Involutive set-theoretic solutions of the Yang-Baxter equation

Jan Okniński
new results come from a joint work with Ferran Cedó

Blankenberge, June 2023

Plan of the talk

1) set-theoretic solutions (X, r) and their permutation groups $\mathcal{G}(X, r)$

2) two approaches: decomposability and retractability of solutions

3) another algebraic tool: braces

4) simple solutions

5) solutions of square-free cardinality

Set-theoretic solutions of the YBE

A fundamental problem is to construct (and classify) all **set-theoretic solutions of the Yang-Baxter equation**. These are the bijective maps

$$r : X \times X \to X \times X,$$

defined for a nonempty set X, satisfying

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

considered as maps $X \times X \times X \to X \times X \times X$.

A set-theoretic solution $r : X \times X \to X \times X$, written in the form

$$r(x, y) = (\sigma_x(y), \gamma_y(x)), \quad \text{for } x, y \in X,$$

is **non-degenerate** if σ_x and γ_x are bijective maps from X to X, for all $x \in X$. And it is **involutive** if $r^2 = \mathrm{id}$.

For such solutions one easily verifies that

$$\gamma_y(x) = \sigma^{-1}_{\sigma_x(y)}(x), \quad \text{for all } x, y \in X.$$

Convention. In this talk, a solution of the YBE means a finite involutive, non-degenerate, set-theoretic solution of the Yang-Baxter equation.

By Sym_X we denote the symmetric group on the set X.

Every solution (X, r) of the YBE is equipped with a permutation group acting on X:

$$\mathcal{G}(X, r) = \langle \sigma_x \mid x \in X \rangle \subseteq \mathrm{Sym}_X$$

An example. Let X be a finite set and fix some $\sigma \in \mathrm{Sym}_X$. Then

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

defines a solution (X, r), called **a permutation solution**.

So here $\mathcal{G}(X, r) = \langle \sigma \rangle$ is a cyclic group.

If $\sigma = \mathrm{id}$ then (X, r) is called a **trivial solution**.

The **structure group:** $G(X,r) = \mathrm{gr}\langle X : xy = \sigma_x(y)\gamma_y(x); x, y \in X\rangle$.

The group $G(X,r)$ embeds into $F_n \rtimes \mathcal{G}(X,r) \subseteq F_n \rtimes \mathrm{Sym}_X$, where F_n is the free abelian group of rank n, in such a way that the projection onto F_n is a bijection (Etingof, Schedler, Soloviev, 1999).

We have a natural epimorphism $G(X,r) \longrightarrow \mathcal{G}(X,r)$.

Theorem 1 (Etingof, Schedler and Soloviev, 1999)

The groups $G(X,r)$ and $\mathcal{G}(X,r)$ are solvable.

First approach - decomposability of solutions

We say that a solution (X, r) is **decomposable** if

$$X = Y \cup Z$$

(a disjoint union) for some nonempty subsets $Y, Z \subseteq X$ such that for $y \in Y, z \in Z$ we have

$$\sigma_y(Y), \gamma_y(Y) \subseteq Y, \qquad \sigma_z(Z), \gamma_z(Z) \subseteq Z.$$

Lemma 2

(X, r) is indecomposable if and only if $\mathcal{G}(X, r)$ is transitive as a permutation group on X.

Theorem 3 (Etingof, Schedler, Soloviev)

If $|X| = p$ is a prime and (X, r) is an indecomposable solution, then $r(x, y) = (\sigma(y), \sigma^{-1}(x))$, for a permutation $\sigma \in \mathrm{Sym}_X$ which is a cycle of length p. (So, this is the permutation solution determined by σ.)

An important result of Rump (2005) shows that all **square-free** (meaning that $\sigma_x(x) = x$ for every $x \in X$) solutions (X, r), with $|X| > 1$, are decomposable.
However, it turned out that this is no longer true in full generality.

Ballester-Bolinches proposed (Oberwolfach, 2019) the question of describing all **primitive solutions**, i.e. those solutions with a primitive permutation group $\mathcal{G}(X, r)$.

