University of Exeter

Indecomposable solutions to the YBE

Ilaria Colazzo

I.Colazzo@exeter.ac.uk

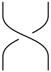
June 7, 2023

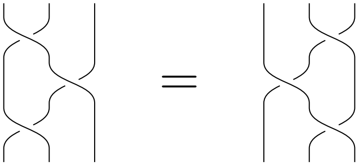
Advances in Group Theory and Applications 2023

Solutions of the Yang-Baxter equation

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

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

Write $r =$  . Then $(*)$ becomes



Set-theoretic solutions to the Yang-Baxter equation

Let (X, r) be a set-theoretic solution to the YBE. Write

$$r(x, y) = (\lambda_x(y), \rho_y(x))$$

where $\lambda_x, \rho_x : X \to X$.

- (X, r) is involutive if $r^2 = \mathrm{id}$.
- (X, r) is finite if X is finite.
- (X, r) is non-degenerate if λ_x and ρ_x are bijective for all $x \in X$.

Convention. From now on

solution = finite bijective non-degenerate set-theoretic solution to the YBE.

Examples

X a set.

- $r(x, y) = (y, x)$ is an involutive (i.e. $r^2 = \mathrm{id}_{X\times X}$) non-degenerate solution.
- f, g permutaion of X. Then $r(x, y) = (f(y), g(x))$ is a solution if and only if $fg = gf$.

  Morever, (X, r) is involutive if and only if $g = f^{-1}$

  (X, r) is called a permutational solution or a Lyubashenko's solution.

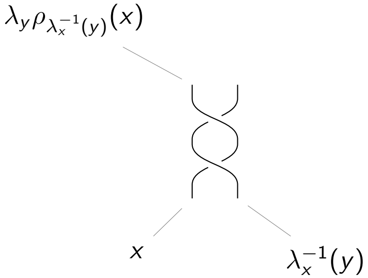
G a group.

- $r(x, y) = (y, y^{-1}xy)$ is a bijective non-degenerate solution.

The derived solution

Let (X, r) be a solution. The left derived solution (X, s) is the solution $s : X \times X \to X \times X, (x, y) \mapsto (y, \sigma_y(x))$ where

$$\sigma_y(x) = \lambda_y \rho_{\lambda_x^{-1}(y)}(x).$$



Derived solutions and racks

Let (X, r) a solution and (X, s) its derived solution. Define a binary operation on X in the following way $x \triangleright y = \sigma_x(y)$. Then $(X, \triangleright)$ is a rack, i.e.

- the maps σ_x are bijective, and
- $x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z)$, for all $x, y, z \in X$.

Conversely, if $(X, \triangleright)$ is a rack that the map $s : X \times X \to X \times X$ defined by $r(x, y) = (y, y \triangleright x)$ is a solution.
We call such a solution, solution associated to the rack $(X, \triangleright)$.

Example

Let G be a group and define $x \triangleright y = x^{-1}yx$. Then $(G, \triangleright)$ is a rack (called conjugation rack) and its associated solution if

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

Indecomposable solutions

A solution (X, r) is decomposable if there exists a partition $\emptyset \neq Y, Z \subseteq X$ such that $X = Y \cup Z$ and $Y \cap Y = \emptyset$ such that

$$r(Y \times Y) \subseteq Y \times Y \quad \text{and} \quad r(Z \times Z) \subseteq Z \times Z.$$

Otherwise, the solution is said to be indecomposable.

Indecomposable solutions

Fact. A solution (X, r) is indecomposable if and only if the group

$$\mathrm{gr}(\lambda_x, \rho_y \colon x, y \in X)$$

acts transitively on X.

Indecomposable solutions

Examples

- Let X be a set with n elements and let f be a cycle of length n. Then $r : X \times X \to X \times X, (x, y) \mapsto (f(y), x)$ is an indecomposable solution.
- Let $X = \{1, 2, 3, 4\}$, $\lambda_x = \text{id}$ for any $x \in X$ and

$$\rho_x = \begin{cases} (3\ 4) & \text{if } x = 1, 2 \\ (1\ 2) & \text{if } x = 3, 4. \end{cases}$$

Then $r : X \times X \to X \times X, (x, y) \mapsto (\lambda_x(y), \rho_y(x))$ is a decomposable solution with orbits $\{1, 2\}$ and $\{3, 4\}$.

Problem. Construct indecomposable solutions.

