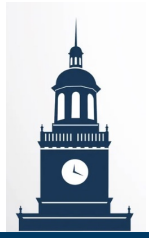


Dihedral Solutions of the set-theoretical Yang-Baxter equation

Alex W. Nowak (joint w. Anna Zamojska-Dzienio)

Howard University

March 31, 2026

Panglobal Algebra and Logic Seminar

Contents

- Various nonassociative algebras
- The set-theoretical Yang-Baxter equation
- Dihedral Solutions

A Menagerie of Nonassociative Operations

Quasigroups and loops

- A *quasigroup* $(Q, \circ, \backslash_\circ, /^\circ)$ is a nonassociative group. That means...

Quasigroups and loops

- A *quasigroup* $(Q, \circ, \backslash_\circ, /^\circ)$ is a nonassociative group. That means...
  - The multiplication table forms a Latin square.

Quasigroups and loops

- A *quasigroup* $(Q, \circ, \backslash_\circ, /^\circ)$ is a nonassociative group. That means...
  - The multiplication table forms a Latin square.
  - The multiplication $\circ$ has a left division $\backslash_\circ$ and right division $/^\circ$

$$a\backslash_\circ(a \circ x) = x = (x \circ a)/^\circ a$$
$$a \circ (a\backslash_\circ x) = x = (x/^\circ a) \circ a$$

Quasigroups and loops

- A *quasigroup* $(Q, \circ, \backslash_\circ, /^\circ)$ is a nonassociative group. That means...
  - The multiplication table forms a Latin square.
  - The multiplication $\circ$ has a left division $\backslash_\circ$ and right division $/^\circ$

$$a\backslash_\circ(a \circ x) = x = (x \circ a)/^\circ a$$
$$a \circ (a\backslash_\circ x) = x = (x/^\circ a) \circ a$$

  - For each $a \in Q$ the left and right multiplication maps

$$L_a^\circ : x \mapsto a \circ x \qquad (L_a^\circ)^{-1} : x \mapsto a\backslash_\circ x$$
$$R_a^\circ : x \mapsto x \circ a \qquad (R_a^\circ)^{-1} : x \mapsto x/^\circ a$$

    are invertible.

Left quasigroups, racks, quandles

- A left quasigroup $(Q, \circ, \backslash_\circ)$ only possesses a left division.

Left quasigroups, racks, quandles

- A left quasigroup $(Q, \circ, \backslash_\circ)$ only possesses a left division.
- A *rack* is a left quasigroup which is also *left distributive*

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

Left quasigroups, racks, quandles

- A left quasigroup $(Q, \circ, \backslash_\circ)$ only possesses a left division.
- A *rack* is a left quasigroup which is also *left distributive*

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

  - Each $L_a^\circ \in \mathrm{Aut}(Q, \circ, \backslash_\circ)$

Left quasigroups, racks, quandles

- A left quasigroup $(Q, \circ, \backslash_\circ)$ only possesses a left division.
- A *rack* is a left quasigroup which is also *left distributive*

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

  - Each $L_a^\circ \in \mathrm{Aut}(Q, \circ, \backslash_\circ)$
- A *quandle* is a rack which is also idempotent: $x \circ x = x$.

Loops

- A *loop* $(Q, +, e)$ is a quasigroup with identity.

Loops

- A *loop* $(Q, +, e)$ is a quasigroup with identity.
  - $e = x \backslash_{\circ} x = y /^{\circ} y \quad \forall x, y \in Q$

Loops

- A *loop* $(Q, +, e)$ is a quasigroup with identity.
  - $e = x \backslash_\circ x = y /^\circ y \quad \forall x, y \in Q$
- Any quasigroup $(Q, \circ, \backslash_\circ, /^\circ)$ comes with *loop isotopes* $(Q, +, e \circ e)$:

$$x + y := (R_e^\circ)^{-1}(x) \circ (L_e^\circ)(y) = (x /^\circ e) \circ (e \backslash_\circ y)$$

