Skew braces, cabling and indecomposable solutions to the YBE

Leandro Vendramin

Vrije Universiteit Brussel

A conference in honor of Alberto Facchini
January 2023

Problem (Drinfeld)

Study set-theoretic solutions (to the YBE).

A set-theoretic solution (to the YBE) is a pair (X, r), where X is a set and $r\colon X \times X \to X \times X$ is a bijective map such that

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r).$$

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.

Problem

Construct (finite) set-theoretical solutions.

We deal with non-degenerate solutions, i.e. solutions

$$r(x, y) = (\sigma_x(y), \tau_y(x)),$$

where all maps $\sigma_x \colon X \to X$ and $\tau_x \colon X \to X$ are bijective. By convention, all our solutions will be non-degenerate.

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 contraint programming techniques.

Problem

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

The permutation group of an involutive solution (X, r) is the group

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

This group naturally acts on X.

An involutive solution (X, r) is indecomposable if $\mathcal{G}(X, r)$ acts transitively on X. A solution is decomposable if it is not indecomposable.

Fact:
(X, r) is decomposable if and only if $X = Y \cup Z$ (disjoint union) for non-empty subsets $Y, Z \subseteq X$ such that $r(Y \times Y) \subseteq Y \times Y$ and $r(Z \times Z) \subseteq Z \times Z$.

Example:

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

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

Then $\mathcal{G}(X,r) \simeq \mathbb{D}_8$ acts transitively on X. Thus (X,r) is indecomposable.

Example:
Let $X = \{1, 2, 3, 4\}$ and

$$r(x, y) = (\sigma_x(y), \tau_y(x)),$$

where

$$\sigma_1 = \sigma_2 = \tau_1 = \tau_2 = \mathrm{id}, \quad \sigma_3 = \tau_3 = (34), \quad \sigma_4 = \tau_4 = (12)(34).$$

Then (X, r) is decomposable. In fact, $X = \{1, 2\} \cup \{3, 4\}$ is a decomposition.

Problem

Prove that "almost all" finite involutive solutions are decomposable.

For example, prove that

$$\lim_{n\to\infty} \frac{\#\text{decomposable inv. solutions of size } n}{\#\text{inv. solutions of size } n} = 1.$$

Problem

Construct indecomposable involutive solutions (up to isomorphism) of “small” size.

A concrete instance of the problem is the construction (say, with computers) of all indecomposable solutions of size ≤ 48.

The diagonal of an involutive solution (X, r), where

$$r(x, y) = (\sigma_x(y), \tau_y(x)),$$

is the map

$$T\colon X \to X, \quad T(x) = \tau_x^{-1}(x).$$

Remarks:

- Etingof, Schedler and Soloviev proved that T is bijective with inverse $x \mapsto \sigma_x^{-1}(x)$.
- $r(T(x), x) = (T(x), x)$ for all x.
- The cycle structure of T is invariant under isomorphisms.

Theorem (Rump)

Let (X, r) be a finite involutive solution such that $T = \mathrm{id}$. Then (X, r) is decomposable.

Rump's theorem proved a conjecture of Gateva-Ivanova.

Theorem (with Ramírez)

Let (X,r) be a finite involutive solution of size $n=|X|$. If T is an n-cycle, then (X,r) is indecomposable.

Problem

Can we construct these solutions?

Theorem (with Ramírez)

Let (X, r) be a finite involutive solution of size $n = |X|$. If T is an $(n-1)$-cycle, then (X, r) is decomposable.

Theorem (with Ramírez)

Let (X, r) be a finite involutive solution of size $n = |X|$. If T is an $(n-2)$-cycle and n is odd, then (X, r) is decomposable.

Similarly:

Theorem (with Ramírez)

Let (X, r) be a finite involutive solution of size $n = |X|$. If T is an $(n-3)$-cycle and $3 \nmid n$, then (X, r) is decomposable.

Theorem (Camp-Mora and Sastriques)

Let (X, r) be a finite involutive solution of size $n = |X|$. If $\gcd(|T|, n) = 1$, then (X, r) is decomposable.

Ring theory (more precisely, skew braces) will help us to understand what is going on here.

If R is a ring, the operation

$$x \circ y = x + xy + y$$

is always associative with neutral element 0. We say that R is a radical ring if $(R, \circ)$ is a group.