Involutive indecomposable solutions

Facts. Let (X, r) be an **involutive** solution. Then

- $\rho_y(x) = \lambda^{-1}_{\lambda_x(y)}(x)$, for all $x, y \in X$.
- (X, r) is indecomposable if and only if $\mathrm{gr}(\lambda_x \colon x \in X)$ is transitive on X.

The diagonal map

Let (X, r) be a **involutive** solution. The map $T : X \to X$ defined by

$$T(x) = \lambda_x^{-1}(x).$$

is bijective and it is called the diagonal map.

Important. The cycle decomposition of T is an invariant for solutions and gives information about decomposability.

Square-free solutions

A solution (X, r) is square-free if $r(x, x) = (x, x)$ (i.e., $T = \mathrm{id}$).

Theorem (Rump, conjecture by Gateva-Ivanova)**.** If (X, r) is a square-free **involutive** solution, then (X, r) is decomposable.

Problem. What can we say about the cycle decomposition of T for (in)decomposable solutions?

Some results

Let (X, r) be a solution and assume $|X| = n$.

- (Ramírez & Vendramin) If T is a n-cycle, then (X, r) is indecomposable.
- (Ramírez & Vendramin) If T is a $(n-1)$-cycle, then (X, r) is decomposable.
- (Ramírez & Vendramin) If T is a $(n-2)$-cycle, n odd, then (X, r) is decomposable.
- (Ramírez & Vendramin) If T is a $(n-3)$-cycle, $\gcd(n, 3) = 1$ odd, then (X, r) is decomposable.
- (Camp-Mora & Sastriques) If $\gcd(\text{order}(T), n) = 1$, then (X, r) is decomposable.

Skew braces

A skew brace is a triple $(B, +, \circ)$ such that $(B, +)$ and $(B, \circ)$ are (not necessarily abelian) groups and the following holds

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

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

- $(B, +)$ is the additive structure of $(B, +, \circ)$.
- $(B, \circ)$ is the multiplicative structure of $(B, +, \circ)$.

Skew braces

Examples

- Let $(G, +)$ be (any) group. Then $(G, +, +)$ and $(G, +^{op}, +)$ are skew braces.
- Any radical ring is a skew brace.

Definition. Let (X, r) be a solution. Define the structure group

$$G(X, r) = \mathrm{gr}(X \mid x \circ y = \lambda_x(y) \circ \rho_y(x)).$$

has a structure of skew brace with additive structure isomorphic to $\mathbb{Z}^{|X|}$.

Facts.

- If B is a skew brace, then $r_B(a, b) = (-a + a \circ b, (-a + a \circ b)' \circ a \circ b)$ is a solution.
  If, in addition, $(B, +)$ is abelian then r_B is involutive.
- If (X, r) is an **involutive** solution then (X, r) extends to $(G(X, r), r_{G(X,r)})$.
- If (X, r) is an **involutive** solution then $\iota : X \to G(X, r)$, $x \to x$ is injective.

Idea: cabling

Lebed, Ramírez & Vendramin

Let (X,r) be an involutive solution. For $k \geq 1$, the map $\iota^{(k)} : X \to G(X,r)$, $x \mapsto kx$ is injective.

$$\begin{array}{ccc} (X,r) & \overset{\text{extend}}{\longrightarrow} & (G(X,r), r_{G(x,r)}) \\ & & \downarrow \\ & & r^{(k)} \end{array} \qquad \text{pull-back using } \iota^{(k)}$$

k-cabled solution

Theorem (Lebed, Ramírez & Vendramin)**.**

- The diagonal map of $r^{(k)}$ is T^k.
- If (X, r) indecomposable and $\gcd(|X|, k) = 1$, then $r^{(k)}$ is indecomposable.

  Taking $k = |T|$ Camp-Mora & Sastriques theorem reduces to Rump's theorem.

Question. What about cabling for non-involutive solutions?

Main issues (1)

Let (X, r) be a solution. One of the main issues is that $\iota : X \to G(X, r)$, $x \mapsto x$ is not an injective map.

Example. Let $X = \{1, 2, 3, 4\}$ be a set, $f = (1\ 2)$ and $g = (3\ 4)$, then $fg = gf$ and the map $r(x, y) = (f(y), g(x))$ is a solution. It is easy to see that (X, r) is not injective. Indeed in $G(X, r)$ we have $1 = 2$ and $3 = 4$.

The injectivization

Let (X, r) be a e solution and let $\iota : X \to G(X, r)$ $x \mapsto x$. Then

$$\mathrm{Inj}(X, r) = (\iota(X), r_{G(X,r)}|_{\iota(X)\times\iota(X)})$$

is a solution and

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

Injective solutions

A solution (X, r) is injective if the map $\iota : X \to G(X, r)$ is injective.

