Skew braces

Leandro Vendramin
Joint work with Agata Smoktunowicz

Universidad de Buenos Aires

Groups, rings and the Yang–Baxter equation
Spa, Belgium – June 2017

Alexander von Humboldt
Stiftung/Foundation

In 1992 Drinfeld propose to study set-theoretical solutions of the Yang–Baxter equation (YBE).

A set-theoretical solution 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 $\sigma, \tau : X \to X$ be bijections such that $\sigma\tau = \tau\sigma$. Then

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

is a solution.

More examples:

Let X be a group. Then:

- $r(x, y) = (xyx^{-1}, x)$ is a solution.
- $r(x, y) = (xy^{-1}x^{-1}, xy^2)$ is a solution.

Main problem

Construct (finite) set-theoretical solutions.

Applications:

- Representations of the braid group.
- Combinatorial knot theory.

The first papers devoted to set-theoretical solutions are those of Etingof, Schedler and Soloviev and Gateva-Ivanova and Van den Bergh.

Both papers deal with non-degenerate involutive solutions, i.e. solutions $r\colon X \times X \to X \times X$ such that $r^2 = \mathrm{id}$ and

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

where σ_x and τ_x are permutations of X for each $x \in X$.

Let us review the theory of non-degenerate involutive solutions.

Number $s(n)$ of finite non-degenerate involutive solutions of size n.

n	1	2	3	4	5	6	7	8	9
$s(n)$	1	2	5	23	88	595	3456	34528	?

Problems

- Compute $s(9)$.
- Estimate $s(n)$ for $n \to \infty$.

The **structure group** of a solution (X, r) is defined as

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

The group $G(X, r)$ acts on X by

$$x \cdot y = \sigma_x(y), \quad x, y \in X.$$

Theorem (Etingof, Schedler, Soloviev)

Let (X, r) be an involutive non-degenerate solution. Then there exists a bijective 1-cocycle

$$\pi \colon G(X, r) \to \mathbb{Z}^{(X)}$$

such that $x \mapsto x$, $x \in X$.

Recall that π is a 1-cocycle if and only if

$$\pi(gh) = \pi(g) + g \cdot \pi(h)$$

for all $g, h \in G(X, r)$.

Corollary

Let (X, r) be an involutive non-degenerate solution. Then the canonical map $X \to G(X, r)$ is injective.

Theorem (Etingof, Schedler, Soloviev)

Let (X, r) be a finite involutive non-degenerate solution. Then $G(X, r)$ is solvable.

Theorem (Gateva-Ivanova and Van den Bergh)

Let (X, r) be a finite involutive non-degenerate solution. Then $G(X, r)$ is torsion-free

Theorem (Chouraqui)

Let (X, r) be a finite involutive non-degenerate solution. Then $G(X, r)$ is a Garside group.

One can use bijective 1-cocycles to classify solutions but these cocycles are hard to compute. Braces were introduced by Rump as a tool for studying non-degenerate involutive solutions.

Definition:
A brace[1] is an abelian group $(A, +)$ with another group structure, defined by $(a, b) \mapsto ab$, such that

$$a(b + c) + a = ab + ac$$

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

Examples:

- $\mathbb{Z}/2 \times \mathbb{Z}/4$ with $(a, b)(c, d) = (a + c, b + d + 2(a + b)d)$.
- $\mathbb{Z}/p \times \mathbb{Z}/p$ with $(a, b)(c, d) = (a + c + bd, b + d)$.

[1] This definition was given by Cedó, Jespers and Okniński.

Theorem (Rump)

Let A be an abelian group. There exists a bijective correspondence between

- braces with additive group isomorphic to A, and
- pairs (G, π), where $\pi : G \to A$ is a bijective 1-cocycle.

Theorem (Rump)

Let A be a brace. Then $r_A : A \times A \to A \times A$,

$$r_A(a,b) = (ab - a, (ab-a)^{-1}ab),$$

is a non-degenerate involutive solution of the YBE.

Now we can translate the classification result of Etingof, Schedler and Soloviev into the language of braces.

Theorem

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

$$r_{G(X,r)}|_{X\times X} = r.$$

Radical rings are examples of braces!

This means that one can use methods from ring theory to study solutions of the YBE.

Using results of Catino and Rizzo and Bachiller one can classify finite braces. With Guarnieri we computed the number $b(n)$ of braces of size n (up to isomorphism).

n	1	2	3	4	5	6	7	8	9	10
$b(n)$	1	1	1	4	1	2	1	27	4	2
n	11	12	13	14	15	16	17	18	19	20
$b(n)$	1	10	1	2	1	357	1	8	1	11
n	21	22	23	24	25	26	27	28	29	30
$b(n)$	2	2	1	96	4	2	37	9	1	4

Problem

Compute $b(2^k)$ for $k \geq 5$.

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

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

Then (X, r) induces a solution on $\mathrm{Ret}(X, r) = X/\sim$.

An involutive solution (X, r) is said to be retractable if there exist $x, y \in X$ with $x \neq y$ such that $\sigma_x = \sigma_y$. We say that (X, r) is multipermutation if there exists n such that $\mathrm{Ret}^n(X, r)$ has only one element.

Conjecture (Gateva-Ivanova, 2004)

Let (X, r) be a non-degenerate involutive solution with X finite. Assume that $r(x, x) = (x, x)$ for all $x \in X$. Then $\sigma_x = \sigma_y$ for some $x \neq y$.

Cedó, Jespers y Okniński and independently Gateva-Ivanova and Cameron proved that the conjecture is true if the group

$$L(X, r) = \langle \sigma_x : x \in X \rangle$$

is abelian.