Some loop-quasigroup correspondences

Quasigroups:

- Involutory Latin quandle $(Q, \circ, \circ, /^\circ)$
  - $a \circ (a \circ x) = x$, i.e., $L_a^\circ = (L_a^\circ)^{-1}$
  - $a \circ (x \circ y) = (a \circ x) \circ (a \circ y)$, i.e. each $L_a^\circ \in \mathrm{Aut}(Q)$
  - $x \circ x = x$.
- Hall triple system $(Q, \circ, \circ, \circ)$
  - $a \circ (a \circ x) = x = (x \circ a) \circ a$, i.e. $L_a^\circ = (L_a^\circ)^{-1} = R_a^\circ$
  - $a \circ (x \circ y) = (a \circ x) \circ (a \circ y)$, i.e. each $L_a^\circ \in \mathrm{Aut}(Q)$
  - $x \circ x = x$

Loops:

- Uniquely 2-divisible Bruck loop
  - $x + (y + (x + z)) = (x + (y + x)) + z$
  - $-(x + y) = -x - y$, i.e. inversion is an automorphism
  - $x \mapsto x + x =: 2x$ is invertible
- Commutative Moufang loops of exponent 3 (CML_3)
  - $(x + x) + (y + z) = (x + y) + (x + z)$
  - $\langle x \rangle \cong \mathbb{Z}_{/3}$

The Set-Theoretical Yang-Baxter Equation

Yang-Baxter equation

- $R \in \mathrm{End}(V \otimes V)$ is a solution of the *quantum Yang-Baxter equation* (QYBE) if

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12}.$$

  - $R_{ij} \in \mathrm{End}(V \otimes V \otimes V)$ acts on the ith and jth tensor factors.

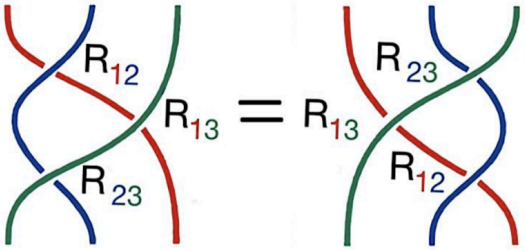
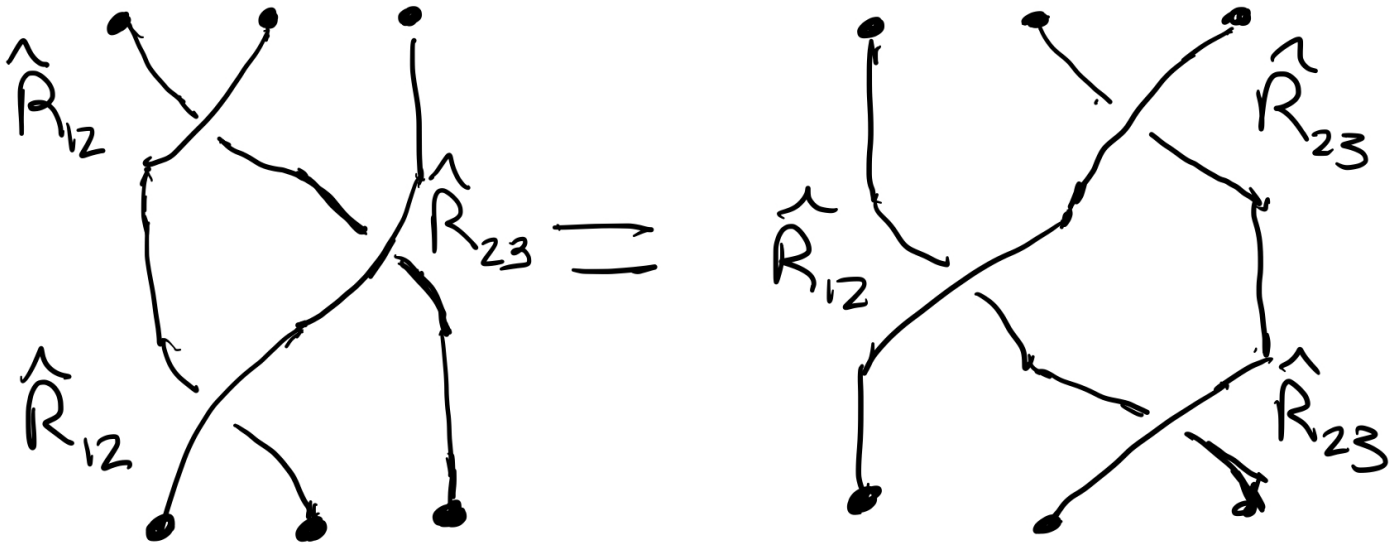


