

What is a skew brace?

Leandro Vendramin

Vrije Universiteit Brussel

Hopf orders & Galois module theory
June 2025



I will discuss **some problems** related to a discrete version of the Yang–Baxter equation. In particular, I will concentrate on the algebraic **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

$$r: X \times X \rightarrow X \times X, \quad r(x, y) = (\sigma_x(y), \tau_y(x)),$$

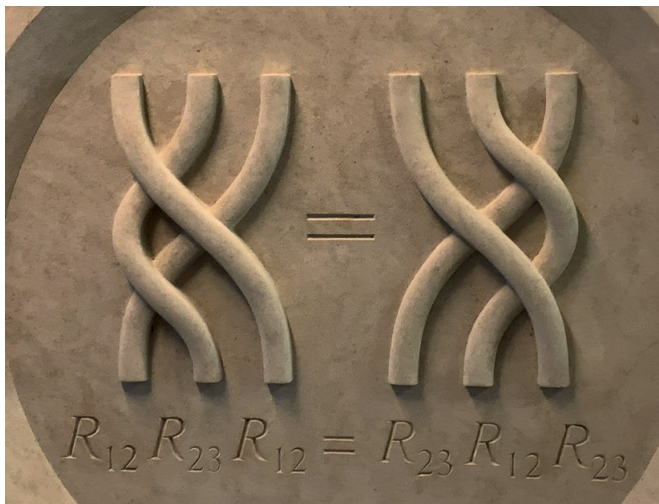
is a bijective map such that

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

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

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

The Yang–Baxter equation



Examples:

- ▶ The flip: $r(x, y) = (y, x)$.
- ▶ Let X be a set and $\sigma, \tau: X \rightarrow X$ 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.

Why?

These solutions...

- ▶ have very nice algebraic and combinatorial properties;
- ▶ appear in the representation theory of braid groups;
- ▶ produce combinatorial invariants of knots;
- ▶ motivate challenging problems in other research areas;
- ▶ physical applications: Doikou and Smoktunowicz, Gombor and Pozsgay.

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

If (X, r) is **involutive**, then

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

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?

Daimy Van Caudenberg (2024) proved that there are **77182093** solutions (up to isomorphism).

More challenging:

Problem

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

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.

Indecomposable solutions are related to the theory of **permutation groups**.

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

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

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

$$\begin{aligned}x_1^2 &= x_2x_4, & x_1x_3 &= x_3x_1, & x_1x_4 &= x_4x_3, \\ x_2x_1 &= x_3x_2, & x_2^2 &= x_4^2, & x_3^2 &= x_4x_2.\end{aligned}$$

A concrete example

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

$$\begin{aligned}x_1 &\mapsto \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, & x_2 &\mapsto \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \\x_3 &\mapsto \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, & x_4 &\mapsto \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.\end{aligned}$$

A concrete example

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

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

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 additive **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 $r_A: A \times A \rightarrow A \times A$,

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

is a solution to the YBE.

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

Applied to the skew brace of a **group factorization**, the previous formula produces the solutions found by Weinstein and Xu for **factorizable Poisson Lie groups**.

Let (X, r) be a solution.

Facts:

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

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 $\iota: X \rightarrow G(X, r)$ is the canonical map.

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

Skew braces have a **universal property**:

Theorem (with Smoktunowicz)

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

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

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

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

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

Let us discuss some algebraic problems related to the structure of skew braces.

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?

Recall that a **solvable group** is a group that can be constructed from abelian groups using extensions.

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 vector space.

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.

Skew braces are **ring-like objects**. One has an addition

$$(x, y) \mapsto x + y$$

that may be non-commutative, and a “multiplication”

$$(x, y) \mapsto x * y = -x + x \circ y - y$$

which generally is non-associative.

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 and Lie 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.

Important fact:

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

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

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

$$\text{Ret}(X, r) = (X/\sim, \bar{r}),$$

the retraction of X .

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

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.

Example:

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

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

and

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

Then (X, r) is MP.