Second approach - retract and multipermutation level

The **retract relation** on a solution (X, r) of the YBE (Etingof, Schedler and Soloviev, 1999) is the equivalence relation $\sim$ on X defined by:

$$x \sim y \quad \text{if and only if } \sigma_x = \sigma_y.$$

Then r induces a solution $\overline{r}$ on the set $\overline{X} = X/\sim$. The retract of the solution (X, r) is $\mathrm{Ret}(X, r) = (\overline{X}, \overline{r})$.

A solution (X, r) is said to be **irretractable** if $\sigma_x \neq \sigma_y$ for all distinct elements $x, y \in X$, otherwise the solution (X, r) is **retractable**.

One defines $\mathrm{Ret}^{n+1}(X, r) = \mathrm{Ret}(\mathrm{Ret}^n(X, r))$ for $n \geq 1$; where $\mathrm{Ret}^1(X, r) = \mathrm{Ret}(X, r)$.

And (X, r) is called a **multipermutation solution of level** n if $\mathrm{Ret}^n(X, n)$ is a solution of cardinality 1 and n is the smallest integer with this property.

Example 4

Let $X = \{1, 2, 3, 4\}$. Define permutations

$$\sigma_1 = (2, 3),\ \sigma_2 = (1, 4),\ \sigma_3 = (1, 2, 4, 3),\ \sigma_4 = (1, 3, 4, 2) \in \mathrm{Sym}_X .$$

Then (X, r) is a solution of the YBE, where $r(x, y) = (\sigma_x(y), \sigma^{-1}_{\sigma_x(y)}(x))$, for all $x, y \in X$.

Here $\mathcal{G}(X, r) = \langle \sigma_1, \sigma_2, \sigma_3, \sigma_4 \rangle$ is isomorphic to the dihedral group of order 8.

It is clear that $\mathcal{G}(X, r)$ acts transitively on X.

This is an example of an indecomposable and irretractable solution.

Let (X, r) and (Y, s) be solutions of the YBE. We write

$$r(x,y) = (\sigma_x(y), \gamma_y(x)) \quad \text{and} \quad s(t,z) = (\sigma'_t(z), \gamma'_z(t)),$$

for $x, y \in X$ and $t, z \in Y$.

A **homomorphism of solutions** $f\colon (X, r) \longrightarrow (Y, s)$ is a map $f\colon X \longrightarrow Y$ such that

$$f(\sigma_x(y)) = \sigma'_{f(x)}(f(y)) \text{ and } f(\gamma_y(x)) = \gamma'_{f(y)}(f(x)), \text{ for } x, y \in X.$$

One verifies that f is a homomorphism of solutions if and only if $f(\sigma_x(y)) = \sigma'_{f(x)}(f(y))$, for $x, y \in X$.

An example. The natural map $(X, r) \longrightarrow \mathrm{Ret}(X, r)$ is a homomorphism of solutions.

Newer tools - left braces (Rump, 2007)

A **left brace** is a set B with two binary operations, $+$ and $\cdot$, such that:
$(B, +)$ is an abelian group (the additive group of B),
$(B, \cdot)$ is a group (the multiplicative group of B),
and for $a, b, c \in B$

$$a \cdot (b + c) \;=\; (a \cdot b) + (a \cdot c) - a.$$

If we denote by $0, 1$ the neutral elements of $(B, +)$ and $(B, \cdot)$, then $1 = 0$.

Motivating examples include nilpotent rings R, that lead to left (and right) braces $(R, +, \cdot\ )$ with $\cdot$ defined by $a \cdot b = a + b - ab$.

Also: if $(B, +)$ is an abelian group and $\cdot$ and $+$ coincide, then $(B, +, \cdot\ )$ is a left (and right) brace.

In any left brace B there is an action $\lambda\colon (B,\cdot) \to \mathrm{Aut}(B,+)$, called **the lambda map** of B, defined by

$$\lambda(a) = \lambda_a \qquad \text{and} \quad \lambda_a(b) = a \cdot b - a,$$

for $a, b \in B$. We shall write $ab = a \cdot b$, for all $a, b \in B$.

A **trivial brace** is a left brace B such that $ab = a + b$, for all $a, b \in B$.

The **socle** of a left brace B is

$$\mathrm{Soc}(B) = \ker(\lambda) = \{a \in B \mid ab = a + b, \text{ for all } b \in B\}.$$

A **left ideal** of a left brace B is a subgroup L of the additive group of B such that $\lambda_a(L) \subseteq L$, for all $a \in B$.

