi_3} A_1(E_1, A_1, E_3). \tag{2.6}$$

Also $A_1\theta = E_3$ implies $A_1\theta^4 = E_2$, i.e. $A_1(E_1, A_3, A_1) = E_2$, so

$$A_3 =^{\pi_2} A_1(E_1, E_2, A_1). \tag{2.7}$$

Analogously, from $A_1\theta = E_3$ it follows $A_1\theta^3 = A_3$, i.e. $A_1(E_1, A_2, E_2) = A_3$. Using (2.6) and (2.7) in the last equality, we get

$$A_1(E_1,^{\pi_3} A_1(E_1, A_1, E_3), E_2) =^{\pi_2} A_1(E_1, E_2, A_1). \tag{2.8}$$

Conversely, if (2.6), (2.7) and (2.8) hold, then (2.6) implies $A_1\theta = E_3$. From (2.7) follows $A_3\theta =^{\pi_2} A_1(E_1, A_1, E_3)$, so $A_3\theta = E_2$. Using (2.6) and (2.7) in (2.8), we obtain $A_1(E_1, A_2, E_2) = A_3$, so $A_2 =^{\pi_2} A_1(E_1, A_3, E_2), \Rightarrow A_2\theta =^{\pi_2} A_1(E_1, E_2, A_1)$. Using (2.7) in the last equality, we get $A_2\theta = A_3$.

3. If $A_1\theta = A_3, A_2\theta = E_2, A_3\theta = E_3$, then $\theta^2 = (E_1, A_3, E_2)$, $\theta^3 = (E_1, E_3, A_1)$, $\theta^4 = (E_1, A_2, A_3)$, $\theta^5 = \varepsilon$. From $A_2\theta = E_2$ it follows

$$A_1 =^{\pi_2} A_2(E_1, E_2, A_2). \tag{2.9}$$

Also $A_2\theta = E_2$ implies $A_2\theta^4 = E_3$, i.e. $A_2(E_1, A_2, A_3) = E_3$, so

$$A_3 =^{\pi_3} A_2(E_1, A_2, E_3). \tag{2.10}$$

Analogously, $A_2\theta = E_2$ implies $A_2\theta^3 = A_3$, i.e. $A_2(E_1, E_3, A_1) = A_3$. Using (2.9) and (2.10) in the last equality, we get

$$A_2(E_1, E_3,^{\pi_2} A_2(E_1, E_2, A_2)) =^{\pi_3} A_2(E_1, A_2, E_3). \tag{2.11}$$

Conversely, if (2.9), (2.10) and (2.11) hold, then (2.9) implies $A_2\theta = E_2$ and from (2.10) it follows $A_3\theta =^{\pi_3} A_2(E_1, E_2, A_2)$, so $A_3\theta = E_3$. Using (2.9) and (2.10) in (2.11), we obtain $A_2(E_1, E_3, A_1) = A_3$, so $A_1 =^{\pi_3} A_2(E_1, E_3, A_3)$, which implies $A_1\theta =^{\pi_3} A_2(E_1, A_2, E_3)$. Using (2.10) in the last equality, we get $A_1\theta = A_3$.

4. If $A_1\theta = E_2, A_2\theta = E_3, A_3\theta = A_3$, then $\theta^2 = \varepsilon$. From $A_1\theta = E_2$ it follows

$$A_2 =^{\pi_3} A_1(E_1, A_1, E_2). \tag{2.12}$$

Using (2.12) in $A_3\theta = A_3$, we get

$$A_3(E_1, A_1, {}^{\pi_3}A_1(E_1, A_1, E_2)) = A_3. \tag{2.13}$$

Conversely, if (2.12) and (2.13) hold, then from (2.12) it follows $A_1\theta = E_2$ and $A_2\theta = {}^{\pi_3}A_1(E_1, E_2, A_1)$, so $A_2\theta = E_3$. Using (2.12) in (2.13), we obtain $A_3\theta = A_3$.

5. If $A_1\theta = A_3, A_2\theta = E_3, A_3\theta = E_2$, then $\theta^2 = (E_1, A_3, E_3)$, $\theta^3 = (E_1, E_2, A_2)$. From $A_3\theta = E_2$ it follows $A_3\theta^3 = A_3$, i. e. $A_3(E_1, E_2, A_2) = A_3(E_1, E_2, E_3)$, so $A_2 = E_3$, which is a contradiction as A_2 is a quasigroup operation.

6. If $A_1\theta = E_2, A_2\theta = A_3, A_3\theta = E_3$, then $\theta^2 = (E_1, E_2, A_3)$. From $A_1\theta = E_2$ it follows $A_1\theta^2 = A_1$, i.e. $A_1(E_1, E_2, A_3) = A_1(E_1, E_2, E_3)$, so $A_3 = E_3$, which is a contradiction as A_3 is a quasigroup operation. □

Corollary 1. *If a ternary quasigroup (Q, A) satisfies the identity*

$$A(E_1(x_1^3), A(x_1^3), {}^{(23)}A(x_1^3)) = E_3(x_1^3), \tag{2.14}$$

then, for $\forall a \in Q$, its 1-retract $B(x, y) = A(a, x, y)$ is self-orthogonal.

Proof. Let (Q, A) be a ternary quasigroup which satisfies the identity (2.14). Replacing $x_2 \mapsto x_3, x_3 \mapsto x_2$ in (2.14), we obtain:

$$A(E_1(x_1, x_3, x_2), A(x_1, x_3, x_2), {}^{(23)}A(x_1, x_3, x_2)) = E_3(x_1, x_3, x_2),$$

which implies $A(E_1(x_1^3), {}^{(23)}A(x_1^3), A(x_1^3)) = E_2(x_1^3)$, so

$${}^{(23)}A(E_1, A, {}^{(23)}A) = E_2. \tag{2.15}$$

Taking $x_1 = a$, where $a \in Q$, in (2.14) and (2.15), and using the 1-retract $B(x, y) = A(a, x, y)$, we get $B(B, {}^{(12)}B) = E$ and ${}^{(12)}B(B, {}^{(12)}B) = F$, respectively, hence $B \perp {}^{(12)}B$, i. e. B is self-orthogonal. □

Lemma 3. *The triple (A_1, E_1, A_2) is a paratopy of the system $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ if and only if one of the following statements holds:*

1. $A_2 = {}^{\pi_3}A_1(A_1, E_1, E_2)$, $A_3 = {}^{\pi_3}A_1(E_2, A_1, E_1)$;

2. $A_1 = {}^{\pi_2}A_3(E_3, A_3, E_2)$, $A_2 = {}^{\pi_1}A_3(A_3, E_3, E_1)$ *and*
$A_3({}^{\pi_2}A_3(E_3, A_3, E_2), E_1, {}^{\pi_1}A_3(A_3, E_3, E_1)) = A_3$;

3. $A_2 = {}^{\pi_3}A_1(A_1, E_1, E_3)$, $A_3 = {}^{\pi_2}A_1(E_2, E_1, A_1)$ *and*
$A_1({}^{\pi_2}A_1(E_2, E_1, A_1), {}^{\pi_3}A_1(A_1, E_1, E_3), E_1) = E_2$;

4. $A_1 = {}^{\pi_3}A_2(A_2, E_3, {}^{\pi_3}A_2(E_2, A_2, E_3))$, $A_3 = {}^{\pi_3}A_2(E_2, A_2, E_3)$ *and*
$A_2({}^{\pi_3}A_2(A_2, E_3, {}^{\pi_3}A_2(E_2, A_2, E_3)), E_1, A_2) = E_2$;

5. $A_1 = {}^{\pi_1}A_2(E_3, E_1, A_2)$, $A_3 = {}^{\pi_2}A_2(E_2, E_3, A_2)$ *and*
$A_2({}^{\pi_2}A_2(E_2, E_3, A_2), {}^{\pi_1}A_2(E_3, E_1, A_2), E_3) = A_2$.

Proof. Let the tuple (A_1, E_1, A_2) be a paratopy of the system Σ. As $E_1\theta = A_1, E_2\theta = E_1, E_3\theta = A_2$, we obtain $\Sigma = \Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, A_1, E_1, A_2\}$, i. e. $\{A_1\theta, A_2\theta, A_3\theta\} = \{E_2, E_3, A_3\}$.

1. If $A_1\theta = E_2, A_2\theta = A_3, A_3\theta = E_3$, then $\theta^2 = (E_2, A_1, A_3), \theta^3 = \varepsilon$. The equality $A_1\theta = E_2$, i. e. $A_1(A_1, E_1, A_2) = E_2$, implies

$$A_2 = {}^{\pi_3}A_1(A_1, E_1, E_2). \tag{3.1}$$

Also, from $A_1\theta = E_2$, we get $A_1\theta^2 = E_1$, i.e. $A_1(E_2, A_1, A_3) = E_1$, so

$$A_3 =^{\pi_3} A_1(E_2, A_1, E_1). \tag{3.2}$$

Conversely, if the equalities (3.1) and (3.2) hold, then (3.1) implies $A_1(A_1, E_1, A_2) = E_2$, hence $A_1\theta = E_2$. Also, from (3.1) it follows $A_2\theta =^{\pi_3} A_1(E_2, A_1, E_1)$ so, using (3.2) in the last equality, we get $A_2\theta = A_3$. From the equality (3.2) it follows $A_3\theta =^{\pi_3} A_1(E_1, E_2, A_1)$, hence $A_3\theta = E_3$.

2. If $A_1\theta = E_3, A_2\theta = E_2, A_3\theta = A_3$, then $\theta^2 = (E_3, A_1, E_2)$, $\theta^3 = (A_2, E_3, E_1)$. From $A_3\theta = A_3$ it follows $A_3\theta^2 = A_3$, i. e. $A_3(E_3, A_1, E_2) = A_3$, so

$$A_1 =^{\pi_2} A_3(E_3, A_3, E_2). \tag{3.3}$$

Also, from $A_3\theta = A_3$ it follows $A_3\theta^3 = A_3$, hence

$$A_2 =^{\pi_1} A_3(A_3, E_3, E_1). \tag{3.4}$$

Using (3.3) and (3.4) in $A_3\theta = A_3$, we obtain

$$A_3(^{\pi_2}A_3(E_3, A_3, E_2), E_1,^{\pi_1} A_3(A_3, E_3, E_1)) = A_3. \tag{3.5}$$

Conversely, if (3.3), (3.4) and (3.5) hold, then using (3.3) and (3.4) in (3.5) we get

$$A_3(A_1, E_1, A_2) = A_3, \tag{3.6}$$

i. e. $A_3\theta = A_3$. From (3.4) it follows $A_3(A_2, E_3, E_1) = A_3$, so

$$E_3 =^{\pi_2} A_3(A_2, A_3, E_1). \tag{3.7}$$

As (3.3) implies $A_1\theta =^{\pi_2} A_3(A_2, A_3, E_1)$, using (3.7) in the last equality we get $A_1\theta = E_3$. From (3.3) it follows $A_3(E_3, A_1, E_2) = A_3$, so

$$E_2 =^{\pi_3} A_3(E_3, A_1, A_3). \tag{3.8}$$

From (3.6) it follows $A_2 =^{\pi_3} A_3(A_1, E_1, A_3), \Rightarrow A_2\theta =^{\pi_3} A_3(E_3, A_1, A_3)$. Using (3.8) in the last equality, we get $A_2\theta = E_2$.

3. If $A_1\theta = E_3, A_2\theta = A_3, A_3\theta = E_2$, then $\theta^2 = (E_3, A_1, A_3)$, $\theta^3 = (A_2, E_3, E_2)$, $\theta^4 = (A_3, A_2, E_1)$, $\theta^5 = (E_2, A_3, A_1)$, $\theta^6 = \varepsilon$. From $A_1\theta = E_3$ it follows

$$A_2 =^{\pi_3} A_1(A_1, E_1, E_3). \tag{3.9}$$

Also, $A_1\theta = E_3$ implies $A_1\theta^5 = E_3\theta^4 \Rightarrow A_1(E_2, A_3, A_1) = E_1$, so

$$A_3 =^{\pi_2} A_1(E_2, E_1, A_1). \tag{3.10}$$

The equality $A_1\theta = E_3$ implies $A_1\theta^4 = E_3\theta^3, \Rightarrow A_1(A_3, A_2, E_1) = E_2$. Using (3.9) and (3.10) in the last equality, we obtain

$$A_1(^{\pi_2}A_1(E_2, E_1, A_1),^{\pi_3} A_1(A_1, E_1, E_3), E_1) = E_2. \tag{3.11}$$

Conversely, if (3.9), (3.10) and (3.11) hold, then from (3.9) we have $A_1(A_1, E_1, A_2) = E_3$, so $A_1\theta = E_3$. From (3.10) it follows $A_3\theta =^{\pi_2} A_1(E_1, A_1, E_3)$, i. e. $A_3\theta = E_2$. Using (3.9) and (3.10) in (3.11) we obtain $A_1(A_3, A_2, E_1) = E_2$, so $A_2 = {}^{\pi_2}A_1(A_3, E_2, E_1), \Rightarrow A_2\theta =^{\pi_2} A_1(E_2, E_1, A_1)$ and, using (3.10), we get $A_2\theta = A_3$.

4. If $A_1\theta = A_3, A_2\theta = E_2, A_3\theta = E_3$, then $\theta^2 = (A_3, A_1, E_2)$, $\theta^3 = (E_3, A_3, E_1)$ $\theta^4 = (A_2, E_3, A_1)$, $\theta^5 = (E_2, A_2, A_3)$, $\theta^6 = \varepsilon$. From $A_2\theta = E_2$ it follows $A_2\theta^5 = E_2\theta^4$, i. e. $A_2(E_2, A_2, A_3) = E_3$, so

$$A_3 =^{\pi_3} A_2(E_2, A_2, E_3). \tag{3.12}$$

Also $A_2\theta = E_2$ implies $A_2\theta^4 = E_2\theta^3$, i. e. $A_2(A_2, E_3, A_1)$, so $A_1 =^{\pi_3} A_2(A_2, E_3, A_3)$ and, using (3.12), we obtain

$$A_1 =^{\pi_3} A_2(A_2, E_3,^{\pi_3} A_2(E_2, A_2, E_3)). \tag{3.13}$$

Now, using (3.12) and (3.13) in the equality $A_2\theta = E_2$, we have

$$A_2({}^{\pi_3}A_2(A_2, E_3,^{\pi_3} A_2(E_2, A_2, E_3)), E_1, A_2) = E_2. \tag{3.14}$$

Conversely, if (3.12), (3.13) and (3.14) hold, then using (3.13) in (3.14), we get $A_2(A_1, E_1, A_2) = E_2$, which implies $A_2\theta = E_2$. From (3.12) it follows $A_3\theta = {}^{\pi_3}A_2(E_1, E_2, A_2) = E_3$. Using (3.12) in (3.13) we obtain $A_1 =^{\pi_3} A_2(A_2, E_3, A_3)$, which implies the equality $A_1\theta =^{\pi_3} A_2(E_2, A_2, E_3)$. So, using (3.12) in the last equality, we have $A_1\theta = A_3$.

