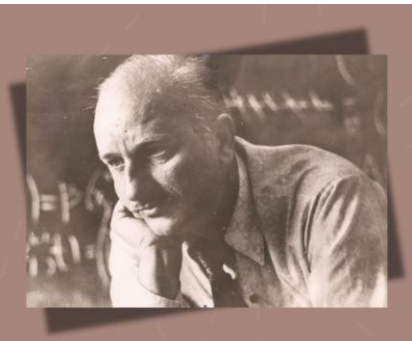


MATHEMATICAL WEEK IN CHISINAU, DEDICATED TO THE CENTENARY OF VALENTIN BELOUSOV (1925-1988)

Book of Abstracts

Conference **Quasigroups and Related Systems** (ConfQRS-2025)

Moldova State University, Chisinau, July 2-4, 2025

ORGANISERS

Vladimir Andrunachievici Institute of Mathematics and Computer Science,
Faculty of Mathematics and Computer Science of Moldova State University

SPONSORS

INTERNATIONAL MATHEMATICAL UNION CDC

PREMIER ENERGY

ALLIED TESTING

ISBN 978-9975-62-880-8

Moldova State University

Vladimir Andrunachievici Institute of Mathematics and Computer Science,
Faculty of Mathematics and Computer Science

Book of Abstracts

Conference **Quasigroups and Related Systems** (ConfQRS-2025)

Moldova State University, Chisinau, July 2-4, 2025

Chișinău, 2025

512.548(082)
Q 31

ISBN 978-9975-62-880-8

Conference Quasigroups and Related Systems

(ConfQRS-2025)

Mathematical Week in Chișinău dedicated to the centenary of Valentin Belousov (1925-1988)

Organizers: *Vladimir Andrunachievici Institute of Mathematics and Computer Science, Faculty of Mathematics and Computer Science, Moldova State University*

Program committee

Jonathan D. H. SMITH (USA), Aleš DRÁPAL (Czech Rep.), J. D. PHILLIPS (USA), David STANOVSKY (Czech Rep.), Petr VOJTECHOVSKY (USA), Wieslaw DUDEK (Poland), Fedir SOKHATSKY (Ukraine), Tomas KEPKA (Czech Rep.), Gary MULLEN (USA), Alexander GRISHKOV (Brazil), Aleco GVARAMIYA (Georgia), Piroska CSÖRGŐ (Hungary), Ian WANLESS (Australia), Victor SHCHERBACOV (Moldova), Vladimir IZBASH (Moldova), Parascovia SYRBU (Moldova), Liubomir CHIRIAC (Moldova)

Local Organizing committee

Vladimir Izbash, Parascovia Syrbu, Victor Shcherbacov, Florin Damian, Liubomir Chiriac, Eugene Kuznetsov, Tatiana Rotari, Elena Cuznețov, Nadezhda Malyutina

Edited by: P. Syrbu, E. Kuznetsov

DESCRIEREA CIP A CAMEREI NAŢIONALE A CĂRŢII DIN REPUBLICA MOLDOVA

Conference "Quasigroups and Related Systems" : (ConfQRS-2025) : Mathematical Week in Chișinău dedicated to the centenary of Valentin Belousov (1925-1988) : Book of Abstracts, Chisinau, July 2-4, 2025 / edited by: P. Syrbu, E. Kuznetsov – Chișinău : Editura USM, 2025. – 59 p.
Antetit.: Moldova State University, Vladimir Andrunachievici Institute of Mathematics and Computer Science, Faculty of Mathematics and Computer Science. – Referinţe bibliogr. la sfârşitul art. – Index: p. 57. – [50] ex.

ISBN 978-9975-62-880-8.

512.548(082)
Q 31

Printing of this book is supported by the Institutional Research Program of the Moldova State University for 2024 − 2027 years, subprogram 011303 "SATGED"

© **Editura USM, 2025**

SOME HASH FUNCTIONS BASED ON QUASIGROUPS

Cernov Vladimir, Shcherbacov Victor, Malyutina Nadegda *

Vladimir Andrunachievici Institute of Mathematics and Computer Sciernce, Moldova State University, Chisinau, Republic of Moldova

volodya.black@gmail.com, vscerb@gmail.com, 231003.bab.nadezhda@mail.ru

Hashing plays a key role in modern information technologies, providing efficient storage, retrieval and integrity checking of data. Traditional hashing methods such as MD5, SHA-1 and their variants, although widely used, face limitations in the case of large data volumes and increased security requirements.

In recent years, there has been increased interest in alternative hashing methods based on abstract algebraic structures. Quasigroups and groupoids are important representatives of these structures with unique properties for hashing applications.

Definition 1. A function H() that maps an arbitrary length message M to a fixed length hash value H(M) is a OneWay Hash Function (OWHF), if it satisfies the following propertities:

1.The description of H() is publicly known and should not require any secret information for its operation.

2.Given M, it is easy to compute H(M).

3. Given H(M) in the rang of H(), it is hard to find a message M for given H(M), and given M and H(M), it is hard to find a message $M_0(\neq M)$ *such that* $H(M_0) = H(M)$.[1,2].

We give construction of hashing function based on quasigroup.

Definition 2. *Let* $H_Q() : Q \to Q$ *be projection defined as:*

$$H_Q(q_1q_2...q_n) = ((...(a \star q_1) \star q_2 \star ...) \star q_n$$

Then $H_Q()$ *is said to be hash function over quasigroup* $(Q;\star)$*. The element a is a fixed element from Q.* [1,2]

An algorithm for constructing quasigroups of order n used in the hashing process has been developed. The set of these quasigroups is written to a separate file, which will be the key during hashing. To obtain the final hash value, a chain hashing method was applied, where intermediate hash values are concatenated. This method ensures the uniqueness of the result and its collision resistance.

* *Speaking author* : Cernov V.

A hash function "hash_function"was developed based on a given quasigroup and parameter k. The constructed structure demonstrates the possibility of using this method to create hash values. At the stage of software application implementation, the "docx_to_num"function was implemented to convert text documents into a sequence of bits, which will be presented as an initial message.

The proposed hashing method demonstrates the possibility of effective use in applications requiring fast and reliable data matching and integrity checking.

References:

1. J. Dvorsky, E. Ochodkova, and V. Snasel. *Hash functions based on large quasigroups.* Velokonocni kryptologie, pages 1вЂ“8, 2002.
2. J. Dvorsky, E. Ochodkova, and V. Snasel. *Hashovaci funkce zalozena na kvazigrupach.* In Workshop Milkulasska kryptobesidka, Praha, 2000 (in Czech).

ON TOPOLOGICAL QUASIGROUPS OBEYING CERTAIN LAWS

Liubomir Chiriac , Natalia Bobeica , Natalia Lupashco , Artiom Pirlog
Pedagogical State University of Chisinau
llchiriac@gmail.com, nbobeica1978@gmail.com, nlupashco@gmail.com, pirlog.artiom.andrei@gmail.com

A non-empty set G is said to be a *groupoid* with respect to a binary operation denoted by $\{\cdot\}$, if for every ordered pair (a, b) of elements of G there is a unique element $ab \in G$.

A quasigroup is a binary algebraic structure in which one-sided multiplication is a bijection in that all equations of the form $ax = b$ and $ya = b$ have unique solutions [1].

A groupoid G is called a primitive groupoid with divisions, if there exist two binary operation $l : G \times G \to G$, $r : G \times G \to G$ such that $l(a, b) \cdot a = b, a \cdot r(a, b) = b$ for all $a, b \in G$. Thus a primitive groupoid with divisions is a universal algebra with three binary operations.

A primitive groupoid G with divisions is called a quasigroup if the equations $ax = b$ and $ya = b$ have unique solutions. In a quasigroup G the divisions l, r are unique. If the multiplication operation in a quasigroup $(G, \cdot)$ with a topology is continuous, then G is called a semitopoligical quasigroup. If in a semitopological quasigroup G the divisions l and r are continuous, then G is called a topological quasigroup.

A groupoid $(G, \cdot)$ is called *medial* if it satisfies the law $xy \cdot zt = xz \cdot yt$ for all $x, y, z, t \in G$. A groupoid $(G, \cdot)$ is called *paramedial* if it satisfies the law $xy \cdot zt = ty \cdot zx$ for all $x, y, z, t \in G$.

A groupoid $(G, \cdot)$ is called *bicommutative* if it satisfies the law $xy \cdot zt = tz \cdot yx$ for all $x, y, z, t \in G$.

A groupoid $(G, \cdot)$ is said to be *subtractive*, if the following conditions holds: $b \cdot (ba) = a$ and $a \cdot bc = c \cdot ba$ for all $x, y, z, t \in G$.

A groupoid $(G, \cdot)$ is called *AD-groupoid* if it satisfies the law $a \cdot bc = c \cdot ba$ for all $a, b, c \in G$.

A groupoid $(G, \cdot)$ is called a *groupoid Abel-Grassmann* or *AG-groupoid* if it satisfies the left invertive law $(ab) \cdot c = (cb) \cdot a$ for all $a, b, c \in G$.

While if an *AG-groupoid* $(G, \cdot)$ satisfying the identity $a \cdot (b \cdot c) = b \cdot (a \cdot c)$ for all $a, b, c \in G$ is called *AG^{**}-groupoid.*

We define a *Ward groupoid* as any groupoid $(G, \cdot)$ containing an element $e \in G$ such that $a^2 = a \cdot a = e$ and $(ab) \cdot c = a \cdot (c \cdot (e \cdot b))$, for all $a, b, c \in G$. A groupoid $(G, \cdot)$ is called a *Schröder Second Law groupoid* if it satisfies the law $(ab) \cdot (ba) = a$ for all $a, b \in G$ [6]. The identity $(ab) \cdot (ba) = b$ for all $a, b \in G$ is known as *Stein's Third Law* [6]. The concept of (n, m)-identities was introduced by M.M. Choban and L.L. Chiriac in [2].

Main Results

We study the problems formulated below.

Problem 1. Let G be an $AD-groupoid$. Under which conditions G with a locally compact Hausdorff topology can be "transformed"into a topological quasigroup?

Robert Ellis, in 1957, proved that a group with a locally compact Hausdorff topology making all translations continuous also has jointly continuous multiplication and continuous inversion, and is thus a topological group.

We examine a similar problem for quasigroup structure. We extend the theorem of R.Ellis to the case of AD- groupoids, which satisfies certain conditions.

The mappings $r_a : G \to G$, $(x \to xa)$ and $l_a : G \to G$, $(x \to ax)$ are called respectively the right and left translation by a.

Theorem 1. *Let τ be a locally compact Hausdorff topology defined on an $AD-$ groupoid $(G, \cdot)$, $e \in G$, and the following conditions hold:*

1. $xe = x$ for every $x \in G$,

2. $x^2 = x \cdot x = e$ for every $x \in G$,

3. if $xa = ya$ then $x = y$ for all $x, y, a \in G$.

Then $(G, \cdot, \tau)$ is a topological Ward, subtractive and AD-quasigroup with a $(2, 1)$-identity e if and only if r_a is open and continuous for each $a \in G$.

Quasigroup $(G, \cdot)$ is a $T-quasigroup$ if and only if there exist an abelian group $(G, +)$, its automorphisms φ and ψ, and a fixed element $a \in G$ such that $x \cdot y = \varphi(x) + \psi(y) + a$ for all $x, y \in G$.

Problem 2. Let Q be a $T-$*quasigroup*. Under which conditions the Q is a quasigroup (of its T - forms $(Q(+),\varphi,\psi,a)$ satisfying the identities P_i, where $i=1,2,...,k$?

Theorem 2. *Let G be a $T-$quasigroup. Then G is $AG-$quasigroup if and only if any for of its $T-$forms $(Q(+),\varphi,\psi)$ is $\varphi^2(x)=\psi(x)$.*

Problem 3. Under which conditions the binary topological groupoid with the algebraic properties $P_1,P_2,...,P_k$ can be "transformed"into a topological quasigroup with the algebraic properties $P_1,P_2,...,P_k$?

Theorem 3. *If $(G,\cdot)$ is an AG and AD-multiplicative topological groupoids and the following conditions hold:*

1. $x^2=x\cdot x=x$ for every $x\in G$,

2. $(xy)\cdot(yx)=x$ for all $x,y\in G$.

3. if $xa=ya$ then $x=y$ for all $x,y,a\in G$,

then $(G,\cdot)$ is a Schröder, medial, AG and AD-topological quasigroups.

Theorem 4. *If $(G,\cdot)$ is an AD-multiplicative topological groupoids and the following conditions hold:*

1. $x^2=x\cdot x=x$ for every $x\in G$,

2. $(xy)\cdot(yx)=y$ for all $x,y\in G$.

3. if $xa=ya$ then $x=y$ for all $x,y,a\in G$,

then $(G,\cdot)$ is a Stein and AD-topological quasigroups.

Theorem 5. *Let $(G,\cdot)$ be a topological AG^{**}-quasigroup with an $(1,2)$-identity e and $x^2=e$ for every $x\in G$. If P is an open compact neighborhood such that $e\in P$, then P contains an open compact AG^{**}-subquasigroup $(Q,\cdot)$ with an $(1,2)$-identity of $(G,\cdot)$.*

In the context of topological groups an analogous result appears in the work of Pontrjagin ([7], Theorem 16).

We give a new method of constructing non-associative topological quasigroups obeying certain laws.

The results established here are related to the work in ([3,4,5]).

Theorem 6. *Let $(G,+,\tau)$ be a commutative topological group where G is not a singleton. For (x_1,y_1) and (x_2,y_2) in $G\times G$ define*

$$(x_1,y_1)\circ(x_2,y_2)=(x_1+y_1-x_2,x_2+y_2-y_1).$$

Then $(G\times G,\circ,\tau_G)$, relative to the product topology τ_G, is a paramedial, non-medial and non-associative topological quasigroup. Moreover, if (G,τ) is T_i-space, then $(G\times G,\tau_G)$ is T_i-space too, where $i=1,2,3,3.5$.

Theorem 7. *Let $(G,+,\tau)$ be a commutative topological group where G is not a singleton. For (x_1,y_1) and (x_2,y_2) in $G\times G$ define*

$$(x_1,y_1)\circ(x_2,y_2)=(-x_1-x_2,y_1+y_2)$$

Then $(G\times G, \circ, \tau_G)$, relative to the product topology τ_G, is a medial, semimedial, paramedial, bicommutative, Manin, Cote and GA non-associative topological quasigroup. Moreover, if (G, τ) is $T_i - space$, then $(G \times G, \tau_G)$ is $T_i - space$ too, where $i = 1, 2, 3, 3.5$.

References

1. V. D. Belousov Foundations of the theory of quasigroups and loops, Moscow, Nauka, 1967, 223 pp.
2. M. M. Choban, L. L. Kiriyak, *The topological quasigroups with multiple identities*. Quasigroups and Related Systems, **9**, (2002), p.19-31.
3. Natalia Bobeica, Liubomir Chiriac, *On Topological AG-groupoids and Paramedial Quasigroups with Multiple Identities*, ROMAI Journal 6, 1(2010), p. 1-14.
4. L. L. Chiriac, L. Chiriac Jr, N. Bobeica, *On topological groupoids and multiple identities*, Buletinul Academiei de Ştiinţe a RM, Matematica, 1(59), 2009, p.67-78.
5. Liubomir Chiriac, Natalia Bobeica, *On topological quasigroups and multiple identities*, Topology and its Applications, Volume 340, 1 December 2023, 108759, https://doi.org/10.1016/j.topol.2023.108759
6. A. Sade, *Quasigroupes obeissant a certaines lois*. Rev. Fas. Sci. Univ. Istambul, 22, 1957, 151-184.
7. L. S. Pontrjagin, *Neprerivnie gruppi*, Moskow, Nauka, 1984.

CHARACTERIZATION OF QUANDLES WITH TRIVIAL COLORING INVARIANT

Chwiedziuk Ondrej

Charles University, Prague, Czechia

ondra@chwiedziuk.cz

The problem of *knot recognition*, where we aim to decide whether two given knots are equivalent, is one of the central questions in knot theory. Among the many invariants developed to study knots, *coloring invariants using quandles* form one notable approach.

A **quandle** is an algebraic structure Q with a binary operation $*$, satisfying the following axioms for all $a, b, c \in Q$:

- $a * a = a$,
- for every $a, b \in Q$, there exists a unique $x \in Q$ such that $a * x = b$,
- $a * (b * c) = (a * b) * (a * c)$.

These axioms mirror the behavior of knot diagrams under *Reidemeister moves*, the local transformations that describe when two diagrams represent the same knot. Each knot can be represented by a two-dimensional diagram with crossing information preserved. Reidemeister moves describe how we can deform such diagrams without changing the knot itself.

To each knot K, we assign a *fundamental quandle* $Q(K)$, which is a quandle generated freely by the arcs of the diagram, subject to relations determined by the crossings. The fundamental quandle is a *complete invariant*: two knots have isomorphic fundamental quandles if and only if they are equivalent (see [1]). However, fundamental quandles are difficult to compute directly. To make this more tractable, we consider *colorings*: homomorphisms from $Q(K)$ to a fixed finite quandle Q. The number of such colorings is denoted by $\mathrm{Col}_Q(K)$.

Some colorings, however, carry no meaningful informationвЂ”for instance, *trivial colorings*, where all arcs are mapped to the same element of Q. In the following theorem, we characterize the finite quandles that admit only trivial colorings for every knot:

Theorem 1. *Let Q be a finite quandle. The following are equivalent:*

1. *For all knots K, we have $Col_Q(K) = |Q|$,*
2. *Q is reductive,*
3. *$Col_Q(K)$ is a Vassiliev invariant.*

Before explaining the proof, we define *reductive* quandles. A quandle Q is called reductive if every connected subquandle of Q has size 1. A quandle is *connected* if the group of inner automorphisms, generated by left translations, acts transitively on Q. Fundamental quandles are connected, and this property is preserved under quandle homomorphisms [1].

To prove the equivalence of (1) and (2), we showed that for every finite connected quandle Q of size greater than 1, there exists a knot K such that $\mathrm{Col}_Q(K) > |Q|$. This construction adapts ideas from the group-theoretic setting discussed in [2]. We then applied the characterization of reductive quandles from [3], which completes the equivalence (1) $\Leftrightarrow$ (2).