An **ideal** of a left brace B is a normal subgroup I of the multiplicative group of B such that $\lambda_a(I) \subseteq I$, for all $a \in B$.

One easily verifies that for all $a, b \in B$ we have

$$ab^{-1} = a - \lambda_{ab^{-1}}(b) \quad \text{and} \quad a - b = a\lambda_{a^{-1}b}(b^{-1}).$$

In particular, every ideal I of a left brace B also is a subgroup of the additive group of B.

Then B/I inherits a left brace structure from B.

Example. $\mathrm{Soc}(B)$ is an ideal of the left brace B.

Example. Every Sylow subgroup of $(B, +)$ is a left ideal of B.

If (X, r) is a solution of the YBE, with $r(x, y) = (\sigma_x(y), \gamma_y(x))$, then its structure group

$$G(X, r) = \mathrm{gr}(x \in X \mid xy = \sigma_x(y)\gamma_y(x), \text{ for all } x, y \in X)$$

has a structure of left brace with lambda map satisfying $\lambda_x(y) = \sigma_x(y)$, for $x, y \in X$; where the additive group of $G(X, r)$ is the free abelian group with basis X.

The map $x \mapsto \sigma_x$, from X to $\mathcal{G}(X, r)$, extends to a group epimorphism $\phi : G(X, r) \longrightarrow \mathcal{G}(X, r)$ and $\ker(\phi) = \mathrm{Soc}(G(X, r))$.

This leads to the **natural structure of left brace** on $\mathcal{G}(X, r)$; such that ϕ is a homomorphism of left braces.

The **solution of the YBE associated** to a left brace B is (B, r_B), where

$$r_B(a, b) = (\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}(a)), \quad \text{for } a, b \in B.$$

Lemma 5

Let B be a left brace. Then $B/\operatorname{Soc}(B) \cong \mathcal{G}(B, r_B)$ as left braces.

It follows that the group $(B, \cdot)$ of a finite left brace B is solvable (because by Theorem 1 permutation groups $\mathcal{G}(X, r)$ are solvable).

Primitive solutions

Let G be a transitive permutation group on the set X (so $G \subseteq \mathrm{Sym}_X$).

A set $Y \subseteq X$ is called an **imprimitivity subset** if

$$gY = hY \quad \text{or} \quad gY \cap hY = \emptyset \quad \text{for all} \quad g, h \in G.$$

Clearly $Y = X$ and $Y = \{y\}, y \in Y$, satisfy this condition; they are called **trivial imprimitivity subsets**.

G is a **primitive** permutation group (on X) if X has no nontrivial imprimitivity subsets.

Otherwise, $X = \bigcup_{g \in G} gY$, so that $|Y|$ divides $|X|$.

Definition 6 (Ballester-Bolinches)

A solution (X, r) of the YBE is said to be **primitive** if its permutation group $\mathcal{G}(X, r)$ acts primitively on X.

Lemma 7

Let (X, r) be an irretractable solution of the YBE. Consider the group $G = \mathcal{G}(X, r)$ with its natural structure of left brace. Then, the map $\varphi : X \longrightarrow G$ defined by

$$\varphi(x) = \sigma_x \quad \text{for } x \in X$$

is an injective homomorphism of solutions of the YBE from (X, r) to the solution (G, r_G) associated to the left brace $G = \mathcal{G}(X, r)$.

Let $\varphi' : X \longrightarrow \varphi(X)$ be the bijection defined by $\varphi'(x) = \sigma_x$.

Let $\widetilde{\varphi} : G \longrightarrow \mathcal{G}(G, r_G)$ be the map defined by

$$\widetilde{\varphi}(g) = \lambda_g \quad \text{for } g \in G.$$

One shows that $(\varphi', \widetilde{\varphi})$ yields an isomorphism of permutation groups

$$\mathcal{G}(X, r) \longrightarrow \mathcal{G}(G, r_G)$$

of the sets X and $\varphi(X)$.

Conclusion: we may replace (X, r) by the solution (X', r'), where

$$X' = \{\sigma_x \mid x \in X\} \subseteq G = \mathcal{G}(X, r) \quad \text{and} \quad r' = (r_G)_{|X'}.$$

Theorem 8 (Cedó, Jespers, JO; 2020)

Let (X, r) be a primitive solution of the YBE with $|X| > 1$. Then $|X|$ is prime. Furthermore, $\sigma_x = \sigma_y$, for all $x, y \in X$, and σ_x is a cycle of length $|X|$. (So (X, r) is as in Theorem 3.)