5. If $A_1\theta = A_3, A_2\theta = E_3, A_3\theta = E_2$, then $\theta^2 = (A_3, A_1, E_3)$, $\theta^3 = (E_2, A_3, A_2)$, $\theta^4 = \varepsilon$. From the equality $A_2\theta = E_3$ we get

$$A_1 =^{\pi_1} A_2(E_3, E_1, A_2). \tag{3.15}$$

Also, from $A_2\theta = E_3$ it follows $A_2\theta^3 = E_3\theta^2$, i. e. $A_2(E_2, A_3, A_2) = E_3$, so

$$A_3 =^{\pi_2} A_2(E_2, E_3, A_2). \tag{3.16}$$

Moreover, $A_2\theta = E_3$ implies $A_2\theta^2 = A_2$, i. e. $A_2(A_3, A_1, E_3) = A_2$. Using (3.15) and (3.16) in the last equality we get

$$A_2({}^{\pi_2}A_2(E_2, E_3, A_2),^{\pi_1} A_2(E_3, E_1, A_2), E_3) = A_2. \tag{3.17}$$

Conversely, let (3.15), (3.16) and (3.17) hold. Then from (3.15) it follows $A_2\theta = E_3$ and (3.16) implies $A_3\theta =^{\pi_2} A_2(E_1, A_2, E_3) = E_2$. Using (3.15) and (3.16) in (3.17) we get $A_2(A_3, A_1, E_3) = A_2$, which implies $A_1 =^{\pi_2} A_2(A_3, A_2, E_3)$, so $A_1\theta = {}^{\pi_2}A_2(E_2, E_3, A_2)$. Using (3.16) in the last equality, we get $A_1\theta = A_3$.

6. If $A_1\theta = E_2, A_2\theta = E_3, A_3\theta = A_3$, then $\theta^2 = (E_2, A_1, E_3)$, $\theta^3 = (E_1, E_2, A_2)$ and $A_1\theta^3 = E_2\theta^2$, so $A_1(E_1, E_2, A_2) = A_1$, i. e. $A_1(E_1, E_2, A_2) = A_1(E_1, E_2, E_3)$, hence $A_2 = E_3$, which is a contradiction as A_2 is a quasigroup operation. □

Lemma 4. *The triple* (A_1, A_2, E_1) *is a paratopy of the system* $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ *if and only if one of the following statements holds:*

1. $A_1 =^{\pi_3} A_3(E_2, E_3, A_3)$, $A_2 =^{\pi_1} A_3(A_3, E_1, E_2)$ *and*
$A_3(^{\pi_3}A_3(E_2, E_3, A_3),^{\pi_1} A_3(A_3, E_1, E_2), E_1) = A_3$;
2. $A_2 =^{\pi_2} A_1(A_1, E_2, E_1)$, $A_3 =^{\pi_2} A_1(E_2,^{\pi_2} A_1(A_1, E_2, E_1), A_1)$ *and*
$A_1(E_3, A_1,^{\pi_2} A_1(E_2,^{\pi_2} A_1(A_1, E_2, E_1), A_1)) = E_1$;
3. $A_2 =^{\pi_2} A_1(A_1, E_3, E_1)$, $A_3 =^{\pi_2} A_1(E_3, E_1, A_1)$;
4. $A_1 =^{\pi_1} A_2(E_2, A_2, E_1)$, $A_3 =^{\pi_3} A_2(E_3, A_2, E_2)$ *and*
$A_2(^{\pi_3}A_2(E_3, A_2, E_2), E_2,^{\pi_1} A_2(E_2, A_2, E_1)) = A_2$;
5. $A_1 =^{\pi_1} A_2(E_3, A_2, E_1)$, $A_3 =^{\pi_2} A_2(E_3, E_2, A_2)$ *and*
$A_2(A_2,^{\pi_1} A_2(E_3, A_2, E_1), E_2) =^{\pi_2} A_2(E_3, E_2, A_2)$.

Proof. Let the tuple (A_1, A_2, E_1) be a paratopy of the system Σ. As $E_1\theta = A_1, E_2\theta = A_2$, $E_3\theta = E_1$, we obtain $\Sigma = \Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, A_1, A_2, E_1\}$, i.e. $\{A_1\theta, A_2\theta, A_3\theta\} = \{E_2, E_3, A_3\}$.

1. If $A_1\theta = E_2, A_2\theta = E_3, A_3\theta = A_3$, then $\theta^2 = (E_2, E_3, A_1)$, $\theta^3 = (A_2, E_1, E_2)$, $\theta^4 = (E_3, A_1, A_2)$, $\theta^5 = \varepsilon$. As $A_3\theta = A_3, \Rightarrow A_3\theta^2 = A_3, \Rightarrow A_3(E_2, E_3, A_1) = A_3$, we get

$$A_1 =^{\pi_3} A_3(E_2, E_3, A_3). \tag{4.1}$$

Also the equality $A_3\theta = A_3$ implies $A_3\theta^3 = A_3$, i. e. $A_3(A_2, E_1, E_2) = A_3$, hence

$$A_2 =^{\pi_1} A_3(A_3, E_1, E_2). \tag{4.2}$$

Using (4.1) and (4.2) in $A_3\theta = A_3$ we obtain

$$A_3(^{\pi_3}A_3(E_2, E_3, A_3),^{\pi_1} A_3(A_3, E_1, E_2), E_1) = A_3. \tag{4.3}$$

Conversely, if (4.1), (4.2) and (4.3) hold then, using (4.1) and (4.2) in (4.3), we get $A_3\theta = A_3$. From (4.2) it follows $A_3(A_2, E_1, E_2) = A_3$, so

$$^{\pi_3}A_3(A_2, E_1, A_3) = E_2. \tag{4.4}$$

From (4.1) we obtain $A_1\theta =^{\pi_3} A_3(A_2, E_1, A_3)$, and using (4.4) in the last equality we get $A_1\theta = E_2$. Also from (4.1) it follows $A_3(E_2, E_3, A_1) = A_3$, so

$$^{\pi_2}A_3(E_2, A_3, A_1) = E_3. \tag{4.5}$$

Using (4.1) and (4.2) in (4.3) we get $A_3(A_1, A_2, E_1) = A_3$, so $A_2 =^{\pi_2} A_3(A_1, A_3, E_1)$, which implies $A_2\theta =^{\pi_2} A_3(E_2, A_3, A_1)$ and, using (4.5), we obtain $A_2\theta = E_3$.

2. If $A_1\theta = E_2, A_2\theta = A_3, A_3\theta = E_3$, then $\theta^2 = (E_2, A_3, A_1)$, $\theta^3 = (A_2, E_3, E_2)$, $\theta^4 = (A_3, E_1, A_2)$, $\theta^5 = (E_3, A_1, A_3)$, $\theta^6 = \varepsilon$. From $A_1\theta = E_2$ it follows

$$A_2 =^{\pi_2} A_1(A_1, E_2, E_1). \tag{4.6}$$

Also, $A_1\theta = E_2$ implies $A_1\theta^2 = A_2$, i. e. $A_1(E_2, A_3, A_1) = A_2$, so $A_3 = {}^{\pi_2}A_1(E_2, A_2, A_1)$. Using (4.6) in the last equality we obtain

$$A_3 =^{\pi_2} A_1(E_2,^{\pi_2} A_1(A_1, E_2, E_1), A_1). \tag{4.7}$$

From $A_1\theta = E_2$ we also get $A_1\theta^5 = E_1$, i. e. $A_1(E_3, A_1, A_3) = E_1$ and, using (4.7),

$$A_1(E_3, A_1, {}^{\pi_2} A_1(E_2, {}^{\pi_2} A_1(A_1, E_2, E_1), A_1)) = E_1. \tag{4.8}$$

Conversely, if (4.6), (4.7) and (4.8) hold, then from (4.6) we get $A_1\theta = E_2$. Also, from (4.6) it follows $A_2\theta =^{\pi_2} A_1(E_2, A_2, A_1)$. Using (4.6) and (4.7), from the last equality we obtain $A_2\theta = A_3$. Using (4.7) in (4.8), we have $A_1(E_3, A_1, A_3) = E_1$, so $A_3 =^{\pi_3} A_1(E_3, A_1, E_1) \Rightarrow A_3\theta =^{\pi_3} A_1(E_1, E_2, A_1)$, hence $A_3\theta = E_3$.

3. If $A_1\theta = E_3, A_2\theta = A_3, A_3\theta = E_2$, then $\theta^2 = (E_3, A_3, A_1), \theta^3 = \varepsilon$. From $A_1\theta = E_3$ it follows

$$A_2 =^{\pi_2} A_1(A_1, E_3, E_1). \tag{4.9}$$

Also $A_1\theta = E_3$ implies $A_1\theta^2 = E_1$, i. e. $A_1(E_3, A_3, A_1) = E_1$, hence

$$A_3 =^{\pi_2} A_1(E_3, E_1, A_1). \tag{4.10}$$

Conversely, let (4.9) and (4.10) hold. Then the equality (4.9) implies $A_1\theta = E_3$ and $A_2\theta =^{\pi_2} A_1(E_3, E_1, A_1)$. Using (4.10) in the last equality, we obtain $A_2\theta = A_3$. From (4.10) it follows $A_3\theta =^{\pi_2} A_1(E_1, A_1, E_3)$, so $A_3\theta = E_2$.

4. If $A_1\theta = A_3, A_2\theta = E_2, A_3\theta = E_3$, then $\theta^2 = (A_3, E_2, A_1)$, $\theta^3 = (E_3, A_2, A_3)$, $\theta^4 = \varepsilon$. From $A_2\theta = E_2$ it follows

$$A_1 =^{\pi_1} A_2(E_2, A_2, E_1). \tag{4.11}$$

Also $A_2\theta = E_2, \Rightarrow A_2\theta^3 = E_2, \Rightarrow A_2(E_3, A_2, A_3) = E_2$, so

$$A_3 =^{\pi_3} A_2(E_3, A_2, E_2). \tag{4.12}$$

From $A_2\theta = E_2$, we have $A_2\theta^2 = A_2$, i. e. $A_2(A_3, E_2, A_1) = A_2$. Using (4.11) and (4.12) in the last equality we get

$$A_2({}^{\pi_3} A_2(E_3, A_2, E_2), E_2, {}^{\pi_1} A_2(E_2, A_2, E_1)) = A_2. \tag{4.13}$$

Conversely, if (4.11), (4.12) and (4.13) hold, then from (4.11) it follows $A_2\theta = E_2$, and (4.12) implies $A_3\theta =^{\pi_3} A_2(E_1, E_2, A_2)$, so $A_3\theta = E_3$. Using (4.11) and (4.12) in (4.13), we obtain: $A_2(A_3, E_2, A_1) = A_2, \Rightarrow A_1 =^{\pi_3} A_2(A_3, E_2, A_2)$, hence the equality $A_1\theta =^{\pi_3} A_2(E_3, A_2, E_2)$ holds. Now, using (4.12) in the last equality, we have $A_1\theta = A_3$.

5. If $A_1\theta = A_3, A_2\theta = E_3, A_3\theta = E_2$, then $\theta^2 = (A_3, E_3, A_1)$, $\theta^3 = (E_2, E_1, A_3)$, $\theta^4 = (A_2, A_1, E_2)$, $\theta^5 = (E_3, A_3, A_2)$, $\theta^6 = \varepsilon$. From $A_2\theta = E_3$ it follows

$$A_1 =^{\pi_1} A_2(E_3, A_2, E_1). \tag{4.14}$$

Also, from $A_2\theta = E_3$ we get $A_2\theta^5 = E_2$, i.e. $A_2(E_3, A_3, A_2) = E_2$, so

$$A_3 =^{\pi_2} A_2(E_3, E_2, A_2). \tag{4.15}$$

Once again $A_2\theta = E_3$ implies $A_2\theta^4 = A_3$, i. e. $A_2(A_2, A_1, E_2) = A_3$. Using (4.14) and (4.15) in the last equality, we obtain

$$A_2(A_2,^{\pi_1} A_2(E_3, A_2, E_1), E_2) =^{\pi_2} A_2(E_3, E_2, A_2). \tag{4.16}$$

Conversely, if (4.14), (4.15) and (4.16) hold, then from (4.14) it follows $A_2\theta = E_3$, and (4.15) implies $A_3\theta =^{\pi_2} A_2(E_1, A_2, E_3)$, so $A_3\theta = E_2$. Using (4.14) and (4.15) in (4.16), we get $A_2(A_2, A_1, E_2) = A_3$, hence $A_1 =^{\pi_2} A_2(A_2, A_3, E_2)$, which implies $A_1\theta =^{\pi_2} A_2(E_3, E_2, A_2)$. Using (4.15) in the last equality, we get $A_1\theta = A_3$.