For the implication (2) $\Leftrightarrow$ (3), we followed the argument in [4]. A key lemma states that if a Vassiliev invariant is bounded in terms of the braid index, then it must be constant on all knots. Since $\mathrm{Col}_Q(K)$ is constant if and only if all colorings are trivial, we conclude that $\mathrm{Col}_Q(K)$ is a Vassiliev invariant if and only if Q is reductive.

The results presented in this abstract are part of author's bachelor's thesis [5], where the full proofs, additional examples, and broader context of the problem are provided. A preprint is currently being prepared.

References:

1. JOYCE, D. A classifying invariant of knots, the knot quandle. *Journal of Pure and Applied Algebra*, **23** (1982), 37–65.
2. JOHNSON, D. Homomorphs of knot groups. *Proceedings of the American Mathematical Society,*, **78** (1980), 135–138.
3. BONATTO, M., CRANS, A., NASYBULLOV, T. a WHITNEY, G. Quandles with orbit series conditions. *Journal of Algebra*, **567** (2021), 284–309.
4. EISERMANN, M. The number of knot group representations is not a vassiliev invariant. *Proceedings of the American Mathematical Society,* **128** (2000), 1555–1561.
5. CHWIEDZIUK, O. *Coloring invariants of knots*, Bachelor's thesis, Charles University, Prague, 2024.

ON RECURSIVE DIFFERENTIABILITY OF QUASIGROUPS PROLONGATIONS

Cuznetov Elena, Syrbu Parascovia *

Moldova State University, Chisinau, Republic of Moldova

lenkacuznetova95@gmail.com, parascovia.syrbu@gmail.com

The recursive derivative of order k of a quasigroup $(Q, \cdot)$, denoted by $(\overset{k}{\cdot})$, where k is a natural number, is defined as follows:

$$x \overset{0}{\cdot} y = x \cdot y, \;\; x \overset{1}{\cdot} y = y \cdot (x \cdot y),$$

$$x \overset{k}{\cdot} y = (x \overset{\cdots}{\overset{k-2}{\cdot}} y) \cdot (x \overset{k-1}{\cdot} y),$$

for all $k \geq 2$. A quasigroup $(Q, \cdot)$ is called recursively r -differentiable if its recursive derivatives $(\overset{k}{\cdot})$ are quasigroup operations, for all $k = 1, \ldots, r$.

It is known that there exist recursively 1-differentiable binary quasigroups of any order $q \neq 2, 6$ and possibly $q \neq 14, 18, 26$ [4,6]. Also, it is known that the maximum order of recursive differentiability of a binary quasigroup of order q does not exeed $q - 2$ [5].

A prolongation of a finite quasigroup is a process of extending the quasigroup by adding one or more new elements and redefining the operation to create a new quasigroup of a larger order. The notion of prolongation was introduced by Belousov in 1967, although the construction of quasigroups prolongations was first studied by Bruck in 1944, who considered finite idempotent quasigroups for this purpose [1-3]. Later, some other methods of quasigroups prolongations have been proposed.

Belousov's method of prolongation is based on complete mappings: a complete mapping of a quasigroup $(Q, \cdot)$ is a bijection $x \to \theta(x)$ of Q upon Q, such that the mapping θ_1, where $x \cdot \theta(x) = \theta_1(x)$, is a bijection as well. The

* *Speaking author*: Cuznetov E.

characterization of all quasigroups, in particular groups, which possess a complete mapping remains at present an open question [3]. In finite case, the complete mappings of quasigroups define transversals of the corresponding Cayley tables. A transversal of a latin square of order q is a set of q cells, taken by one from each row and each column, such that the elements in these cells are pairwise different.

The recursive differentiability of quasigroups is studied in the present work. We consider methods of prolongation of recursively differentiable quasigroups that keep this property. Necessary and sufficient conditions when a prolongation of a recursively differentiable quasigroup is recursively differentiable are given, including for well known prolongation methods by Bruck and Belousov.

A new method of quasigroups prolongation is proposed, using two transversals that intersect in exactly one cell. The total number of such prolongations and their recursive differentiability is studied for quasigroups of small order. Regarding the proposed method of prolongation it is shown that:
1. The total number of latin squares of order 5, having 2 transversals which intersect exactly in one cell, one of which is on the main diagonal, with a fixed order of elements, is 240;
2. There does not exist recursively 1-differentiable prolongations of quasigroups of order 5, obtained using the main diagonal with the fixed order $\{2,3,4,5,1\}$ or $\{1,2,3,4,5\}$, and an arbitrary second transversal which intersect the main diagonal exactly in one cell.

Acknowledgments. The Institutional Research Program of the Moldova State University for 2024 – 2027 years, subprograms 011302 "MANSDP"and 011303 "SATGET has supported part of the research for this paper.

References:

1. V. Belousov. *Foundations of the Theory of Quasigroups and Loops (Russian)*. Nauka, Moscow, 1967.
2. R. H. Bruck. Some results in the theory of quasigroups. *Trans. Amer. Math. Soc.*, **55** (1944), 19–52.
3. A. D. Keedwell, J. Denes. *Latin Squares and their Applications. 2nd Edition.*. Elsevier Science, 2015.
4. V. Markov, A. Nechaev, S. Skazhenik, E. Tveritinov. Pseudogeometries with clusters and an example of a recursive $[4,2,3]_{42}$ - code. *J. Math. Sci.*, **163(5)** (2009), 563–571.
5. P. Syrbu. On the order of recursive differentiability of finite binary quasigroups. *Bul. Acad. Ştiinţe Repub. Mold.*, **3(103)** (2023), 103–106.
6. P. Syrbu, E. Cuzneţov. On recursively differentiable k - quasigroups. *Bul. Acad. Ştiinţe Repub. Mold.*, **2(99)** (2022), 68–75.

AN ALTERNATIVE APPROACH TO FINITE SIMPLE MOUFANG LOOPS

Drapal Ales

Charles University, Prague, Czech Republic

drapal@karlin.mff.cuni.cz

Finite simple Moufang loops were classified by Liebeck, using earlier results of Doro. The proof relies on classification of finite simple groups and on the concept of groups with triality. Functorial connections between Moufang loops and groups with triality have been influential ever since, culminating in the monograph of Jonothan Hall.

These connections are certainly important and deep. Nevertheless, it seems that it is possible to get many important results by much simpler means, avoiding the formalism of groups with triality. I will report several fresh results in this category.

In these results the triality concept is present only in the rudimentary form of the outer automorphisms of $G = \mathrm{Mlt}(Q)$, Q a simple finite Moufang loop. I will explain how to prove that G has to be simple and has to possess a split group D of outer automorphisms isomorphic to S_3, and how to construct from such a simple group a Moufang loop in a direct way. The classification then follows by proving that different realizations of D induce isotopic (and thus isomorphic) simple Moufang groups. The outer automorphisms in question are the involutory isomorphisms (1) $R_x \mapsto L_x^{-1}$, (2) $R_x \mapsto L_x R_x$ and (3) $L_x \mapsto L_x R_x$ that were known already to Glauberman.

The dependence on the CFSG remains since we need to know all finite simple groups that possess a split group of outer automorphisms isomorphic to S_3.

Finite simple Moufang loops arise from Zorn algebras $\mathrm{Zrn}(F)$, F a field. If time allows, I will mention new characterizations of these algebras and certain new results on $\mathrm{Aut}(\mathrm{Zrn}(F)) \cong G_2(F)$.

ON TOTALLY PARASTROPHIC-ORTHOGONAL TERNARY QUASIGROUPS

Fryz Iryna

Vasyl' Stus Donetsk National University, Ukraine

iryna.fryz@ukr.net

Quasigroup algebras possessing the orthogonality property are associated with other discrete structures and applicable in algebra, combinatorics, cryptography, coding theory etc. For example, there is an important connection between sets of mutually orthogonal operations or quasigroups (resp. hypercubes) and maximum distance separable codes [1]. Increasing the number of orthogonal operations in such sets allows one to maximize the Hamming distance, thereby improving the capability for error detection and correction.

A triplet of ternary quasigroups defined on the same set is called *orthogonal* if each possible triplet of the elements of the carrier set occurs exactly once when the corresponding Latin cubes are superimposed; *strongly orthogonal* if the triplet is orthogonal and all corresponding subcubes (Latin squares) are orthogonal. A set of ternary quasigroups are orthogonal if each triplet of this set is orthogonal.

For every permutation σ from the symmetric group S_4, a *σ-parastrophe* ${}^{\sigma}f$ of an invertible ternary operation f is defined by

$$ {}^{\sigma}f(x_{1\sigma}, x_{2\sigma}, x_{3\sigma}) = x_{4\sigma} :\Longleftrightarrow f(x_1, x_2, x_3) = x_4. $$

A ternary quasigroup is called *asymmetric* if all its parastrophes are pairwise different; *totally self-orthogonal* if its all different principal parastrophes are orthogonal; *totally-parastrophic orthogonal* or, more briefly, a *top quasigroup* if all different parastrophes are orthogonal.

A ternary groupoid is called a *group isotope* if it is isotopic to a ternary quasigroup derived from a group. Each group isotope $(Q; f)$ for every element $0 \in Q$ has a 0-canonical decomposition $(+, \alpha_1, \alpha_2, \alpha_3, a)$ ("*canonical*" means always exists and unique), i.e.

$$ f(x_1, x_2, x_3) = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + a, $$

for some group $(Q; +, 0)$, permutations α_1, α_2, α_3 with $\alpha_1 0 = \alpha_2 0 = \alpha_3 0$ and $a \in Q$; $(Q; +, 0)$ is called 0-*canonical decomposition group* [2].

Let $\mathfrak{P}(H)$ denote the class of all quasigroups whose parastrophic symmetry group includes the subgroup H of the group S_4. Note that $\mathfrak{P}(H)$ is a variety and parastrophic symmetry groups of parastrophic quasigroups are conjugated [3]. The symmetric group S_4 has 11 pairwise unconjugated subgroups. The

corresponding list of parastrophic symmetry groups one can find in [3] and [4]. For example, the following subgroups of S_4 are unconjugated:

$$\mathrm{C}_4 = \{\iota, (12), (34), (12)(34)\}, \quad \mathrm{K}_4 = \{\iota, (12)(34), (13)(24), (14)(23)\},$$

$$\mathrm{Z}_4 = \{\iota, (12)(34), (1423), (1324)\}.$$

A quasigroup possessing the corresponding parastrophic symmetry group has 6 pairwise different parastrophes. These classes are studied in [4], in particular canonical decompositions of ternary group isotopes belonging to these varieties are stated. The corresponding statements are given below.

Theorem 1. [4] *A ternary group isotope $(Q; f)$ belongs to $\mathfrak{P}(\mathrm{C}_4)$ if and only if there exists an abelian group $(Q, +, 0)$, its permutation α and an element $a \in Q$ such that $\alpha 0 = 0$ and*

$$f(x_1, x_2, x_3) = \alpha x_1 + \alpha x_2 - x_3 + a. \tag{1}$$

Theorem 2. [4] *A ternary group isotope $(Q; f)$ belongs to $\mathfrak{P}(\mathrm{K}_4)$ if and only if there exists a group $(Q, +, 0)$, its involuting automorphisms α and β and an element $a \in Q$ such that $\alpha a = \beta a = -a$, $\beta\alpha = I_a\alpha\beta$ and*

$$f(x_1, x_2, x_3) = -\beta\alpha x_1 + \alpha x_2 + \beta x_3 + a. \tag{2}$$

Theorem 3. [4] *A ternary group isotope $(Q; f)$ belongs to $\mathfrak{P}(\mathrm{Z}_4)$ if and only if there exists an abelian group $(Q, +, 0)$, its automorphism α and an element $a \in Q$ such that $\alpha^4 = \iota$, $\alpha^3 a = -a$ and*

$$f(x_1, x_2, x_3) = \alpha x_1 + \alpha^3 x_2 - \alpha^2 x_3 + a. \tag{3}$$

The necessary and sufficient conditions for a medial ternary asymmetric quasigroup to be a (strongly) totally self-orthogonal are given in [5], to be a top quasigroup are submitted for publication in a join work with F. Sokhatsky.

Here, we continue the study of group isotopes which have parastrophic symmetry groups C_4, K_4, Z_4. In the series of statements given below, the necessary and sufficient conditions for a group isotope with parastrophic symmetry groups C_4, K_4, Z_4 to be a top quasigroup are stated.

Theorem 4. *A ternary group isotope $(Q; f)$ defined by (1) with the group of parastrophic symmetry C_4 is*

1) *self-orthogonal if and only if $\alpha + \iota$ and $2\alpha - \iota$ are permutations of Q;*
2) *strongly self-orthogonal if and only if $\alpha+\iota$, $2\alpha-\iota$ and $\alpha-\iota$ are permutations of Q;*
3) *a top-quasigroup if and only if $\alpha+\iota$, $2\alpha-\iota$, $\alpha-\iota$, $\alpha-2\iota$ are permutations of Q;*

4) not a strongly top-quasigroup.

Example 1. *Let $\mathbb{Z}_m$ be a ring of integers modulo m. By Theorem 1, $(\mathbb{Z}_m; f)$ with*

$$f(x, y, z) = 7x + 7y - z$$

is a quasigroup which belongs to $\mathfrak{P}(\mathrm{C}_4)$ if and only if m is relatively prime to 7. By Theorem 4, it is a top quasigroup if and only if m is relatively prime to 2, 3, 5, 7, 13.

Theorem 5. *A ternary central quasigroup $(Q; f)$ defined by (2) with the group of parastrophic symmetry K_4 is*

1) a top-quasigroup if and only if it is self-orthogonal;

2) a top-quasigroup if and only if

$$\alpha + \iota, \quad \beta + \iota, \quad \alpha - \beta, \quad \alpha + \beta - \beta\alpha + 3\iota$$

are automorphisms of $(Q; +)$;

3) not a strongly top-quasigroup.

Theorem 6. *A ternary group isotope $(Q; f)$ defined by (3) with the group of parastrophic symmetry Z_4 is*

1) a top-quasigroup if and only if it is self-orthogonal;

2) a top-quasigroup if and only if $\alpha + \iota$, $\alpha - \iota$ are automorphisms of $(Q; +)$;

3) not a strongly top-quasigroup.

Example 2. *Let $\mathbb{Z}_{13}$ be a ring of integers modulo 13. By Theorem 3, $(\mathbb{Z}_{13}; f)$ with $\alpha = 5$ and*

$$f(x, y, z) = 5x + 8y + z$$

is a quasigroup which belongs to $\mathfrak{P}(\mathrm{Z}_4)$. By Theorem 6, it is a top quasigroup.

References:

1. E.T. Ethier, G.L. Mullen. Strong forms of orthogonality for sets of hypercubes. *Discrete Math.*, **321**, Iss. 12-13 (2012), 2050–2061.

2. F.N. Sokhatsky, O.E. Kyrnasovsky. Canonical decompositions of multiary group isotopes. *Izvestiia Gomelskogo gosydarstvennogo yniversyteta im. F.Scoryny. Voprosy algebry – 17*, **3(6)** (2001), 88-97 (in Russian).

3. F. Sokhatsky, Ye. Pirus. Classification of ternary quasigroups according to their parastrophic symmetry groups, I. *Visnyk DonNu. Series A: Natural Sciences*, **1-2** (2018), 70-82.

4. Ye. Pirus. Classification of ternary quasigroups according to their parastrophic symmetry groups, II. *Visnyk DonNu. Series A: Natural Sciences*, **1-2** (2019), 66-75.

5. I. Fryz, F. Sokhatsky. Construction of medial ternary self-orthogonal quasigroups. *Bul. Acad. Stiinte Repub. Mold. Mat.*, **3**(100) (2022), 41-55.

ON (α, β, γ)-QUASIGROUPS

Ilemobade Richard*, Jaiyéọlá Temitope
Obafemi Awolowo University, Ile-Ife, Nigeria
University of Lagos, Akoka, Nigeria
richardilemobade@gmail.com, tjayeola@oauife.edu.ng,
tgjaiyeola@unilag.edu.ng

(α, β, γ)-quasigroups, or (α, β, γ)-inverse quasigroups (as they are commonly referred to in the literature), generalize various types of inverse property quasigroups and loops. In particular, they generalize *CI*-, *WIP*-, m-inverse, and (r, s, t)-inverse loops. In this work, we examine certain isotopic properties of (α, β, γ)-quasigroups and explore their potential cryptographic applications.

PROPERTIES OF AC-GROUPOIDS

Izbas Vladimir, Izbas Ana-Maria *
[1]*Moldova State University, Chisinau, Republic of Moldova*
[2]*University of Groningen, The Netherlands*
vladimir.izbas@math.md, anamaria.izbas@gmail.com

In [3] we introduce the concepts of right (left) $AC-$groupoids over an arbitrary group, generelizing the concept of groupoid "automorphic by the cyclic group" of A. Sade [2]. Necessary and sufficient conditions are found in [3] which transform a right (left) $AC-$groupoid into a quasigroup (either idempotent or commutative one). This is a continuation of the research from [3]. Some other properties of right (left) $AC-$groupoids are investigated. We find the conditions when the (right, left) AC-groupoid has a one-sided unit. We also construct all finite idempotent commutative (right, left) AC-groupoids defined on an arbitrary group of any odd order.

A groupoid $(Q, *)$ is called *right* AC-groupoid (respectively *left* AC-groupoid), if a group $(Q, +)$ exists so that the right translations $R_a^+ : R_a^+(x) = x + a$ (respectively left translations $L_a^+ : L_a^+(x) = a+x$) of the group are automorphisms of the groupoid , i.e.

$$(x * y) + a = R_a^+(x * y) = R_a^+(x) * R_a^+(x) = (x + a) * (y + a) \qquad (1)$$

(respectively,

$$a + (x * y) = L_a^+(x * y) = L_a^+(x) * L_a^+(x) = (a + x) * (a + y)), \qquad (2)$$

Speaking author: Ilemobade R.
Speaking author: Izbas V.

whatever $a, x, y \in Q$.

The structure of (right, left) AC-groupoids is given by the following statements.