The proof is based on the replacement of (X, r) by (X', r') (because primitive $\Rightarrow$ irretractable) and on a careful analysis of the brace structure (interplay of the multiplicative and the additive structures) of $\mathcal{G}(G, r_G)$; using in particular the classical result on the structure of solvable primitive permutation groups.

Simple solutions - recent results

Definition 9 (Vendramin, 2016)

A solution (X, r) of the YBE is **simple** if $|X| > 1$ and for every epimorphism $f : (X, r) \longrightarrow (Y, s)$ of solutions either f is an isomorphism or $|Y| = 1$.

It was shown that every indecomposable solution of the YBE is a so called dynamical extension (introduced by Vendramin) of a simple solution.

At that time, the only known simple solutions were:
- permutation solutions of prime cardinality p (as in Theorem 3);
- 2 solutions of cardinality 4 (as in Example 4);
- and 3 solutions of cardinality 9 (found by L.Vendramin with a computer).

Lemma 10

Let (X, r) be a simple solution of the YBE. If $|X| > 2$ then (X, r) is indecomposable.

As seen in Theorem 3, if (X, r) is an indecomposable solution of the YBE and $|X|$ is a prime, then it is a permutation solution (in particular it is retractable).
Actually, such solutions are simple.

Lemma 11

Let (X, r) be a simple solution of the YBE. If $|X|$ is not prime, then (X, r) is irretractable.

Recent constructions of simple solutions

Examples obtained so far are constructed:

1. via an approached based on systems of imprimitivity,
2. via simple left braces,
3. via asymmetric products of braces.

We present some constructions based on 1. and 2.

1. Let $(A, +)$ be a nontrivial (finite) abelian group. Let $(j_a)_{a \in A}$ be a family of elements of A such that $j_a = j_{-a}$ for all $a \in A$. We define

$$r\colon A^2 \times A^2 \longrightarrow A^2 \times A^2 \qquad \text{by:}$$

$$r((a_1, a_2), (c_1, c_2)) = \left(\sigma_{(a_1,a_2)}(c_1, c_2), \sigma^{-1}_{\sigma_{(a_1,a_2)}(c_1,c_2)}(a_1, a_2)\right),$$

where

$$\sigma_{(a_1,a_2)}(c_1, c_2) = (c_1 + a_2, c_2 - j_{c_1+a_2-a_1}),$$

for all $a_1, a_2, c_1, c_2 \in A$. It is easy to see that $\sigma_{(a_1,a_2)} \in \mathrm{Sym}_{A^2}$.

One verifies that this is a solution of the YBE.

It is clear that the sets $\{(a, x) : x \in A\}, a \in A$, form a system of imprimitivity for the action of the group $\mathcal{G}(A^2, r)$ on A^2.

Let $a \in A$ be a nonzero element. Let

$$V_{a,1} = \mathrm{gr}(j_c - j_{c+a} \mid c \in A) \subseteq A.$$

For every $i > 1$, define inductively

$$V_{a,i} = V_{a,i-1} + \mathrm{gr}(j_c - j_{c+v} \mid c \in A,\ v \in V_{a,i-1}).$$

Let $V_a = \sum_{i=1}^{\infty} V_{a,i}$. Note that $V_a = \bigcup_{i=1}^{\infty} V_{a,i} \subseteq A$.

Theorem 12

The solution (A^2, r) is simple if and only if $V_a = A$ for every $a \in A, a \neq 0$.

A modification of this approach allows also to construct several concrete examples of simple solutions of size nm^2, for every $n, m > 1$.

2. Recall that a non-zero left brace B is **simple** if $\{0\}$ and B are the only ideals of B.

Theorem 13

Let B be a finite non-trivial simple left brace such that there exists an orbit $X \subseteq B$ under the action of the lambda map such that $B = \mathrm{gr}(X)_+$. Then the solution (X, r) of the YBE, where

$$r(x, y) = (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x)), \quad \textit{for all } x, y \in X,$$

is a simple solution of the YBE.