Example of a radical ring:

$$R = \left\{ \frac{2x}{2y+1} : x, y \in \mathbb{Z} \right\}.$$

Theorem (Rump)

Let A be a radical ring. Then $r\colon A \times A \to A \times A$,

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

is an involutive solution.

Here z' denotes the inverse of the element z with respect to the circle operation.

Natural questions:

- Do we need radical rings to produce set-theoretic solutions?
- What about non-involutive solutions?

Definition:

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

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

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

Remarks:

1. This definition is motivated by the work on Cedó, Jespers and Okniński.
2. The map $\lambda \colon (A, \circ) \to \mathrm{Aut}(A, +)$, $a \mapsto \lambda_a$, $\lambda_a(b) = -a + a \circ b$, is a group homomorphism.

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)

Let A be 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. Moreover,

$$r_A^2=\mathrm{id}_{A\times A}\iff (A,+)\text{ is abelian.}$$

Skew braces "classify" solutions. We need the structure group of the solution (first considered by Etingof, Schedler and Soloviev):

$$G(X,r) = \langle X : xy = uv \text{ whenever } r(x,y) = (u,v) \rangle.$$

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.

Fact: If (X,r) is involutive, then ι is injective.

Now we know that $G(X,r)$ is a skew brace. Moreover, the permutation group $\mathcal{G}(X,r)$ is also a skew brace!

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

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

These results are based on similar results by Etingof, Schedler and Soloviev, Rump, and Lu, Yan and Zhu.

Skew braces are related to regular subgroups of the holomorph!

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

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, Childs and Featherstonhaugh, 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.

Skew braces and skew brace homomorphisms form (a very interesting) category. A concrete description of this fact appears in the recent work[1] of Bourn, Facchini and Pompili.

[1] D. Bourne, A. Facchini, M. Pompili. *Aspects of the category of skew braces*. Communications in Algebra, to appear.

Let us go back to solutions.

Let (X,r) be a finite involutive solution. For $k \geq 1$, let

$$\iota^{(k)}\colon X \to G(X,r), \quad x \mapsto kx = \underbrace{x + \cdots + x}_{k\text{-times}}$$

Theorem (with Lebed and Ramírez)

The map $\iota^{(k)}$ is injective.

From a solution we contruct other solutions by using cabling techniques. Let (X, r) be an involutive solution and $k > 0$. Then we extend the map r to $r_{G(X,r)}$ and we push this back using $\iota^{(k)}$:

$$r \rightsquigarrow r_{G(X,r)} \rightsquigarrow r^{(k)}$$

Crucial fact:
The diagonal map of $r^{(k)}$ is T^k.

Theorem (with Lebed and Ramírez)

If (X,r) is involutive, indecomposable and $\gcd(|X|,k)=1$, then $(X,r^{(k)})$ is indecomposable.

The theorem of Camp-Mora and Sastriques now follows from the previus theorem with $k=|T|$.

Theorem (with Lebed and Ramírez)

Let p and q be different prime numbers. Let (X, r) be a finite involutive indecomposable solution of size pq. In the cycle decomposition of T, there can be no cycle of length s with $(p-1)q < s < pq$ and $\gcd(s, p) = 1$.

Examples:

Let (X, r) be a finite indecomposable solution.

- If $|X| = 14$, then in T there are no cycles of sizes 9, 11, 13.
- If $|X| = 15$, then in T there are no cycles of sizes 11, 13, 14.

Our brace-theoretic techniques have other consequences.

Motivated by the theory of Garside groups Dehornoy defined the class of a finite involutive solution (X, r) as the minimal m such that

$$\sigma_{T^{m-1}(x)} \cdots \sigma_{T(x)} \sigma_x = \mathrm{id}$$

for all $x \in X$.

Fact:
The Dehornoy class of a solution always exists and is finite.

Theorem (with Lebed and Ramírez)

The Dehornoy class of a finite involutive solution (X, r) is the least common multiple of the orders of the σ_x in the additive group of the skew brace $\mathcal{G}(X, r)$.

Consequence:

If (X, r) is a finite indecomposable solution, then the Dehornoy class of (X, r) is the additive order of any σ_x.

Problem

What about non-involutive solutions?

Cabling techniques could be used in the context of skew braces, at least for skew braces with abelian additive group.

Problem

What about arbitrary skew braces?

Problem

Can we use "cabling techniques" in the context of Hopf–Galois structures?