The right AC-groupoid $(Q, *)$ is determined by the function $f : Q \to Q, g(x) = 0 * x$ and the group $(Q, +)$ with the neutral element 0, by the formula $x * y = f(x - y) + y$ for any $x, y \in Q$. We will denote this groupoid by $(Q, *_f)$ or $(Q, *_f, +, 0)$ [3].

The left AC-groupoid $(Q, *)$ is determined by the mapping $g : Q \to Q, f(x) = x * 0$ and the group $(Q, +)$ with the neutral element 0, by $x * y = x + g(-x + y)$ for any $x, y \in Q$. We will denote this groupoid by $(Q,_g *)$ or $(Q,_g *, +, 0)$[3].

So

$$x *_f y = f(x - y) + y \tag{3}$$

$$x_g * y = x + g(-x + y) \tag{4}$$

for any $x, y \in Q$.

If $(Q, +)$ is a group that satisfies the identity $2x = 0$ and $|Q| > 2$, then the right (left) $AC-$groupoid $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) is not commutative. From this statement it follows that the commutativity of the group does not ensure the commutativity of the right $AC-$groupoid $(Q, *_f, +, 0)$ (respectively the left $AC-$groupoid ($(Q,_g *, +, 0)$)).

Theorem 1. *Let $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) be a right (left) AC-groupoid defined over the group $(Q, +)$. Then:*

1. *$(Q, *_f, +, 0)$ is a groupoid with a right unit if and only if the mapping $f(x) = x * 0$ that determines it is the identical mapping $f(x) = x$. In this case $x *_f y = x, x, y \in Q$ (the semigroup of right units).*

2. *$(Q, *_f, +, 0)$ is a groupoid with a left unit if and only if the mapping $f(x) = x * 0$ that determines it is the null function $f(x) = 0$. In this case $x *_f y = y, x, y \in Q$ (the semigroup of left units).*

3. *$(Q,_g *, +, 0))$ is a groupoid with a right unit if and only if the mapping $g(x) = 0 * x$ that determines it is the null mapping $g(x) = 0$. In this case $x_g * y = x, x, y \in Q$ (the semigroup of right units).*

4. *$(Q,_g *, +, 0))$ is a groupoid with a left unit if and only if the mapping $g(x) = 0 * x$ that determines it is the identical mapping $f(x) = x$. In this case $x_g * y = y, x, y \in Q$ (the semigroup of left units).*

5. *$(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) is a groupoid with unit if and only if $|Q| = 1$.*

We also study commutative and idempotent (right, left) $AC-$groupoids defined over a group .

Theorem 2. *For any system of elements* $\alpha_1, \alpha_2.\alpha_3, ..., \alpha_m$ *in the finite group* $(Q, +)$ *of order* $|Q| = 2m + 1$ *there exists a unique function* $f : Q \to Q$ *that satisfies properties* $f(0) = 0, f(x_i) = \alpha_i, i \in \{1, 2, 3, ..., m\}$ *and* $f(-x) = f(x) - x, \forall x \in Q$.

Theorem 3. *There are* $(4m+2)^m m!$ *right* $AC-$*groupoids (respectively left* $AC-$*groupoids), commutative and idempotent defined over a group of order* $2m + 1$.

Remark that in Theorem 3 some of the pairs of constructed groupoids may be isotopic, or even isomorphic.

Acknowledgments. The Institutional Research Program of the Moldova State University for 2024 – 2027 years, subprograms 011303 "SATGET has supported part of the research for this paper.

References:

1. V. Belousov. *Foundations of the Theory of Quasigroups and Loops (Russian)*. Nauka, Moscow, 1967.
2. A. Sade. Groupoides automorphes par le groupe cyclique, *Can. J. Math.*, **9** (1957), 321-335.
3. V. Izbas, A-M. Izbas. About AC-Groupoids, *Proceedings of the International Conference IMCS-60, MSU, October 19-13,*(**2024**), *Republic of Moldova*, **71-76**.
4. S. K. Stein. On the foundation of quasigroups, *Trans. Amer. Math. Soc.*, (1957), vol. **85**, pp. 228-256.
5. S. K. Stein. Homogeneous quasigroups, *Pacific J. Math.*, (1964), vol.**14**, pp. 1091-1102.
6. M. Hosszu. Homogeneous groupoids, *Ann. Univ. Sci. Budapest. Eotvos. Sect. Math.*, (1960/1961), vol.**3-4**, pp. 95-99.

CLASSIFICATION OF IDENTITIES OF CIP-QUASIGROUPS UP TO PARASTROPHIC SYMMETRY

Krainichuk Halyna

Vinnytsia National Technical University, Vinnytsia, Ukraine

kraynichuk@ukr.net

A quasigroup (invertible) operation is a function defined on a finite or infinite set if it is invertible in each of its variables. By definition [1], a quasigroup is a set Q with the operation $(\cdot)$ defined on it if, for arbitrary a, b, the equation $a \cdot x = b$, $y \cdot a = b$ has a unique solution. Such a quasigroup is called a binary quasigroup.

For the classification of quasigroup identities, it is more convenient to use another definition of a quasigroup [2]. A quasigroup is an algebra $(Q;\cdot;\overset{\ell}{\cdot};\overset{r}{\cdot})$ with the identities

$$(x\cdot y)\overset{\ell}{\cdot} y = x, \quad (x\overset{\ell}{\cdot} y)\cdot y = x, \quad x\overset{r}{\cdot}(x\cdot y) = y, \quad x\cdot(x\overset{r}{\cdot} y) = y.$$

Here the operation $(\cdot)$ is called the *main*, the operations $\overset{\ell}{(\cdot)}$, $\overset{r}{(\cdot)}$ are the *left* and *right* divisions of the operation $(\cdot)$. These operations are also called the *left* and *right inverse* of the operation $(\cdot)$, since they are the inverses of the operation $(\cdot)$ in the semigroup $(\mathcal{O}_2,\underset{\ell}{\oplus})$ and $(\mathcal{O}_2,\underset{r}{\oplus})$, respectively, where $\mathcal{O}_2$ denotes the set of all binary operations defined on the set Q and the following equalities hold

$$(f\underset{\ell}{\oplus}g)(x,y) := f(g(x,y),y), \qquad (f\underset{r}{\oplus}g) := f(x,g(x,y)).$$

An algebra $(Q;\cdot;\overset{\ell}{\cdot};\overset{r}{\cdot})$ is called a *loop*, if it has a neutral element e: $ex = xe = x$ [1].

For study, a quasigroup is best viewed as an algebra with all its parastrophes in the signature: $(Q;\cdot,\overset{\ell}{\cdot},\overset{r}{\cdot},\overset{s}{\cdot},\overset{s\ell}{\cdot},\overset{sr}{\cdot})$, shorthand $(Q;\cdot)$, where $(\cdot)$ is the main operation. If we replace the main operation $(\cdot)$ with its σ-parastrophe $\overset{\sigma}{(\cdot)}$, we obtain the algebra $(Q;\overset{\sigma}{\cdot},\overset{\ell\sigma}{\cdot},\overset{r\sigma}{\cdot},\overset{s\sigma}{\cdot},\overset{s\sigma}{\cdot},\overset{sr\sigma}{\cdot})$, which is called the σ-parastrophe of this quasigroup. Since $\overset{\sigma}{(\cdot)}$ is the main operation, the shorthand for the σ-parastrophe is $(Q;\overset{\sigma}{\cdot})$.

Let $(Q;\circ)$ be a quasigroup and P be a statement defined in $(Q;\circ)$. The *Parastrophic orbit* $\mathrm{Po}(P)$ and the *parastrophic symmetry set* $\mathrm{Ps}^{\circ}(P)$ of the statement P are defined by the equalities:

$$\mathrm{Po}(P) := \{{}^{\sigma}P \mid \sigma\in S_3\}, \qquad \mathrm{Ps}^{\circ}(P) := \{\sigma \mid {}^{\sigma}P \text{ is true in } (Q;\circ)\}.$$

The identity ${}^{\sigma}(\omega=\upsilon)$ is called *σ-parastrophic* to the identity $\omega=\upsilon$, if it is obtained with $\omega=\upsilon$ by replacing the main operation with its σ^{-1}-parastrophe. The identity holds in the quasigroup $(Q;\cdot)$ if and only if the σ^{-1}-parastrophe of this identity holds in the σ-parastrophe of this quasigroup.

Intuitively, this definition was used by V. D. Belousov [3], when describing parastrophic identities of minimal length. The idea of transforming parastrophic identities appeared in A. Sade [4], his method was used by Sh. K. Stein [5] and he obtained some parastrophic identities for one parastrophic orbit of varieties. V. D. Belousov systematized the results known at that time and the methods of their investigation in the work [6]. Further parastrophic identities of minimal length were classified by the author in the work [7]. With the advent of the full definition of CIP-quasigroups [8], the task of specifying the full classification

of CIP-quasigroup identities up to parastrophic symmetry arose. The initial results of this study are described in [9, 10].

Preliminaries

A quasigroup $(Q;\cdot)$ is called [8]:
1) – *a middle MCIP quasigroup*, if there exists a transformation α such that $\alpha(x)\cdot yx = y$;
2) – *a left LCIP quasigroup*, if there exists a transformation β such that $yx\cdot y = \beta(x)$
3) – *a right RCIP quasigroup*, if there exists a transformation γ such that $y\cdot xy = \gamma(x)$,
where α, β, γ are called the mean, left, and right invertibility functions, respectively.

The bijections L_a, R_a, M_a of the quasigroup $(Q;\cdot)$ are called *left*, *right*, and *middle* translations, if

$$L_a(x) := a\cdot x, \qquad R_a(x) := x\cdot a, \qquad M_a(x) := x \overset{r}{\cdot} a.$$

From here,

$$L_a^{-1}(x) = a \overset{r}{\cdot} x, \qquad R_a^{-1}(x) = x \overset{\ell}{\cdot} a, \qquad M_a^{-1}(x) = a \overset{\ell}{\cdot} x.$$

In [9] it was established that each equality of two sets of translations of different directions defines exactly one class of quasigroups. Namely, the parastrophic orbit of (middle, left, right) CIP-quasigroups is defined by the following translation equalities:

${}^{\ell}\mathcal{M} = {}^{r}\mathcal{M}$ ${}^{rs}\mathcal{M} = {}^{\ell s}\mathcal{M}$	$L_x^{-1} = R_{\alpha(x)}$ $R_x^{-1} = L_{\alpha(x)}$	$\alpha(x)\cdot yx = y$	CIP $MCIP$	$\mathfrak{C} = {}^{s}\mathfrak{C}$
${}^{\iota}\mathcal{M} = {}^{rs}\mathcal{M}$ ${}^{s}\mathcal{M} = {}^{r}\mathcal{M}$	$R_x^{-1} = M_{\beta(x)}$ $M_x^{-1} = R_{\beta(x)}$	$xy\cdot x = \beta(y)$	$LCIP$	${}^{\ell}\mathfrak{C} = {}^{\ell s}\mathfrak{C}$
${}^{\ell s}\mathcal{M} = {}^{\iota}\mathcal{M}$ ${}^{s}\mathcal{M} = {}^{\ell}\mathcal{M}$	$L_x = M_{\gamma(x)}$ $M_x^{-1} = L_{\gamma(x)}^{-1}$	$x\cdot yx = \gamma(y)$	$RCIP$	${}^{r}\mathfrak{C} = {}^{rs}\mathfrak{C}$

In [10], defining identities were found, namely, each variety of the parastrophic orbit CIP of quasigroups can be described by the following identities:

Variety	Defining formula	Defining identity
$\mathfrak{C} = {}^{s}\mathfrak{C}$	$\alpha(x)\cdot yx = y$	$xy\cdot (xz \overset{r}{\cdot} z) = y$
${}^{\ell}\mathfrak{C} = {}^{sr}\mathfrak{C}$	$yx\cdot y = \beta(x)$	$yx\cdot y = zx\cdot z$
${}^{r}\mathfrak{C} = {}^{s\ell}\mathfrak{C}$	$y\cdot xy = \gamma(x)$	$y\cdot xy = z\cdot xz$

For each variety of parastrophic orbit CIP of quasigroups, the invertibility function has the form of dependencies between translations:

$$\mathfrak{C} = {}^{s}\mathfrak{C}: \ (\forall z) \ \ \alpha = M_z R_z = {}^{\iota}M_z {}^{r}M_z;$$
$${}^{\ell}\mathfrak{C} = {}^{sr}\mathfrak{C}: \ (\forall z) \ \ \beta = R_z L_z = {}^{r}M_z {}^{\ell s}M_z;$$
$${}^{r}\mathfrak{C} = {}^{s\ell}\mathfrak{C}: \ \ (\forall z) \ \ \gamma = L_z R_z = {}^{\ell s}M_z {}^{r}M_z.$$

The defining identities in these manifolds have length three, i.e. three different subject variables.

The research problem in these abstracts is to find minimal identities that define CIP-quasigroups. To do this, we first find dependencies between the invertibility functions.

Main results

According to the presented general identities in the definitions of CIP-quasigroups, the general form of σ-parastrophic identities is given in the following table.

σ	$MCIP$	$LCIP$	$RCIP$
ι	$\alpha(x)\cdot yx = y$ $\alpha(x)y\cdot x = y$	$yx\cdot y = \beta(x)$	$y\cdot xy = \gamma(x)$
s	$xy\cdot {}^{s}\alpha(x) = y$ $x\cdot (y\cdot {}^{s}\alpha(x)) = y$	$y\cdot xy = {}^{s}\beta(x)$	$yx\cdot y = {}^{s}\gamma(x)$
ℓ	$yx\cdot y = {}^{\ell}\alpha(x)$	${}^{\ell}\beta(x)\cdot yx = y$ ${}^{\ell}\beta(x)y\cdot x = y$	${}^{\ell}\gamma(xy)\cdot x = y$ $y\cdot ({}^{\ell}\gamma(x)\cdot y) = x$
r	$y\cdot ({}^{r}\alpha(x)\cdot y) = x$ ${}^{r}\alpha(xy)\cdot x = y$	$(y\cdot {}^{r}\beta(x))\cdot y = x$ $x\cdot {}^{r}\beta(yx) = y$	$xy\cdot {}^{r}\gamma(x) = y$ $x\cdot (y\cdot {}^{r}\gamma(x)) = y$
$s\ell$	$(y\cdot {}^{s\ell}\alpha(x))\cdot y = x$ $x\cdot {}^{s\ell}\alpha(yx) = x$	$y\cdot ({}^{s\ell}\beta(x)\cdot y) = x$ ${}^{s\ell}\beta(xy)\cdot x = y$	${}^{s\ell}\gamma(x)\cdot yx = y$ $({}^{s\ell}\gamma(x)\cdot y)\cdot x = y$
sr	$y\cdot xy = {}^{sr}\alpha(x)$	$xy\cdot {}^{r}\beta(x) = y$ $x\cdot (y\cdot {}^{sr}\beta(x)) = y$	$x\cdot {}^{sr}\gamma(yx) = y$ $(y\cdot {}^{sr}\gamma(x))\cdot y = x$

In one cell, the identities are equivalent, i.e., they define the same class of quasigroups; in different cells of one column, the identities are σ-parastrophically equivalent, i.e., they define parastrophic classes of quasigroups. The following theorem follows from this table.

Theorem 1. *Invertibility functions of CIP-quasigroups have the following dependencies between them:* ${}^{\iota}\alpha = {}^{\ell}\beta = {}^{s\ell}\gamma$, ${}^{s}\alpha = {}^{sr}\beta = {}^{r}\gamma$, ${}^{\ell}\alpha = {}^{\iota}\beta = {}^{s}\gamma$, ${}^{r}\alpha = {}^{s\ell}\beta = {}^{\ell}\gamma$, ${}^{s\ell}\alpha = {}^{r}\beta = {}^{sr}\gamma$, ${}^{sr}\alpha = {}^{s}\beta = {}^{\iota}\gamma$.

It was also established by V.D. Belousov that the formulas

$$xy\cdot\alpha(x) = y, \qquad x\cdot y\alpha(x) = y, \qquad \alpha(x)\cdot yx = y, \qquad \alpha(x)y\cdot x = y \tag{1}$$

are equivalent in the quasigroup $(Q;\cdot)$. However, for this purpose, no conditions for the reversibility functions were defined. Taking into account the results of Theorem 1, we have the following refined statement.

Proposition 1. *The identities* (1) *are equivalent in the quasigroup* $(Q;\cdot)$ *provided, if*

$$^{\iota}\alpha(x) = {}^{s}\alpha(x) = {}^{\ell}\beta(x) = {}^{sr}\beta(x) = {}^{r}\gamma(x) = {}^{s\ell}\gamma(x) = x^2.$$

Each of these identities describes the class of all middle MCIP-quasigroups with the invertibility function x^2.

Let S_3 be act on a set of K. If k is an element of the set K such that ${}^{s}k = k$ and k does not match any element of $\mathrm{Po}(k)$, then the element k is one-sided symmetrical.

Taking into account the translation transformations and the dependence between the invertibility functions from Theorem 1, we obtain the following minimal identities for all varieties of CIP-quasigroups.

	$o(x)\backslash{}^{\sigma}o(x)$	$^{\iota}o(x) = {}^{s}o(x) = x^2$	${}^{\ell}o(x) = {}^{s\ell}o(x) = x \overset{\ell}{\cdot} x$	${}^{r}o(x) = {}^{sr}o(x) = x \overset{r}{\cdot} x$
$MCIP$	$\alpha(x)$	$x^2 \cdot yx = y$	$(x \overset{\ell}{\cdot} x) \cdot yx = y$	$(x \overset{r}{\cdot} x) \cdot yx = y$
		$x^2y \cdot x = y,$	$(x \overset{\ell}{\cdot} x)y \cdot x = y,$	$(x \overset{r}{\cdot} x)y \cdot x = y$
		$xy \cdot x^2 = y$	$xy \cdot (x \overset{\ell}{\cdot} x) = y$	$xy \cdot (x \overset{r}{\cdot} x) = y$
		$x \cdot yx^2 = y$	$x \cdot y(x \overset{\ell}{\cdot} x) = y$	$x \cdot y(x \overset{r}{\cdot} x) = y$
			$(y \overset{\ell}{\cdot} yx)x = x$	$x(xy \overset{r}{\cdot} y) = x$
$LCIP$	$\beta(x)$	$yx \cdot y = x^2$	$(yx \cdot y)x = x$	$x(yx \cdot y) = x$
		$yx^2 \cdot y = x$	$y(x \overset{\ell}{\cdot} x) \cdot y = x$	$y(x \overset{r}{\cdot} x) \cdot y = x$
		$x \cdot (yx)^2 = y$	$y \cdot (xy \overset{\ell}{\cdot} xy) = y$	$y \cdot (xy \overset{r}{\cdot} xy) = y$
$RCIP$	$\gamma(x)$	$y \cdot xy = x^2$	$(y \cdot xy)x = x$	$x(y \cdot xy) = x$
		$y \cdot x^2y = x$	$y \cdot (x \overset{\ell}{\cdot} x)y = x$	$y \cdot (x \overset{r}{\cdot} x)y = x$
		$(xy)^2 \cdot x = y$	$(xy \overset{\ell}{\cdot} xy)x = y$	$(xy \overset{r}{\cdot} xy) \cdot x = y$

Each cell of this table has equivalent formulas that define the same variety of quasigroups with the corresponding invertibility function.