Several classes of simple left braces have been recently constructed (Bachiller, Cedó, Jespers, JO). They can be used in this context.

In particular, for every distinct primes $p_1, \ldots, p_n$ there exist integers $k_1, \ldots, k_n$ such that for every $m_1 > k_1, \ldots, m_n > k_n$ there exists a simple left brace of size $p^{m_1} \cdots p^{m_n}$.

Solutions of square-free cardinality

The main result is quite surprising and it reads as follows.

Theorem 14

Let n be a positive integer. Let $p_1, \ldots, p_n$ be distinct prime numbers. Let (X, r) be an indecomposable solution of the YBE of cardinality $|X| = p_1 \cdots p_n$. Then (X, r) is a multipermutation solution of level $\leq n$. In particular, (X, r) is not a simple solution if $n > 1$.

The proof is based on a detailed study of the brace structure on the permutation group $\mathcal{G}(X, r)$ associated to such a solution.

It goes by induction on n.

But first, the structure of $\mathcal{G}(X, r)$ is described in the case of multipermutation solutions (used in the inductive step);
this assumption is then removed in the proof of the main theorem!

Theorem 15

Let $p_1, \dots, p_n$ be distinct prime numbers. Assume that (X, r) is an indecomposable multipermutation solution of the YBE of cardinality $p_1 \cdots p_n$. Let P_i be the Sylow p_i-subgroup of the additive group of the left brace $\mathcal{G}(X, r)$, for $i = 1, \dots, n$. Then the following conditions hold.

(i) *Every P_i is a trivial brace over an elementary abelian p_i-group.*

(ii) *There exists a permutation $\sigma \in \mathrm{Sym}_n$ such that*

$$P_{\sigma(1)} \subseteq P_{\sigma(1)}P_{\sigma(2)} \ \subseteq \ \cdots \ \subseteq \ P_{\sigma(1)}P_{\sigma(2)}\cdots P_{\sigma(n)} = \mathcal{G}(X, r)$$

are ideals of the left brace $\mathcal{G}(X, r)$, $P_{\sigma(1)} \subseteq \mathrm{Soc}(\mathcal{G}(X, r))$ and

$$(P_{\sigma(1)}\cdots P_{\sigma(i)})/(P_{\sigma(1)}\cdots P_{\sigma(i-1)}) \subseteq \mathrm{Soc}(\mathcal{G}(X, r)/(P_{\sigma(1)}\cdots P_{\sigma(i-1)}))$$

for every $1 < i \leq n$.

In particular, $|X|$ and $|\mathcal{G}(X, r)|$ have the same prime divisors.

Tools 1: inductive step

If $n = 1$, (X, r) is a permutation solution with $\mathcal{G}(X, r) \simeq C_{p_1}$, by Theorem 3.

Let $n > 1$. By [Cedo, Jespers, Kubat, van Antwerpen, Verwimp, 2023]: the solution $(\mathcal{G}(X, r), r_{\mathcal{G}})$ associated to the left brace $\mathcal{G}(X, r)$ is also a multipermutation solution.

In particular, $\mathrm{Soc}(\mathcal{G}(X, r))$ is a nontrivial ideal. Then $\mathrm{Soc}(\mathcal{G}(X, r))$ is an abelian normal subgroup and we choose a Sylow p-subgroup P of $\mathrm{Soc}(\mathcal{G}(X, r))$ for some p.

Then P is normal in $\mathcal{G}(X, r)$. And P-orbits on X form a system of imprimitivity $S = \{P(x) : x \in X\}$ for $\mathcal{G}(X, r)$ on X.

So $p = p_i$ for some i; say $p = p_1$. Then $|P(x)| = p$ for $x \in X$ and $|S| = p_2 \cdots p_n$. And $\mathcal{G}(X, r)$ acts on S.

Let K be the kernel of this action. One shows that $K = P$ is an ideal of $\mathcal{G}(X, r)$. Moreover, r induces a solution (S, s) of the YBE.
This allows an inductive step when proving Theorem 15.