6. If $A_1\theta = E_3, A_2\theta = E_2, A_3\theta = A_3$, then $\theta^2 = (E_3, E_2, A_1)$, $\theta^3 = (E_1, A_2, E_3)$. The equality $A_3\theta = A_3$ implies $A_3\theta^3 = A_3$, so $A_3(E_1, A_2, E_3) = A_3(E_1, E_2, E_3) \Rightarrow A_2 = E_2$, which is a contradiction as A_2 is a quasigroup operation. □

Lemma 5. *The triple (E_2, A_1, A_2) is a paratopy of the system $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ if and only if one of the following statements holds:*
1. $A_2 =^{\pi_3} A_1(E_2, A_1, E_1)$, $A_3 =^{\pi_3} A_1(A_1, E_1, E_2)$;
2. $A_1 =^{\pi_1} A_3(A_3, E_3, E_1)$, $A_2 =^{\pi_2} A_3(E_3, A_3, E_2)$ *and*
$A_3(E_2,^{\pi_1} A_3(A_3, E_3, E_1),^{\pi_2} A_3(E_3, A_3, E_2)) = A_3$;
3. $A_2 =^{\pi_3} A_1(E_2, A_1, E_3)$, $A_3 =^{\pi_1} A_1(E_2, E_1, A_1)$ *and*
$A_1(^{\pi_3} A_1(E_2, A_1, E_3),^{\pi_1} A_1(E_2, E_1, A_1), E_2) = E_1$;
4. $A_3 =^{\pi_3} A_2(A_2, E_1, E_3)$, $A_1 =^{\pi_3} A_2(E_3, A_2,^{\pi_3} A_2(A_2, E_1, E_3))$ *and*
$A_2(E_2,^{\pi_3} A_2(E_3, A_2,^{\pi_3} A_2(A_2, E_1, E_3)), A_2) = E_1$;
5. $A_1 =^{\pi_2} A_2(E_2, E_3, A_2)$, $A_3 =^{\pi_1} A_2(E_3, E_1, A_2)$ *and*
$A_2(^{\pi_2} A_2(E_2, E_3, A_2),^{\pi_1} A_2(E_3, E_1, A_2), E_3) = A_2$.

Proof. Let the tuple (E_2, A_1, A_2) be a paratopy of the system Σ. As $E_1\theta = E_2, E_2\theta = A_1, E_3\theta = A_2$, we obtain $\Sigma = \Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, A_1, A_2, E_2\}$, i. e. $\{A_1\theta, A_2\theta, A_3\theta\} = \{E_1, E_3, A_3\}$.

1. If $A_1\theta = E_1, A_2\theta = A_3, A_3\theta = E_3$, then $\theta^2 = (A_1, E_1, A_3)$, $\theta^3 = \varepsilon$. From $A_1\theta = E_1$ it follows

$$A_2 =^{\pi_3} A_1(E_2, A_1, E_1). \tag{5.1}$$

Also $A_1\theta = E_1$ implies $A_1\theta^2 = E_2$, i. e. $A_1(A_1, E_1, A_3) = E_2$, so

$$A_3 =^{\pi_3} A_1(A_1, E_1, E_2). \tag{5.2}$$

Conversely, if (5.1) and (5.2) hold, then from (5.1) it follows $A_1\theta = E_1$. Moreover, (5.1) implies $A_2\theta =^{\pi_3} A_1(A_1, E_1, E_2)$ and, using (5.2) in the last equality, we get $A_2\theta = A_3$. From (5.2) it follows $A_3\theta =^{\pi_3} A_1(E_1, E_2, A_1)$, therefore $A_3\theta = E_3$.

2. If $A_1\theta = E_3, A_2\theta = E_1, A_3\theta = A_3$, then $\theta^2 = (A_1, E_3, E_1)$, $\theta^3 = (E_3, A_2, E_2)$, $\theta^4 = (A_2, E_1, A_1)$, $\theta^5 = \varepsilon$. As $A_3\theta = A_3, \Rightarrow A_3\theta^2 = A_3, \Rightarrow A_3(A_1, E_3, E_1) = A_3$, we get

$$A_1 =^{\pi_1} A_3(A_3, E_3, E_1). \tag{5.3}$$

Also, $A_3\theta = A_3$ implies $A_3\theta^3 = A_3$, i. e. $A_3(E_3, A_2, E_2) = A_3$, hence

$$A_2 =^{\pi_2} A_3(E_3, A_3, E_2). \tag{5.4}$$

Using (5.3) and (5.4) in $A_3\theta = A_3$, we have

$$A_3(E_2,^{\pi_1} A_3(A_3, E_3, E_1),^{\pi_2} A_3(E_3, A_3, E_2)) = A_3. \tag{5.5}$$

Conversely, if (5.3), (5.4) and (5.5) hold then, using (5.3) and (5.4) in (5.5), we get

$$A_3(E_2, A_1, A_2) = A_3, \tag{5.6}$$

so $A_3\theta = A_3$. From (5.4) it follows $A_3(E_3, A_2, E_2) = A_3$, i.e.

$$E_3 =^{\pi_1} A_3(A_3, A_2, E_2). \tag{5.7}$$

From (5.3) it follows $A_1\theta =^{\pi_1} A_3(A_3, A_2, E_2)$. Using (5.7) in the last equality we obtain $A_1\theta = E_3$. From (5.3) we get $A_3(A_1, E_3, E_1) = A_3$, hence

$$E_1 =^{\pi_3} A_3(A_1, E_3, A_3). \tag{5.8}$$

The equality (5.6) implies $A_2 =^{\pi_3} A_3(E_2, A_1, A_3) \Rightarrow A_2\theta =^{\pi_3} A_3(A_1, E_3, A_3)$. Using (5.8) in the last equality, we get $A_2\theta = E_1$.

3. If $A_1\theta = E_3, A_2\theta = A_3, A_3\theta = E_1$, then $\theta^2 = (A_1, E_3, A_3)$, $\theta^3 = (E_3, A_2, E_1)$, $\theta^4 = (A_2, A_3, E_2)$, $\theta^5 = (A_3, E_1, A_1)$, $\theta^6 = \varepsilon$. From $A_1\theta = E_3$ it follows

$$A_2 =^{\pi_3} A_1(E_2, A_1, E_3). \tag{5.9}$$

Also $A_1\theta = E_3$ implies $A_1\theta^5 = E_2$, i. e. $A_1(A_3, E_1, A_1) = E_2$, hence

$$A_3 =^{\pi_1} A_1(E_2, E_1, A_1). \tag{5.10}$$

Moreover, from $A_1\theta = E_3$ we get $A_1\theta^4 = E_1$, i.e. $A_1(A_2, A_3, E_2) = E_1$. Using (5.9) and (5.10) in the last equality, we obtain

$$A_1(^{\pi_3}A_1(E_2, A_1, E_3),^{\pi_1} A_1(E_2, E_1, A_1), E_2) = E_1. \tag{5.11}$$

Conversely, if (5.9), (5.10) and (5.11) hold, then from (5.9) it follows $A_1\theta = E_3$ and (5.10) implies $A_3\theta =^{\pi_1} A_1(A_1, E_2, E_3)$, so $A_3\theta = E_1$. Using (5.9) and (5.10) in (5.11) we obtain $A_1(A_2, A_3, E_2) = E_1$, which implies $A_2 =^{\pi_1} A_1(E_1, A_3, E_2)$, so $A_2\theta =^{\pi_1} A_1(E_2, E_1, A_1)$. Using (5.10) in the last equality, we get $A_2\theta = A_3$.

4. If $A_1\theta = A_3, A_2\theta = E_1, A_3\theta = E_3$, then $\theta^2 = (A_1, A_3, E_1)$, $\theta^3 = (A_3, E_3, E_2)$, $\theta^4 = (E_3, A_2, A_1)$, $\theta^5 = (A_2, E_1, A_3)$, $\theta^6 = \varepsilon$. From $A_2\theta = E_1$ it follows $A_2\theta^5 = E_3$, i. e. $A_2(A_2, E_1, A_3) = E_3$, so

$$A_3 =^{\pi_3} A_2(A_2, E_1, E_3). \tag{5.12}$$

Also, $A_2\theta = E_1$ implies $A_2\theta^4 = A_3$, i.e. $A_2(E_3, A_2, A_1) = A_3$, so $A_1 = {}^{\pi_3}A_2(E_3, A_2, A_3)$. Using (5.12) in the last equality we get

$$A_1 =^{\pi_3} A_2(E_3, A_2,^{\pi_3} A_2(A_2, E_1, E_3)). \tag{5.13}$$

Using (5.13) in $A_2\theta = E_1$, we obtain

$$A_2(E_2,^{\pi_3} A_2(E_3, A_2,^{\pi_3} A_2(A_2, E_1, E_3)), A_2) = E_1. \tag{5.14}$$

Conversely, if (5.12), (5.13) and (5.14) hold, then using (5.13) in (5.14), we get $A_2\theta = E_1$. From (5.12) it follows $A_3\theta =^{\pi_3} A_2(E_1, E_2, A_2)$, so $A_3\theta = E_3$. Using (5.12) in (5.13), we obtain $A_1 =^{\pi_3} A_2(E_3, A_2, A_3)$, which implies $A_1\theta = {}^{\pi_3}A_2(A_2, E_1, E_3)$. Using (5.12) in the last equality, we get $A_1\theta = A_3$.

5. If $A_1\theta = A_3, A_2\theta = E_3, A_3\theta = E_1$, then $\theta^2 = (A_1, A_3, E_3)$, $\theta^3 = (A_3, E_1, A_2)$, $\theta^4 = \varepsilon$. From $A_2\theta = E_3$ it follows

$$A_1 =^{\pi_2} A_2(E_2, E_3, A_2). \tag{5.15}$$

Also $A_2\theta = E_3$ implies $A_2\theta^3 = E_3$, i. e. $A_2(A_3, E_1, A_2) = E_3$, hence

$$A_3 =^{\pi_1} A_2(E_3, E_1, A_2). \tag{5.16}$$

From $A_2\theta = E_3$ it follows $A_2\theta^2 = A_2$, i.e. $A_2(A_1, A_3, E_3) = A_2$. Using (5.15) and (5.16) in the last equality, we obtain

$$A_2({}^{\pi_2}A_2(E_2, E_3, A_2),^{\pi_1} A_2(E_3, E_1, A_2), E_3) = A_2. \tag{5.17}$$

Conversely, if (5.15), (5.16) and (5.17) hold, then from (5.15) it follows $A_2\theta = E_3$ and from (5.16) we get $A_3\theta =^{\pi_1} A_2(A_2, E_2, E_3)$, so $A_3\theta = E_1$. Using (5.15) and (5.16) in (5.17), we obtain $A_2(A_1, A_3, E_3) = A_2$, hence $A_1 =^{\pi_1} A_2(A_2, A_3, E_3)$, which implies $A_1\theta =^{\pi_1} A_2(E_3, E_1, A_2)$ and, using (5.16) in the last equality, we get $A_1\theta = A_3$.

6. If $A_1\theta = E_1, A_2\theta = E_3, A_3\theta = A_3$, then $\theta^2 = (A_1, E_1, E_3)$, $\theta^3 = (E_1, E_2, A_2)$. From $A_1\theta = E_1$ it follows $A_1\theta^3 = E_1\theta^2$, so $A_1(E_1, E_2, A_2) = A_1(E_1, E_2, E_3)$, hence $A_2 = E_3$, which is a contradiction as A_2 is a quasigroup operation. □

Lemma 6. *The triple (A_1, E_2, A_2) is a paratopy of the system $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ if and only if one of the following statements holds:*
1. $A_2 =^{\pi_3} A_1(A_1, E_2, E_1)$, $A_3(A_1, E_2,^{\pi_3} A_1(A_1, E_2, E_1)) = A_3$;
2. $A_2 =^{(13)} A_1$, $A_3(A_1, E_2,^{(13)} A_1) = A_3$ *and* $A_1(A_1, E_2,^{(13)} A_1) = E_3$;
3. $A_2 =^{\pi_3} A_1(A_1, E_2, E_3)$, $A_3 =^{\pi_1} A_1(E_1, E_2, A_1)$ *and*
$A_1({}^{\pi_3}A_1(A_1, E_2, E_3), E_2, E_1) =^{\pi_1} A_1(E_1, E_2, A_1)$;
4. $A_1 =^{\pi_1} A_2(E_1, E_2, A_2)$, $A_3 =^{\pi_3} A_2(A_2, E_2, E_3)$ *and*
$A_2(E_3, E_2,^{\pi_1} A_2(E_1, E_2, A_2) =^{\pi_3} A_2(A_2, E_2, E_3)$.

Proof. Let the tuple (A_1, E_2, A_2) be a paratopy of the system Σ. Using $E_1\theta = A_1, E_2\theta = E_2, E_3\theta = A_2$, we obtain $\Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, A_1, A_2, E_2\}$, i. e. $\{A_1\theta, A_2\theta, A_3\theta\} = \{E_1, E_3, A_3\}$.

1. If $A_1\theta = E_1, A_2\theta = E_3, A_3\theta = A_3$, then $\theta^2 = \varepsilon$. From $A_1\theta = E_1$ it follows

$$A_2 =^{\pi_3} A_1(A_1, E_2, E_1), \tag{6.1}$$

so, using (6.1) in $A_3\theta = A_3$, we get

$$A_3(A_1, E_2,^{\pi_3} A_1(A_1, E_2, E_1)) = A_3. \tag{6.2}$$

Conversely, if (6.1) and (6.2) hold, then from (6.1) it follows $A_1\theta = E_1$ and $A_2\theta = {}^{\pi_3}A_1(E_1, E_2, A_1)$, so $A_2\theta = E_3$. Using (6.1) in (6.2), we obtain $A_3\theta = A_3$.

2. If $A_1\theta = E_3, A_2\theta = E_1, A_3\theta = A_3$, then $\theta^2 = (E_1, E_3, E_2)$, $\theta^3 = (A_2, E_2, A_1)$, $\theta^4 = \varepsilon$. From $A_1\theta = E_3$ it follows $A_1\theta^2 = A_2$, i. e. $A_1(E_3, E_2, E_1) = A_2$, so

$$A_2 =^{(13)} A_1. \tag{6.3}$$

Using (6.3) in $A_3\theta = A_3$, we get

$$A_3(A_1, E_2,^{(13)} A_1) = A_3. \tag{6.4}$$

Now, $A_1\theta = E_3$ and (6.3) imply

$$A_1(A_1, E_2,^{(13)} A_1) = E_3. \tag{6.5}$$

Conversely, if (6.3), (6.4) and (6.5) hold, then (6.3) and (6.5) imply

$$A_1(A_1, E_2, A_2) = E_3, \tag{6.6}$$

so $A_1\theta = E_3$, and from (6.3) it follows $A_2 = A_1(E_3, E_2, E_1)$, hence

$$E_1 =^{\pi_3} A_1(E_3, E_2, A_2). \tag{6.7}$$

The equality (6.6) implies $A_2 =^{\pi_3} A_1(A_1, E_2, E_3)$, hence $A_2\theta =^{\pi_3} A_1(E_3, E_2, A_2)$ and, using (6.7), we obtain $A_2\theta = E_1$. Now, using (6.3) in (6.4), we get $A_3\theta = A_3$.