Examples.

- (X, r) a solution $\mathrm{Inj}(X, r)$ is an injective solution.
- Solutions associated to skew braces are injective.
- Irretractable solutions are injective.

We can focus on injective solutions

Theorem (IC & Van Antwerpen). Let (X, r) be a solution. Then

$$(X, r) \text{ is decomposable} \iff \text{Inj}(X, r) \text{ is decomposable.}$$

Hence, we can focus simply on **injective** solutions.

Main issues (2)

Recall that in the definition of the k-cabled solution it was crucial that the map $\iota^{(k)}: X \to G(X,r)$, $x \mapsto kx$ is injective.
However, this fails for injective solutions.

Example. Let $X = \{x_1, x_2, x_3\}$ and $\sigma_1 = (2\ 3)$, $\sigma_2 = (1\ 3)$ and $\sigma_3 = (1\ 2)$. The solution

$$r(x_j, x_k) = (x_k, x_{\sigma_k(j)})$$

is injective and indecomposable. But in $G(X,r)$ one has that $2x_1 = 2x_2 = 2x_3$.

The structure monoid

Let (X, r) be a solution. The structure monoid is the monoid

$$M(X,r) = \langle X \mid x \circ y = \lambda_x(y) \circ \rho_y(x) \rangle.$$

Facts.

- If (X, r) is a solution then (X, r) extends in a unique way a solution r_M on $M(X, r)$ such that

  $$r_{M(X,r)}(\iota \times \iota) = (\iota \times \iota) r$$

  where $\iota : X \to G(X, r)$ is the canonical map.
- $M(X,r) \overset{\text{regular}}{\hookrightarrow} A(X,r) \rtimes \operatorname{Sym} X$, where $A(X,r) = \langle X \mid x + z = z + \sigma_z(x) \rangle$ is the structure monoid associated to the derived solution.

k-cabled solutions

Prop (IC, Van Antwerpen). Let (X, r) be an injective solution. Then $kX = \{(kx, \lambda_{kx})\} \subseteq M(X, r)$ defines a subsolution (kX, r_k) of $(M(X, r), r_M)$.

Definition. Let (X, r) be an injective solution and let $r^k = (\varphi_k^{-1} \times \varphi_k^{-1}) r_k (\varphi_k \times \varphi)$ where $\varphi_k : X \to kX, x \mapsto kx$. Then $(X, r^{(k)})$ is the k-cabled solution.

Prop. Let (X, r) be an injective solution

- If k is an integer, then $(X, r^{(k)})$ is injective.
- If k, k' are integers, then $(X, (r^{(k)})^{(k')}) = (X, r^{(kk')})$.

Theorem (IC, Van Antwerpen)**.**

- The diagonal of $r^{(k)}$ is T^k.
- If (X, r) indecomposable and $\gcd(|X|, k)$, then $r^{(k)}$ is indecomposable.

Decomposability results

Theorem (Darné). Let $(X, \triangleright)$ be a rack with $|X| > 1$ such that $x \triangleright x = x$ (i.e. $(X, \triangleright)$ is a quandle), and let $(X, r_\triangleright)$ the solutions associated to $(X, \triangleright)$. If the structure group $G(X, r_\triangleright)$ is nilpotent and not isomorphic to $\mathbb{Z}$, then $(X, r_\triangleright)$ is decomposable.

We obtained a completely group theoretical proof of this result.

Corollary. Let $(X, \triangleright)$ be a rack and let $(X, r_\triangleright)$ the solutions associated to $(X, \triangleright)$. If the structure group $G(X, r_\triangleright)$ is nilpotent and not isomorphic to $\mathbb{Z}$, then $(X, r_\triangleright)$ is decomposable.

Is nilpotent an essential assumption?

Example. Consider the group S_3 and consider the conjugation quandle on S_3, i.e. $x \triangleright y = x^{-1}yx$ and (S_3, s) its associated solution. We can restrict the map s to $X = \{(1\ 2), (2\ 3), (1\ 3)\}$. One can prove that

- $(X, s_{X \times X})$ is a square-free, indecomposable solution.
- $G(X, s_{X \times X})$ is not nilpotent.

Square-free solutions

Let (X, r) be a solution and (X, s) its derived solution. If (X, r) is square-free and $A_g(X, r) = G(X, s)$ is nilpotent, then (X, r) is decomposable.

Thank you!!!