Tools 2: semidirect products of braces

Let B be a left brace. Suppose that I is an ideal of B and L is a left ideal of B such that $I \cap L = \{0\}$ and $B = IL$. If $a \in I$ and $b \in L$, then

$$b \cdot b^{-1}ab = ab = \lambda_a(b) \cdot \lambda^{-1}_{\lambda_a(b)}(a).$$

Since $I \cap L = \{0\}$, and $b, \lambda_a(b) \in L$, and $b^{-1}ab, \lambda^{-1}_{\lambda_a(b)}(a) \in I$, we get

$$\lambda_a(b) = b, \quad \text{which means that} \quad ab = a + b$$

for all $a \in I$ and $b \in L$.

The map $\alpha\colon (L, \cdot) \longrightarrow \mathrm{Aut}(I, +, \cdot)$, defined by $\alpha(b)(a) = \lambda_b(a)$ for all $a \in I$ and $b \in L$, is a homomorphism of groups.

Then B is the semidirect product $I \rtimes_\alpha L$ of the left braces I and L; namely a left brace with addition defined for all $a_1, a_2 \in I$, $b_1, b_2 \in L$ by

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

(The multiplicative group of B is a semidirect product of the multiplicative groups of I and L.)

Tools 3: abelian normal Sylow subgroups

The proof of Theorem 14 uses a sufficient condition for retractability of a solution (X, r).

Lemma 16

Let (X, r) be a solution of the YBE. Then $\lambda_g(\sigma_x) = \sigma_{g(x)}$, for all $g \in \mathcal{G}(X, r)$ and all $x \in X$.

Theorem 17

Let (X, r) be a solution of the YBE. Suppose that $\mathcal{G}(X, r)$ has an abelian normal Sylow p-subgroup T, for some prime divisor p of $|\mathcal{G}(X, r)|$. Then (X, r) is retractable.

Proof.

Since the p-Sylow subgroup P of the additive group of the left brace $\mathcal{G}(X, r)$ is a left ideal and $|T| = |P|$, we get that $T = P$ and it is an ideal of the left brace $\mathcal{G}(X, r)$.

Let C be the Hall p'-subgroup of the additive group of the left brace $\mathcal{G}(X,r)$. Then $\mathcal{G}(X,r) = TC$ is a semidirect product (as left braces) of the ideal T and the left ideal C.

By using the structure of the semidirect product, we know that $t + c = tc$ for $t \in T, c \in C$, and consequently

$$\lambda_t(t_1c_1) = -t + tt_1c_1 = -t + tt_1 + c_1 = (-t + tt_1)c_1 = \lambda_t(t_1)c_1 \quad (1)$$

for all $t, t_1 \in T$ and $c_1 \in C$.

Since T is a finite non-zero left brace with abelian multiplicative group, by [Rump] $\mathrm{Soc}(T) \neq \{\mathrm{id}\}$. Let $t \in \mathrm{Soc}(T) \setminus \{\mathrm{id}\}$. There exists $x \in X$ such that $t(x) \neq x$. Let $t_x \in T$ and $c_x \in C$ be such that $\sigma_x = t_xc_x$.

By Lemma 16 and (1), we get

$$\sigma_{t(x)} = \lambda_t(\sigma_x) = \lambda_t(t_xc_x) \overset{(1)}{=} \lambda_t(t_x)c_x = t_xc_x = \sigma_x.$$

Therefore (X,r) is retractable and the result follows.

An example

From Theorem 14 wee know that if (X, r) is an indecomposable solution of the YBE of cardinality $p_1 \cdots p_n$, where $p_1, \dots, p_n$ are n distinct prime numbers, then (X, r) is a multipermutation solution of level $\leq n$.

We continue with an example showing that indecomposable solutions of the YBE of cardinality $p_1 \cdots p_n$ and multipermutation level n indeed exist.

Let (X_0, r_0) denote the solution of cardinality $|X_0| = 1$.

Let $|X_1| = p_1$ and let (X_1, r_1) be an indecomposable solution of the YBE. We know that $\mathcal{G}(X_1, r_1) = \mathbb{Z}_{p_1}$.