Image from Bardakov et. al., (1).

YBE and braids

- With $\tau : x \otimes y \mapsto y \otimes x$ the "flip map," R is a QYBE solution iff $\hat{R} := \tau R$ is a solution of the *braid equation*

$$\hat{R}_{12}\hat{R}_{23}\hat{R}_{12} = \hat{R}_{23}\hat{R}_{12}\hat{R}_{23}$$



Set theoretical YBE

- Drinfeld proposed study of set-theoretical solutions (SYBE) as a simplification.
  - Let Q be a set. $r : Q^2 \to Q^2$ is a *set-theoretical solution* of the QYBE if

$$r_{12} r_{23} r_{12} = r_{23} r_{12} r_{23}.$$

Set theoretical YBE

- Drinfeld proposed study of set-theoretical solutions (SYBE) as a simplification.
  - Let Q be a set. $r : Q^2 \to Q^2$ is a *set-theoretical solution* of the QYBE if

$$r_{12} r_{23} r_{12} = r_{23} r_{12} r_{23}.$$

  - (Q, r) is a *braided set*.

Set theoretical YBE

- Drinfeld proposed study of set-theoretical solutions (SYBE) as a simplification.
  - Let Q be a set. $r : Q^2 \to Q^2$ is a *set-theoretical solution* of the QYBE if
  $$r_{12} r_{23} r_{12} = r_{23} r_{12} r_{23}.$$
  - (Q, r) is a *braided set*.

- *Involutive solutions*, $r^2 = 1_{Q \times Q}$, get the most attention.

Set theoretical YBE

- Drinfeld proposed study of set-theoretical solutions (SYBE) as a simplification.
  - Let Q be a set. $r : Q^2 \to Q^2$ is a *set-theoretical solution* of the QYBE if
  $$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}.$$
  - (Q, r) is a *braided set*.

- *Involutive solutions*, $r^2 = 1_{Q\times Q}$, get the most attention.
  Examples: $\tau(x, y) = (y, x)$, the trivial solution,
  $r(x, y) = (\varphi(y), \varphi^{-1}(x))$ for $\varphi \in S_Q$.

Universal algebraic approach to SYBE

- Think of potential solutions r as a pair of binary operations:

$$r(x, y) = (x \circ y, x \bullet y).$$

Universal algebraic approach to SYBE

- Think of potential solutions r as a pair of binary operations:

$$r(x, y) = (x \circ y, x \bullet y).$$

- (Q, r) is a braided set iff $(Q, \circ, \bullet)$ satisfies:

$$\begin{aligned} x \circ (y \circ z) &= (x \circ y) \circ ((x \bullet y) \circ z) \\ (x \circ y) \bullet ((x \bullet y) \circ z) &= (x \bullet (y \circ z)) \circ (y \bullet z) \\ (x \bullet y) \bullet z &= (x \bullet (y \circ z)) \bullet (y \bullet z) \end{aligned}$$

- *Derived solutions* come from racks: $r(x, y) = (x \circ y, x)$

(Non)degeneracy

- A solution $r(x, y) = (x \circ y, x \bullet y)$ is *nondegenerate* if there is a left-quasigroup $(Q, \circ, \backslash_\circ)$ and a right quasigroup $(Q, \bullet, /^\bullet)$

(Non)degeneracy

- A solution $r(x, y) = (x \circ y, x \bullet y)$ is *nondegenerate* if there is a left-quasigroup $(Q, \circ, \backslash_\circ)$ and a right quasigroup $(Q, \bullet, /^\bullet)$
  - In this case, we call $(Q, \circ, \backslash_\circ, \bullet, /^\bullet)$ a *birack*.