Proposition 2. *The identities* $yx \cdot y = \beta(x)$, $x \cdot \beta(yx) = y$, $(y \cdot \beta(x)) \cdot y = x$ *are equivalent in the quasigroup* $(Q;\cdot)$ *provided, if*

$$^{\iota}\beta(x) = {}^{r}\beta(x) = {}^{\ell}\alpha(x) = {}^{s\ell}\alpha(x) = {}^{s}\gamma(x) = {}^{sr}\gamma(x) = x^2.$$

Each of these formulas describes a variety of left LCIP quasigroups with the invertibility function x^2, *or more precisely, a class of semisymmetric idempotent quasigroups.*

Proposition 3. *The identities* (1) $y \cdot xy = \gamma(x)$, $\gamma(xy) \cdot x = y$, $y \cdot (\gamma(x) \cdot y) = x$ *are equivalent in the quasigroup* $(Q;\cdot)$ *provided, if*

$$^{\iota}\gamma(x) = {}^{\ell}\gamma(x) = {}^{r}\alpha(x) = {}^{sr}\alpha(x) = {}^{s}\beta(x) = {}^{s\ell}\beta(x) = x^2.$$

Each of these formulas describes a variety of right RCIP quasigroups with the invertibility function x^2, or more precisely, a class of semi-symmetric idempotent quasigroups.

References:

1. Belousov V. D. *Fundamentals of the theory of quasigroups and loops.* Moskva: Nauka, (1967), 223.

2. Sokhatsky F. M. Parastrophic symmetry in quasigroup theory. *Visnyk Donetsk national university. Ser. A: natural sciences*, **1-2** (2016), 70–83.

3. Belousov V. D. *Parastrophic-orthogonal quasigroups* // Preprint of the Academy of Sciences of the Moldavian SSR, Publ. Shtiintsa, Chisinau, (1983), 50.

4. Sade A. *Produit direct singulier de quasigroupes orthogonaux et anti-abéliens* //Ann. Soc. Sci. Brux., Sér. I. (1960), Vol. 74, 91–99.

5. Stein Sherman K.*On the foundations of quasigroups* // Trans. Amer. Math. Soc. (1957), Vol. 85, 228–256.

6. Belousov V. D. *Parastrophic-orthogonal quasigroups*// Quasigroups Related Systems(2005), Vol. 13, no. 1, 25–72.

7. Krainichuk H. V. *Classification of binary quasigroup functional equations and identities of the length three.* Visnyk Donetsk national university, Ser. Pђ: natural sciences (2017), No. 1–2, 37–66.

8. F.M. Sokhatsky, A.V. Lutsenko, *The bunch of varieties of inverse property quasigroups.* Visnyk DonNU, A: natural Sciences (2018), Vol.1-2, 56–69.

9. Sokhatsky F. M., Lutsenko A. V. *Classification of quasigroups according to directions of translations I.* Commentationes Mathematicae Universitatis Carolinae (2020), Vol. 61, No. 4, 567–579.

10. Sokhatsky F. M., Lutsenko A. V. *Classification of quasigroups according to directions of translations IP†.* Commentationes Mathematicae Universitatis Carolinae (2021), Vol. 62, No. 3, 309–323.

LOGICAL SCHEMES OF SOME ASYMMETRIC QUASIGROUPS FOR LW-CRYPTOGRAPHY

Krainichuk Halyna, Ivanova Liudmyla*

Vinnytsia National Technical University, Vinnytsia, Ukraine

kraynichuk@ukr.net, milaivanova2609@gmail.com

To implement quasigroups in hardware for lightweight cryptography, such minimized logical formulas are needed so that the hardware complexity is the smallest. The main purpose is to find logical schemes of asymmetric quasigroups and calculate their hardware complexity for use in low-resource cryptography.

f	00	01	10	11
00	01	11	10	00
01	10	00	01	11
10	00	10	11	01
11	11	01	00	10

${}^{\ell}f$	00	01	10	11
00	10	01	11	00
01	00	11	01	10
10	01	10	00	11
11	11	00	10	01

${}^{r}f$	00	01	10	11
00	11	00	10	01
01	01	10	00	11
10	00	11	01	10
11	10	01	11	00

${}^{s}f$	00	01	10	11
00	01	10	00	11
01	11	00	10	01
10	10	01	11	00
11	00	11	01	10

${}^{s\ell}f$	00	01	10	11
00	10	00	01	11
01	01	11	10	00
10	11	01	00	10
11	00	10	11	01

${}^{sr}f$	00	01	10	11
00	11	01	00	10
01	00	10	11	01
10	10	00	01	11
11	01	11	10	00

Let $(Z_2^2; f)$ be an asymmetric [1] quasigroup [2], where $Z_2^2 := \{00; 01; 10; 11\}$. All parastrophes left ${}^{\ell}f$, right ${}^{r}f$ and dual to them ${}^{s}f$, ${}^{s\ell}f$, ${}^{sr}f$ are found:

Using the Quine-McCluskey method [3], the following logical formulas were obtained for each parastrophe of the quasigroup: ${}^{\sigma}L = z_1 \vee z_2$, where $z_1 := x_1 y_1$, $z_2 := x_2 y_2$ and $\sigma := \{\iota; \ell; r; s; s\ell; sr\}$.

$$L = x_2 \oplus (y_1 \oplus y_2) \vee \overline{x_1 \oplus (x_2 \oplus y_1)}; \quad {}^{s}L = x_1 \oplus (x_2 \oplus y_2) \vee \overline{x_1 \oplus (y_1 \oplus y_2)};$$

$${}^{\ell}L = \overline{x_1 \oplus (x_2 \oplus y_2)} \vee x_1 \oplus (y_1 \oplus y_2); \quad {}^{sl}L = \overline{x_2 \oplus (y_1 \oplus y_2)} \vee x_1 \oplus (x_2 \oplus y_1);$$

$${}^{r}L = \overline{x_1 \oplus (x_2 \oplus y_2)} \vee \overline{x_1 \oplus (y_1 \oplus y_2)}; \quad {}^{sr}L = \overline{x_2 \oplus (y_1 \oplus y_2)} \vee \overline{x_1 \oplus (x_2 \oplus y_1)}.$$

Taking into account the values of logical structural elements from [4], the Latin squares complexity for hardware is

$$L = {}^{s}L = {}^{\ell}L = {}^{s\ell}L = 11.34 \text{ GE}, \qquad {}^{r}L = {}^{sr}L = 12.01 \text{ GE},$$

where $(\oplus)$ denotes XOR and the value GE (Gate Equivalent) denotes a unit of measurement that determines the manufacturing complexity of a technology regardless of the complexity of the digital electronic circuits.

References:

1. Sokhatsky F. M. Parastrophic symmetry in quasigroup theory. *Visnyk Donetsk national university. Ser. A: natural sciences*, **1-2** (2016), 70–83.

2. Belousov V. D. *Fundamentals of the theory of quasigroups and loops.* Moskva: Nauka, (1967), 223.

3. N.R. Kondratenko, A.V. Ostapenko-Bozhenova. *Chapters of discrete mathematics for information protection problems*, (2022), 89.

4. Virtual Silicon. *Standard cell library UMCL18G212T3 based on the UMC L180 0.18 μm 1P6M Logic process.* Official release, (2004), p.1.

* *Speaking author*: L.E. Ivanova

PRE-AFFINE NETS AND LOOP TRANSVERSALS

Kuznetsov Eugene
Moldova State University, Chisinau, Republic of Moldova
kuznet1964@mail.ru

This study began with the work [1] of V.D. Belousov, in which one class of finite algebraic nets was studied (when the genus of the net coincides with its order). All necessary definitions can be found in the works [3, 2].

Definition 1. *A set $\langle P, L, I\rangle$ of objects of 2 types (P - points and L - lines) with an incidence relation I is called a* ***net*** *(**algebraic net**) if the following conditions are satisfied:*

1. *The set L can be separated into disjoint classes $L_1, L_2, \ldots, L_k$.*
2. *Two lines from different classes are incident to exactly one point.*
3. *Each point $X \in P$ is incident to exactly one line from each class L_i .*

The number k is called the *genus* of the net N, and the net N is then called a k-net. It is known [2] that each line L contains the same number n of points, and the number of lines in each class L_i is also equal to n . The number n is called the *order* of the net.

The inequality $k \leqslant n+1$ always holds for k-nets. If $k = n+1$, then such k-net is called an *affine plane*. It is natural to consider the case $k = n$. V.D. Belousov called such k-nets as *pre-affine* nets in work [1]. He proved the following theorem

Theorem 1. *Let $\langle P, L, I\rangle$ be a pre-affine net. Then it can always be embedded (as a subnet) into some affine plane of the same order.*

It is known (see [2]) that any k-net $\langle P, L, I\rangle$ of order n is in 1-1 correspondence with a system $\langle F, E, A_3, \ldots, A_k\rangle$ of k orthogonal binary operations of order n (where F, E are left and right selectors, and $A_3, \ldots, A_k$ are quasigroups). Then (see [2]) we obtain the corollary

Corollary 2. *Any system of $(n-2)$ pairwise orthogonal quasigroups of order n can always be supplemented (by adding of some quasigroup) to a complete system of $(n-1)$ pairwise orthogonal quasigroups.*

The last statement was proved in [2] by non-constructive enumerating method. Therefore arose the question of finding an explicit method for constructing this additional quasigroup.

Let us remember the basic facts from the theory of the finite affine planes and its coordinatization (see [6]).

Definition 2. *[6] A system $\langle E, (x,t,y), 0, 1\rangle$ is called a* ***DK-ternar*** *(i.e. a set E with ternary operation (x,t,y) and distinguished elements $0, 1 \in E$), if the following conditions hold:*

1. $(x, 0, y) = x$,
2. $(x, 1, y) = y$,
3. $(x, t, x) = x$,
4. $(0, t, 1) = t$,
5. *if a, b, c, d are arbitrary elements from E and $a \neq b$, then the system*

$$\begin{cases} (x, a, y) = c \\ (x, b, y) = d \end{cases}$$

has an unique solution in $E \times E$.

Definition 3. *A set M of permutations on a set X is called* ***sharply 2-transitive*** *if for any two pairs (a, b) and (c, d) of different elements from X there exists an unique permutation $\alpha \in M$ satisfying the following conditions:*

$$\alpha(a) = c, \qquad \alpha(b) = d.$$

Lemma 3. *[6] Let π be an arbitrary finite projective plane. We can introduce on the plane π the coordinates $(a, b), (m), (\infty)$ for points and $[a, b], [m], [\infty]$ for lines (where the set E is a finite set with the distinguished elements $0, 1$ and $a, b, m \in E$) such that if we define a ternary operation (x, t, y) on the set E by the formula*

$$(x, t, y) = z \quad \stackrel{def}{\Longleftrightarrow} \quad (x, y) \in [t, z],$$

then the system $\langle E, (x, t, y), 0, 1\rangle$ be a DK-ternar.

Now let a system $\langle E, (x,t,y), 0, 1\rangle$ be a DK-ternar. Let us define the following binary operation (x, ∞, y) on the set E:

$$(x, \infty, 0) \stackrel{def}{=} x,$$
$$\begin{cases} (x, \infty, y) = u \\ (x, y) \neq (u, 0) \end{cases} \stackrel{def}{\Longleftrightarrow} (x, t, y) \neq (u, t, 0) \quad \forall t \in E.$$

Lemma 4. *[6] Operation (x, ∞, y) satisfies the following conditions:*

1. $$\begin{cases} (x, \infty, y) = (u, \infty, v) \\ (x, y) \neq (u, v) \end{cases} \Longleftrightarrow (x, t, y) \neq (u, t, v) \quad \forall t \in E.$$

2. $(x, \infty, x) = 0$.

3. *if a, b, c are arbitrary elements from E, then the system*

$$\begin{cases} (x, a, y) = b \\ (x, \infty, y) = c \end{cases}$$

has a unique solution in $E \times E$.

Let $\langle E, (x, t, y), 0, 1\rangle$ be a finite DK-ternar. Let us introduce points (a, b) and lines $[a, b], [m]$ (where $a, b, m \in E$) and define the following incidence relation I between points and lines:

$$\begin{array}{rcl} (a, b)\ I\ [c, d] & \Longleftrightarrow & (a, c, b) = d, \\ (a, b)\ I\ [d] & \Longleftrightarrow & (a, \infty, b) = d, \end{array} \tag{1}$$

Lemma 5. *[6] The incidence system $\langle X, L, I\rangle$, where*

$$\begin{array}{c} X = \{(a, b) \mid a, b \in E\}, \\ L = \{[a, b], [m] \mid a, b, m \in E\}, \\ I \text{ is the incidence relation, defined above in (1),} \end{array}$$

is an affine plane.

Lemma 6. *[6] (**Cell permutations**) Let the system $\langle E, (x, t, y), 0, 1\rangle$ be a finite DK-ternar. Let a, b be an arbitrary elements from E and $a \neq b$. Then every unary operation $\alpha_{a,b}(t) = (a, t, b)$ is a permutation on the set E.*

Lemma 7. *[6] Cell permutations $\{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ of the finite DK-ternar $\langle E, (x, t, y), 0, 1\rangle$ satisfy the following conditions:*

1. *All cell permutations are distinct;*

2. *The set M of all cell permutations is sharply 2-transitive on the set E;*

3. *A permutation $\alpha_{a,b}$ is a fixed-point-free cell permutation on the set E iff the following condition holds*

$$(a, \infty, b) = (0, \infty, 1).$$

4. *There exists the fixed-point-free permutation ν_0 on the set E such that we can represent the set A of all fixed-point-free cell permutations together with the identity cell permutation $\alpha_{0,1}$ in the following form:*

$$A = \{\alpha_{a,b} \,|\, b = \nu_0(a), \quad a \in E\} = \{\alpha_{a,\nu_0(a)}\}_{a\in E}.$$

Lemma 8. *[6] Let $M = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ be a set of permutations on the set E (E is a finite set with distinguished elements 0 and 1), and the following conditions hold:*

1. $\alpha_{0,1} = id$.
2. $\alpha_{a,b}(0) = a,\ \alpha_{a,b}(1) = b$.
3. *The set M is a sharply 2-transitive set of permutations on E.*

Let us suppose by definition:

$$(x,t,y) \stackrel{def}{=} \alpha_{x,y}(t) \quad if \quad x \neq y,$$
$$(x,t,x) \stackrel{def}{=} x.$$

Then the system $\langle E, (x,t,y), 0, 1\rangle$ is a finite DK-ternar.

Next theorem show a connection between a finite sharply 2-transitive sets of permutations and loop transversals in the symmetric group S_n.

Theorem 9. *[5] Let E be a finite set and $card\, M = n$. Then the following conditions are equivalent:*

1. *A set T of permutations of degree n is a sharply 2-transitive set of permutations on the set E and $id \in T$.*
2. *A set T of permutations of degree n is a loop transversal in S_n to $St_{a,b}(S_n)$ (where a, b are arbitrary fixed elements from E and $a \neq b$).*
3. *A system $\langle E \times E - \{\triangle\}, \overset{(T)}{\cdot}, \langle a,b\rangle\rangle$ is a sharply 2-transitive permutation loop of degree n (a definition of permutation loop see in [8]).*

Lemma 10. *[6] Let $T_{a,b} = \{\alpha_{x,y}\}_{x,y\in E,\ x\neq y}$ be a loop transversal in S_n to $St_{a,b}(S_n)$ (where a, b are arbitrary fixed elements from E and $a \neq b$). Let a system $\langle E \times E - \{\triangle\}, \overset{(T_{a,b})}{\cdot}, \langle a,b\rangle\rangle$ be a loop transversal operation corresponding to the transversal $T_{a,b}$. Then*

$$\langle x,y\rangle \overset{(T_{a,b})}{\cdot} \langle u,v\rangle = \langle \alpha_{x,y}(u), \alpha_{x,y}(v)\rangle. \tag{2}$$

As it is shown above, there exist a 1-1 correspondences between

- a finite projective plane π of order n;
- a finite DK-ternar $\langle E, (x,t,y), 0, 1\rangle$ which gives a coordinatization of the projective plane π;

- a sharply 2-transitive permutation loop $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ of cell permutations of the DK-ternar $\langle E, (x,t,y), 0, 1\rangle$;

- a loop transversal $T_{a,b} = \{\alpha_{x,y}\}_{x,y\in E,\ x\neq y}$ in the symmetric group S_n to $St_{a,b}(S_n)$ (where a, b are arbitrary fixed elements from E and $a \neq b$);

- a loop transversal operation $\langle E \times E - \{\triangle\}, \overset{(T_{a,b})}{\cdot}, \langle a, b\rangle\rangle$ corresponding to the transversal $T_{a,b}$ (in [6] this loop is called a **loop of pairs** of the DK-ternar $\langle E, (x,t,y), 0, 1\rangle$).

Below for simplicity we shall consider that $\langle a, b\rangle = \langle 0, 1\rangle$.

Lemma 11. *A set*

$$H_0^* = \{\langle 0, a\rangle \,|\, a \in E - \{0\}\}$$

forms a subloop in the loop of pairs $L^* = \langle E \times E - \{\triangle\}, \overset{(T_{0,1})}{\cdot}, \langle a, b\rangle\rangle$.