3. If $A_1\theta = E_3, A_2\theta = A_3, A_3\theta = E_1$, then $\theta^2 = (E_3, E_2, A_3)$, $\theta^3 = (A_2, E_2, E_1)$, $\theta^4 = (A_3, E_2, A_1)$, $\theta^5 = \varepsilon$. From $A_1\theta = E_3$ it follows

$$A_2 =^{\pi_3} A_1(A_1, E_2, E_3). \tag{6.8}$$

Also $A_1\theta = E_3$ implies $A_1\theta^4 = E_1$, i. e. $A_1(A_3, E_2, A_1) = E_1$, so

$$A_3 =^{\pi_1} A_1(E_1, E_2, A_1). \tag{6.9}$$

Using once again $A_1\theta = E_3$ we have $A_1\theta^3 = A_3$, i. e. $A_1(A_2, E_2, E_1) = A_3$. Using (6.8) and (6.9) in the last equality, we get

$$A_1({}^{\pi_3}A_1(A_1, E_2, E_3), E_2, E_1) =^{\pi_1} A_1(E_1, E_2, A_1). \tag{6.10}$$

Conversely, if (6.8), (6.9) and (6.10) hold, then (6.8) implies $A_1\theta = E_3$. From (6.9) it follows $A_3\theta =^{\pi_1} A_1(A_1, E_2, E_3)$, so $A_3\theta = E_1$. Using (6.8) and (6.9) in (6.10), we obtain $A_1(A_2, E_2, E_1) = A_3$, so $A_2 =^{\pi_1} A_1(A_3, E_2, E_1), \Rightarrow A_2\theta =^{\pi_1} A_1(E_1, E_2, A_1)$ and, using (6.9), we get $A_2\theta = A_3$.

4. If $A_1\theta = A_3, A_2\theta = E_1, A_3\theta = E_3$, then $\theta^2 = (A_3, E_2, E_1)$, $\theta^3 = (E_3, E_2, A_1)$, $\theta^4 = (A_2, E_2, A_3)$, $\theta^5 = \varepsilon$. From $A_2\theta = E_1$ it follows

$$A_1 =^{\pi_1} A_2(E_1, E_2, A_2), \tag{6.11}$$

which implies $A_2\theta^4 = E_3$, i. e. $A_2(A_2, E_2, A_3) = E_3$, so

$$A_3 =^{\pi_3} A_2(A_2, E_2, E_3). \tag{6.12}$$

Analogously, $A_2\theta = E_1$ implies $A_2\theta^3 = A_3$, i. e. $A_2(E_3, E_2, A_1) = A_3$. Using (6.11) and (6.12) in the last equality, we get

$$A_2(E_3, E_2, ^{\pi_1} A_2(E_1, E_2, A_2)) =^{\pi_3} A_2(A_2, E_2, E_3). \tag{6.13}$$

Conversely, if (6.11), (6.12) and (6.13) hold, then (6.11) implies $A_2\theta = E_1$ and from (6.12) it follows $A_3\theta =^{\pi_3} A_2(E_1, E_2, A_2)$, so $A_3\theta = E_3$. Using (6.11) and (6.12) in (6.13), we obtain $A_2(E_3, E_2, A_1) = A_3$, so $A_1 =^{\pi_3} A_2(E_3, E_2, A_3)$, which implies $A_1\theta =^{\pi_3} A_2(A_2, E_2, E_3)$. Using (6.12) in the last equality, we get $A_1\theta = A_3$.

5. If $A_1\theta = E_1, A_2\theta = A_3, A_3\theta = E_3$, then $\theta^2 = (E_1, E_2, A_3)$. From $A_1\theta = E_1$ it follows $A_1\theta^2 = A_1$, i. e. $A_1(E_1, E_2, A_3) = A_1(E_1, E_2, E_3)$, so $A_3 = E_3$, which is a contradiction as A_3 is a quasigroup operation.

6. If $A_1\theta = A_3, A_2\theta = E_3, A_3\theta = E_1$, then $\theta^2 = (A_3, E_2, E_3)$, $\theta^3 = (E_1, E_2, A_2)$. From $A_3\theta = E_1$ it follows $A_3\theta^3 = A_3$, i. e. $A_3(E_1, E_2, A_2) = A_3(E_1, E_2, E_3)$, so $A_2 = E_3$, which is a contradiction as A_2 is a quasigroup operation. □

Corollary 2. *If a ternary quasigroup (Q, A) satisfies the identity $A(A, E_2, ^{(13)} A) = E_3$ then, for $\forall a \in Q$, its 2-retract $B(x, y) = A(x, a, y)$ is self-orthogonal.*

The proof is analogous to that of Corollary 1.

Lemma 7. *The triple (A_1, A_2, E_2) is a paratopy of the system $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ if and only if one of the following statements holds:*
1. $A_2 =^{\pi_2} A_1(A_1, E_1, E_2)$, $A_3 =^{\pi_3} A_1(A_1, E_3, E_1)$ *and* $A_1(E_1, ^{\pi_3} A_1(A_1, E_3, E_1), ^{\pi_2} A_1(A_1, E_1, E_2)) = A_1$;
2. $A_1 =^{\pi_1} A_2(E_1, A_2, E_2)$, $A_3 =^{\pi_1} A_2(^{\pi_1} A_2(E_1, A_2, E_2), E_1, A_2)$ *and* $A_2(A_2, E_3, ^{\pi_1} A_2(^{\pi_1} A_2(E_1, A_2, E_2), E_1, A_2))) = E_2$;
3. $A_1 =^{\pi_1} A_2(E_3, A_2, E_2)$, $A_3 =^{\pi_1} A_2(E_2, E_3, A_2)$;
4. $A_1 =^{\pi_2} A_3(E_2, A_3, E_1)$, $A_2 =^{\pi_3} A_3(E_3, E_1, A_3)$ *and* $A_3(^{\pi_2} A_3(E_2, A_3, E_1), ^{\pi_3} A_3(E_3, E_1, A_3), E_2) = A_3$;
5. $A_2 =^{\pi_2} A_1(A_1, E_3, E_2)$, $A_3 =^{\pi_1} A_1(E_1, E_3, A_1)$ *and* $A_1(^{\pi_2} A_1(A_1, E_3, E_2), A_1, E_1) =^{\pi_1} A_1(E_1, E_3, A_1)$.

Proof. Let the tuple (A_1, A_2, E_2) be a paratopy of the system Σ. As $E_1\theta = A_1, E_2\theta = A_2, E_3\theta = E_2$, we obtain $\Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, A_1, A_2, E_2\}$, i. e. $\{A_1\theta, A_2\theta, A_3\theta\} = \{E_1, E_3, A_3\}$.

1. If $A_1\theta = E_1, A_2\theta = A_3, A_3\theta = E_3$, then $\theta^2 = (E_1, A_3, A_2)$, $\theta^3 = (A_1, E_3, A_3)$, $\theta^4 = \varepsilon$. From $A_1\theta = E_1$ it follows

$$A_2 =^{\pi_2} A_1(A_1, E_1, E_2). \tag{7.1}$$

Also $A_1\theta = E_1$ implies $A_2\theta^3 = E_1$, i. e. $A_1(A_1, E_3, A_3) = E_1$, so

$$A_3 =^{\pi_3} A_1(A_1, E_3, E_1). \tag{7.2}$$

The equality $A_1\theta = E_1$ also implies $A_1\theta^2 = A_1$, i. e. $A_1(E_1, A_3, A_2) = A_1$. Using (7.1) and (7.2) in the last equality we get

$$A_1(E_1,^{\pi_3} A_1(A_1, E_3, E_1),^{\pi_2} A_1(A_1, E_1, E_2)) = A_1. \tag{7.3}$$

Conversely, if (7.1), (7.2) and (7.3) hold, then from (7.1) it follows $A_1\theta = E_1$. The equality (7.2) implies $A_3\theta =^{\pi_3} A_1(E_1, E_2, A_1)$, so $A_3\theta = E_3$. Using (7.1) and (7.2) in (7.3), we obtain $A_1(E_1, A_3, A_2) = A_1$, which implies $A_2 =^{\pi_3} A_1(E_1, A_3, A_1)$, hence $A_2\theta =^{\pi_3} A_1(A_1, E_3, E_1)$. Using (7.2) in the last equality, we get $A_2\theta = A_3$.

2. If $A_1\theta = A_3, A_2\theta = E_1, A_3\theta = E_3$, then $\theta^2 = (A_3, E_1, A_2)$, $\theta^3 = (E_3, A_1, E_1)$, $\theta^4 = (E_2, A_3, A_1)$, $\theta^5 = (A_2, E_3, A_3)$, $\theta^6 = \varepsilon$. From $A_2\theta = E_1$ it follows

$$A_1 =^{\pi_1} A_2(E_1, A_2, E_2). \tag{7.4}$$

Also $A_2\theta = E_1$ implies $A_2\theta^2 = A_1, \Rightarrow A_2(A_3, E_1, A_2) = A_1, \Rightarrow A_3 =^{\pi_1} A_2(A_1, E_1, A_2)$. Using (7.4) in the last equality we obtain

$$A_3 =^{\pi_1} A_2(^{\pi_1}A_2(E_1, A_2, E_2), E_1, A_2). \tag{7.5}$$

The equality $A_2\theta = E_1$ also implies $A_2\theta^5 = E_2$, i.e. $A_2(A_2, E_3, A_3) = E_2$. Now using (7.5) in the last equality we get

$$A_2(A_2, E_3,^{\pi_1} A_2(^{\pi_1}A_2(E_1, A_2, E_2), E_1, A_2)) = E_2. \tag{7.6}$$

Conversely, if (7.4), (7.5) and (7.6) hold, then from (7.4) we get $A_2\theta = E_1$. Also, from (7.4) it follows $A_1\theta =^{\pi_1} A_2(A_1, E_1, A_2)$. Using (7.4) and (7.5) in the last equality we obtain $A_1\theta = A_3$. Using (7.4) and (7.5) in (7.6), we have $A_2(A_2, E_3, A_3) = E_2$, so $A_3 =^{\pi_3} A_2(A_2, E_3, E_2) \Rightarrow A_3\theta =^{\pi_3} A_2(E_1, E_2, A_2)$, hence $A_3\theta = E_3$.

3. If $A_1\theta = A_3$, $A_2\theta = E_3$, $A_3\theta = E_1$ then $\theta^2 = (A_3, E_3, A_2)$, $\theta^3 = \varepsilon$. From $A_2\theta = E_3$ it follows

$$A_1 =^{\pi_1} A_2(E_3, A_2, E_2). \tag{7.7}$$

Also $A_2\theta = E_3$ implies $A_2\theta^2 = E_2$, i. e. $A_2(A_3, E_3, A_2) = E_2$, hence

$$A_3 =^{\pi_1} A_2(E_2, E_3, A_2). \tag{7.8}$$

Conversely, if (7.7) and (7.8) hold, then from (7.7) follows $A_2\theta = E_3$ and $A_1\theta = {}^{\pi_1}A_2(E_2, E_3, A_2)$. Using (7.8) in the last equality we obtain $A_1\theta = A_3$. The equality (7.8) implies also $A_3\theta =^{\pi_1} A_2(A_2, E_2, E_3)$, so $A_3\theta = E_1$.

4. If $A_1\theta = E_3, A_2\theta = E_1, A_3\theta = A_3$, then $\theta^2 = (E_3, E_1, A_2)$, $\theta^3 = (E_2, A_1, E_1)$, $\theta^4 = (A_2, E_3, A_1)$, $\theta^5 = \varepsilon$. From $A_3\theta = A_3$ it follows $A_3\theta^2 = A_3$, i. e. $A_3(E_3, E_1, A_2) = A_3$, so

$$A_2 =^{\pi_3} A_3(E_3, E_1, A_3). \tag{7.9}$$

Also the equality $A_3\theta = A_3$ implies $A_3\theta^3 = A_3$, i. e. $A_3(E_2, A_1, E_1) = A_3$, hence

$$A_1 =^{\pi_2} A_3(E_2, A_3, E_1). \tag{7.10}$$

Using (7.9) and (7.10) in $A_3\theta = A_3$ we obtain

$$A_3({}^{\pi_2}A_3(E_2, A_3, E_1), {}^{\pi_3}A_3(E_3, E_1, A_3), E_2) = A_3. \tag{7.11}$$

Conversely, if (7.9), (7.10) and (7.11) hold, then using (7.9) and (7.10) in (7.11) we get

$$A_3(A_1, A_2, E_2) = A_3, \tag{7.12}$$

i. e. $A_3\theta = A_3$. From (7.10) it follows $A_3(E_2, A_1, E_1) = A_3$, so

$${}^{\pi_3}A_3(E_2, A_1, A_3) = E_1. \tag{7.13}$$

From (7.9) we obtain $A_2\theta = {}^{\pi_3}A_3(E_2, A_1, A_3)$ so, using (7.13) in the last equality, we get $A_2\theta = E_1$. Also from (7.9) it follows $A_3(E_3, E_1, A_2) = A_3$, so

$${}^{\pi_1}A_3(A_3, E_1, A_2) = E_3. \tag{7.14}$$

From (7.12) we get $A_1 = {}^{\pi_1}A_3(A_3, A_2, E_2)$, which implies $A_1\theta = {}^{\pi_1}A_3(A_3, E_1, A_2)$. Using (7.14) in the last equality we obtain $A_1\theta = E_3$.

5. If $A_1\theta = E_3, A_2\theta = A_3, A_3\theta = E_1$, then $\theta^2 = (E_3, A_3, A_2)$, $\theta^3 = (E_2, E_1, A_3)$, $\theta^4 = (A_2, A_1, E_1)$, $\theta^5 = (A_3, E_3, A_1)$, $\theta^6 = \varepsilon$. From $A_1\theta = E_3$ it follows

$$A_2 = {}^{\pi_2}A_1(A_1, E_3, E_2). \tag{7.15}$$

Also, from $A_1\theta = E_3$ we get $A_1\theta^5 = E_1$, i. e. $A_1(A_3, E_3, A_1) = E_1$, so

$$A_3 = {}^{\pi_1}A_1(E_1, E_3, A_1). \tag{7.16}$$

The equality $A_1\theta = E_3$ also implies $A_1\theta^4 = A_3$, i. e. $A_1(A_2, A_1, E_1) = A_3$. Using (7.15) and (7.16) in the last equality, we obtain

$$A_1({}^{\pi_2}A_1(A_1, E_3, E_2), A_1, E_1) = {}^{\pi_1}A_1(E_1, E_3, A_1). \tag{7.17}$$

Conversely, if (7.15), (7.16) and (7.17) hold, then from (7.15) it follows $A_1\theta = E_3$. The equality (7.16) implies $A_3\theta = {}^{\pi_1}A_1(A_1, E_2, E_3)$ so $A_3\theta = E_1$. Using (7.15) and (7.16) in (7.17), we get $A_1(A_2, A_1, E_1) = A_3$, hence $A_2 = {}^{\pi_1}A_1(A_3, A_1, E_1)$, which implies $A_2\theta = {}^{\pi_1}A_1(E_1, E_3, A_1)$. Using (7.16) in the last equality, we get $A_2\theta = A_3$.