(Non)degeneracy

- A solution $r(x, y) = (x \circ y, x \bullet y)$ is *nondegenerate* if there is a left-quasigroup $(Q, \circ, \backslash_\circ)$ and a right quasigroup $(Q, \bullet, /^\bullet)$
  - In this case, we call $(Q, \circ, \backslash_\circ, \bullet, /^\bullet)$ a *birack*.

- If we have a full quasigroup $(Q, \circ, \backslash_\circ, /^\circ)$, then r is *Latin*

(Non)degeneracy

- A solution $r(x, y) = (x \circ y, x \bullet y)$ is *nondegenerate* if there is a left-quasigroup $(Q, \circ, \backslash_\circ)$ and a right quasigroup $(Q, \bullet, /^\bullet)$
  - In this case, we call $(Q, \circ, \backslash_\circ, \bullet, /^\bullet)$ a *birack*.

- If we have a full quasigroup $(Q, \circ, \backslash_\circ, /^\circ)$, then r is *Latin*

- The *diagonal* maps $S : x \mapsto x \backslash_\circ x$ and $T : x \mapsto x /^\bullet x$ show up a lot in the theory.

Dihedral solutions

Solutions from CML_3

- My entry into SYBE was the following class of solutions:

$$\rho : (x, y) \mapsto (-x + y, -x),$$

where $(Q, +)$ is a CML_3 (Smith, 2016).

Solutions from CML_3

- My entry into SYBE was the following class of solutions:

$$\rho : (x, y) \mapsto (-x + y, -x),$$

where $(Q, +)$ is a CML_3 (Smith, 2016).

  - $\rho(x, y) = (2x + y, -x)$ with $(Q, +)$ a 2-div. Bruck loop generalizes

Solutions from CML_3

- My entry into SYBE was the following class of solutions:

$$\rho : (x, y) \mapsto (-x + y, -x),$$

where $(Q, +)$ is a CML_3 (Smith, 2016).

  - $\rho(x, y) = (2x + y, -x)$ with $(Q, +)$ a 2-div. Bruck loop generalizes

- The derived solution associated with ρ is

$$\rho' : (x, y) \mapsto (-(x + y), x).$$

Solutions from CML_3

- My entry into SYBE was the following class of solutions:

$$\rho : (x, y) \mapsto (-x + y, -x),$$

where $(Q, +)$ is a CML_3 (Smith, 2016).

  - $\rho(x, y) = (2x + y, -x)$ with $(Q, +)$ a 2-div. Bruck loop generalizes

- The derived solution associated with ρ is

$$\rho' : (x, y) \mapsto (-(x + y), x).$$

  - $\rho'(x, y) = (2x - y, x)$ for Bruck loops

Properties of CML_3 solutions

Properties of $\rho(x,y) = (-x+y, -x)$ and $\rho'(x,y) = (-(x+y), x)$:

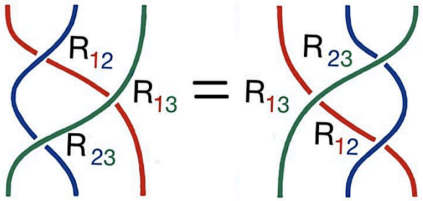
- They're not involutive, but they have order 3 ($r^3 = 1_{Q\times Q}$), and ...

