Some problems on skew braces

Leandro Vendramin

Vrije Universiteit Brussel

Advances in Group Theory and Applications 2023
June 2023

I will discuss some problems related to the structure of skew braces.

Why skew braces?

- The original motivation is the study of set-theoretic solutions to the Yang–Baxter equation (YBE).
- The definition extends that of Rump and is motivated by the work of Cedó, Jespers and Okninski.
- Skew braces put together several ideas that were flying around for years.

A solution (to the YBE) is a pair (X, r), where X is a set and

$$r\colon X \times X \to X \times X, \quad r(x,y) = (\sigma_x(y), \tau_y(x)),$$

is a bijective map such that

- the maps $\sigma_x\colon X \to X$ are bijective for all $x \in X$,
- the maps $\tau_x\colon X \to X$ are bijective for all $x \in X$, and
- $r_1 r_2 r_1 = r_2 r_1 r_2$, where

$$r_1 = r \times \mathrm{id} \quad \text{and} \quad r_2 = \mathrm{id} \times r.$$

First works: Gateva–Ivanova and Van den Bergh; Etingof, Schedler and Soloviev; Gateva–Ivanova and Majid.

Examples:

- The flip: $r(x,y) = (y,x)$.
- Let X be a set and $\sigma, \tau \colon X \to X$ be bijections such that $\sigma\tau = \tau\sigma$. Then

$$r(x,y) = (\sigma(y), \tau(x))$$

  is a solution.
- Let $X = \mathbb{Z}/n$. Then

$$r(x,y) = (2x - y, x) \quad \text{and} \quad r(x,y) = (y-1, x+1)$$

  are solutions.

More examples:
If X is a group, then

$$r(x,y) = (xyx^{-1}, x) \quad \text{and} \quad r(x,y) = (xy^{-1}x^{-1}, xy^2)$$

are solutions.

We can start with involutive solutions. A solution (X, r) is involutive if $r^2 = \mathrm{id}$.

If (X, r) is involutive, then

$$\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x)$$

for all $x, y \in X$.

How many solutions are there?

The number of involutive solutions.

n	4	5	6	7	8	9	10
sols	23	88	595	3456	34530	321931	4895272

Solutions of size 9 and 10 were computed with Akgün and Mereb using constraint programming techniques.

Problem

How many involutive solutions (up to isomorphism) of size 11 are there?

More challenging:

Problem

Estimate the number of solutions of size n for $n \to \infty$.

An involutive solution (X, r) is indecomposable if the group

$$\mathcal{G}(X, r) = \langle \sigma_x : x \in X \rangle$$

acts transitively on X.

Problem

Construct indecomposable solutions of small size.

More challenging:

Problem

Prove that "almost all" solutions are non-indecomposable.

Let (X, r) be a solution. The structure group of (X, r) is the group $G(X, r)$ with generators X and relations

$$xy = uv$$

whenever $r(x, y) = (u, v)$.

Facts:

- The group $G(X, r)$ acts on X.
- The solution r on X "extends" to a solution on $G(X, r)$.

A concrete example

Let $X = \{1,2,3,4\}$ and $r(x,y) = (\sigma_x(y), \tau_y(x))$ be the solution given by

$$\begin{array}{llll} \sigma_1 = (12), & \sigma_2 = (1324), & \sigma_3 = (34), & \sigma_4 = (1423), \\ \tau_1 = (14), & \tau_2 = (1243), & \tau_3 = (23), & \tau_4 = (1342). \end{array}$$

The group $G(X,r)$ with generators x_1, x_2, x_3, x_4 and relations

$$\begin{array}{lll} x_1^2 = x_2 x_4, & x_1 x_3 = x_3 x_1, & x_1 x_4 = x_4 x_3, \\ x_2 x_1 = x_3 x_2, & x_2^2 = x_4^2, & x_3^2 = x_4 x_2. \end{array}$$

A concrete example

The group $G(X,r)$ admits a faithful linear representation inside $\mathbf{GL}_5(\mathbb{Z})$ given by

$$x_1 \mapsto \begin{pmatrix} 0&1&0&0&1\\ 1&0&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \qquad x_2 \mapsto \begin{pmatrix} 0&0&0&1&0\\ 0&0&1&0&1\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&0&1 \end{pmatrix},$$

$$x_3 \mapsto \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&1&1\\ 0&0&1&0&0\\ 0&0&0&0&1 \end{pmatrix}, \qquad x_4 \mapsto \begin{pmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 0&1&0&0&0\\ 1&0&0&0&1\\ 0&0&0&0&1 \end{pmatrix}.$$

A concrete example

Moreover, the map $G(X,r) \to \mathbb{Z}^4$,

$$x_1 \mapsto \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad x_2 \mapsto \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad x_3 \mapsto \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad x_4 \mapsto \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

is bijective.