The number of (not multipermutation) involutive solutions.

n	4	5	6	7	8	9	10
sols	23	88	595	3456	34530	321931	4895272
not MP	2	4	41	161	2375	16015	28832

Are there easy ways of detecting multipermutation solutions? Yes!
There are results related to the **permutation group**

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

of the solution.

Facts

Let (X, r) be a finite and involutive solution.

1. If $\mathcal{G}(X, r)$ is **cyclic**, then (X, r) is multipermutation.
2. If $\mathcal{G}(X, r)$ is **abelian**, then (X, r) is multipermutation.
3. If $\mathcal{G}(X, r)$ has **abelian Sylow subgroups** and has the **Sylow tower property**, then (X, r) is multipermutation.

(1) was proved by Rump; (2) was proved by Cedó, Jespers and Okniński and independently by Cameron and Gateva-Ivanova; (3) was proved by Ballester-Bolínches, Meng and Romero.

With Bachiller and Cedó we found a characterization of multipermutation solutions in terms of **left orderability of groups**.

A group G is said to be **left orderable** if $<$ is a total ordering on G such that the following holds:

$$x < y \implies zx < zy$$

for all $x, y, z \in G$.

Examples:

Torsion-free abelian groups, free groups, braid groups.

Theorem (with Bachiller and Cedó)

Let (X, r) be a finite involutive solution. Then (X, r) is multipermutation if and only if the group $G(X, r)$ is left orderable.

The implication $\implies$ was proved by Jespers and Okniński and independently by Chouraqui.

Corollary (with Acri and Łutowski)

Let (X, r) be a finite involutive solution. If all Sylow subgroups of $\mathcal{G}(X, r)$ are cyclic, then (X, r) is multipermutation.

The following problem was formulated around 80 years ago:

Kaplansky's unit problem

Let G be a torsion-free group. Does the group algebra $\mathbb{C}[G]$ have only trivial units?

Recall that a **trivial unit** of $\mathbb{C}[G]$ is an element of the form λg , where $\lambda \in \mathbb{C} \setminus \{0\}$ and $g \in G$.

Gardam **disproved the conjecture** for the complex numbers and fields of characteristic two, while Murray did so for fields with positive characteristics.

Kaplansky's question has an affirmative answer if G is **abelian**.

Kaplansky's question has an affirmative answer if G admits a left ordering.

Kaplansky's question has an affirmative solution if G has the so-called **unique product property**.

A group G has the **unique product property** if for all finite non-empty subsets A and B of G there exists $x \in G$ that can be written uniquely as $x = ab$ with $a \in A$ and $b \in B$.

Problem

When $G(X, r)$ has the unique product property?

Example (Jespers and Okniński)

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

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

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

$$\begin{aligned}x_1^2 &= x_2x_4, & x_1x_3 &= x_3x_1, & x_1x_4 &= x_4x_3, \\ x_2x_1 &= x_3x_2, & x_2^2 &= x_4^2, & x_3^2 &= x_4x_2,\end{aligned}$$

does not have the **unique product property**.

Let $x = x_1x_2^{-1}$ and $y = x_1x_3^{-1}$ and

$$S = \{x^2y, y^2x, xyx^{-1}, (y^2x)^{-1}, (xy)^{-2}, y, (xy)^2x, (xy)^2, \\ (xyx)^{-1}, yxy, y^{-1}, x, xyx, x^{-1}\}.$$

To prove that $G(X, r)$ does not have the **unique product property** it is enough to prove that each $s \in S^2 = \{s_1s_2 : s_1, s_2 \in S\}$ admits **at least two different decompositions** of the form $s = ab = uv$ for $a, b, u, v \in S$.

This set S is taken from the work of Promislow.

Our $G(X, r)$ is a finitely presented group. How can we do all these calculations?

We use a **faithful linear representation** of $G(X, r)$:

$$\begin{aligned} x_1 &\mapsto \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, & x_2 &\mapsto \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \\ x_3 &\mapsto \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, & x_4 &\mapsto \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Theorem (Etingof, Schedler and Soloviev)

Let (X, r) be a finite involutive solution. If $|X| = n$, then $G(X, r) \hookrightarrow \mathbf{GL}_{n+1}(\mathbb{Z})$.