6. If $A_1\theta = E_1, A_2\theta = E_3, A_3\theta = A_3$, then $\theta^2 = (E_1, E_3, A_2)$, $\theta^3 = (A_1, E_2, E_3)$. The equality $A_3\theta = A_3$ implies $A_3\theta^3 = A_3$, so $A_3(A_1, E_2, E_3) = A_3(E_1, E_2, E_3) \Rightarrow A_1 = E_1$, which is a contradiction as A_1 is a quasigroup operation. □

Lemma 8. *The triple (E_3, A_1, A_2) is a paratopy of the system $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ if and only if one of the following statements holds:*
1. $A_1 = {}^{\pi_2}A_2(E_3, E_1, A_2)$, $A_3 = {}^{\pi_2}A_2(A_2, E_3, E_1)$;
2. $A_2 = {}^{\pi_1}A_3(A_3, E_1, E_2)$, $A_1 = {}^{\pi_3}A_3(E_2, E_3, A_3)$ *and*
$A_3(E_3, {}^{\pi_3}A_3(E_2, E_3, A_3), {}^{\pi_1}A_3(A_3, E_1, E_2)) = A_3$;
3. $A_1 = {}^{\pi_2}A_2(E_3, E_2, A_2)$, $A_3 = {}^{\pi_1}A_2(E_3, A_2, E_1)$ *and*
$A_2({}^{\pi_2}A_2(E_3, E_2, A_2), E_3, {}^{\pi_1}A_2(E_3, A_2, E_1)) = E_1$;

4. $A_2 =^{\pi_3} A_1(E_3, A_1, E_1)$, $A_3 =^{\pi_2} A_1(A_1, E_2, E_1)$ *and* $A_1(E_2,^{\pi_3} A_1(E_3, A_1, E_1), A_1) =^{\pi_2} A_1(A_1, E_2, E_1)$;
5. $A_2 =^{\pi_3} A_1(E_3, A_1, E_2)$, $A_3 =^{\pi_1} A_1(E_2, A_1, E_1)$ *and* $A_1(^{\pi_3} A_1(E_3, A_1, E_2), E_2,^{\pi_1} A_1(E_2, A_1, E_1)) = A_1$.

Proof. Let the tuple (E_3, A_1, A_2) be a paratopy of the system Σ. As $E_1\theta = E_3, E_2\theta = A_1, E_3\theta = A_2$, we obtain $\Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, A_1, A_2, E_3\}$, i.e. $\{A_1\theta, A_2\theta, A_3\theta\} = \{E_1, E_2, A_3\}$.

1. If $A_1\theta = A_3, A_2\theta = E_1, A_3\theta = E_2$, then $\theta^2 = (A_2, A_3, E_1)$, $\theta^3 = \varepsilon$. From $A_2\theta = E_1$ it follows

$$A_1 =^{\pi_2} A_2(E_3, E_1, A_2). \tag{8.1}$$

Also $A_2\theta = E_1$ implies $A_2\theta^2 = E_3$, i. e. $A_2(A_2, A_3, E_1) = E_3$, so

$$A_3 =^{\pi_2} A_2(A_2, E_3, E_1). \tag{8.2}$$

Conversely, if (8.1) and (8.2) hold, then from (8.1) it follows $A_2\theta = E_1$. Moreover, (8.1) implies $A_1\theta =^{\pi_2} A_2(A_2, E_3, E_1)$, using (8.2) in the last equality, we get $A_1\theta = A_3$. From (8.2) it follows $A_3\theta =^{\pi_2} A_2(E_1, A_2, E_3)$, therefore $A_3\theta = E_2$.

2. If $A_1\theta = E_1, A_2\theta = E_2, A_3\theta = A_3$ then $\theta^2 = (A_2, E_1, E_2)$, $\theta^3 = (E_2, E_3, A_1)$, $\theta^4 = (A_1, A_2, E_1)$, $\theta^5 = \varepsilon$. From $A_3\theta = A_3$ it follows $A_3\theta^2 = A_3$, i.e. $A_3(A_2, E_1, E_2) = A_3$, so

$$A_2 =^{\pi_1} A_3(A_3, E_1, E_2). \tag{8.3}$$

Also, $A_3\theta = A_3$ implies $A_3\theta^3 = A_3$, i. e. $A_3(E_2, E_3, A_1) = A_3$, hence

$$A_1 =^{\pi_3} A_3(E_2, E_3, A_3). \tag{8.4}$$

Using (8.3) and (8.4) in $A_3\theta = A_3$, we get

$$A_3(E_3,^{\pi_3} A_3(E_2, E_3, A_3),^{\pi_1} A_3(A_3, E_1, E_2)) = A_3. \tag{8.5}$$

Conversely, if (8.3), (8.4) and (8.5) hold, then using (8.3) and (8.4) in (8.5), we obtain

$$A_3(E_3, A_1, A_2) = A_3, \tag{8.6}$$

i. e. $A_3\theta = A_3$. From (8.4) it follows $A_3(E_2, E_3, A_1) = A_3$, so

$$E_2 =^{\pi_1} A_3(A_3, E_3, A_1). \tag{8.7}$$

From (8.3) it follows $A_2\theta =^{\pi_1} A_3(A_3, E_3, A_1)$. Using (8.7) in the last equality we obtain $A_2\theta = E_2$. From (8.3) we get $A_3(A_2, E_1, E_2) = A_3$, then

$$E_1 =^{\pi_2} A_3(A_2, A_3, E_2). \tag{8.8}$$

The equality (8.6) implies $A_1 =^{\pi_2} A_3(E_3, A_3, A_2)$, hence $A_1\theta =^{\pi_2} A_3(A_2, A_3, E_2)$. Using (8.8) in the last equality, we get $A_1\theta = E_1$.

3. If $A_1\theta = A_3, A_2\theta = E_2, A_3\theta = E_1$, then $\theta^2 = (A_2, A_3, E_2)$, $\theta^3 = (E_2, E_1, A_1)$, $\theta^4 = (A_1, E_3, A_3)$, $\theta^5 = (A_3, A_2, E_1)$, $\theta^6 = \varepsilon$. From $A_2\theta = E_2$ it follows

$$A_1 =^{\pi_2} A_2(E_3, E_2, A_2). \tag{8.9}$$

Also $A_2\theta = E_2$ implies $A_2\theta^5 = E_3$, i.e. $A_2(A_3, A_2, E_1) = E_3$, hence

$$A_3 =^{\pi_1} A_2(E_3, A_2, E_1). \tag{8.10}$$

Moreover, from $A_2\theta = E_2$ we get $A_2\theta^4 = E_1$, i.e. $A_2(A_1, E_3, A_3) = E_1$. Using (8.9) and (8.10) in the last equality, we obtain

$$A_2(^{\pi_2}A_2(E_3, E_2, A_2), E_3, ^{\pi_1} A_2(E_3, A_2, E_1)) = E_1. \tag{8.11}$$

Conversely, if (8.9), (8.10) and (8.11) hold, then from (8.9) it follows $A_2\theta = E_2$ and (8.10) implies $A_3\theta =^{\pi_1} A_2(A_2, E_2, E_3)$, so $A_3\theta = E_1$. Using (8.9) and (8.10) in (8.11) we obtain $A_2(A_1, E_3, A_3) = E_1$, which implies $A_1 =^{\pi_1} A_2(E_1, E_3, A_3)$, so $A_1\theta =^{\pi_1} A_2(E_3, A_2, E_1)$. Using (8.10) in the last equality we get $A_1\theta = A_3$.

4. If $A_1\theta = E_1, A_2\theta = A_3, A_3\theta = E_2$, then $\theta^2 = (A_2, E_1, A_3)$, $\theta^3 = (A_3, E_3, E_2)$, $\theta^4 = (E_2, A_2, A_1)$, $\theta^5 = (A_1, A_3, E_1)$, $\theta^6 = \varepsilon$. From $A_1\theta = E_1$ it follows

$$A_2 =^{\pi_3} A_1(E_3, A_1, E_1). \tag{8.12}$$

Also $A_1\theta = E_1$ implies $A_1\theta^5 = E_2$, i. e. $A_1(A_1, A_3, E_1) = E_2$, so

$$A_3 =^{\pi_2} A_1(A_1, E_2, E_1). \tag{8.13}$$

Analogously, $A_1\theta = E_1$ implies $A_1\theta^4 = A_3$, i.e. $A_1(E_2, A_2, A_1) = A_3$. Using (8.12) and (8.13) in the last equality we get

$$A_1(E_2, ^{\pi_3} A_1(E_3, A_1, E_1), A_1) =^{\pi_2} A_1(A_1, E_2, E_1). \tag{8.14}$$

Conversely, if (8.12), (8.13) and (8.14) hold, then (8.12) implies $A_1\theta = E_1$. From (8.13) it follows $A_3\theta =^{\pi_2} A_1(E_1, A_1, E_3)$, so $A_3\theta = E_2$. Using (8.12) and (8.13) in (8.14), we obtain $A_1(E_2, A_2, A_1) = A_3$, which implies $A_2 =^{\pi_2} A_1(E_2, A_3, A_1)$, so $A_2\theta =^{\pi_2} A_1(A_1, E_2, E_1)$. Finally, using (8.13) in the last equality, we get $A_2\theta = A_3$.

5. If $A_1\theta = E_2, A_2\theta = A_3, A_3\theta = E_1$, then $\theta^2 = (A_2, E_2, A_3)$, $\theta^3 = (A_3, A_1, E_1)$, $\theta^4 = \varepsilon$. From $A_1\theta = E_2$ it follows

$$A_2 =^{\pi_3} A_1(E_3, A_1, E_2). \tag{8.15}$$

Also $A_1\theta = E_2$ implies $A_1\theta^3 = E_2$, i.e. $A_1(A_3, A_1, E_1) = E_2$, hence

$$A_3 =^{\pi_1} A_1(E_2, A_1, E_1). \tag{8.16}$$

From $A_1\theta = E_2$ it follows $A_1\theta^2 = A_1$, i. e. $A_1(A_2, E_2, A_3) = A_1$. Using (8.15) and (8.16) in the last equality, we obtain

$$A_1(^{\pi_3}A_1(E_3, A_1, E_2), E_2, ^{\pi_1} A_1(E_2, A_1, E_1)) = A_1. \tag{8.17}$$

Conversely, if (8.15), (8.16) and (8.17), then from (8.15) it follows $A_1\theta = E_2$. From (8.16) we get $A_3\theta =^{\pi_1} A_1(A_1, E_2, E_3)$, so $A_3\theta = E_1$. Using (8.15) and (8.16) in (8.17), we obtain $A_1(A_2, E_2, A_3) = A_1$, hence $A_2 =^{\pi_1} A_1(A_1, E_2, A_3)$, which implies $A_2\theta =^{\pi_1} A_1(E_2, A_1, E_1)$ and using (8.16) in the last equality, we get $A_2\theta = A_3$.

6. If $A_1\theta = E_2, A_2\theta = E_1, A_3\theta = A_3$, then $\theta^2 = (A_2, E_2, E_1)$, $\theta^3 = (E_1, A_1, E_3)$. From $A_2\theta = E_1$ it follows $A_2\theta^3 = E_1\theta^2$, so $A_2(E_1, A_1, E_3) = A_2(E_1, E_2, E_3)$, hence $A_1 = E_2$, which is a contradiction as A_1 is a quasigroup operation. □

Lemma 9. *The triple* (A_1, E_3, A_2) *is a paratopy of the system* $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ *if and only if one of the following statements holds:*
1. $A_1 =^{\pi_1} A_2(E_2, E_3, A_2)$, $A_3 =^{\pi_1} A_2(E_3, A_2, E_2)$;
2. $A_2 =^{\pi_3} A_1(A_1, E_3, E_1)$, $A_3 =^{\pi_2} A_1(A_1, E_1, E_2)$ *and*
$A_1(E_1,^{\pi_3} A_1(A_1, E_3, E_1),^{\pi_2} A_1(A_1, E_1, E_2)) = A_1$;
3. $A_2 =^{\pi_2} A_3(E_2, A_3, E_1)$, $A_1 =^{\pi_3} A_3(E_3, E_1, A_3)$ *and*
$A_3(^{\pi_3} A_3(E_3, E_1, A_3), E_3,^{\pi_2} A_3(E_2, A_3, E_1)) = A_3$;
4. $A_2 =^{\pi_3} A_1(A_1, E_3, E_2)$, $A_3 =^{\pi_1} A_1(E_1, A_1, E_2)$ *and*
$A_1(^{\pi_3} A_1(A_1, E_3, E_2), E_1, A_1) =^{\pi_1} A_1(E_1, A_1, E_2)$;
5. $A_1 =^{\pi_1} A_2(E_1, E_3, A_2)$, $A_3 =^{\pi_2} A_2(A_2, E_3, E_2)$ *and*
$A_2(E_3,^{\pi_1} A_2(E_1, E_3, A_2),^{\pi_2} A_2(A_2, E_3, E_2)) = E_2$.

Proof. Let the tuple (A_1, E_3, A_2) be a paratopy of the system Σ. As $E_1\theta = A_1, E_2\theta = E_3, E_3\theta = A_2$, we obtain $\Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, A_1, A_2, E_3\}$, i.e. $\{A_1\theta, A_2\theta, A_3\theta\} = \{E_1, E_2, A_3\}$.