The extra information we have on structure groups is the skew brace structure.

A skew brace is a triple $(A, +, \circ)$, where $(A, +)$ and $(A, \circ)$ are groups and

$$a \circ (b + c) = a \circ b - a + a \circ c$$

holds for all $a, b, c \in A$.

Terminology:

- $(A, +)$ is the additive group of A (even if it is non-abelian) .
- $(A, \circ)$ is the multiplicative group of A.
- A is of abelian type if its additive group is abelian.

Examples:

- Radical rings.
- Trivial skew braces: Any addit ive group G with $g \circ h = g + h$ for all $g, h \in A$.
- An additive exactly factorizable group G (i.e. $G = A + B$ for disjoint subgroups A and B) is a skew brace with

  $$g \circ h = a + h + b,$$

  where $g = a + b$, $a \in A$ and $b \in B$.

Skew braces produce solutions.

Theorem (with Guarnieri)

If A is a skew brace, then $r_A\colon A \times A \to A \times A$,

$$r_A(a,b) = (-a + a \circ b, (-a + a \circ b)' \circ a \circ b)$$

is a solution to the YBE.

Here z' denotes the inverse of z with respect to $\circ$.

Let (X, r) be a solution.

Facts:

- $G(X, r)$ is a skew brace (of abelian type if $r^2 = \mathrm{id}$).
- $\mathcal{G}(X, r)$ is a skew brace (of abelian type if $r^2 = \mathrm{id}$).

Theorem (with Smoktunowicz)

Let (X, r) be a solution. Then there exists a unique skew brace structure over $G(X, r)$ such that its associated solution $r_{G(X,r)}$ satisfies

$$r_{G(X,r)}(\iota \times \iota) = (\iota \times \iota)r,$$

where $\iota \colon X \to G(X, r)$ is the canonical map.

The map ι is injective if $r^2 = \mathrm{id}$.

Skew braces have a universal property:

Theorem (with Smoktunowicz)

Let (X,r) be a solution. If B is a skew brace and $f\colon X\to B$ is a map such that

$$(f\times f)r=r_B(f\times f),$$

then there exists a unique homomorphism $\varphi\colon G(X,r)\to B$ of skew braces such that

$$\varphi\iota=f \qquad \text{and} \qquad (\varphi\times\varphi)r_{G(X,r)}=r_B(\varphi\times\varphi).$$

Similar results were found by Etingof, Schedler and Soloviev, Rump, and Lu, Yan and Zhu.

Etingof, Schedler and Soloviev proved that the multiplicative group of a finite skew brace of abelian type is always solvable.

Question

Is every solvable finite group the multiplicative group of a skew brace of abelian type?

Cedó, Jespers and Del Río have several results in this direction.

Using ideas of Rump and Lie theory, Bachiller proved that not every finite solvable group is the multiplicative group of a skew brace of abelian type.

Problem

Find a minimal counterexample.

Some comments:

- These problems are discrete analogs of (disproved) a conjecture of Milnor in the theory of flat manifolds.
- Bachiller's result depends on heavy computer calculations.
- We need to study the structure of skew braces where the additive group is a field (i.e. the circle algebras introduced by Catino and Rizzo).

We say that a finite group G is an involutive Yang–Baxter group (IYB-group) if it is the multiplicative group of a skew brace of abelian type.

Problem (Rump)

Is there an example of a non-IYB-group where all Sylow subgroups are IYB?

More challenging:

Problem

Which finite solvable groups appear as multiplicative groups of skew braces of abelian type?

Another challenging problem related to solvability is the following conjecture:

Problem (Byott)

Let A be a finite skew brace such that $(A,+)$ is solvable. Is $(A,\circ)$ solvable?

The problem appeared in one of Byott's papers on Hopf–Galois structures. See also Problem 19.91 of *The Kourovka Notebook, by Khukhro and Mazurov*.

Let p be a prime number and G be a finite p-group. For $k \geq 1$, let

$$G^k = \langle g^k : g \in G \rangle.$$

Then G^k is a normal subgroup of G.

We say that G is powerful if the following conditions hold: if $p > 2$, then G/G^p is abelian; or if $p = 2$, then G/G^4 is abelian.

The notion goes back to Lubotzky and Mann and plays an important role in several areas of group theory.

A skew brace A is right nilpotent (RP) if $A^{(n)} = \{0\}$ for some n, where $A^{(1)} = A$ and

$$A^{(k+1)} = A^{(k)} * A = \langle x * a : x \in A^{(k)}, a \in A \rangle_+,$$

and $y * z = -y + y \circ z - z$.

Conjecture (Shalev–Smoktunowicz)

Let p be a prime number and A be a skew brace of abelian type of size p^m. If the multiplicative group of A is powerful, then A is right nilpotent.