Let us study a set $A = \{\alpha_{a,\nu(a)}\}_{a\in E} \subset L$ of all fixed-point-free permutations and the identity permutation (see Lemma 8).

Lemma 12. *A set* $A = \{\alpha_{a,\nu(a)}\}_{a\in E}$ *is a loop transversal in the loop* $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ *to its proper subloop* H_0.

Lemma 13. *There exists an unique left loop transversal in the loop* $L = \{\alpha_{a,b}\}_{a,b\in E,\ a\neq b}$ *to its subloop* H_0.

Corollary 14. *There exist exactly* $n-2$ *different non-reduced left loop transversals in the loop* L *to its subloop* H_0.

Remark 1. *It can be note a correlation between the left loop transversal* A *in the loop* L *to its subloop* H_0 *and the points of the line* $[(0, \infty, 1)]$ *in the projective plane* π*:*

$$\alpha_{x,\nu(x)} \in A \quad \Leftrightarrow \quad (x, \nu(x)) \in [(0, \infty, 1)].$$

There exists an analogical correlation between the non-reduced left loop transversals in the loop L *to its subloop* H_0 *and the points of the lines* $[d]$ $(d \neq 0)$ *in the projective plane* π*:*

$$\alpha_{x,\delta(x)} \in T_c \quad \Leftrightarrow \quad (x, \delta(x)) \in [(0, \infty, c)], \quad c \neq 0, 1.$$

Corollary 15. *A following condition is fulfilled for the loop* $\langle E, \overset{(A)}{\cdot}, 0\rangle$ *and permutation* ν*: for every* $x \in E$

$$\nu(x) = x \overset{(A)}{\cdot} 1.$$

References

[1] Belousov V.D.: About one class of algebraic nets (Russian) , Chisinau, "Stiintsa", Matem. Issled., vyp., 51 (1979), p. 14-22.

[2] Belousov V.D.: Algebraic nets and quasigroups (Russian), Chisinau, "Stiintsa", 1971.

[3] Belousov V.D.: Foundations of quasigroup and loop theory (Russian), Moscow, "Nauka", 1967.

[4] Kuznetsov E.A.: Transversals in groups.1.Elementary properties, Quasigroups and related systems, 1(1994), No. 1, p. 22-42.

[5] Kuznetsov E.A.: Sharply k-transitive sets of permutations and loop transversals in S_n, Quasigroups and related systems, 1(1994), No. 1, p. 43-50.

[6] Kuznetsov E.A.: About some algebraic systems related with projective planes, Quasigroups and related systems, 2(1995), No. 1, p. 6-33.

[7] Kuznetsov E.A.: Loop transversals in S_n by $St_{a,b}(S_n)$ and coordinatizations of projective planes, Bulletin of AS of RM, Mathematics, 2001, 2(36), 125-135.

[8] Bonetti F., Lunardon G., Strambach K.: Cappi di permutazionni, Rend. Math., 12(1979), No. 3-4, p. 383-395.

ISOTOPY, ISOSTROPHY, AND GYSOTOPY IN THE THEORY OF QUASIGROUPS

Malyutina Nadegda, Shcherbacov Victor, Chernov Vladimir *

Shevchenko Transnistria State University, Tiraspol, Moldova State University, Chisinau, Republic of Moldova

231003.bab.nadezhda@mail.ru, vscerb@gmail.com, volodya.black@gmail.com

Modern research in cryptography requires the development of algebraic constructions with complex symmetry and a high degree of internal structure secrecy. One of such directions is the application of quasigroups and their transformations – isotopies, isostrophies and gisotopies – in the design of cryptographically robust algorithms.

* *Speaking author* : Malyutina N.

The structure of isostrophy and gisotopy classes of given groupoids and quasigroups has been investigated. An algorithmic approach to the construction and analysis of various forms of isotopic, isostrophic and gisotopic images of algebraic structures oriented to cryptographic applications has been implemented.

Gisotopy (or generalized isotopy) is a more extensive concept than isotopy, and allows the construction of new algebraic objects that may not satisfy standard properties and axioms.

Definition 1. A groupoid (Q, A) is a gisotope (a gisotopic image) of a kind α of a groupoid (Q, B),where $\alpha \in \{l, r\}$,if there exists an m-tuple of permutations P of the set Q of the kind α such that $T_A^\alpha = T_B^\alpha$, i.e., $(t_A^\alpha) = (t_B^\alpha)_i p_i$ for all suitable values of the index i, where T_A^α, T_B^α are m-tuples of maps of the kind α that correspond to the groupoids (Q, A), (Q, B), respectively [1].

Theorem 1. If (Q, A) is a left quasigroup and T is an isotopy, then there exists a gisotopy GT of the kind l such that $(Q, A)T = (Q, A)GT$, i.e. any isotopy of a left quasigroup is a gisotopy.

Gisotopy is a transformation which preserves the property of orthogonality of squares, groupoids and m-tuples of maps [1].

The following program modules in Python language were developed: programs for construction of isotopic and isostrophic image for a given groupoid or quasi-group, programs for construction of gisotopic images of types l,Il,r,Ir for a given quasigroup or groupoid. The developed programs allow both theoretical analysis and modeling of the application of these structures in cryptographic algorithms.

We consider the application of isostrophy and generalized isotopy in the ElGamal scheme based on the Markovski algorithm [2]. Isostrophy and isotopy can be useful in coding theory, cryptography, and other fields that work with various algebraic systems that have similar or equivalent mathematical properties.

References:

1. V.A. Shcherbacov. *Elements of Quasigroup Theory and Applications*. 1st ed: Chapman and Hall, CRC, Place, 2017.

2. N.N. Malyutina, V.A. Shcherbacov. An analogue of the ElGamal scheme based on the Markovski algorithm . *ROMAI Journal* , **17 (1)** (2021), 105–114.

A STUDY OF EXTRA POLYLOOP AND ITS ALGEBRAIC PROPERTIES

Oyebola Oyeyemi Oluwaseyi, Temitope Gbolahan Jaíyéọlá, Kehinde Gabriel Ilori *

Brandon University, Brandon MB, Canada. Obafemi Awolowo University, Redeemer's University, Nigeria.

oyebolao@brandonu.ca, tjayeola@oauife.edu.ng, kennygilori@gmail.com

In this study, we investigate a special class of non-associative algebraic hyperstructures- extra polyloop, and explore their fundamental algebraic properties . Unlike traditional and classical non-associative algebraic structure *extra loop*, where the binary operation satisfies any of the extra identities

$$(xy \cdot z)x = x(y \cdot zx),\ yx \cdot zx = (y \cdot xz)x,\ xy \cdot xz = x(yx \cdot z),$$

non-associative algebraic hyperstructures exhibit more diverse and complex behaviours. We focus on a key class of non-associative algebraic hyperstructure - extra polyloops, and analyze their structural algebraic properties, identities, and substructures. Furthermore, we examine conditions under which certain non-associative algebraic hyperstructures admit wweak associativity or power associativity. The interplay between non-associativity and other algebraic properties , such as flexibility, left alternative property, and right alternative property is explored.

References:

1. M. Al-Tahan and B. Davvaz. N-ary hyperstructures associated to the genotypes of F_2-offspring. International Journal of Biomathematics. Singapore, **10(8)**, (2017), 175-188.
2. M. Al-Tahan and B.Davvaz. Algebraic hyperstructures associated with biological inheritance. *Mathematical Biosciences*. Netherlands,**285**, 112-118.
3. F. Fenyves. Extra loops I, *Publicationes Mathematicae Debrecen*, **15**, (1968), 235-238.
4. F. Fenyves. Extra loops II, *Publicationes Mathematicae Debrecen*, **16**, (1969).
5. K. G. Ilori, T. G. JJaíyéọlá, O. O. Oyebola. Analysis of Weak Associativity in Some Hyper-Algebraic Structures that Represent Dismutation Reactions, *MATCH Commun. Math. Comput. Chem.*, **94** (2025), 385-406.
6. Khalafi A.D. and B. Davvaz . Algebraic hyperstructures associated to convex analysis and applications, *Faculty of Sciences and Mathematics, University of Nis (Filomat)*. Serbia, **26(1)**, (2012), 55-65.
7. F. Marty, Sur une généralization de la notion de groupe, *8th Congress Math, Scandenaves Stockholm*, (1934), 45-49.
8. O. O. Oyebola and T. G. Jaiyeola, Non-associative algebraic hyperstructures and their applications to biological inheritance, *Nonograffas Matematicas Garcia de Galdeano* **42**, (2019), 229-241.

* *Speaking author*: O. Oyebola

BOL MOUFANG RINGS AND THINGS, YET AGAIN

Phillips John D.

Northern Michigan University, USA

E-mail: phillips.jd1@gmail.com

We give some new structural results about loops of Bol Moufang type, and move on to connections with Lie Rings.

ON LCA GROUPS WHOSE CLOSED CO-POLYTHETIC SUBGROUPS HAVE COMMUTATIVE RING OF CONTINUOUS ENDOMORPHISMS

Popa Valeriu

Moldova State University, Chişinău, Republic of Moldova

valeriu.popa@math.md

Let $\mathcal{L}$ be the class of locally compact abelian groups. For $X \in \mathcal{L}$, we let $E(X)$ denote the ring of continuous endomorphisms of X, $k(X)$ the subgroup of compact elements of X, $t(X)$ the torsion subgroup of X, and $S_0(X)$ the set of prime numbers p with the property that $t_p(X)$, the p-primary component of X, is non-zero. For any prime p, we set $X[p] = \{x \in X \mid px = 0\}$ and denote by $\mathbb{Z}(p)$ the cyclic group of order p, taken with the discrete topology. Also, we denote by $\mathbb{T}$ the group of reals modulo one with its usual compact topology.

Definition 1. A group $X \in \mathcal{L}$ is said to be co-polythetic in case there exists a continuous injective homomorphism from X into a group of the form $\mathbb{T}^n$ for some $n \in \mathbb{N}$.

Theorem 1. Let X be a group in $\mathcal{L}$ with $t(X) \neq \{0\}$. If every closed co-polythetic subgroup of X has commutative ring of continuous endomorphisms, then $k(X) = X$ and $X[p] \cong \mathbb{Z}(p)$ for all $p \in S_0(X)$.

Theorem 2. If X is a torsionfree group in $\mathcal{L}$ all of whose nonzero discrete subgroups are of rank one, then every closed co-polythetic subgroup of X has commutative ring of continuous endomorphisms.

Theorem 3. For a group $X \in \mathcal{L}$, the following statements are equivalent:

(i) Every closed co-polythetic subgroup of X has commutative ring of continuous endomorphisms.

(ii) X satisfies one of the following conditions:

(1) X is torsionfree and every its nonzero discrete subgroup is of rank one.

(2) $X = A \times Y$, where $A \cong \mathbb{T}$ and Y is a torsionfree group in $\mathcal{L}$ with $k(Y) = Y$.

(3) X contains no copies of $\mathbb{T}$, $k(X) = X$, and $X[p] \cong \mathbb{Z}(p)$ for all $p \in S_0(X)$.

ON 4-QUASIGROUPS WITH EXACTLY FIVE DISTINCT PARASTROPHES

Rotari Tatiana, Syrbu Parascovia *

Moldova State University, Chisinau, Republic of Moldova

tatiana.rotari@usarb.md, parascovia.syrbu@gmail.com

An n-groupoid (Q, A) is called an n-quasigroup if each of the elements $x_1, x_2, \ldots, x_{n+1}$ in the equality $A(x_1, x_2, \ldots, x_n) = x_{n+1}$ is uniquely determined by the remaining n. The operation ${}^{\sigma}A$, defined by the equivalence

$$A(x_1, x_2, \ldots, x_n) = x_{n+1} \Leftrightarrow {}^{\sigma}A((x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = x_{\sigma(n+1)},$$

where $\sigma \in S_{n+1}$, is called a parastrophe of (Q, A).

The set $H = \{\sigma \in S_{n+1} | {}^{\sigma}A = A\}$, where (Q, A) is an n-quasigroup,is a subgroup of S_{n+1}. Moreover, if $\tau \in S_{n+1}$ then ${}^{\beta}A = {}^{\tau}A$ if and only if $\beta \in H\tau$. Hence, the number of distinct parastrophes of an n-quasigroup devides $(n+1)!$. Remark that every set of representatives of $\{H\tau | \tau \in S_{n+1}\}$ is a maximum set of distinct parastrophes of (Q, A).

C.C. Lindner and D. Steadly shown in [1] that finite binary quasigroups with a prescribed number of distinct parastrofes exist of every order $q \geq 4$, suggesting that this problem can be extended to n-ary quasigroups. The problem was completely solved in the ternary case, for $1, 3, 4, 6, 12$ and 24 distinct parastrophes by M. McLeish [2]. The spectrum of ternary quasigroups with exactly 2 or 8 distinct parastrophes is only partly described.

n-Quasigroups with orthogonal maximum sets of $k \geq n$ distinct parastrophes are called totally parastrophic-orthogonal quasigroups. We study the maximum sets of distinct parastrophes of a 4-ary quasigroup, the spectrum of finite 4-ary quasigroups with a given maximum number of distinct parastrophes and the spectrum of totally parastrophic-orthogonal 4-quasigroups.

---

* *Speaking author*: Rotari T.

Theorem 1. *A 4-ary quasigroup (Q, A), which is linear over an abelian group $(Q, +)$, has exactly five distinct parastrophes if and only if there exist an automorphism $\alpha \in Aut(Q, +)$ and an element $c \in Q$ such that the operation $A(x_1, x_2, x_3, x_4)$ has one of the following forms: $\alpha(x_1)+\alpha(x_2)+\alpha(x_3)+\alpha(x_4)+c$, $\alpha(x_1)+I(x_2)+I(x_3)+I(x_4)+c$, $I(x_1)+\alpha(x_2)+I(x_3)+I(x_4)+c$, $I(x_1)+I(x_2)+\alpha(x_3)+I(x_4)+c$, $I(x_1)+I(x_2)+I(x_3)+\alpha(x_4)+c$, where $I(x) = -x, \forall x \in Q$.*

Theorem 2. *A 4-quasigroup, linear over an abelian group $(Q, +)$, with exactly five distinct parastrophes, is totally parastrophic-orthogonal if and only if there exist $\alpha \in Aut(Q, +)$ such that $3\alpha + I$ and $(\alpha + \varepsilon)^3$ are bijections.*

Corollary. *There exist totally parastrophic-orthogonal linear 4-ary quasigroups with exactly five distinct parastrophes of every odd order $q \geq 3$.*

References:

1. C.C. Lindner and D. Steedley. On the number of conjugates of a quasigroup. *Alg. Universalis.*, **5** (1975), 191–196.

2. M. McLeish. On the number of conjugates of n-ary quasigroups. *Can. J. Math. Vol. XXXI*, **3** (1979), 637–654.

ON SCHWEITZER QUAZIGROUPS

Diduric Natalia, Malyutina Nadegda, Shcherbacov Victor *

Moldova State University, Chisinau, Republic of Moldova

vscerb@gmail.com, natnikkr83@mail.ru

Definition 1. A quasigroup $(Q, \cdot)$ is called a Schweitzer quasigroup, if in $(Q, \cdot)$ the following identity is true: $yz \cdot yx = xz$.

Theorem 1. There exist Schweitzer quasigroups $(K, \cdot)$ which:
1. are isotopic to an abelian group and have a right identity element,
2. are Moufang quasigroups, i.e. $(x(y \cdot xz)) = (x \cdot yf_x)x \cdot z$,
3. are Abel-Grassman quasigroups, i.e. $(x \cdot yz = z \cdot yx)$,
4. are right transitive quasigroups, i.e. $(xy \cdot zy = xz)$,
5. are medial quasigroups, i.e. $(xy \cdot uv = xu \cdot yv)$,
6. have a non-empty distributant.

Examples of Schweitzer quasigroups.

* *Speaking author*: Shcherbacov V. A.

*:	0	1	2	3	4	5	6	7	8
0	0	2	1	4	3	6	5	8	7
1	1	0	2	5	8	3	7	6	4
2	2	1	0	7	6	8	4	3	5
3	3	6	8	0	4	7	1	5	2
4	4	7	5	3	0	2	8	1	6
5	5	4	7	8	1	0	6	2	3
6	6	8	3	2	7	5	0	4	1
7	7	5	4	6	2	1	3	0	8
8	8	3	6	1	5	4	2	7	0

*:	0	1	2	3	4	5	6	7	8	9
0	0	1	3	2	5	4	8	9	6	7
1	1	0	4	5	2	3	9	8	7	6
2	2	5	0	6	7	1	3	4	8	9
3	3	4	8	0	1	9	6	7	2	5
4	4	3	9	1	0	8	7	6	5	2
5	5	2	1	7	6	0	4	3	9	8
6	6	7	2	8	9	5	0	1	3	4
7	7	6	5	9	8	2	1	0	4	3
8	8	9	6	3	4	7	2	5	0	1
9	9	8	7	4	3	6	5	2	1	0

References:

1. A. Gvaramiya, M.M. Gluhov, Solution of the main algorithmic problems in some classes of quasigroups with identities, USSR Academy of Sciences, *Siberian Mathematical Journal*, Volume X, Moscow, 1969.

2. V.D. Belousov, Fundamentals of the theory of quasigroups and loops, Publisher: Nauka, Moscow, 1967.

3. V.D. Belousov. I.A. Florya, Quasigroups with the property of invertibility, *Izvestiya of the Academy of Sciences of the Moldavian SSR*, 1966, No. 4.