1. If $A_1\theta = A_3, A_2\theta = E_2, A_3\theta = E_1$, then $\theta^2 = (A_3, A_2, E_2)$, $\theta^3 = \varepsilon$. From $A_2\theta = E_2$ it follows

$$A_1 =^{\pi_1} A_2(E_2, E_3, A_2). \tag{9.1}$$

Also $A_2\theta = E_2$ implies $A_2\theta^2 = E_3$, i.e. $A_2(A_3, A_2, E_2) = E_3$, so

$$A_3 =^{\pi_1} A_2(E_3, A_2, E_2). \tag{9.2}$$

Conversely, if (9.1) and (9.2) hold, then from (9.1) it follows $A_2\theta = E_2$. Moreover, (9.1) implies $A_1\theta =^{\pi_1} A_2(E_3, A_2, E_2)$, using (9.2) in the last equality, we get $A_1\theta = A_3$. From (9.2) it follows $A_3\theta =^{\pi_1} A_2(A_2, E_2, E_3)$, therefore $A_3\theta = E_1$.

2. If $A_1\theta = E_1, A_2\theta = A_3, A_3\theta = E_2$, then $\theta^2 = (E_1, A_2, A_3)$, $\theta^3 = (A_1, A_3, E_2)$, $\theta^4 = \varepsilon$. From $A_1\theta = E_1$ it follows

$$A_2 =^{\pi_3} A_1(A_1, E_3, E_1). \tag{9.3}$$

Also, $A_1\theta = E_1$ implies $A_1\theta^3 = E_1$, i. e. $A_1(A_1, A_3, E_2) = E_1$, hence

$$A_3 =^{\pi_2} A_1(A_1, E_1, E_2). \tag{9.4}$$

Moreover, from $A_1\theta = E_1$ it follows $A_1\theta^2 = A_1$, i. e. $A_1(E_1, A_2, A_3) = A_1$. Using (9.3) and (9.4) in the last equality, we get

$$A_1(E_1,^{\pi_3} A_1(A_1, E_3, E_1),^{\pi_2} A_1(A_1, E_1, E_2)) = A_1. \tag{9.5}$$

Conversely, if (9.3), (9.4) and (9.5) hold, then from (9.3) it follows $A_1\theta = E_1$ and (9.4) implies $A_3\theta =^{\pi_2} A_1(E_1, A_1, E_3)$, therefore $A_3\theta = E_2$. Using (9.3) and (9.4) in (9.5), we obtain $A_1(E_1, A_2, A_3) = A_1$, so $A_2 =^{\pi_2} A_1(E_1, A_1, A_3)$, which implies $A_2\theta =^{\pi_2} A_1(A_1, E_1, E_2)$. Using (9.4) in the last equality, we get $A_2\theta = A_3$.

3. If $A_1\theta = E_2, A_2\theta = E_1, A_3\theta = A_3$, then $\theta^2 = (E_2, A_2, E_1)$, $\theta^3 = (E_3, E_1, A_1)$, $\theta^4 = (A_2, A_1, E_2)$, $\theta^5 = \varepsilon$. From $A_3\theta = A_3$ it follows $A_3\theta^2 = A_3$, i.e. $A_3(E_2, A_2, E_1) = A_3$, so

$$A_2 =^{\pi_2} A_3(E_2, A_3, E_1). \tag{9.6}$$

Also, $A_3\theta = A_3$ implies $A_3\theta^3 = A_3$, i.e. $A_3(E_3, E_1, A_1) = A_3$, hence

$$A_1 =^{\pi_3} A_3(E_3, E_1, A_3). \tag{9.7}$$

Using (9.6) and (9.7) in $A_3\theta = A_3$, we get

$$A_3(^{\pi_3}A_3(E_3, E_1, A_3), E_3,^{\pi_2} A_3(E_2, A_3, E_1)) = A_3. \tag{9.8}$$

Conversely, if (9.6), (9.7) and (9.8) hold, then using (9.6) and (9.7) in (9.8), we obtain

$$A_3(A_1, E_3, A_2) = A_3, \tag{9.9}$$

therefore $A_3\theta = A_3$. From (9.7) it follows $A_3(E_3, E_1, A_1) = A_3$, so

$$E_1 =^{\pi_2} A_3(E_3, A_3, A_1). \tag{9.10}$$

From (9.6) it follows $A_2\theta =^{\pi_2} A_3(E_3, A_3, A_1)$. Using (9.10) in the last equality we obtain $A_2\theta = E_1$. From (9.6) we get $A_3(E_2, A_1, A_1) = A_3$, then

$$E_2 =^{\pi_1} A_3(A_3, A_2, E_1). \tag{9.11}$$

The equality (9.9) implies $A_1 =^{\pi_1} A_3(A_3, E_3, A_2)$, so $A_1\theta =^{\pi_1} A_3(A_3, A_2, E_1)$. Using (9.11) in the last equality, we get $A_1\theta = E_2$.

4. If $A_1\theta = E_2, A_2\theta = A_3, A_3\theta = E_1$, then $\theta^2 = (E_2, A_2, A_3)$, $\theta^3 = (E_3, A_3, E_1)$, $\theta^4 = (A_2, E_1, A_1)$, $\theta^5 = (A_3, A_1, E_2)$, $\theta^6 = \varepsilon$. From $A_1\theta = E_2$ it follows

$$A_2 =^{\pi_3} A_1(A_1, E_3, E_2). \tag{9.12}$$

Also $A_1\theta = E_2$ implies $A_1\theta^5 = E_1$, i. e. $A_2(A_3, A_1, E_2) = E_3$, hence

$$A_3 =^{\pi_1} A_1(E_1, A_1, E_2). \tag{9.13}$$

Moreover, from $A_1\theta = E_2$, we get $A_1\theta^4 = A_3$, i. e. $A_1(A_2, E_1, A_1) = A_3$. Using (9.12) and (9.13) in the last equality, we obtain

$$A_1(^{\pi_3}A_1(A_1, E_3, E_2), E_1, A_1) =^{\pi_1} A_1(E_1, A_1, E_2). \tag{9.14}$$

Conversely, if (9.12), (9.13) and (9.14) hold, then from (9.12) it follows $A_1\theta = E_2$ and (9.13) implies $A_3\theta =^{\pi_1} A_1(A_1, E_2, E_3)$, so $A_3\theta = E_1$. Using (9.12) and (9.13)

in (9.14) we obtain $A_1(A_2, E_1, A_1) = A_3$, which implies $A_2 =^{\pi_1} A_1(A_3, E_1, A_1)$, so $A_1\theta =^{\pi_1} A_1(E_1, A_1, E_2)$. Using (9.13) in the last equality we get $A_1\theta = A_3$.

5. If $A_1\theta = A_3, A_2\theta = E_1, A_3\theta = E_2$, then $\theta^2 = (A_3, A_2, E_1)$, $\theta^3 = (E_2, E_1, A_1)$, $\theta^4 = (E_3, A_1, A_3)$, $\theta^5 = (A_2, A_3, E_2)$, $\theta^6 = \varepsilon$. From $A_2\theta = E_1$ it follows

$$A_1 =^{\pi_1} A_2(E_1, E_3, A_2). \tag{9.15}$$

Also $A_2\theta = E_1$ implies $A_2\theta^5 = E_3$, i. e. $A_2(A_2, A_3, E_2) = E_3$, so

$$A_3 =^{\pi_2} A_2(A_2, E_3, E_2). \tag{9.16}$$

Analogously, $A_2\theta = E_1$ implies $A_2\theta^4 = E_2$, i. e. $A_2(E_3, A_1, A_3) = E_2$. Using (9.15) and (9.16) in the last equality we get

$$A_2(E_3,^{\pi_1} A_2(E_1, E_3, A_2),^{\pi_2} A_2(A_2, E_3, E_2)) = E_2. \tag{9.17}$$

Conversely, if (9.15), (9.16) and (9.17) hold, then (9.15) implies $A_2\theta = E_1$. From (9.16) it follows $A_3\theta =^{\pi_2} A_2(E_1, A_2, E_3)$, so $A_3\theta = E_2$. Using (9.15) and (9.16) in (9.17), we obtain $A_2(E_3, A_1, A_3) = E_2$, which implies $A_1 =^{\pi_2} A_2(E_3, E_2, A_3)$, so $A_1\theta =^{\pi_2} A_2(A_2, E_3, E_2)$. Using (9.16) in the last equality, we get $A_1\theta = A_3$.

6. If $A_1\theta = E_1, A_2\theta = E_2, A_3\theta = A_3$, then $\theta^2 = (E_1, A_2, E_2)$, $\theta^3 = (A_1, E_2, E_3)$. From $A_2\theta = E_2$ it follows $A_2\theta^3 = E_2\theta^2$, so $A_2(A_1, E_2, E_3) = A_2(E_1, E_2, E_3)$, hence $A_1 = E_1$, which is a contradiction as A_1 is a quasigroup operation. □

Lemma 10. *The triple (A_1, A_2, E_3) is a paratopy of the system $\Sigma = \{A_1, A_2, A_3, E_1, E_2, E_3\}$ if and only if one of the following statements holds:*
1. $A_2 =^{\pi_2} A_1(A_1, E_1, E_3)$, $A_3(A_1,^{\pi_2} A_1(A_1, E_1, E_3), E_3) = A_3$;
2. $A_2 =^{(12)} A_1$, $A_3(A_1,^{(12)} A_1, E_3) = A_3$ *and* $A_1(A_1,^{(13)} A_1, E_3) = E_2$;
3. $A_2 =^{\pi_2} A_1(A_1, E_2, E_3)$, $A_3 =^{\pi_1} A_1(E_1, A_1, E_3)$ *and*
$A_1(^{\pi_2} A_1(A_1, E_2, E_3), E_1, E_3) =^{\pi_1} A_1(E_1, A_1, E_3)$;
4. $A_1 =^{\pi_1} A_2(E_1, A_2, E_3)$, $A_3 =^{\pi_2} A_2(A_2, E_2, E_3)$ *and*
$A_2(E_2,^{\pi_1} A_2(E_1, A_2, E_3), E_3) =^{\pi_2} A_2(A_2, E_2, E_3)$.

Proof. Let the tuple (A_1, A_2, E_3) be a paratopy of the system Σ. As $E_1\theta = A_1, E_2\theta = A_2, E_3\theta = E_3$, we obtain $\Sigma\theta = \{A_1\theta, A_2\theta, A_3\theta, A_1, A_2, E_3\}$, i.e. $\{A_1\theta, A_2\theta, A_3\theta\} = \{E_1, E_2, A_3\}$.

1. If $A_1\theta = E_1, A_2\theta = E_2, A_3\theta = A_3$, then $\theta^2 = \varepsilon$. From $A_1\theta = E_1$ it follows

$$A_2 =^{\pi_2} A_1(A_1, E_1, E_3). \tag{10.1}$$

Using (10.1) in $A_3\theta = A_3$, we get

$$A_3(A_1,^{\pi_2} A_1(A_1, E_1, E_3), E_3) = A_3. \tag{10.2}$$

Conversely, if (10.1) and (10.2) hold, then from (10.1) it follows $A_1\theta = E_1$ and $A_2\theta =^{\pi_2} A_1(E_1, A_1, E_3)$, so $A_2\theta = E_2$. Using (10.1) in (10.2), we obtain $A_3\theta = A_3$.

2. If $A_1\theta = E_2, A_2\theta = E_1, A_3\theta = A_3$, then $\theta^2 = (E_2, E_1, E_3)$, $\theta^3 = (A_2, A_1, E_3)$, $\theta^4 = \varepsilon$. From $A_1\theta = E_2$ it follows $A_1\theta^2 = A_2$, so

$$A_2 =^{(12)} A_1. \tag{10.3}$$

Using (10.3) in $A_3\theta = A_3$, we get

$$A_3(A_1,^{(12)} A_1, E_3) = A_3. \tag{10.4}$$

The equality $A_1\theta = E_2$ and (10.3) imply

$$A_1(A_1,^{(12)} A_1, E_3) = E_2. \tag{10.5}$$

Conversely, if (10.3), (10.4) and (10.5) hold, then (10.3) and (10.5) imply

$$A_1(A_1, A_2, E_3) = E_2, \tag{10.6}$$

so $A_1\theta = E_2$. From (10.3) it follows

$$E_1 =^{\pi_2} A_1(E_2, A_2, E_3). \tag{10.7}$$

The equality (10.6) implies $A_2 =^{\pi_2} A_1(A_1, E_2, E_3)$, hence $A_2\theta =^{\pi_2} A_1(E_2, A_2, E_3)$. Using (10.7) in the last equality, we obtain $A_2\theta = E_1$. From (10.3) and (10.4) it follows $A_3\theta = A_3$.

3. If $A_1\theta = E_2, A_2\theta = A_3, A_3\theta = E_1$, then $\theta^2 = (E_2, A_3, E_3)$, $\theta^3 = (A_2, E_1, E_3)$, $\theta^4 = (A_3, A_1, E_3)$, $\theta^5 = \varepsilon$. From $A_1\theta = E_2$ it follows

$$A_2 =^{\pi_2} A_1(A_1, E_2, E_3). \tag{10.8}$$

Also $A_1\theta = E_2$ implies $A_1\theta^4 = E_1$, i. e. $A_1(A_3, A_1, E_3) = E_1$, so

$$A_3 =^{\pi_1} A_1(E_1, A_1, E_3). \tag{10.9}$$

In a similar way, $A_1\theta = E_2$ implies $A_1\theta^3 = A_3$, i. e. $A_1(A_2, E_1, E_3) = A_3$. Using (10.8) and (10.9) in the last equality, we get

$$A_1(^{\pi_2}A_1(A_1, E_2, E_3), E_1, E_3) =^{\pi_1} A_1(E_1, A_1, E_3). \tag{10.10}$$

Conversely, if (10.8), (10.9) and (10.10) hold, then (10.8) implies $A_1\theta = E_2$. From (10.9) it follows $A_3\theta =^{\pi_1} A_1(A_1, E_2, E_3)$, so $A_3\theta = E_1$. Using (10.8) and (10.9) in (10.10), we obtain $A_1(A_2, E_1, E_3) = A_3$, so $A_2 =^{\pi_1} A_1(A_3, E_1, E_3)$, which implies $A_2\theta =^{\pi_1} A_1(E_1, A_1, E_3)$. Using (10.9) in the last equality, we get $A_2\theta = A_3$.