Properties of CML_3 solutions

Properties of $\rho(x, y) = (-x + y, -x)$ and $\rho'(x, y) = (-(x + y), x)$:

- They're not involutive, but they have order 3 ($r^3 = 1_{Q\times Q}$), and ...
- the map that satisfies the non-braided YBE is involutive!

$$(\tau r)^2 = 1_{Q\times Q}.$$

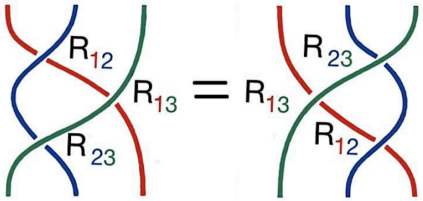


Properties of CML_3 solutions

Properties of $\rho(x, y) = (-x + y, -x)$ and $\rho'(x, y) = (-(x + y), x)$:

- They're not involutive, but they have order 3 ($r^3 = 1_{Q\times Q}$), and ...
- the map that satisfies the non-braided YBE is involutive!

$$(\tau r)^2 = 1_{Q\times Q}.$$



- They're *Latin*.

Dihedral/triality sets

- Since $\langle r, \tau \mid \tau^2 = (\tau r)^2 = 1 \rangle \cong D_\infty$, we decided to call solutions r such that $(\tau r)^2 = 1_{Q \times Q}$ *braided dihedral sets* (BDS)

Dihedral/triality sets

- Since $\langle r, \tau \mid \tau^2 = (\tau r)^2 = 1 \rangle \cong D_\infty$, we decided to call solutions r such that $(\tau r)^2 = 1_{Q \times Q}$ *braided dihedral sets* (BDS)
- Since $\langle r, \tau \mid r^3 = \tau^2 = (\tau r)^2 = 1 \rangle \cong S_3$, we decided to call solutions r such that $r^3 = (\tau r)^2 = 1_{Q \times Q}$ *braided triality sets* (BTS).

Question

How much can a Latin BTS (LBTS) differ from ρ and ρ'?

Dihedral/triality sets

- Since $\langle r, \tau \mid \tau^2 = (\tau r)^2 = 1 \rangle \cong D_\infty$, we decided to call solutions r such that $(\tau r)^2 = 1_{Q \times Q}$ *braided dihedral sets* (BDS)
- Since $\langle r, \tau \mid r^3 = \tau^2 = (\tau r)^2 = 1 \rangle \cong S_3$, we decided to call solutions r such that $r^3 = (\tau r)^2 = 1_{Q \times Q}$ *braided triality sets* (BTS).

Question

How much can a Latin BTS (LBTS) differ from ρ and ρ'?

- Turns out, not that much.

Dihedral/triality sets

- Since $\langle r, \tau \mid \tau^2 = (\tau r)^2 = 1 \rangle \cong D_\infty$, we decided to call solutions r such that $(\tau r)^2 = 1_{Q \times Q}$ *braided dihedral sets* (BDS)
- Since $\langle r, \tau \mid r^3 = \tau^2 = (\tau r)^2 = 1 \rangle \cong S_3$, we decided to call solutions r such that $r^3 = (\tau r)^2 = 1_{Q \times Q}$ *braided triality sets* (BTS).

Question

How much can a Latin BTS (LBTS) differ from ρ and ρ'?

- Turns out, not that much.

Theorem (N., Zamojska-Dzienio, 2025)

Let $r(x, y) = (x \circ y, x \bullet y)$ be an LBTS. Then there is a CML_3-factorization $Q = Q_e + P$ such that $r|_{Q_e}$ has the form ρ and $r|_P$ has the form ρ'.

LBDS-quasigroups

Lemma

For any LBDS r, we have $r(x,y) = (x \circ y, x^S)$, where $x^S = x \backslash_\circ x$.

LBDS-quasigroups

Lemma

For any LBDS r, we have $r(x, y) = (x \circ y, x^S)$, where $x^S = x \backslash_\circ x$.

- Tedious proof based on `Prover9` output.