Here there is a counterexample:

Let $X = \{1, \ldots, 8\}$ and

$$r(x, y) = (\varphi_x(y), \varphi_y(x)),$$

where

$$\begin{aligned}
\varphi_1 &= (57), & \varphi_2 &= (68),\\
\varphi_3 &= (26)(48)(57), & \varphi_4 &= (15)(37)(68),\\
\varphi_5 &= (13), & \varphi_6 &= (24),\\
\varphi_7 &= (13)(26)(48), & \varphi_8 &= (15)(24)(37).
\end{aligned}$$

This counterexample was found using extensions of solutions. This theory of extensions and the corresponding cohomology of solutions was later developed in collaboration with Victoria Lebed.

Do we really understand retractability?

A group G is left orderable if there exists a total order $<$ such that $x < y \implies zx < zy$ for all $x, y, z \in G$.

Theorem (with Bachiller and Cedó)

A non-degenerate involutive solution (X, r) with $|X| \geq 3$ is a multipermutation solution if and only if the group $G(X, r)$ is left orderable.

Remark:
The implication $\Rightarrow$ was proved by Chouraqui and independently by Jespers and Okniński.

What if we want to study non-involutive solutions? Things are more complicated...

One still has the **structure group** but now in general the canonical map $X \to G(X,r)$ is not injective!

Example:
Let $X = \{1,2,3,4\}$, $\sigma = (12)$ and $\tau = (34)$. Then (X,r), where

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

is a solution. In $G(X,r)$:

$$x_1 x_1 = x_{\sigma(1)} x_{\tau(1)} = x_2 x_1 \implies x_1 = x_2.$$

One still has the **structure group** but now in general $G(X,r)$ has torsion and it is not solvable.

Example:
Let G be a non-abelian finite simple group and let X be a non-trivial conjugacy class of G. Then

$$r(x,y) = (xyx^{-1}, x)$$

is a solution. But:

- The commutator of $G(X,r)$ is a nontrivial finite group!
- $G(X,r)$ admits a quotient isomorphic to G, so $G(X,r)$ is not solvable!

Do we still have the bijective 1-cocycle? Yes, but we need to replace the free abelian group on X by

$$A(X,r) = \langle X : y_1 y = y_2 y_1 \rangle,$$

where

$$(x,y) \xrightarrow{r} (x_1,y_1) \xrightarrow{r} (x_2,y_2).$$

Theorem (Lu, Yan, Zhu; Soloviev)

Let (X,r) be a non-degenerate solution. Then there exists a bijective 1-cocycle

$$\pi\colon G(X,r) \to A(X,r).$$

Definition:
A skew brace is a group $(A, +)$ with another group structure, defined by $(a, b) \mapsto ab$, such that

$$a(b + c) = ab - a + ac$$

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

Skew braces have connections with different topics: rings, near-rings, triply factorizable groups, combinatorial knot theory, regular subgroups, Hopf–Galois extensions...

Theorem (with Smoktunowicz)

Let A be an (not necessarily) additive group that admits an exact factorization $A = B + C$. Then

$$aa' = b + a' + c,$$

where $a = b + c$, is a skew brace with additive group A and multiplicative group $B \times C$.

Proof: Use the bijective map $f\colon B \times C \to A$, $(b, c) \mapsto b - c$, to transport the structure of $B \times C$ into A.

As in the classical case, skew braces are equivalent to bijective 1-cocycles. The 1-cocycles have values in an arbitrary group!

To construct non-degenerate solutions with skew braces we need the following lemma.

Lemma

Let A be a skew brace. Then $\lambda\colon (A,\cdot) \to \mathrm{Aut}(A,+)$, $a \mapsto \lambda_a$, where $\lambda_a(b) = -a + ab$, is a group homomorphism.

Now we can construct non-degenerate solutions!

Theorem

Let A be a skew brace. Then $r_A : A \times A \to A \times A$,

$$r_A(a,b) = (\lambda_a(b), \lambda_a(b)^{-1}ab),$$

is a non-degenerate solution of the YBE.

Corollary (with Smoktunowicz)

Let A be a skew brace. Then (A, r_A) is a biquandle.

The pair (A, r_A) is a biquandle if and only if for each $a \in A$ there exists a unique $b \in A$ such that

$$r(a, b) = (a, b).$$

Biquandles are those solutions of the YBE that can be used to construct a coloring invariant of a knot. This means that one could use skew braces in combinatorial knot theory.

Theorem (with Smoktunowicz)

Let A be a finite skew brace. Then the solution r_A a permutation of even order. Moreover, the order of r_A is

$$2\exp(G/Z(G)),$$

where G is the additive group of the skew brace.

We translate the results of Lu, Yan, Zhu and Soloviev in the language of skew braces.

Theorem

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.

Based on the results of Catino and Rizzo, we can construct small skew braces. Let $c(n)$ be the number of non-isomorphic skew braces of size n.

n	1	2	3	4	5	6	7	8
$c(n)$	1	1	1	4	1	6	1	47
n	9	10	11	12	13	14	15	16
$c(n)$	4	6	1	38	1	6	1	1605
n	17	18	19	20	21	22	23	24
$c(n)$	1	49	1	43	8	6	1	855
n	25	26	27	28	29	30	31	32
$c(n)$	4	6	101	29	1	36	1	?

Problems:

- Classify simple skew braces.
- Develop the cohomology and the theory of extensions of non-involutive solutions and skew braces.
- Study knot invariants produced by skew braces and their cohomology.
- Construct/enumerate skew braces of small size.
- Is there a skew brace with solvable additive group and non-solvable multiplicative group?
- Is there a skew brace with nilpotent multiplicative group and non-solvable additive group?

Thanks!