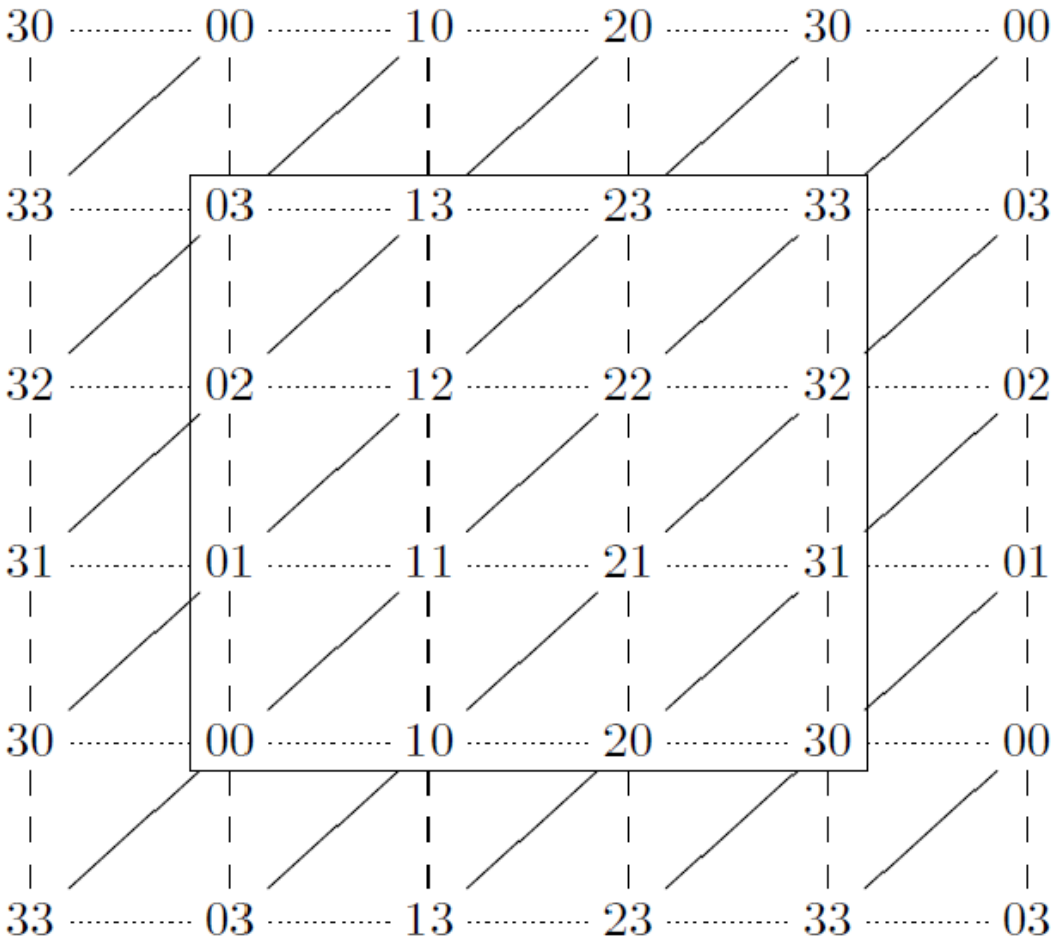
ALGEBRAIC NETS AND QUANTUM QUASIGROUPS

Smith Jonathan D.H.
Iowa State University, Ames, Iowa, U.S.A.
jdhsmith@iastate.edu

A 3-*net* or 3-*web* is a set W of *points* which decomposes in three ways

$$W \cong H \times V \cong V \times D \cong D \times H \tag{1}$$

as a product of pencils H, V, D of *lines* respectively described as *horizontal*, *vertical*, and *diagonal* [1], [4,p.88]. These lines are respectively dotted, dashed, and solid in the example illustrated below, based on a triangulation of the torus. Here, the ordered pair (x, y) labelling a point is exhibited simply as xy.



Quasigroups coordinatize and are determined by webs, to within isotopy. The coordinatizing quasigroup in the example is subtraction of integers modulo

4. Web geometry was first motivated by the now obsolete topic of nomography. Contemporary applications include the Wigner function phase space approach to quantum mechanics, and the role of curvature in general relativity. The problem of quantizing web geometry emerges as a potentially important part of the general problem of appropriately quantizing spacetime. Quasigroup theory provides an approach to this problem.

A quasigroup $(Q, \cdot)$ is *semisymmetric* if $(x \cdot y) \circ y = x$, where $x \circ y = y \cdot x$ denotes the opposite of the original multiplication. The *semisymmetrization* of a quasigroup $(Q, \cdot, /, \backslash)$ is defined by the semisymmetric multiplication

$$(x_1, x_2, x_3) \cdot (y_1, y_2, y_3) = \big(x_2 \backslash y_3, x_3 / y_1, x_1 \circ y_2\big) \tag{2}$$

on Q^3 [4]. A *homotopy* $(f, g, h)\colon (Q, \cdot) \to (P, *)$ between quasigroups, so with $x^f * y^g = (x \cdot y)^h$ for all x, y in Q, semisymmetrizes to a homomorphism

$$Q^3 \to P^3; (x, y, z) \mapsto (x^f, y^g, z^h) \tag{3}$$

between their semisymmetrizations. In particular, isotopic quasigroups have isomorphic semisymmetrizations. Web geometry clarifies the role of isotopy: The respective bijections f, g, h of an isotopy (f, g, h) permute the labels of the vertical, horizontal, and diagonal lines of the web coordinatized by the domain and codomain of the isotopy. Conversely, the semisymmetrization of a quasigroup encodes the web geometry that it coordinatizes. Quantizing quasigroups to quantum quasigroups [3,6,7], the problem of quantizing web geometry reduces to the problem of semisymmetrizing quantum quasigroups [8].

Quantum quasigroups are structures appearing in a *symmetric monoidal category* $(\mathbf{V}, \otimes, \mathbf{1})$, which is like a commutative Monoid* on the class $\mathbf{V}_0$ of objects, with *tensor* product $\otimes$ and unit $\mathbf{1}$, where the categorical relation of natural isomorphism replaces the set-theoretical notion of algebraic identity. Thus, commutativity appears as an involutive natural isomorphism $\tau_{A,B}$ or

$$\tau\colon A \otimes B \to B \otimes A; x \otimes y \mapsto y \otimes x \tag{4}$$

described as the *swap* in quantum information theory. Quantum quasigroups include (classical) quasigroups in the category $(\mathbf{Set}, \times, \top)$ (with a singleton $\top$ as unit), quantum groups in the category $\big(\underline{\underline{\mathbb{C}}}, \otimes, \mathbb{C}\big)$ of complex vector spaces (the usual setting for quantum mechanics) with the 1-dimensional space as unit, and linear quasigroups in the *linear* category $\big(\underline{S}, \oplus, \{\,0\,\}\big)$ of modules over a commutative, unital ring S, with the direct sum $\oplus$ as product and the trivial module $\{\,0\,\}$ as unit. Generically, an elementary notation $x \otimes y$ is used to track an object $A \otimes B$, as in (4) — compare [3]. In particular, the tensor notation $x \otimes y$ provides a very convenient notation for an ordered pair $(x, y) \in A \times B$.

*Following the convention of capitalizing algebraic structures on potentially proper classes.

A *quantum quasigroup* (A, ∇, Δ) has a *multiplication* $\nabla\colon A \otimes A \to A$ and a *comultiplication* $\Delta\colon A \to A \otimes A; x \mapsto x^L \otimes y^R$ which are mutually homomorphic. Its *left composite* is

$$\mathsf{G}\colon A \otimes A \xrightarrow{\Delta \otimes 1_A} A \otimes A \otimes A \xrightarrow{1_A \otimes \nabla} A \otimes A \tag{5}$$

and its *right composite* is

$$\partial\colon A \otimes A \xrightarrow{1_A \otimes \Delta} A \otimes A \otimes A \xrightarrow{\nabla \otimes 1_A} A \otimes A\,; \tag{6}$$

both are required to be invertible. As a quantum quasigroup in $(\mathbf{Set}, \times, \top)$, a classical quasigroup $(Q, \cdot, /, \backslash)$ has *diagonal* comultiplication $a \mapsto a \otimes a$ and left composite $a \otimes b \mapsto a \otimes a \cdot b$, inverted by $c \otimes d \mapsto c \otimes c \backslash d$ [6, Prop. 3.11].

The tightest version of a quantum quasigroup is a *quantum* T-*quasigroup* $(Q, \nabla_i, \Delta_i)_{i \in \mathbb{Z}/3}$, which consists of three quantum quasigroups indexed by the additive group of residues modulo 3, such that the *composite diagrams*

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\partial_i} & A \otimes A \\ {\scriptstyle\tau}\uparrow\downarrow & & \uparrow\downarrow{\scriptstyle\tau} \\ A \otimes A & \xleftarrow[\mathsf{G}_{i+1}]{} & A \otimes A \end{array} \tag{7}$$

commute in $\mathbf{V}$ for each $i \in \mathbb{Z}/3$ [7, (3.3)]. Thus, $\tau \mathsf{G}_{i+1} \tau$ is identified as the inverse of the right composite ∂_i, while $\tau \partial_{i-1} \tau$ is identified as the inverse of the left composite G_i. For example, a classical quasigroup $(Q, \cdot, /, \backslash)$ determines a quantum T-quasigroup in $(\mathbf{Set}, \times, \top)$, with respective multiplications

$$\nabla_0\colon Q \otimes Q \to Q; x \otimes y \mapsto x \circ y\,, \tag{8}$$

$$\nabla_1\colon Q \otimes Q \to Q; x \otimes y \mapsto x \backslash y\,, \tag{9}$$

$$\nabla_2\colon Q \otimes Q \to Q; x \otimes y \mapsto x / y \tag{10}$$

and the diagonal comultiplication Δ_i for each $i \in \mathbb{Z}/3$. Note the use of the opposite quasigroup multiplication for the index 0 or 3.

A quantum T-quasigroup $(Q, \nabla_i, \Delta_i)_{i \in \mathbb{Z}/3}$ in $\big(\underline{S}, \oplus, \{\,0\,\}\big)$ is said to be *linear*. In matrix form, the multiplications

$$\nabla_i\colon Q \oplus Q \to Q; \begin{bmatrix} x & y \end{bmatrix} \mapsto \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} \rho_i \\ \lambda_i \end{bmatrix} \tag{11}$$

and comultiplications

$$\Delta_i\colon Q \to Q \oplus Q; \begin{bmatrix} x \end{bmatrix} \mapsto \begin{bmatrix} x \end{bmatrix} \begin{bmatrix} L_i & R_i \end{bmatrix} \tag{12}$$

are given by automorphisms $\lambda_i, \rho_i, L_i, R_i$ of Q. Their mutual homomorphism amounts to the mutual commutativity of the two subalgebras $S(\lambda_i, \rho_i)$ and $S(L_i, R_i)$ within the endomorphism ring $\underline{\underline{S}}(Q,Q)$ of Q [6, Prop. 3.39]. The commutativity of the diagrams (7) is equivalent to the equations

$$R_i^{-1} = L_{i+1}\,, \qquad R_i R_{i+1} \rho_{i+1} = -L_i \lambda_i \lambda_{i+1}\,, \tag{13}$$

$$\rho_i^{-1} = \lambda_{i+1}\,, \qquad R_{i+1} \rho_{i+1} \rho_i = -L_{i+1} L_i \lambda_i \tag{14}$$

for each $i \in \mathbb{Z}/_3$ [7, Lemma 4.2].

Theorem 1. [7, Th. 4.7] *For an S-module Q, linear quantum T-quasigroup structures on Q are equivalent to a set $\{ R_0, R_1, R_2, \rho_0, \rho_1, \rho_2 \}$ generating a subgroup B of the automorphism group $\underline{\underline{S}}(Q,Q)^*$ of Q such that:*

1. *The subset $\{ R_0, R_1, R_2 \}$ commutes with the subset $\{ \rho_0, \rho_1, \rho_2 \}$;*
2. *There is a central element Ω in the group B such that the equations*

$$\Omega = R_{i-1} R_i R_{i+1} = (-\rho_{j-1}^{-1})(-\rho_j^{-1})(-\rho_{j+1}^{-1}) \tag{15}$$

hold for each $i, j \in \mathbb{Z}/_3$.

In the context of Theorem 1, a classical linear quasigroup (i.e., with diagonal comultiplications) has $\Omega = R_0 = R_1 = R_2 = 1_Q$. Writing elements of $A = Q^3$ as row matrices $a = \begin{bmatrix} a_1 & a_2 & a_3 \end{bmatrix}$, the classical semisymmetrization (2) may be expressed in the form $(a \oplus b)\nabla = a\mathrm{P} + b\Lambda$ with matrices

$$\mathrm{P} = \begin{bmatrix} 0 & 0 & \rho_3 \\ \rho_1 & 0 & 0 \\ 0 & \rho_2 & 0 \end{bmatrix} \quad \text{and} \quad \Lambda = \begin{bmatrix} 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \\ \lambda_1 & 0 & 0 \end{bmatrix}. \tag{16}$$

The first matrix, sometimes described as the *Rho-matrix* in this setting, is read as (capital) "rho." By (14), $\Lambda\mathrm{P} = 1_A$. As an initial step in the quantization of web geometry, we ask which linear quantum quasigroup structures provide comultiplications to extend this semisymmetrization multiplication ∇.

It is convenient to introduce a *circulant notation*

$$C(\alpha, \beta, \gamma) := \begin{bmatrix} \alpha & \rho_3 \beta \rho_1^{-1} & \gamma \\ \rho_1 \gamma \rho_3^{-1} & \rho_1 \alpha \rho_1^{-1} & \rho_2^{-1} \beta \rho_3 \\ \beta & \rho_3^{-1} \gamma \rho_2 & \rho_3^{-1} \alpha \rho_3 \end{bmatrix}, \tag{17}$$

in which α, β, γ are endomorphisms of the S-module Q. Such a matrix is said to be *monomial* if two of these endomorphisms are zero.

Theorem 2. [8, Th. 3.13] *The comultiplication*

$$\Delta \colon A \to A \oplus A; \begin{bmatrix} a \end{bmatrix} \mapsto \begin{bmatrix} a \end{bmatrix} \begin{bmatrix} L & L^{-1} \end{bmatrix} \tag{18}$$

extends ∇ *if and only if* $L = C(\alpha, \beta, \gamma)$ *is invertible.*

The classical semisymmetrization corresponds to $L = 1_A = C(1_Q, 0_Q, 0_Q)$. Now, a quantum quasigroup is said to be *quantum semisymmetric* if the diagram

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\supset} & A \otimes A \\ {\scriptstyle\tau}\uparrow\downarrow & & \uparrow\downarrow{\scriptstyle\tau} \\ A \otimes A & \xleftarrow[\mathsf{G}]{} & A \otimes A \end{array} \tag{19}$$

commutes [2, Def'n. 4.11]. In Theorem 2, this means that $L^3 = -\mathrm{P}^3 = \Omega^{-1}$.

Theorem 3. [8, Th. 4.1] *Monomial quantum semisymmetric extensions are*

$$L = C(\Omega^{-1/3}, 0, 0) = \Omega^{-1/3} 1_A \,, \tag{20}$$

$$L = C(0, -\rho_3^{-1}\Omega^{2/3}, 0) \,, \tag{21}$$

$$L = C(0, 0, -\zeta\rho_3) \,. \tag{22}$$

Here, the S*-automorphism* ζ *of* Q *with* $\zeta^3 = 1_Q$ *commutes with* ρ_1, ρ_2, *and* ρ_3.

If the linear quasigroup structure comes from real or complex affine geometry, Bezout's Theorem from algebraic geometry yields a complete classification of the quantum semisymmetric extensions [8, Th. 5.11]. There are 27 such in the complex case. In the real case, there are only the 3 monomial comultiplications from Theorem 3.

References:

1. V.D. Belousov. *Algebraic nets and quasigroups* (Russian). Ştiinţa, Chişinău, 1971.
2. B. Im, A. Nowak, J.D.H. Smith. Symmetry classes of quantum quasigroups. *J. Pure Appl. Alg.*, **225** (2024), 107722. DOI: 10.1016/j.jpaa.2024.107722
3. C.B. Jay. Languages for monoidal categories. *J. Pure Appl. Algebra* **59** (1989), 61–85.
4. J.D.H. Smith, A.B. Romanowska. *Post-Modern Algebra*. Wiley, New York, NY, 1999.
5. J.D.H. Smith. Quasigroup homotopies, semisymmetrization, and reversible automata. *Internat. J. Algebra Comput.*, **18** (2008), 1203–1221.
6. J.D.H. Smith. Quantum quasigroups and loops. *J. Algebra*, **456** (2016), 46–75.
7. J.D.H. Smith. Equational quantum quasigroups. *Algebr. Represent. Theory*, (2024), 10300, 33 pages. DOI: 10.1007/s10468-024-10300-x
8. J.D.H. Smith. Quantization of web geometry: semisymmetrization of linear quantum quasigroups. Preprint, 2025.

QUASIGROUPS AND LOOPS UP TO ORDER 5

Sokhatsky Fedir

Pidstryhach Institute for Applied Problems of Mechanics and Mathematics of NASU, Ukraine

fmsokha@ukr.net

"The counting of Latin squares has a long history, but the published accounts contain many errors. Euler in 1782, and Cayley in 1890, both knew the number of reduced Latin squares up to order five. In 1915, MacMahon approached the problem in a different way, but initially obtained the wrong value for order five." [1]

Unfortunately, the author does not know of an analytical proof of the number of quasigroups to order 5.

Knowing the number of quasigroups of a certain order is too little information for their study and application. It is necessary to have formulas for their definition, and it is desirable that this formula be canonical, that is, for an arbitrary quasigroup of a certain class such a formula must exist and be unique. Thus, one of the main problems is the following

"*To find canonical formulas determining all quasigroups of a certain class.*"

Here, we give canonical formulas for each quasigroup up to order five. The number of quasigroups is obtained as a corollary.

Notation: $Z_m := \{0, 1, 2, \ldots, m-1\}$; S_m is the symmetric group of order m, i.e. a set of all permutations of Z_m; $S'_{m-1} := \{\alpha \in S_m \mid \alpha(0) = 0\}$; $\mathbb{Z}_m := (Z_m; +, 0)$ is additive group modulo m. Cross-section of a partition π of a set is the set of all representatives from each element of π.

Theorem 1. *Let $(Q; *)$ be a quasigroup and 0 be an element of the set Q. Then*

$$x * y = \alpha(x) \diamond \beta(y) \qquad \text{with} \quad \alpha(0) = 0, \;\; 0 \diamond x = x \diamond 0 = x \tag{1}$$

is a canonical decomposition of the quasigroup.

In other words for each quasigroups defined on Q and for each element $0 \in Q$, there exists a unique triplet $(\diamond, \alpha, \beta)$ with (1).

Corollary. *The number of quasigroups of order m is equal to*

$$\frac{m! \cdot (m-1)!}{|\mathfrak{L}|},$$

where $\mathfrak{L}$ is the set of all 0-loops of order m.