LBDS-quasigroups

Lemma

For any LBDS r, we have $r(x, y) = (x \circ y, x^S)$, where $x^S = x \backslash_\circ x$.

- Tedious proof based on `Prover9` output.
- Lemma reduces LBDS to a variety of quasigroups:

$$x \circ (y \circ z) = (x \circ y) \circ (x^S \circ z)$$
$$x^S \circ (x \circ y) = y$$

LBDS-quasigroups

Lemma

For any LBDS r, we have $r(x,y) = (x \circ y, x^S)$, where $x^S = x \backslash_\circ x$.

- Tedious proof based on `Prover9` output.
- Lemma reduces LBDS to a variety of quasigroups:

$$x \circ (y \circ z) = (x \circ y) \circ (x^S \circ z)$$
$$x^S \circ (x \circ y) = y$$

- Call this the variety of *LBDS*-quasigroups.

Bruck loop isotopes

- Fix $f \in Q$, and set $e = f /^{\circ} f$. If $(Q, \circ, \backslash_{\circ}, /^{\circ})$ is an LBDS-quasigroup, then $x + y = (x /^{\circ} e) \circ (e \circ x)$ is a uniquely 2-divisible Bruck loop $(Q, +, e)$ and S is an involutive automorphism of this loop.

Bruck loop isotopes

- Fix $f \in Q$, and set $e = f/^{\circ}f$. If $(Q, \circ, \backslash_{\circ}, /^{\circ})$ is an LBDS-quasigroup, then $x + y = (x/^{\circ}e) \circ (e \circ x)$ is a uniquely 2-divisible Bruck loop $(Q, +, e)$ and S is an involutive automorphism of this loop.
- Conversely, if $(Q, +, e)$ is a uniquely 2-divisible Bruck loop with involutive automorphism S, then $x \circ y = 2x - y^S$ specifies an LBDS-quasigroup.

Bruck loop isotopes

- Fix $f \in Q$, and set $e = f/^{\circ}f$. If $(Q, \circ, \backslash_{\circ}, /^{\circ})$ is an LBDS-quasigroup, then $x + y = (x/^{\circ}e) \circ (e \circ x)$ is a uniquely 2-divisible Bruck loop $(Q, +, e)$ and S is an involutive automorphism of this loop.
- Conversely, if $(Q, +, e)$ is a uniquely 2-divisible Bruck loop with involutive automorphism S, then $x \circ y = 2x - y^S$ specifies an LBDS-quasigroup.

Theorem (N, Zamojska-Dzienio, 2025)

There is a one-to-one correspondence between isomorphism classes of LBDS-quasigroups and conjugacy classes of involutions in automorphism groups of uniquely 2-divisible Bruck loops.

Squaring right division

- Can specify LBDS $(Q, +, e, S)$, where $(Q, +, e)$ is a Bruck loop and S is loop involution.

Squaring right division

- Can specify LBDS $(Q, +, e, S)$, where $(Q, +, e)$ is a Bruck loop and S is loop involution.
- Define $\mathrm{Sq}_{/^\circ}(x) = x/^\circ x$ and $Q_e = \{x \in Q \mid \mathrm{Sq}_{/^\circ}(x) = e\}$.

Squaring right division

- Can specify LBDS $(Q, +, e, S)$, where $(Q, +, e)$ is a Bruck loop and S is loop involution.
- Define $\mathrm{Sq}_{/\circ}(x) = x/^{\circ}x$ and $Q_e = \{x \in Q \mid \mathrm{Sq}_{/\circ}(x) = e\}$.
- $\mathrm{Sq}_{/\circ}(Q) = \{x \in Q \mid x^S = x\}$.