Suppose that we have constructed indecomposable solutions (X_i, r_i) of the YBE of cardinality $p_1 \cdots p_i$, for all $1 \leq i < n$, such that

$$\mathrm{Ret}(X_i, r_i) = (X_{i-1}, r_{i-1}) \text{ and } \mathcal{G}(X_i, r_i) \cong \mathbb{Z}_{p_i}^{|X_{i-1}|} \rtimes_\alpha \mathcal{G}(X_{i-1}, r_{i-1}),$$

as left braces, where

$$\alpha\colon \mathcal{G}(X_{i-1}, r_{i-1}) \longrightarrow \mathrm{Aut}(\mathbb{Z}_{p_i}^{|X_{i-1}|}) \quad \text{is defined by}$$

$$\alpha(g)((a_x)_{x \in X_{i-1}}) = (a_{g^{-1}(x)})_{x \in X_{i-1}},$$

for all $g \in \mathcal{G}(X_{i-1}, r_{i-1})$ and $a_x \in \mathbb{Z}_{p_i}$.

Let $X_n = \mathbb{Z}_{p_n} \times X_{n-1}$. We define $r_n\colon X_n \times X_n \longrightarrow X_n \times X_n$ by

$$r_n((a,x),(b,y)) = (\sigma_{(a,x)}(b,y), \sigma^{-1}_{\sigma_{(a,x)}(b,y)}(a,x))$$

for all $(a,x),(b,y) \in X_n$, where

$$\sigma_{(a,x)}(b,y) = (b + \delta_{x,\sigma_x(y)}, \sigma_x(y))$$

and the permutations σ_x correspond to the solution (X_{n-1}, r_{n-1}).

Then (X_n, r_n) is an indecomposable solution of permutation level n and

$$\mathcal{G}(X_n, r_n) \cong \mathbb{Z}_{p_n} \wr (\mathbb{Z}_{p_{n-1}} \wr (\dots (\mathbb{Z}_{p_2} \wr \mathbb{Z}/_{p_1}) \dots)).$$

Beyond the square-free case

Theorem 18

Let (X, r) be a finite indecomposable multipermutation solution of the YBE. Then, for every prime number p

$$p \text{ is a divisor of } |X| \text{ if and only if } p \text{ is a divisor of } |\mathcal{G}(X, r)|.$$

The proof is based on an induction on $n = |X|$ and on the fact that

$$\mathcal{G}(\operatorname{Ret}(X, r)) \cong \mathcal{G}(X, r)/\operatorname{Soc}(\mathcal{G}(X, r)).$$

Hence, prime divisors of $|X|$ behave in this case in the same way as in the case where $|X|$ is square-free.

Leandro Vendramin found an example of an indecomposable solution (X, r) of the YBE with $|X| = 8$, such that $\mathcal{G}(X, r) \cong \mathrm{Sym}_4$, showing that the above result does not hold for irretractable solutions.

The example is determined by the following permutations:

$$
\begin{aligned}
&\sigma_1 = (1,2)(3,4)(5,6)(7,8), \quad \sigma_2 = (1,2)(3,6)(4,7)(5,8),\\
&\sigma_3 = (1,5,4,3)(2,6,7,8), \quad \sigma_4 = (1,3,6,7)(2,8,5,4),\\
&\sigma_5 = (1,7)(2,4)(3,8)(5,6), \quad \sigma_6 = (1,7,6,3)(2,4,5,8),\\
&\sigma_7 = (1,3,4,5)(2,8,7,6), \quad \sigma_8 = (1,5)(2,6)(3,8)(4,7).
\end{aligned}
$$

Let $Y = \{1, 2\}$ and let (Y, s) be the unique indecomposable solution of cardinality 2. Let $f : X \longrightarrow Y$ be the map defined by $f(1) = f(4) = f(6) = f(8) = 1$ and $f(2) = f(3) = f(5) = f(7) = 2$. Then f is an epimorphism of solutions from (X, r) to (Y, s).

So (X, r) is an indecomposable irretractable solution which is not simple.

Some references

1. F. Cedó, E. Jespers and J. Okniński, Primitive set-theoretic solutions of the Yang-Baxter equation, Commun. Contemp. Math. 9 (2022) 2150105, 10 pp.

2. F. Cedó and J. Okniński, Constructing finite simple solutions of the Yang-Baxter equation, Adv. Math. 391 (2021), 107968, 39 pp.

3. F. Cedó and J. Okniński, New simple solutions of the Yang-Baxter equation and solutions associated to simple left braces, J. Algebra 600 (2022), 125–151.

4. F. Cedó and J. Okniński, Indecomposable solutions of the Yang-Baxter equation of square-free cardinality, preprint arXiv:2212.06753.