Group isotopes

Theorem 2. *Let ω be the set of all quasigroups isotopic to a group $G := (Z_m; \star, 0)$ and T be a cross-section of $S'_{m-1}/AutG$. Then*

$$x * y = \gamma(\alpha^{-1}(x) \star \beta^{-1}(y))$$

is a canonical decomposition of $(Z_m; *) \in \omega$, if $\alpha \in S'_{m-1}$ and $\gamma \in T$.

Corollary 1. *Let $G := (Q; +, 0)$ be a group of the order m. Then there are exactly*

$$\frac{m! \cdot \big((m-1)!\big)^2}{|AutG|}$$

different isotopes of the group G.

For example, there are exactly

$$\frac{7! \cdot (6!)^2}{6} = \frac{5040 \cdot (720)^2}{6} = 435\,456\,000$$

group isotopes of order 7.

Semisymmetric anticommutative (SA) loops

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

Semisymmetricity:
$x \circ (y \circ x) = y$, equiv. $(x \circ y) \circ x = y$,
equiv. $\circ = \overset{\ell}{\circ} = \overset{r}{\circ}$, equiv. $\overset{s}{\circ} = \overset{s\ell}{\circ} = \overset{sr}{\circ}$.
Anticommutativity:
$x \circ y = y \circ x \Rightarrow (x = 0 \vee y = 0 \vee x = y)$,
therefore $\circ \neq \overset{s}{\circ}$. (2)

Theorem 3. *If (α, β, γ) is an isotopism of SA loops, then $\alpha = \beta = \gamma$. Each autotopism of an SA loop is its automorphism.*

Lemma 4. *Let $\mathcal{L} := (Z_m; \circ, 0)$ be an SA loop. Then*

1. *each loop isotopic to $\mathcal{L}$ is isomorphic to a loop $(Z_m; \underset{ab}{\triangle}, a \circ b)$, where*

$$x \underset{ab}{\triangle} y := (b \circ x) \circ (y \circ a); \tag{3}$$

2. *the operations $\underset{ab}{\triangle}$ and $\underset{a'b'}{\triangle}$ are isomorphic if and only if there exists an automorphism θ of the SA loop such that $a' = \theta(a)$ and $b' = \theta(b)$.*

Roughly speaking, isomorphy relation on the operation set $\{\underset{ab}{\triangle} \mid a, b \in Q\}$ coincides with the action of the group $Aut(Z_m; \circ, 0)$ on the set $Q \times Q$.

Theorem 5. *Let an SA loop $(Z_m; \circ, 0)$ be generated by any two different nonzero elements. Then each loop isotopic to $(Z_m; \circ, 0)$ is isomorphic to exactly one of the loops: $(Z_m; \circ, 0)$, $(Z_m; \underset{01}{\triangle}, 1)$, $(Z_m; \underset{10}{\triangle}, 1)$, $(Z_m; \underset{11}{\triangle}, 0)$, $(Z_m; \underset{12}{\triangle}, 1 \circ 2)$, where*

$$\begin{aligned} x \underset{01}{\triangle} y &:= (1 \circ x) \circ (y \circ 0); & x \underset{10}{\triangle} y &:= (0 \circ x) \circ (y \circ 1); \\ x \underset{11}{\triangle} y &:= (1 \circ x) \circ (y \circ 1); & x \underset{12}{\triangle} y &:= (2 \circ x) \circ (y \circ 1). \end{aligned} \tag{4}$$

Theorem 6. *Let $\varkappa$ be the isotopy class containing an SA loop $\mathcal{L} := (Z_m; \circ, 0)$ and Π be a cross-section of $S'_{m-1}/Aut\mathcal{L}$. Then*

$$f(x, y) = \gamma(\alpha^{-1}(x) \circ \beta^{-1}(y)) \tag{5}$$

is a canonical decomposition of $(Z_m; f) \in \varkappa$, if $\gamma \in \Pi$.

Quasigroups of small orders

Quasigroups on $Z_2 := \{0, 1\}$. There are only two quasigroups on Z_2 – addition modulo 2 (exclusive disjunction) and the logical equivalency. The addition is a 0-loop and it is a group. The canonical decomposition of these quasigroups is

$$x * y = x + \beta y, \qquad \beta \in S_2.$$

Quasigroups on $Z_3 := \{0, 1, 2\}$. There is only one 0-loop on Z_3 – addition modulo 3. The canonical decomposition of these quasigroups is

$$x * y = \pm x + \beta y, \qquad \beta \in S_3.$$

Therefore, there are 12 quasigroups on three-element set.

Quasigroups on $Z_4 := \{0, 1, 2, 3\}$. Each quasigroup is isotopic to either the cyclic group $\mathbb{Z}_4$ or Klein four-group $\mathbb{Z}_2 \times \mathbb{Z}_2$ [1,2,3].

Corollary 2. *Each isotope of cyclic group $\mathbb{Z}_4$ coincides with exactly one of the quasigroups $(Z_4; f)$ with*

$$f(x, y) = \gamma(\alpha^{-1}(x) + \beta^{-1}(y)),$$

where $\alpha \in S'_3$, $\beta \in S_4$, $\gamma \in \{\iota, (12), (13)\}$.

Corollary 3. *Each isotope of Klein four-group $\mathbb{Z}_2\times\mathbb{Z}_2$ coincides with exactly one of the quasigroup $(\mathbb{Z}_2^2; g)$ with*

$$g(x,y)=\alpha^{-1}(x)\oplus\beta^{-1}(y),$$

where $\alpha\in S_3'$, $\beta\in S_4$.

Consequently, the number of quasigroups isotopic to $\mathbb{Z}_4$ equals $3\cdot 6\cdot 24=432$, quasigroups isotopic to Klein four-group $\mathbb{Z}_2\times\mathbb{Z}_2$ is $6\cdot 24=144$. Thus, there are $432+144=576$ quasigroups of order 4.

Theorem 7. [3] *Every quasigroup operation f on the carrier set $Z_2^2=\{00,01,10,11\}$ is uniquely defined by one of the following formulaes:*

$$f(\bar{x},\bar{y})=\bar{x}A\oplus\bar{y}B\oplus\bar{a}; \tag{1}$$

$$f(\bar{x},\bar{y})=(\bar{x}A+\bar{y}B+\bar{a})C; \tag{2}$$

where $(\oplus)$, $(+)$ are additive groups of the rings $\mathbb{Z}_2\times\mathbb{Z}_2$ and $\mathbb{Z}_4$, $\bar{a}\in Z_2^2$, $A,B\in\mathbb{U}$, $C\in\mathbb{V}$, where

$$\mathbb{V}:=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\},$$

$$\mathbb{U}:=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}.$$

Note that $+$ is addition modulo 4, but $\oplus$ denotes component-wise addition modulo 2.

Quasigroups on $Z_5:=\{0,1,2,3,5\}$. It is well-known [1, 2] that the set of all quasigroups of order 5 is divided into two isotopy classes. Therefore, each quasigroup of order 5 is isotopic to either the group $\mathbb{Z}_5$ or an arbitrary nonassociative loop, say to SA loop $\mathcal{L}:=(Z_5;\circ,0)$ defined by (2). Nevertheless, we have proved

Theorem 8. *Every quasigroup of order 5 is isotopic to either the group $\mathbb{Z}_5$ or SA loop (2).*

Theorem 9. *The automorphism group of SA loop $(Z_5;\circ,0)$ (2) is the alternating subgroup A_4' of S_4': namely,*

$$\mathrm{Aut}(Z_5;\circ,0)=\{\theta_{ab}\mid\ a\neq b,\ a,b=1,2,3,4\}=A_4',$$

$$\theta_{ab}:=\begin{pmatrix}0&1&2&3&4\\0&a&b&a\circ b&b\circ a\end{pmatrix}.$$

Corollary 4. *Each loop isotopic to SA loop (2) is isomorphic to exactly one of the loops $(Z_5;\circ,0)$, $(Z_5;\underset{01}{\triangle},1)$, $(Z_5;\underset{10}{\triangle},1)$, $(Z_5;\underset{11}{\triangle},0)$, $(Z_5;\underset{12}{\triangle},3)$ defined by (4).*

Corollary 5. *Each quasigroup isotopic to SA loop* (2) *coincides with exactly one of the quasigroups* (5)*, where* $\alpha, \beta \in S_5$ *and*

$$\gamma \in \{\iota,\ (01),\ (02),\ (03),\ (04),\ (12),\ (012),\ (021),\ (03)(12),\ (04)(12)\}.$$

Consequently, the number of quasigroups isotopic to SA loop (2) equals

$$(5!)^2 \cdot 10 = 144\,000.$$

Corollary 6. *Every quasigroup isotopic to* $\mathbb{Z}_5$ *coincides with exactly one quasigroup* $(Z_5; f)$*, where*

$$f(x, y) := \gamma(\alpha^{-1}(x) + \beta^{-1}(y)),$$

$\alpha \in S_4'$, $\beta \in S_5$ *and* $\gamma \in \{\iota, (12), (13), (14), (23), (24)\}$.

Consequently, the number of group isotopes of the order 5 equals $24 \cdot 120 \cdot 6 = 17\,280$. Therefore, the number of all quasigroups of order 5 is

$$144\,000 + 17\,280 = 161\,280.$$

References:

1. Wikipedia. Small Latin squares and quasigroups. https://en.wikipedia.org/wiki

2. F. M. Sokhatsky, H. V. Krainichuk, V. A. Luzhetsky, Canonical and matrix figuration of quasigroups of the fourth order. *Applied problems of mechanics and mathematics* вЂ“ 2024. вЂ“ Issue 22. вЂ“ P. 95вЂ“105.(Ukrainian)

FORMULAS FOR DETERMINING SOME QUASIGROUPS OF THE ORDER 8

Sokhatsky Fedir, Buniak Bohdan *

[1] *Pidstryhach Institute for Applied Problems of Mechanics and Mathematics of NASU, Ukraine*

[2] *Department of Information Security of Vinnytsia National Technical University, Ukraine*

fmsokha@ukr.net, bbuniak@ukr.net

This is a continuation of the research from [1]. A semisymmetric anticommutative loop $(Q; \circ, 0)$ is called *SA loop*.

* *Speaking author*: Buniak B.

Theorem 1. *Every SA loop of order 8 is isomorphic to* $(Z_8;\circ,0)$*, where* $Z_8 := \{0,1,\ldots,7\}$ *and*

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

Semisymmetricity:
$x \circ (y \circ x) = y$ is equivalent to
$(x \circ y) \circ x = y$

Anticommutativity:
$x \circ y = y \circ x \Rightarrow$
$\Rightarrow (x = 0 \vee y = 0 \vee x = y).$ (1)

Theorem 2. *Each automorphism of the SA loop* $(Z_8;\circ,0)$ *equals*

$$\theta_{ab} := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & a & b & L_a(b) & L_a^2(b) & L_a^3(b) & L_a^4(b) & L_a^5(b) \end{pmatrix},$$

where $L_a(b) := a \circ b$*,* $a, b \in Z_8$ *and so the automorphism group has 42 elements.*

Theorem 3. *Each loop isotopic to* $(Z_8;\circ,0)$ *is isomorphic to exactly one of the following loops:* $(Z_8;\circ,0)$*,* $(Z_8;\underset{01}{\triangle},1)$*,* $(Z_8;\underset{10}{\triangle},1)$*,* $(Z_8;\underset{11}{\triangle},0)$*,* $(Z_8;\underset{12}{\triangle},3)$*, where*

$$x \underset{01}{\triangle} y := (1 \circ x) \circ (y \circ 0); \qquad x \underset{10}{\triangle} y := (0 \circ x) \circ (y \circ 1);$$
$$x \underset{11}{\triangle} y := (1 \circ x) \circ (y \circ 1); \qquad x \underset{12}{\triangle} y := (2 \circ x) \circ (y \circ 1).$$

Theorem 4. *Each quasigroup isotopic to* $(Z_8;\circ,0)$ *coincides with exactly one of the following*

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

where γ *belongs to a cross-section of* $S_7'/Aut\mathcal{L}$*,* S_7' *is the set of all permutations* δ *of* Z_8 *such that* $\delta(0) = 0$ *and* α, β *are permutations of* Z_8*.*

Corollary. *There are 195 084 288 000 quasigroups isotopic to* $(Z_8;\circ,0)$*.*

Theorem 5. *Let* ω *be the set of all quasigroups isotopic to a group* $G := (Z_8;+,0)$ *and* T *be a cross-section of* $S_8'/AutG$ *(*$S_8' := \{\alpha \mid \alpha(0) = 0\}$*), then*

$$x * y = \gamma(\alpha^{-1}(x) + \beta^{-1}(y)) \tag{2}$$

is a canonical decomposition of $*$*, if* $\alpha(0) = \gamma(0) = 0$ *and* $\gamma \in T$*.* There are five groups of the order 8 and so there are

$$8! \cdot (7!)^2 \left(\frac{1}{4} + \frac{2}{8} + \frac{1}{24} + \frac{1}{168}\right) = 8! \cdot (7!)^2 \cdot \frac{23}{42} = 560\,867\,328\,000.$$

different isotopes of order 8. Thus, we found formulas for 560 867 328 000 + 195 084 288 000 = 755 951 616 000 quasigroups of the order 8.

References:

1. Fedir Sokhatsky. Quasigroups and loops up to order 5. (Here)

SUPERNILPOTENT LOOPS: INTRODUCTION

Stanovský David

Charles University, Prague, Czechia

david.stanovsky@matfyz.cuni.cz

The classical approach to nilpotence of algebraic structures is recursive: define the center, then a central series, and let the class of nilpotence be the length of a shortest central series. In groups, the center consists of all elements that commute with everything. In loops, the center consists of all elements that commute and associate with everything.

In 1970s, universal algebraists found a suitable syntactic condition to define the center of any algebra. However, many characteristic properties of nilpotent groups do not carry over to this more general setting. Perhaps most important among such properties is the fact that there are finite nilpotent algebras, loops in particular, which do not admit a direct decomposition into p-primary components. This issue was addressed relatively recently in a novel way [1] that is based on another fundamental property: the limited essential arity of absorbing polynomial operations. An algebra is called *k-supernilpotent* if all absorbing polynomials of arity bigger than k are constant.

For groups, k-supernilpotence coincides with k-nilpotence. Under mild universal algebraic assumptions (which cover groups and loops), supernilpotence implies nilpotence and a finite algebra is supernilpotent if and only if it is a direct product of nilpotent algebras of prime power order. Therefore, in loops, supernilpotence is a stricly stronger property.

In the present talk, based on the paper [2] with Žaneta Semanišinová, I will introduce the abstract concept of supernilpotence, I will show how it applies in loops, and relate it to existing concepts, namely, central nilpotence and nilpotence of the multiplication group.

References:

1. E. Aichinger and N. Mudrinski, *Some applications of higher commutators in Mal'cev algebras*, Algebra Universalis **63** (2010), no. **4**, 367–403.

2. Ž. Semanišinová and D. Stanovský, *Three concepts of nilpotence in loops*, Results in Math. 78/4 (2023), Paper No. 119, 15 p.

ON THE EXISTENCE AND UNIQUENESS OF ONE INVERSION MATRIX OF AN n-IP LOOPS

Ursu Leonid

Tehnical University of Moldova, Chisinau, Republic of Moldova

It is known that an n-IP quasigroup has more than one inversion matrix [1]. The existence and uniqueness of the inversion matrix $[II, j]$ is proved, the inversion substitutions of which keep invariant the loop unit. This matrix, as in the binary case, allows one to study n-IP loops more easily and deeply.

A quasigroup $Q(A)$ of arity n $(n \geq 2)$ is called an n-IP-quasigroup if there exist permutations $\nu_{ij}; i, j \in \overline{i,j}$ of the set Q such that the following identities hold

$$A(\nu_{ij}x_j{}_{j=1}^{i-1}, A(_i^n), \nu_{ij}x_j{}_{j=i+1}^{n}) = x_i, \quad j \in \overline{1,n} \qquad (1)$$

for any $x_1^n \in Q^n$, where $\nu_{ii} = \nu_{i+1i} = \varepsilon$ (the identity permutation of the set Q) [1].

The substitutions ν_{ij} are called inversion substitutions, and

$$\nu_{ij} = \begin{bmatrix} \varepsilon & \nu_{12} & \nu_{13} & \dots & \nu_{1n} & \varepsilon \\ \nu_{21} & \varepsilon & \nu_{23} & \dots & \nu_{2n} & \varepsilon \\ \dots & & & & & \\ \nu_{n1} & \nu_{n2} & \nu_{n3} & \dots & \varepsilon & \varepsilon \end{bmatrix}$$

is the inversion matrix, the i-th row $(i \in \overline{1,n})$ of this matrix is вТЭ<вТЭ<called the i-th inversion system.

A quasigroup B is called an isotope of a quasigroup A (A and B have the same arity n and are defined on the same set Q) if there exists a sequence $T = (\alpha_1^{n+1})$ of permutations of the set Q such that $B(x_1^n) = \alpha_{n+1}^{-1}A(\alpha_i x_i)\}_{i=1}^n$ $\forall\ x_1^n \in Q^n$ and is denoted by $B = A^T$ [1].

If $B = A$, then by the definition of the n-quasigroup, in the equality

$$A(x_1^n) = x_{n+1} \qquad (2)$$

every n elements uniquely determine the $(n+1)$-th element.

Let us fix a number i $(i \in \overline{1,n})$. Therefore, $x_1^{i-1}, x_{n+1}, x_{i+1}^n$ uniquely determines the element x_i. We obtain a new operation that defines the correspondence $\{x_1^{i-1}, x_{n+1}, x_{i+1}^n\} \to x_i$. We denote this operation by ${}^{\pi_i}A$. Thus we have

$${}^{\pi_i}A(x_1^{i-1}, x_{n+1}, x_{i+1}^n) = x_i \qquad (3)$$

The operation ${}^{x_i}A$ defined by equality (3) is equivalent to equality (2) is called the i-th *inverse* operation to the operation A, which is also a quasigroup.

