Skew braces and the Yang-Baxter equation

Leandro Vendramin

Universidad de Buenos Aires

Spa
June 2019

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

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

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 $\sigma_x : X \to X$ and $\tau_x : X \to X$ are bijective.

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 a non-degenerate solution such that $r^2 = \mathrm{id}_{A\times A}$.

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

Do we need radical rings to produce set-theoretic solutions similar to those of Rump?

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 $a, b, c \in A$.

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 $r_A : A \times A \to A \times A$,

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

is a non-degenerate 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):

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

Theorem (with Smoktunowicz)

Let (X,r) be a non-degenerate 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.

Skew braces have a universal property:

Theorem (with Smoktunowicz)

Let (X, r) be a non-degenerate 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.

Radical rings are examples of skew braces!

This means that one can use method from ring theory and group theory to study solutions!

Let us consider non-degenerate involutive solutions.
If $r^2 = \mathrm{id}_{X\times X}$, then

$$x = \sigma_{\sigma_x(y)}(\tau_y(x)), \qquad\qquad y = \tau_{\tau_y(x)}(\sigma_x(y)).$$

Facts:

- The map $T\colon X \to X$, $x \mapsto \tau_x^{-1}(x)$, is bijective.
- $T\sigma_x T^{-1} = \tau_x^{-1}$ for all $x \in X$.
- The groups $\langle \sigma_x : x \in X\rangle$ and $\langle \tau_x : x \in X\rangle$ are isomorphic as permutation groups on X.

Important fact:
Let (X, r) be a non-degenerate involutive solution,

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

For $x, y \in X$ we define

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

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

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

the retraction of X.

The solution (X, r) is retractable if there exist $x, y \in X$ with $x \neq y$ such that $\sigma_x = \sigma_y$ and it is multipermutation if there exist $n \geq 1$ such that $|\mathrm{Ret}^n(X, r)| = 1$.

The number of (not multipermutation) involutive solutions.

n	4	5	6	7	8
solutions	23	88	595	3456	34528
not multipermutation	2	4	41	161	2375

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 $\mathrm{Ret}(X, r)$ is the solution over $\{1, 2, 3\}$ given by

$$\sigma_1 = \tau_1 = \mathrm{id}, \quad \sigma_2 = \sigma_3 = \tau_2 = \tau_3 = (23).$$

Since $\mathrm{Ret}^2(X, r)$ is then the flip over $\{1, 2\}$, it follows that $\mathrm{Ret}^3(X, r)$ has only one element.

Are there easier 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) non-degenerate, finite and involutive.

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–Bolinches, 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 non-degenerate finite involutive solution. Then (X, r) is multipermutation if and only if the group $G(X, r)$ is left orderable.

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

Theorem (with Lebed)

A finite involutive non-degenerate solution (X, r) is multipermutation if and only if $G(X, r)$ is diffuse.

This result implies the following:

Corollary (with Acri and Lutowski)

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

Diffuse groups appear in connection with the following well-known open problem:

Kaplansky 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 $g \in G$.

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 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 $b \in B$.

Diffuse groups have the unique product property. Nobody knows whether these two notions are equivalent.

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

$$\sigma_1=(12),\quad \sigma_2=(1324),\quad \sigma_3=(34),\quad \sigma_4=(1423),$$
$$\tau_1=(14),\quad \tau_2=(1243),\quad \tau_3=(23),\quad \tau_4=(1342).$$

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

$$x_1^2=x_2x_4,\quad x_1x_3=x_3x_1,\quad x_1x_4=x_4x_3,$$
$$x_2x_1=x_3x_2,\quad x_2^2=x_4^2,\quad x_3^2=x_4x_2,$$

does not have the unique product property.

Let $x = x_1 x_2^{-1}$ and $y = x_1 x_3^{-1}$ 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 $s \in S^2 = \{s_1 s_2 : s_1, s_2 \in S\}$ 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 $G(X,r)$:

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

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

Theorem (Etingof, Schedler and Soloviev)

Let (X,r) be a finite involutive non-degenerate 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 some only eight open cases!

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

$$\sigma_1 = \sigma_2 = (3745), \qquad \tau_1 = \tau_2 = (3648),$$
$$\sigma_3 = \sigma_4 = (1826), \qquad \tau_3 = \tau_4 = (1527),$$
$$\sigma_5 = \sigma_7 = (13872465), \qquad \tau_5 = \tau_7 = (16542873),$$
$$\sigma_6 = \sigma_8 = (17842563), \qquad \tau_6 = \tau_8 = (13562478).$$

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

Another approach through “ring theory”.

Fact

Let (X, r) be an involutive non-degenerate finite solution. Then (X, r) is multipermutation if and only if the brace $G(X, r)$ is right nilpotent.

The connection between multipermutation solutions and right nilpotency of braces depends on the work of several different authors: Cedó, Jespers, Okniński, Gateva–Ivanova, Rump, Smoktunowicz.

We say that a group G admits a factorization if $G = AB$ for subgroups A and B of G.

Theorem (Ito)

Let $G = AB$ be a factorizable group. If A and B are abelian, then G is meta-abelian (i.e. $[G, G]$ is abelian).

What about skew brace factorizations?

For skew braces one needs to consider strong left ideals.

A left ideal of a skew brace A is an additive subgroup I of A such that $-a+a\circ x\in I$ for all $a\in A$ and all $x\in I$. Strong left ideals are left ideals that are normal in the additive subgroup of the skew brace. An ideal is a strong left ideal that is also normal in the multiplicative group of the skew brace.

$$\{\text{left ideals}\}\subsetneq\{\text{strong left ideals}\}\subsetneq\{\text{ideals}\}$$

We found an analog of Ito theorem for skew braces.

Theorem (with Jespers, Kubat and Van Antwerpen)

Let $A = B \circ C$ be a factorization of the skew brace A into strong left ideals. If B and C are trivial as skew braces, then A is meta-trivial.

A skew brace A is meta-trivial if there exists a trivial ideal I such that A/I is a trivial skew brace.

Since $\mathcal{G}(X,r)$ is a quotient of the brace $G(X,r)$, we obtain the following corollary:

Corollary

Let (X,r) be a finite non-degenerate involutive solution. If the brace $\mathcal{G}(X,r)$ admits a factorization into trivial strong left ideals, then (X,r) is multipermutation.

It would be nice to find a good analog of the following result:

Theorem (Kegel–Wielandt)

Let $G = AB$ be a finite factorizable group. If A and B are nilpotent, then G is solvable.

The recent construction of simple braces of Cedó, Jespers and Okniński shows that finding a naive brace-theoretic version of this theorem is not possible.

Thanks!