Skew braces and regular subgroups

Let A be an additive group. The holomorph of A is the semidirect product $\mathrm{Hol}(A) = A \rtimes \mathrm{Aut}(A)$, with operation

$$(a, f)(b, g) = (a + f(b), fg).$$

A subgroup G of $\mathrm{Hol}(A)$ acts on A via

$$(x, f) \cdot a = a + f(x).$$

Then G is regular if for any $a, b \in A$ there exists a unique element $(x, f) \in G$ such that $(x, f) \cdot a = b$.

Skew braces and regular subgroups

Some facts:

1. If A is a group and G is a regular subgroup of $\mathrm{Hol}(A)$, then the map $\pi\colon G \to A$, $(x, f) \mapsto x$, is bijective.
2. If A is a skew brace, then $\{(a, \lambda_a) : a \in A\}$ is a regular subgroup of $\mathrm{Hol}(A)$.
3. If A is an additive group and G is a regular subgroup of $\mathrm{Hol}(A)$, then A is a skew brace with

$$a \circ b = a + f(b),$$

where $(\pi|_G)^{-1}(a) = (a, f) \in G$.

These results are heavily based on ideas of Caranti, Dalla Volta and Salla, Catino and Rizzo and Bachiller.

Some remarks:

- These facts were used in collaboration with Guarnieri to construct a huge database of finite skew braces.
- Bardakov, Neshchadim and Yadav improved the algorithm and extended the database.
- The connection between skew braces and regular subgroups of the holomorph yields a connection between skew braces and Hopf–Galois structures.
- Recently, Ballester-Bolinches, Esteban-Romero and Pérez-Calabuig constructed all skew braces of size 64 up to isomorphism.

Isoclinism of skew braces is a certain equivalence relation on skew braces. The notion is based on that of group theory and it was introduced[1] with my Ph.D. student Thomas Letourmy.

[1] arXiv:2211.14414.

A skew brace $(A, +, \circ)$ is said to be a bi-skew brace if $(A, \circ, +)$ is also a skew brace. The notion was introduced by Childs and has applications in Hopf–Galois theory.

Conjecture

Let A and B be finite isoclinic skew braces. Then A is a bi-skew brace if and only if B is a bi-skew brace.

Computer experiments support the conjecture.

Important fact:
Let (X, r) be an involutive solution. For $x, y \in X$ we define

$$x \sim y \Longleftrightarrow \sigma_x = \sigma_y.$$

This equivalence relation induces a solution on $X/{\sim}$,

$$\mathrm{Ret}(X, r) = (X/{\sim}, \overline{r}),$$

the retraction of X.

An involutive solution (X, r) is multipermutation (MP) if there exist $n \geq 1$ such that $|\mathrm{Ret}^n(X, r)| = 1$.

Problem

Prove that "almost all" solutions are MP.

For example, there are 4895272 solutions of size ten and only 28832 are not MP.

Some comments:

- (X, r) is MP $\iff G(X, r)$ is RN $\iff \mathcal{G}(X, r)$ is RN.
- Isoclinism may be helpful here!

Example 1:

Let $X = \{1, 2, 3, 4, 5\}$ and $r(x, y) = (\sigma_x(y), \tau_y(x))$, where

$$\sigma_1 = \sigma_2 = \sigma_3 = \mathrm{id}, \quad \sigma_4 = (45), \quad \sigma_5 = (23)(45)$$

and

$$\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(y).$$

Then (X, r) is MP.

Example 2:
Let $X = \{1,2,3,4\}$ and $r(x,y) = (\sigma_x(y), \tau_y(x))$, where

$$\sigma_1 = \sigma_2 = \mathrm{id}, \quad \sigma_3 = (34), \quad \sigma_4 = (12)(34)$$

and

$$\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(y).$$

Then (X, r) is MP.

We say that two solutions (X, r) and (Y, s) are permutation isoclinic if the skew braces $\mathcal{G}(X, r)$ and $\mathcal{G}(Y, s)$ are isoclinic.

The solutions of Examples 1 and 2 are permutation isoclinic.

Fact:
Let (X, r) and (Y, s) be permutation isoclinic solutions. Then (X, r) is MP if and only if (Y, s) is MP.

Problem

Construct finite solutions (say of small size) up to isoclinism.

We can also say that (X, r) and (Y, s) are isoclinic if and only if the skew braces $G(X, r)$ and $G(Y, s)$ are isoclinic.

Problem

What is the relationship between isoclinic solutions and permutation isoclinic solutions?

Let (X, r) be a solution. Motivated by the theory of braid groups Dehornoy used Garside theory to construct a certain finite quotient of the structure group. These Coxeter-like groups are indeed skew braces of abelian type.

Problem

What about considering the equivalence relation on the space of solutions induced by isoclinism of their Coxeter-like quotients?