Squaring right division

- Can specify LBDS $(Q, +, e, S)$, where $(Q, +, e)$ is a Bruck loop and S is loop involution.
- Define $\mathrm{Sq}_{/\circ}(x) = x/^{\circ}x$ and $Q_e = \{x \in Q \mid \mathrm{Sq}_{/\circ}(x) = e\}$.
- $\mathrm{Sq}_{/\circ}(Q) = \{x \in Q \mid x^S = x\}$.
- $Q_e = \{x \in Q \mid x^S = -x\}$.

Squaring right division

- Can specify LBDS $(Q, +, e, S)$, where $(Q, +, e)$ is a Bruck loop and S is loop involution.
- Define $\mathrm{Sq}_{/^\circ}(x) = x/^\circ x$ and $Q_e = \{x \in Q \mid \mathrm{Sq}_{/^\circ}(x) = e\}$.
- $\mathrm{Sq}_{/^\circ}(Q) = \{x \in Q \mid x^S = x\}$.
- $Q_e = \{x \in Q \mid x^S = -x\}$.

Theorem (N., Zamojska-Dzienio, 2025)

If $Sq_{/^\circ}$ is endomorphic, then we have a split exact sequence

$$\{e\} \to Q_e \to Q \to Sq_{/^\circ}(Q) \to \{e\}$$

LBTS

- LBTS, i.e., LBDS for which $r^3 = 1_{Q \times Q}$ correspond to LBDS-quasigroups in which $(x \circ y) \circ y = x$.

LBTS

- LBTS, i.e., LBDS for which $r^3 = 1_{Q \times Q}$ correspond to LBDS-quasigroups in which $(x \circ y) \circ y = x$.
- Now, the associated loops are CML_3s.

LBTS

- LBTS, i.e., LBDS for which $r^3 = 1_{Q\times Q}$ correspond to LBDS-quasigroups in which $(x \circ y) \circ y = x$.
- Now, the associated loops are CML_3s.
- For all $x \in Q$,

$$x = (-x + x^S) + (-x - x^S),$$

$-x + x^S \in Q_e$ and $-x - x^S \in \mathrm{Sq}_{/\circ}(Q)$

LBTS

- LBTS, i.e., LBDS for which $r^3 = 1_{Q\times Q}$ correspond to LBDS-quasigroups in which $(x \circ y) \circ y = x$.
- Now, the associated loops are CML_3s.
- For all $x \in Q$,
$$x = (-x + x^S) + (-x - x^S),$$
$-x + x^S \in Q_e$ and $-x - x^S \in \mathrm{Sq}_{/\circ}(Q)$
- Whence

Theorem (N., Zamojska-Dzienio, 2025)

Let $r(x, y) = (x \circ y, x \bullet y)$ be an LBTS. Then there is a CML_3-factorization $Q = Q_e + P$ such that $r|_{Q_e}$ has the form ρ and $r|_P$ has the form ρ'.

The isomorphism problem

Let p be any odd prime. Up to isomorphism there are...

- 2 LBDS of order p
- 5 LBDS of order p^2
- 6 LBDS of order $3p$ when $p \neq 3$

The isomorphism problem

Let p be any odd prime. Up to isomorphism there are...

- 2 LBDS of order p
- 5 LBDS of order p^2
- 6 LBDS of order $3p$ when $p \neq 3$
- 24 LBDS of order 3^3 and 263 LBDS of order 3^4
  - No explicit descriptions of these ones, unless underlying Bruck loop is associative.

The isomorphism problem

Let p be any odd prime. Up to isomorphism there are...

- 2 LBDS of order p
- 5 LBDS of order p^2
- 6 LBDS of order $3p$ when $p \neq 3$
- 24 LBDS of order 3^3 and 263 LBDS of order 3^4
  - No explicit descriptions of these ones, unless underlying Bruck loop is associative.
- 18 LBTS of order $\leq 3^4$.

References I

[1] V. Bardakov, M. Elhamdadi, M. Singh, "Yang Baxter equation and related algebraic structures," arXiv:2506.23175.

Thank you for your attention

HMU up at
alexwnowak@gmail.com

Panglobal Algebra and Logic Seminar