4. If $A_1\theta = A_3, A_2\theta = E_1, A_3\theta = E_2$, then $\theta^2 = (A_3, E_1, E_3)$, $\theta^3 = (E_2, A_1, E_3)$, $\theta^4 = (A_2, A_3, E_3)$, $\theta^5 = \varepsilon$. From $A_2\theta = E_1$ it follows

$$A_1 =^{\pi_1} A_2(E_1, A_2, E_3). \tag{10.11}$$

Also $A_2\theta = E_1$ implies $A_2\theta^4 = E_2$, i.e. $A_2(A_2, A_3, E_3) = E_2$, so

$$A_3 =^{\pi_2} A_2(A_2, E_2, E_3). \tag{10.12}$$

Analogously, $A_2\theta = E_1$ implies $A_2\theta^3 = A_3$, i.e. $A_2(E_2, A_1, E_3) = A_3$. Using (10.11) and (10.12) in the last equality, we get

$$A_2(E_2, {}^{\pi_1} A_2(E_1, A_2, E_3), E_3) = {}^{\pi_2} A_2(A_2, E_2, E_3). \tag{10.13}$$

Conversely, if (10.11), (10.12) and (10.13) hold, then (10.11) implies $A_2\theta = E_1$. From (10.12) it follows $A_3\theta = {}^{\pi_2} A_2(E_1, A_2, E_3)$, so $A_3\theta = E_2$. Using (10.11) and (10.12) in (10.13), we obtain $A_2(E_2, A_1, E_3) = A_3$, so $A_1 = {}^{\pi_2} A_2(E_2, A_3, E_3)$, which implies $A_1\theta = {}^{\pi_2} A_2(A_2, E_2, E_3)$. Using (10.12) in the last equality, we get $A_1\theta = A_3$.

5. If $A_1\theta = E_1, A_2\theta = A_3, A_3\theta = E_2$, then $\theta^2 = (E_1, A_3, E_3)$. From $A_1\theta = E_1$ it follows $A_1\theta^2 = A_1$, i.e. $A_1(E_1, A_3, E_3) = A_1(E_1, E_2, E_3)$, so $A_3 = E_2$, which is a contradiction as A_3 is a quasigroup operation.

6. If $A_1\theta = A_3, A_2\theta = E_2, A_3\theta = E_1$, then $\theta^2 = (A_3, E_2, E_3)$. From $A_2\theta = E_2$ it follows $A_2\theta^2 = A_2$, i.e. $A_2(A_3, E_2, E_3) = A_2(E_1, E_2, E_3)$, so $A_3 = E_1$, which is a contradiction as A_3 is a quasigroup operation. □

Corollary 3. *If a ternary quasigroup (Q, A) satisfies the identity $A(A, {}^{(12)} A, E_3) = E_2$ then, for $\forall a \in Q$, its 3-retract $B(x, y) = A(x, y, a)$ is self-orthogonal.*

The proof is analogous to the proof of Corollary 1.

Theorem 2. *There exist 48 orthogonal systems consisting of three ternary quasigroups and ternary selectors E_1, E_2, E_3, that admit at least one paratopy, which components are three ternary quasigroup operations or a ternary selector and two ternary quasigroup operations.* The proof follows from Lemmas 1–10.

The work was partially supported by CSSDT ASM grant 15.817.02.26F.

References

[1] Belousov V. *Systems of orthogonal operations.* Mat. Sbornik, 1968. **77(119): I**, 33–52 (in Russian).

[2] Belousov V. *Parastrofic-orthogonal quasigroups.* Quasigroups and Related Systems, 2005, **14**, 3–51.

[3] Belousov V. *n-Ary quasigroups.* Chisinau, Shtiintsa, 1972 (in Russian).

[4] Belousov V., Yakubov T. *On orthogonal n-ary operations.* Vopr. Kibernetiki, 1975, **16**, 3–17 (in Russian).

[5] Evans T. *Latin cubes orthogonal to their transposes - a ternary analogue of Stein quasigroups.* Aequationes Math., 1973, **9**, 296–297.

[6] Syrbu P. *On orthogonal and self-orthogonal n-ary operations.* Mat. Issled., 1987, **66**, 121–129 (in Russian).

[7] Syrbu P. *On π-quasigroups isotopic to abelian groups.* Bul. Acad. Ştiinţe Repub. Mold., Mat., 2009, No. 3(61), 109–117.

[8] Syrbu P., Ceban D. *On π-quasigroups of type T_1.* Bul. Acad. Ştiinţe Repub. Mold. Mat., 2014, No. 2(75), 36–43.

[9] Ceban D., Syrbu P. *On the holomorph of π-quasigroups of type T_1.* Proceedings IMCS-50. The 3rd Conference of Math. Society of the Republic of Moldova. Chisinau, August 19–23, 2014, 34–37.

[10] Belyavskaya G. *Successively orthogonal systems of k-ary operations.* Quasigroups and Related Systems, 2014, **22**, 165–178.

P. Syrbu, D. Ceban
Department of Mathematics
Moldova State University
Mateevici str., 60, MD-2009, Chisinau
Moldova
E-mail: *syrbuviv@yahoo.com; cebandina@mail.ru*

Received January 20, 2016

BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 118–124
ISSN 1024–7696

On cosets in Steiner loops

Aleš Drápal, Terry S. Griggs

Abstract. We give a complete answer to the question of when the cosets of a Steiner subloop $\bar{W}$ of a Steiner loop $\bar{V}$ form a partition of $\bar{V}$. We also determine when $\bar{W}$ is a normal subloop of $\bar{V}$.

Mathematics subject classification: 05B07, 20N05.
Keywords and phrases: Steiner triple system, Steiner loop, coset, normal subloop.

1 Introduction

Let L be a loop and M be a subloop of L. For all $x \in L$, the set xM (resp. Mx) is a left (resp. right) coset of M. If $L = G$ is a group and $M = H$ is a subgroup then, as is very well known, the cosets form a partition of G, i.e. for $x, y \in G$, either $xH = yH$ (resp. $Hx = Hy$) or $xH \cap yH = \emptyset$ (resp. $Hx \cap Hy = \emptyset$). However the same is not true for loops in general and leads to the following definition (see I.2.10 of [8]).

Definition The loop L has a left (resp. right) coset decomposition modulo M if the set of all left (resp. right) cosets modulo M is a partition of L. We call this the *decomposition property*.

Properties of cosets in loops were studied in [6] where on page 180 the authors remark that "the article should be viewed as a point of departure for a more systematic study". In this paper we will be interested in Steiner loops, a variety of loops not studied in [6]. Again the decomposition property does not generally hold and the aim of this paper is to study those situations where it does. We are able to give a complete description of the structure of such Steiner loops and subloops including normality.

We recall the basic definitions and results which are appropriate for our purposes. A *Steiner triple system* of order v, STS(v), is a pair $(V, \mathcal{B})$ where V is a set of *points* of cardinality v and $\mathcal{B}$ is a set of triples of V, called *blocks*, such that every pair of distinct points is contained in precisely one block. Such systems exist if and only if $v \equiv 1$ or $3 \pmod 6$ [7], see also [2]. Given an STS(v), a *Steiner loop* is defined on the set $\bar{V} = V \cup \{e\}$ by the rules $ex = xe = x$, $xx = e$, for all $x \in \bar{V}$, $xy = z$ if $\{x, y, z\} \in \mathcal{B}$. We say that the Steiner loop is *associated* with the Steiner triple system. The process is reversible. Thus there is a one-one correspondence between all Steiner triple systems and all Steiner loops and the existence spectrum of the latter is $v + 1 \equiv 2$ or $4 \pmod 6$. Note that in this formulation, a Steiner loop of

order 2 is associated with the STS(1) having no blocks and a Steiner loop of order 4 is associated with the STS(3) having one block and containing all three points. The latter Steiner loop is isomorphic to the Klein group $\mathbb{K}_4$. Algebraically a Steiner loop can be characterized as a totally symmetric loop. The variety of such loops is described by the identities $xy = yx$ and $x \cdot yx = y$. In every such loop $xx = e$, where e is the identity element.

In addition we will need the concept of a 3-*group divisible design*, 3-GDD. This is an ordered triple $(V, \mathcal{G}, \mathcal{B})$ where V is a set of *points* of cardinality v, $\mathcal{G}$ is a partition of V into *groups* and $\mathcal{B}$ is a set of triples of V, called *blocks*, such that every pair of distinct points is contained in either precisely one group or one block, but not both. We will only be interested in 3-GDDs which are *uniform*, i.e. $v = gu$ and V is partitioned into u groups all of cardinality g. The 3-GDD is said to be of type g^u. Necessary and sufficient conditions for the existence of 3-GDDs of type g^u were determined in [4], see also [3].

First we observe that if $\bar{W}$ is a subloop of a Steiner loop $\bar{V}$, then it does not follow that the order of $\bar{W}$ divides the order of $\bar{V}$. For example there are 86 701 547 non-isomorphic STS(19)s containing a subsystem STS(7), equivalently Steiner loops of order 20 containing a subloop of order 8,[5]. An example of a situation where the order of the subloop does divide the order of the Steiner loop but the decomposition property does not hold is given by the STS(19) with base set $V = \{0, 1, \ldots, 18\}$ and block set $\mathcal{B}$ generated by the triples $\{0, 1, 8\}$, $\{0, 2, 5\}$, $\{0, 4, 13\}$, under the action of the mapping $i \mapsto i + 1 \pmod{19}$. A subloop of order 4 is $\bar{W} = \{e, 0, 1, 8\}$ and two cosets are $2\bar{W} = \{2, 5, 9, 12\}$ and $5\bar{W} = \{5, 2, 14, 3\}$.

In Section 2, given a Steiner loop $\bar{W}$ of order $w + 1$ we give an exhaustive construction of Steiner loops of order $v + 1$ for which $\bar{W}$ is a subloop with the decomposition property and in Section 3 we determine when $\bar{W}$ is normal. Finally in Section 4, we show that if all subloops of order 2 are normal or if all subloops of order 4 have the decomposition property then the Steiner loop is the elementary Abelian 2-group associated with a projective Steiner triple system.

2 Cosets

Let $S = (V, \mathcal{B})$ be an STS(v) and $\bar{V}$ be its associated Steiner loop. Further let $T = (W, \mathcal{C})$ with $W \subset V$ and $\mathcal{C} \subset \mathcal{B}$ be a proper subsystem STS(w) of S and $\bar{W}$ be its associated Steiner loop. Let $s = (v + 1)/(w + 1)$. We require s to be integral, called the *index* of $\bar{W}$ in $\bar{V}$. Since both $v + 1 \equiv 2$ or $4 \pmod 6$ and $w + 1 \equiv 2$ or $4 \pmod 6$ it follows that $s \equiv 1$ or $2 \pmod 3$. Further $2 \leq s \leq (v + 1)/2$. It will be more instructive to deal first with the two cases: (i) $s = 2$ and (ii) $s = (v + 1)/4$. This will then make it easier to describe the more general case (iii) $2 \leq s \leq (v+1)/4$. Finally we consider the case (iv) $s = (v + 1)/2$.

Case (i): $s = 2$.
Thus $v = 2w + 1$ and the structure of the STS(v) is given by the following well known doubling construction (see Lemma 8.1.2 of [1]). Let $W = \{x_1, x_2, \ldots, x_w\}$

and $V = W \cup \{y_1, y_2, \ldots, y_{w+1}\}$ where the x_i's and y_i's are distinct. Consider a one-factorization of the complete graph K_{w+1} on vertices $V \setminus W$ and let $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_w$ be the one factors. The STS(v) consists of the blocks of the STS(w) on the set W together with all of the blocks $x_i\mathcal{F}_i$, $1 \leq i \leq w$. In the Steiner loop $\bar{V}$, the subloop $\bar{W} = W \cup \{e\}$ and there is one further coset $V \setminus W$.

Case (ii): $s = (v+1)/4$.
Here $w = 3$ and the subloop $\bar{W} = \{e, a, b, c\}$ where the triple $\{a, b, c\} \in \mathcal{B}$. Choose $y \in V$. Then $y\bar{W} = \{y, p, q, r\}$ is a coset where the triples $\{a, y, p\}, \{b, y, q\}, \{c, y, r\} \in \mathcal{B}$. It then follows that $p\bar{W} = q\bar{W} = r\bar{W} = y\bar{W}$ which implies that further triples $\{a, q, r\}, \{b, p, r\}, \{c, p, q\} \in \mathcal{B}$, i.e. the points $\{a, b, c, y, p, q, r\}$ form an STS(7). The structure of the STS(v) is now clear. We must have that $v \equiv 3$ or $7 \pmod{12}$. Put $u = (v-3)/4$. Let $Y_0 = \{a, b, c\}$ and $Y_i = \{y_i, p_i, q_i, r_i\}$, $1 \leq i \leq u$. Then $V = \bigcup_{i=0}^{u} Y_i$. Triples $\{a, b, c\}$, $\{a_i, y_i, p_i\}, \{b_i, y_i, q_i\}, \{c_i, y_i, r_i\}, \{a_i, q_i, r_i\}, \{b_i, p_i, r_i\}, \{c_i, p_i, q_i\} \in \mathcal{B}$. The remaining blocks are the blocks of a 3-GDD of type 4^u on the set $V \setminus \{a, b, c\}$ where the sets Y_i, $1 \leq i \leq u$, form both the groups of the group divisible design and the cosets of the subloop $\bar{W}$. Such 3-GDDs always exist, see [3].

Case (iii): $2 \leq s \leq (v+1)/4$.
We are now able to describe this more general case with reference to the two cases considered above. Let $W = Y_0 = \{x_1, x_2, \ldots, x_w\}$ and $Y_i = \{y_{i,1}, y_{i,2}, \ldots, y_{i,w+1}\}, 1 \leq i \leq s-1$. Let $V = \bigcup_{i=0}^{s-1} Y_i$. For each i, $1 \leq i \leq s-1$, let $\mathcal{F}_{i,1}, \mathcal{F}_{i,2}, \ldots, \mathcal{F}_{i,w}$ be the one factors of a one-factorization of the complete graph K_{w+1} on vertex set Y_i. The blocks of the STS(v) are of three types: (i) the blocks of the STS(w), (ii) the triples $x_j\mathcal{F}_{i,j}$, $1 \leq i \leq s-1$, $1 \leq j \leq w$, (iii) the blocks of a 3-GDD of type $(w+1)^{s-1}$ on the set $\bigcup_{i=1}^{s-1} Y_i$ where the sets Y_i form the groups of the 3-GDD. Such 3-GDDs always exist, see [3]. The subloop $\bar{W} = W \cup \{e\}$ and the sets Y_i are the other cosets.