If in (1) we replace x_j with $\nu_{ij}x_j$, x_i with $A(x_1^n)$, then we obtain

$$A(\{\nu_{ij}x_j\}_{j-1}^{n_1}) = A(x_1^n),$$

that is

$$T_i^2 = \{\nu_{i1}^2, \nu_{i2}^2, \ldots, \nu_n^2, \varepsilon\} \qquad (4)$$

is am autotopy of $Q(A)$.

If in (1) we replace x_j with $\nu_{ij}x_j$ then, according to (4), we obtain

$$\{^{\pi_i}A(x_1^n) = A(\{\nu_{ij}x_j\}_{j=1}^b)\},$$

that is, x_i with $A(x_1^n)$.

Therefore, $x_1^{i-1}, x_{n+1}, x_{i+1}^n$ uniquely determine the element x_i. We obtain a new operation defined by the correspondence $\{x_1^{i-1}, x_{n+1}, x_{i+1}^n\} \Rightarrow x_i$.

If in (1) we replace x_j with $\nu_{ij}x_j$, then, according to (4), we get

$$\{^{\pi_i}A(x_1^n) = A(\{\nu_{ij}x_j\}_{j=1}^b)\},$$

that is, x_i with $A(x_1^n)$. By analogy with isotopy, if $A^{(\pi_i,T_i)} = B$, then B is called an isostrophe of the n-quasigroup $Q(A)$. equalities (1), (5) and (6) are equivavalent. Therefore any of these can be taken as definition of *n-IP*-quasigroup [1].

Note that an *n-IP*-quasigroup has more than one inversion matrix. It is known [1] that the multiplication of two inversion matrices (in the sense of multiplication of the corresponding permutations) is an autotopy matrix for $Q(A)$), and the multiplication of an inversion matrix by an autotopy matrix is an inversion matrix for an $n - IP$-quasigroup $Q(A)$.

An element $e \in Q$ satisfying the equalities

$$A(\overset{i-1}{e}, x, \overset{n+i}{e}) = x$$

for any $x \in Q$ and $i \in \overline{1,n}$, is called a *unit* of an *n-loop* $Q(A)$. It is known [1] that, unlike a binary operation, an n-loop can have more than one unit. For an n-IP-loop $Q(A)$ with unit e[1], the permutations I_{ij} on the set Q are defined by the equalities

$$A(\overset{i-1}{;}x, \overset{j-i-1}{;}J_{ij}x, \overset{n-j}{e}) = e$$

for any $i, j \in \overline{1,n}$ and any $x \in Q$. If it is happened, the first constructed example of a 3-*JP*-loop has the inversion matrix $[J_{ij}]$.

In this connection, Prof. V.D. Belousov formulated the question: *find out if among all inversion matrices of an n-IP-loop with unit e there is always (becomes, turns into, is) the inversion matrix* $[J_{ij}]$?

Theorem 1. *An invertibility matrix ν_{ij} of a multiary IP-uniloop $(Q; A, e)$ coincides with $[I_{ij}]$ matrix if and only if $\nu_{ij}(e) = e$ for all $i, j \in \overline{1, n}$.*

References:

1. V. D. Belousov, n-ary quasigroups. Ştiinţa, Chisinau, 1972.

SUPERNILPOTENT LOOPS: FINITE AXIOMATIZATION

Vojtěchovský Petr

University of Denver, USA

petr.vojtechovsky@du.edu

Supernilpotence is a strenghtening of the notion of nilpotence based on absorption properties of polynomials. For instance, the commutator $[x, y]$ is absorbing since it returns 1 whenever $x = 1$ or $y = 1$. It turns out that supernilpotent groups of class k are precisely nilpotent groups of class k, but this is not the case for general loops.

I will present a short equational basis for supernilpotent loops of class 3 in which linearizers play an important role, in addition to commutators and associators.

I will also discuss the problem of a finite equational basis for supernilpotent loops of class > 3; here we give up on efficiency, employ linearizers recursively and introduce new associators that are more suitable for the inductive argument. This is joint work with David Stanovský.

SUBSQUARES OF LATIN SQUARES

Wanless Ian, Allsop Jack *
Monash University, Australia
E-mail: 1ian.wanless@monash.edu

A *subsquare* of a Latin square is any submatrix which is itself a Latin square. Every Latin square of order n trivially has n^2 subsquares of order 1 and one subsquare of order n. Any subsquare between these two extremes is *proper*. Subsquares of order 2 are called *intercalates*. A Latin square without intercalates is said to be N_2 and a Latin square without proper subsquares is said to be N_∞.

In this talk I will survey results and open questions relating to the number of subsquares in a Latin square. We might be trying to minimise or maximise this number, or to understand its distribution among all Latin squares of a given order. The existence question for N_2 Latin squares was settled a long time ago, but the corresponding question for N_∞ Latin squares has only recently been settled. There has also been exciting progress on understanding the distribution of subsquares among Latin squares of a given order. But some questions remain.

ALGEBRAIC PROPERTIES OF A CLASS OF POWER ASSOCIATIVE LCC-LOOPS AND SOME ASSOCIATED TOTAL INNER MAPPING GROUP QUESTIONS

Tèmítópé Jaiyéọlá*, Olufemi George,
Benard Osoba, Emmanuel Ilojide
Obafemi Awolowo University, University of Lagos, Bells University of Technology, Federal University of Agriculture, Nigeria.
tjayeola@oauife.edu.ng, oogeorge@unilag.edu.ng,
b_osoba@bellsuniversity.edu.ng, ilojidee@funaab.edu.ng

In this paper, we investigated the algebraic properties of a class of LCC-loops (and its dual) which is power associative, tagged 'twist' of LWPC (RWPC) viz. LTWC (RTWC). Its relationship with Frute and crazy loop was discovered. LTWC-loop was shown to be a class of loop which falls into the Syrbu and Grecu (2019) first answer to a question of Stanovský and Vojtěchovský (2014)-minimal generating set for the total inner mapping group of a loop. In addition, we showed that the class of LTWC-loop also provides an alternative solution to 2014 question and in fact, the inner automorphism group of a LTWC-loop

* *Speaking author*: Wanless I.
* *Speaking author*: T.G. Jaiyéọlá

is generated by just one inner mapping. Generalized forms of the left (right) alternative property and flexibility property were introduced and studied in this class of loop. We also explore the properties of the left and right translation of this class of loop and proved some results useful for the construction a finite loop belonging to this same class.

The LWPC and the RWPC loops were introduced by Phillips in [5]. George et al. [1] showed that each of these two loop identities described by

$$\begin{aligned} (xy \cdot x) \ \cdot xz &= x((yx \cdot x)z) \qquad \text{(LWPC)} \\ zx \ \cdot (x \cdot yx) &= (z(x \cdot xy))x \qquad \text{(RWPC)} \end{aligned}$$

is power associative. They established that the following equations of identities are true in loops

$$\text{(LWPC)} = \text{(LCC)} + (\text{P}_\lambda) \text{ and } \text{(RWPC)} = \text{(RCC)} + (\text{P}_\rho), \text{ where}$$

$$\underbrace{(xy \cdot x)x = x(yx \cdot x)}_{P_\lambda} \qquad \underbrace{x(x \cdot yx) = (x \cdot xy)x}_{P_\rho}$$

George and Jaíyéọlá [2] investigated two identities (Q_{12} and Q_7) similar to LWPC and RWPC. These identities may be seen as 'twist' of LWPC and RWPC, a possible name for them might be LTWC and RTWC.

$$\begin{aligned} x((x \cdot yx)z) &= (x \cdot xy) \cdot xz \qquad \text{(LTWC)} \\ (y(xz \cdot x))x &= yx \cdot (zx \cdot x) \qquad \text{(RTWC)} \end{aligned}$$

Similarly, they showed that the following equations of identities are true in loops

$$\text{(LTWC)} = \text{(LCC)} + (\text{P}_\rho) \text{ and } \text{(RTWC)} = \text{(RCC)} + (\text{P}_\lambda).$$

Likewise, since the equation of identities (LWPC)+(RWPC) = (CC) + (WIP) is true in loops, so also is (LTWC)+(RTWC) = (CC) + (WIP).

The purpose of this work is to introduce and study generalized forms of the left (right) alternative property and flexibility properties in LTWC-loop and to show that the inner automorphism group of a LTWC-loop is generated by just one inner mapping.

In this work, we shall show that LTWC-loop is a class of loop which falls into the Syrbu and Grecu's first answer to Question 1.2. In addition, the class of LTWC-loop also provides an alternative solution to Question 1.2. in fact, the inner automorphism group of a LTWC-loop is generated by just one inner mapping.

In a LTWC (RTWC)-loop, the following are equivalent:

1. Flexibility.

2. RAP (LAP).

3. RIP (LIP).

Hence, any LTWC (RTWC)-loop which obeys any of them is an extra loop. Any LTWC (RTWC)-loop is a Moufang loop if and only if it is an extra loop. In a LTWC-loop G, $N_\mu(G) = N_\lambda(G)$. While in a RTWC-loop G, $N_\mu(G) = N_\rho(G)$.

These observations necessitate the introduction of the properties in Definition 1 for investigation in addition to the fact that it was shown in [3] that a LTWC-loop is power associative.

Definition 1. *A power associative loop G is said to obey*

1. *LAP_n-property if $x \cdot x^n y = x^{n+1} y$ where $n \in \mathbb{Z}$, $\forall\ x, y \in G$.*

2. *LAP^n-property if $x^n \cdot xy = x^{n+1} y$ where $n \in \mathbb{Z}$, $\forall\ x, y \in G$.*

3. *$FLEX^n$-property if $x^n \cdot yx = x^n y \cdot x$ where $n \in \mathbb{Z}$, $\forall\ x, y \in G$.*

4. *$FLEX_n$-property if $x \cdot yx^n = xy \cdot x^n$ where $n \in \mathbb{Z}$, $\forall\ x, y \in G$.*

5. *$FLEX_{(2,n+1)}$-property if $x^2 y \cdot x^n = x^2 \cdot yx^n$ where $n \in \mathbb{Z}$, $\forall\ x, y \in G$.*

6. *RAP^n-property if $yx \cdot x^n = yx^{n+1}$ where $n \in \mathbb{Z}$, $\forall\ x, y \in G$.*

7. *RAP_n-property if $yx^n \cdot x = yx^{n+1}$ where $n \in \mathbb{Z}$, $\forall\ x, y \in G$.*

Remark 1. *In any power associative loop: LIP is equivalent to the property LAP^{-1} or LAP_{-1}; RIP is equivalent to the property RAP^{-1} or RAP_{-1},*

Theorem 1. *Let G be a LTWC (RTWC)-loop. G is a Frute loop if and only if G is a crazy loop.*

Remark 2. *Theorem 1(1) is nontrivial because by (Theorem 2.6 (2) of [4]), in a Frute loop, the property $x^{-1}yx = xyx^{-1}$ (which is equivalent to the centrum square property in a diassociative loop) is satisfied but not generally true in Moufang, extra loop or group. Hence, it distinguishes a Frute loop from a Moufang, extra loop and group. In (Theorem 2.2 of [4]), this property is necessary and sufficiency for a group to be a Frute loop and vice versa. But may not be necessary and sufficiency for a Frute loop to be a crazy loop (which is a group and has the property itself).*

Theorem 2. *Let G be a LTWC-loop.*

1. *$x \cdot x^n y = x^n \cdot xy\ \forall x, y \in G,\ n \in \mathbb{Z}$.*

2. *G is left power alternative $\Leftrightarrow$ G has the LAP_n-property for all $n \in \mathbb{Z} \Leftrightarrow$ G has the LAP^n-property for all $n \in \mathbb{Z}$.*

3. *For any fixed $n \in \mathbb{Z}$, G has the LAP^n-property $\Leftrightarrow$ G has the LAP_n-property.*

4. *G has the $FLEX_n$, LAP^1 and $FLEX_{(2,n+1)}$ properties implies that G has the RAP^n property for any fixed $n \in \mathbb{Z}\backslash\{1\}$.*

5. *For any fixed $n \in \mathbb{Z}$, the LPA^{n+1} and LPA^n properties imply the LAP^n and LAP_n properties.*

6. *Left power alternative property implies the LAP^n and LAP_n properties for all $n \in \mathbb{Z}$.*

7. *LAP^n or LAP_n and LPA^n properties imply the LPA^{n+1} property for any fixed $n \in \mathbb{Z}$.*

We shall be discussing some properties of translations of LTWC-loop and their application.

Theorem 3. *In a LTWC loop $(G, \cdot)$ and for each $x, y \in G$:*

1. *$R_x^m = L_x^{2n} R_x^m L_x^{-2n}$ or $[R_x^m, L_x^{2n}] = I$ for any $m, n \in \mathbb{Z}$.*

2. *$R_{x^n} = L_x^{-2} T_x^{n-2} (R_x L_x)^2 L_x^{n-2}$ for any $n \in \mathbb{Z}$.*

3. *$R_{x^n} = T_x^{n-1} R_x L_x^{n-1}$ for any $n \in \mathbb{Z}$.*

4. *$R_{(x,y)} = T_{(x,y)} L_x^{-1} S_x L_x = T_{(x,y)} T_x^{-1}$ where $S_x = R_x^{-1} L_x$ and $T_{(x,y)} = R_x R_y L_x^{-1} R_y^{-1}$ are elements of $Inn(G)$. $Inn(G) = \langle T_{(x,y)} \mid x, y \in G \rangle$ and $TInn(G, \cdot) = \langle T_{(x,y)}, L_{(x,y)}, M_{(x,y)}, U_x \mid x, y \in G \rangle = \langle T_{(x,y)}, L_{(x,y)}, P_{(x,y)}, V_x \mid x, y \in G \rangle$.*

Remark 3. *By Theorem 3(4), LTWC-loop is thus a class of loop which falls into the Syrbu and Grecu (2019) first answer to a question of Stanovský and Vojtěchovský (2014)-minimal generating set for the total inner mapping group of a loop. In addition, the class of LTWC-loop also provides an alternative solution to 2014 question and in fact, the inner automorphism group of a LTWC-loop is generated by just one inner mapping.*

Remark 4. *We have established necessary and sufficient condition for a LTWC-loop to have LAP (RAP) or to be left (right) power alternative.*

Remark 5. *A LTWC-loop G is commutative if and only if $x \cdot yx = yx^2$ or $x\,[x \cdot (x \cdot yx)x] = (x \cdot xy)x^3$ for all $x, y \in G$.*

We shall be using some of the properties of the translations of LTWC-loop for construction. We adopt the following notations for such in a loop $(G, \cdot)$: $\prod_\rho(G, \cdot) = \prod_\rho(G) = \{R_a \mid a \in G\} = \{R(a) \mid a \in G\}$ and $\prod_\lambda(G, \cdot) = \prod_\lambda(G) = \{L_a \mid a \in G\} = \{L(a) \mid a \in G\}$.

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	7	8	5	6
3	3	4	1	2	6	5	8	7
4	4	3	2	1	8	7	6	5
5	5	7	6	8	1	3	2	4
6	6	5	8	7	3	4	1	2
7	7	8	5	6	2	1	4	3
8	8	6	7	5	4	2	3	1

Таблица 1: A LTWC-loop $(G, \cdot)$ of order 8

Theorem 4. *Let G be a loop.*

1. *G is a LTWC-loop if and only if for all $\alpha \in \prod_\rho$, for some $\beta \in \prod_\lambda$, and for some $\alpha' \in \prod_\rho$, $\beta^{-2}\alpha'\beta\alpha\beta \in \prod_\rho$.*
2. *If G is a LTWC-loop, then*
   (a) *$\beta, \beta' \in \prod_\lambda \Rightarrow \beta^{-1}\beta'\beta \in \prod_\lambda$.*
   (b) *for some $\alpha \in \prod_\lambda$ and $\beta \in \prod_\rho$, $\beta\alpha^2 = \alpha^2\beta$.*
   (c) *for some $\alpha \in \prod_\lambda$ and $\beta \in \prod_\rho$, $\alpha^{-2}\left(\beta\alpha^{-1}\right)^{n-2}(\beta\alpha)^2\alpha^{n-2} \in \prod_\rho$ for all $n \in \mathbb{Z}$.*
   (d) *for some $\alpha \in \prod_\lambda$ and $\beta \in \prod_\rho$, $\left(\beta\alpha^{-1}\right)^{n-1}\beta\alpha^{n-1} \in \prod_\rho$ for all $n \in \mathbb{Z}$.*
   (e) *for some $\alpha \in \prod_\lambda$ and $\beta \in \prod_\rho$, $\beta^m\alpha^{2n} = \alpha^{2n}\beta^m \ \forall\ m, n \in \mathbb{Z}$.*
   (f) *for some $\beta, \beta' \in \prod_\lambda$, $\beta\beta' = \beta'\beta$.*
   (g) *for all $\alpha \in \prod_\rho$, for some $\beta \in \prod_\lambda$, and for some $\alpha' \in \prod_\rho$, $\alpha'\beta^{-1}\alpha\beta \in \prod_\lambda$.*

References

[1] O. O. George, J. O. Olaleru, J. O. Adeniran and T. G. Jaíyéọlá *On a class of power associative LCC-loops*, Extracta Mathematicae, **37**(2) (2022), 185-194. doi:10.17398/2605-5686.37.2.185

[2] O. O. George and T. G. Jaiyéọlá, *Nuclear identificatoion of some new loop identities of lenght five*, Buletinul Academiei de

EħtiinEJe a Republicii Moldova. Matematica, **99**(2) (2022), 39вЂ“58. https://doi.org/10.56415/basm.y2022.i2.p39

[3] T. G. Jaiyéọlá and O. O. George, *A class of power associative LCC-loops*, preprint.

[4] T. G. Jaiyéọlá, A. A. Adeniregun, O. O. Oyebola and A. O. Adelakun, *FRUTE loops*, Algebras, Groups and geometries, **37**(2) (2021), 159-179. DOI 10.29083/AGG.37.02.2021

[5] J. D. Phillips, *A short basis for the variety of WIP PACC- loops*, Quasigroups and Related Systems, **14** (2006), 259-271.

Authors

Contents

Bun de tipar 24.06.2025. Formatul 80x100 1/12

Comanda 81/25. Tirajul 50 ex.

Centrul Editorial-Poligrafic al USM

str. Al.Mateevici, 60, Chişinău, MD-2009

e-mail: cep1usm@mail.ru