The same trick works for almost all our solutions but there are **some open cases!**

Example:

Let $X = \{1, \dots, 8\}$ and $r(x, y) = (\sigma_x(y), \tau_y(x))$, where

$$\begin{array}{ll} \sigma_1 = \sigma_2 = (3745), & \tau_1 = \tau_2 = (3648), \\ \sigma_3 = \sigma_4 = (1826), & \tau_3 = \tau_4 = (1527), \\ \sigma_5 = \sigma_7 = (13872465), & \tau_5 = \tau_7 = (16542873), \\ \sigma_6 = \sigma_8 = (17842563), & \tau_6 = \tau_8 = (13562478). \end{array}$$

Then (X, r) is not a multipermutation solution. Does $G(X, r)$ have the **unique product property**?

Skew braces form a category. This is a **very nice** category, with several good properties in common with other classical algebraic structures.

Theorem (Bourn–Facchini–Pompili)

The category of skew braces is a semi-abelian category.

Question:

Can we linearize the notion of skew braces?

Why? Linear objects are always nicer, but... is this enough?

Question:

What should be a Lie-theoretic analog of a skew brace?

Since the beginning, Rump noted a connection between certain skew braces and Lie-theoretic objects. This connection was used by Bachiller to produce a finite solvable group that is not the multiplicative group of a skew brace of abelian type.

The connection between skew braces of abelian type and Lie theory was further studied by Smoktunowicz.

Question:

How do these things fit with the questions raised earlier?

The key idea to linearize skew braces is to replace sets by cocommutative coalgebras.

And now, I will assume that the audience is familiar with Hopf algebras. I also need to assume the audience is fond of using the infamous (yet lovely) Sweedler notation: For a coalgebra C , the comultiplication is denoted by

$$\Delta: C \rightarrow C \otimes C, \quad \Delta(c) = c_1 \otimes c_2$$

(With Angiono and Galindo) A **Hopf brace** is structure over a co-commutative coalgebra (A, Δ, ϵ) consist of the following data:

- ▶ a Hopf algebra structure $(A, \cdot, 1, \Delta, \epsilon, S)$, and
- ▶ a Hopf algebra structure $(A, \circ, 1_\circ, \Delta, \epsilon, T)$,

such that

$$a \circ (bc) = (a_1 \circ b)S(a_2)(a_3 \circ c)$$

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

The key example

Simply take the complex group algebra of a skew brace to obtain a basic example of a [Hopf brace](#). (Please don't confuse the operations!)

Why Hopf algebras? They simultaneously generalize **groups** (via group algebras) and **Lie algebras** (via the universal enveloping algebras of Lie algebras).

The idea is promising, as it allows us to recover **skew braces** as Hopf braces over group algebras.

As in the classical case, Hopf braces form a nice category.

Theorem (Gran–Sciandra)

The category of Hopf braces is semi-abelian.

Gran and Sciandra also showed that the relationship between skew braces and Hopf braces goes far beyond simply taking group algebras:

Theorem (Gran–Sciandra)

The category of skew braces is a localization of the category of Hopf braces.

What about Lie-theoretic analogs of skew braces?

A **left symmetric algebra** is a vector space V with a bilinear map $V \times V \rightarrow V$, $(x, y) \mapsto xy$, such that $x(yz) - (xy)z = y(xz) - (yx)z$ for all $x, y, z \in V$.

Fact: If V is a left symmetric algebra, then V with $[x, y] = xy - yx$ is a Lie algebra.

Hopf braces formalize the fact that left symmetric algebras are Lie theoretical analogs of skew braces of abelian type. A phenomenon already observed by Bachiller and Rump.

Apart from the various papers¹ exploring the connection between skew braces and pre-Lie rings, Gran, and Sciandra, using the **semi-abelian** framework, noted that the so-called **primitive Hopf braces**, which appear as the “kernels” in the canonical short exact sequence of the **torsion theory**, are in fact the universal enveloping algebras of post-Lie algebras.

¹Authored by Smoktunowicz, Shalev and Smoktunowicz, and Trappeniers.

Thanks!