Case (iv): $s = (v+1)/2$.
This is the simplest case to describe. The subloop $\bar{W}$ is of order 2 and comprises the set $\{e, x\}$ for any $x \in V$. The other cosets are the pairs of points which occur in blocks of the STS(v) which contain the point x. Probably more conveniently, this case can also be regarded as a special case of the general Case (iii) where $w = 1$.

We can express all of the above by the following theorem.

Theorem 2.1. *Let $S = (V, \mathcal{B})$ be a Steiner triple system of order v and $T = (W, \mathcal{C})$ be a proper subsystem of order w. Then the Steiner loop $\bar{V}$ associated with S has a coset decomposition modulo $\bar{W}$, the Steiner loop associated with T, if and only if*
(i) $s = (v+1)/(w+1)$ is an integer, and
(ii) S contains $s-1$ subsystems $S_i = (V_i, \mathcal{B}_i)$, $1 \leq i \leq s-1$, of order $2w+1$ where $V_i \cap V_j = W$ and $\mathcal{B}_i \cap \mathcal{B}_j = \mathcal{C}$, $1 \leq i < j \leq s-1$.

The above theorem has an elegant algebraic formulation.

Corollary 2.2. *Let M be a subloop of a finite Steiner loop L. Then L has a coset decomposition modulo M if and only if L can be covered by subloops of order $2|M|$, any two of which intersect in M.*

3 Normality

We begin with a definition.

Definition Let L be a commutative loop and M be a subloop of L. Then M is *normal* if its cosets $xM = Mx$ form a partition of L and induce a factor loop.

This means that for any two cosets xM and yM there exists a coset zM such that for all $a \in xM$ and $b \in yM$, $ab \in zM$. The fact that this does not hold in general for a Steiner loop can be shown by the following easy example.

Example 3.1. Let S be the STS(9) with base set $V = \{0, 1, \ldots, 8\}$ and block set $\mathcal{B}$ consisting of the triples $\{0,1,2\}$, $\{3,4,5\}$, $\{6,7,8\}$, $\{0,3,6\}$, $\{1,4,7\}$, $\{2,5,8\}$, $\{0,4,8\}$, $\{1,5,6\}$, $\{2,3,7\}$, $\{0,5,7\}$, $\{1,3,8\}$, $\{2,4,6\}$. This gives the Steiner loop with the following Cayley table.

	e	0	1	2	3	4	5	6	7	8
e	e	0	1	2	3	4	5	6	7	8
0	0	e	2	1	6	8	7	3	5	4
1	1	2	e	0	8	7	6	5	4	3
2	2	1	0	e	7	6	8	4	3	5
3	3	6	8	7	e	5	4	0	2	1
4	4	8	7	6	5	e	3	2	1	0
5	5	7	6	8	4	3	e	1	0	2
6	6	3	5	4	0	2	1	e	8	7
7	7	5	4	3	2	1	0	8	e	6
8	8	4	3	5	1	0	2	7	6	e

Then $2(3\{e,0\}) \neq 7\{e,0\}$.

In order to determine which Steiner subloops are normal we return to the structure of the STS(v) as described in Case (iii). First note that if $x = e$, the equation $x(yM) = (xy)M$ is satisfied trivially. The other cosets are the sets Y_i, $1 \leq i \leq s-1$, which form the groups of a 3-GDD of type $(w+1)^{s-1}$. Thus normality is equivalent to the 3-GDD having the property that if Y_i and Y_j, $i \neq j$, are groups of the 3-GDD then all of the $(w+1)^2$ products xy, where $x \in Y_i$ and $y \in Y_j$ must lie in the same group. Thus the set of groups themselves define a Steiner triple system and so $s - 1 \equiv 1$ or 3 (mod 6). The construction of a 3-GDD which ensures normality is now clear and can be obtained by a standard design-theoretic technique. Let $Z = (Y, \mathcal{D})$ be an STS($s-1$). Now inflate each point $y \in Y$ by a factor $w+1$, i.e. replace each point by a set of $w+1$ points. Then replace each block $D \in \mathcal{D}$ by a

3-GDD of type $(w+1)^3$, equivalently a Latin square of side $w+1$, on the inflated points.

This is perhaps better illustrated by an example.

Example 3.2. Let $v = 31$ and $w = 3$, so $s = 8$.
Then $T = (W, \mathcal{C})$ is an STS(3). Let $W = \{a, b, c\}$ and $\mathcal{C} = \{abc\}$. Here and throughout the example, for simplicity, we will represent blocks by the concatenation of three points.
Further $S = (V, \mathcal{B})$ is an STS(31) and contains 7 subsystems $(V_i, \mathcal{B}_i)$, $1 \le i \le 7$, whose intersection is T. Let $V_i \backslash W = \{x_i, y_i, z_i, w_i\}$ and $\mathcal{B}_i = \{abc, ax_iy_i, az_iw_i, bx_iz_i, by_iw_i, cx_iw_i, cy_iz_i\}$.
To complete the STS(31) choose an STS(7) on base set $\{1, 2, 3, 4, 5, 6, 7\}$ with block set say $\{123, 145, 167, 246, 257, 347, 356\}$ and a Latin square on set {x,y,z,w}, say

	x	y	z	w
x	x	y	z	w
y	w	x	y	z
z	z	w	x	y
w	y	z	w	x

Now for each block of the STS(7) proceed as follows. We will illustrate using the block 246. Choose one element, say 2, to be the row, a second element, say 4, to be the column and the third element, say 6, to be the entry and assign these to the Latin square to obtain further triples of the STS(31), i.e. $x_2x_4x_6$, $x_2y_4y_6$, $x_2z_4z_6$, $x_2w_4w_6$, $y_2x_4w_6$, $y_2y_4x_6$, $y_2z_4y_6$, $y_2w_4z_6$, $z_2x_4z_6$, $z_2y_4w_6$, $z_2z_4x_6$, $z_2w_4y_6$, $w_2x_4y_6$, $w_2y_4z_6$, $w_2z_4w_6$, $w_2w_4x_6$.
Note that it is permissible to use different Latin squares for each triple but this just complicates the process.

Again we can express all of the above by a theorem.

Theorem 3.3. *Let $S = (V, \mathcal{B})$ be a Steiner triple system of order v and $T = (W, \mathcal{C})$ be a subsystem of order w. Then the Steiner loop $\bar{W}$ associated with T is normal in $\bar{V}$, the Steiner loop associated with S, if and only if*
(i) $s = (v+1)/(w+1) \equiv 2$ or $4 \pmod 6$,
(ii) S contains $s-1$ subsystems $S_i = (V_i, \mathcal{B}_i)$, $1 \le i \le s-1$, of order $2w+1$ where $V_i \cap V_j = W$ and $\mathcal{B}_i \cap \mathcal{B}_j = \mathcal{C}$, $1 \le i < j \le s-1$, and
(iii) for each $i, j : 1 \le i < j \le s-1$, there exists $k : 1 \le k \le s-1$ such that for all blocks $\{x, y, z\} \in \mathcal{B}$ if $x \in V_i \setminus W$ and $y \in V_j \setminus W$ then $z \in V_k \setminus W$.

Finally in this section, it may be worth noting that normality depends critically on the value of s, the index of the subloop $\bar{W}$ in the Steiner loop $\bar{V}$. We have already observed that $s \equiv 1$ or $2 \pmod 3$. Comparing the statements of Theorem 2.1 and Theorem 3.3 it follows that if $s \equiv 1$ or $5 \pmod 6$, then the subloop $\bar{W}$ cannot be normal. If $s = 2$, condition (iii) in Theorem 3.3 does not apply and so the subloop $\bar{W}$ is always normal. We have the situation described in Case (i) of

Section 2. If $s = 4$, condition (iii) in Theorem 3.3 is automatically satisfied and so in this case too, the subloop $\bar{W}$ must be normal. For other values of $s \equiv 2$ or $4 \pmod 6$, both situations can occur; the subloop $\bar{W}$ is normal depending on whether or not condition (iii) holds. Nevertheless, as indicated, we can always construct a Steiner system $S = (V, \mathcal{B})$ so that condition (iii) is satisfied and thus the subloop $\bar{W}$ is normal.

4 Small subloops

In this section we will be interested in Steiner subloops of order 2 or 4, i.e. subloops which contain respectively either a single point or three points of a block of the associated Steiner triple system. First consider subloops of order 2. It is immediate from Theorem 2.1 that in every Steiner loop, every subloop of order 2 has the decomposition property. But the subloops need not be normal as was shown in Example 3.1. This naturally raises the question of when all the subloops of order 2 of a Steiner loop are normal. The answer is easy. A normal subloop of order 2 is always central. Thus the Steiner loop must be the elementary Abelian 2-group of order 2^n associated with the projective $\mathrm{STS}(2^n - 1) = \mathrm{PG}(n-1, 2)$, $n \geq 2$. This result can also be proved combinatorially and this we now do since it will be relevant to when we consider subloops of order 4.

Let $S = (V, \mathcal{B})$ be an $\mathrm{STS}(v)$ where $v \equiv 3$ or $7 \pmod{12}$. Choose $x \in V$ so $\{e, x\}$ is a Steiner subloop of order 2. Let $w = (v-1)/2$, then $w \equiv 1$ or $3 \pmod 6$. The cosets are the pairs $Y_1 = \{y_1, z_1\}, Y_2 = \{y_2, z_2\}, \ldots, Y_w = \{y_w, z_w\}$ where $\{x, y_i, z_i\} \in \mathcal{B}$, $i = 1, 2, \ldots, w$. If $\{e, x\}$ is normal then the system S is completed by choosing an $\mathrm{STS}(w)$ on base set $\{Y_1, Y_2, \ldots, Y_w\}$ and replacing each block $\{Y_i, Y_j, Y_k\}$ by the triples $\{y_i, y_j, y_k\}, \{y_i, z_j, z_k\}, \{z_i, y_j, z_k\}, \{z_i, z_j, y_k\}$. These four triples on six points are known as a *quadrilateral* or *Pasch configuration*. There are $w(w-1)/6 = (v-1)(v-3)/24$ blocks in the $\mathrm{STS}(w)$ and thus also the same number of Pasch configurations. So in total, by considering all v points there will be $v(v-1)(v-3)/24$ Pasch configurations in S. This is the maximum number possible and only occurs in the projective systems [9].

Turning now to subloops of order 4, observe that any such subloop which has the decomposition property, tightly controls the structure of the associated Steiner triple system S. From Theorem 2.1, S must contain $(v-3)/4$ subsystems of order 7, all of which intersect in the block associated with the subloop. From [5], of the 86 701 547 non-isomorphic STS(19)s containing a subsystem STS(7), a mere 2 557 contain 4 or more subsystems of order 7. So the vast majority of Steiner loops obtained from these systems will not contain a subloop of order 4 with the decomposition property.

Example 4.1. Consider the STS(9) in Example 3.1. Let $V' = \{x' : x \in V\}$. Construct an STS(19) on base set $V \cup V' \cup \{\infty\}$ as follows. For each block $\{x, y, z\}$ which is a block of the STS(9), let triples $\{x, y, z\}$, $\{x, y', z'\}$, $\{x', y, z'\}$, $\{x', y', z\}$ be blocks of the STS(19). Complete the system with blocks $\{\infty, x, x'\}$ for each $x \in V$.

On the other hand, consider the STS(19) constructed in the above example. It

contains 12 STS(7)s. Each of the blocks $\{\infty, x, x'\}, x \in V$, is contained in 4 of these STS(7)s and the subloops $\{e, \infty, x, x'\}, x \in V$, have the decomposition property. All other blocks are contained in just a single STS(7). Thus we might ask whether there exist Steiner loops, all of whose subloops of order 4 have the decomposition property. Again the answer is easy and can be proved both algebraically and combinatorially. Choose $x, y, z \in \bar{V}$. If $e \in \{x, y, z\}$ or $\{x, y, z\} \in \mathcal{B}$, then $x(yz) = (xy)z$ trivially. Otherwise $\bar{W} = \{x, y, xy, e\}$ is a subloop of order 4 and $\bar{W} \cup z\bar{W}$ is a subloop of order 8. This latter subloop is associative and so is a group, i.e. induced by a projective Steiner triple system. Combinatorially we can argue as follows. Consider any block of the associated Steiner triple system. It must be contained in $(v-3)/4$ STS(7)s. Since there are $v(v-1)/6$ blocks this gives $v(v-1)(v-3)/(24\times 7)$ different STS(7)s. Finally each STS(7) contains 7 Pasch configurations so there are $v(v-1)(v-3)/24$ of these again the maximum possible and the Steiner loops are the elementary Abelian groups associated with the projective Steiner triple systems.

References

[1] I. Anderson, Combinatorial Designs: Construction Methods, Ellis Horwood, New York, 1990.

[2] C. J. Colbourn and A. Rosa, Triple Systems, Oxford University Press, Oxford, 1999.

[3] G. Ge, Group divisible designs, Handbook of Combinatorial Designs, second edition (ed. C. J. Colbourn and J. H. Dinitz), Chapman and Hall/CRC Press, 255–260, 2007.

[4] H. Hanani, Balanced incomplete block designs and related designs, *Discrete Math.* **11** (1975), 255–369.

[5] P. Kaski, P. R. J. Östergård, S. Topolova and R. Zlatarski, Steiner triple systems of order 19 and 21 with subsystems of order 7, *Discrete Math.* **308** (2008), 2732–2741.

[6] M. Kinyon, K. Pula and P. Vojtěchovský, Incidence properties of cosets in loops, *J. Combin. Designs* **20** (2012), 179–197.

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

[8] H. O. Pflugfelder, Quasigroups and Loops: Introduction, Heldermann Verlag, Berlin, 1990.

[9] D. R. Stinson and Y. J. Wei, Some results on quadrilaterals in Steiner triple systems, *Discrete Math.* **105** (1992), 207–219.

Aleš Drápal
Department of Algebra
Charles University
Sokolovská 83
186 75 Praha 8, CZECH REPUBLIC
E-mail: *drapal@karlin.mff.cuni.cz*

Terry S. Griggs
Department of Mathematics and Statistics
The Open University
Walton Hall
Milton Keynes MK7 6AA, UNITED KINGDOM
E-mail: *t.s.griggs@open.ac.uk*

Received February 2, 2016