University of Exeter

Derived-indecomposable solutions and skew braces with a finiteness condition

Ilaria Colazzo

I.Colazzo@exeter.ac.uk

May 29 – June 2, 2023

Hopf algebras and Galois module theory

Based on a joint work with Maria Ferrara and Marco Trombetti.

I. Colazzo, M. Ferrara, and M. Trombetti,
On derived-indecomposable solutions of the Yang–Baxter equation, 2022. arXiv: 2210.08598.

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 map such that

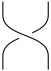
$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r). \qquad (*)$$

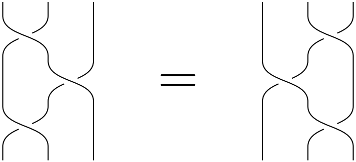
Write $r =$. Then $(*)$ becomes

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 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



Solutions of 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 finite if X is finite.
- (X, r) is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- (X, r) is non-degenerate if it is both left and right non-degenerate.

Convention. From now on

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

Solutions of the Yang-Baxter equation

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

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

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

- (X, r) is finite if X is finite.
- (X, r) is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- (X, r) is non-degenerate if it is both left and right non-degenerate.

Convention. From now on

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

Solutions of the Yang-Baxter equation

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

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

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

- (X, r) is finite if X is finite.
- (X, r) is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- (X, r) is non-degenerate if it is both left and right non-degenerate.

Convention. From now on

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

Solutions of 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 finite if X is finite.
- (X, r) is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- (X, r) is non-degenerate if it is both left and right non-degenerate.

Convention. From now on

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

Solutions of 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 finite if X is finite.
- (X, r) is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- (X, r) is non-degenerate if it is both left and right non-degenerate.

Convention. From now on

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

Solutions to the Yang-Baxter equation

Examples

- Let X be a set and $r : X \times X \to X \times X$ defined by $r(x, y) = (y, x)$ is a solution.
- Let X be a set and $\lambda, \rho : X \to X$ maps such that $\lambda\rho = \rho\lambda$, then $r : X \times X \to X \times X$ defined by $r(x, y) = (\lambda(y), \rho(x))$ is a solution.
- Let G be a group. The map $r : X \times X \to X \times X$ defined by $r(x, y) = (y, y^{-1}xy)$ is a solution.

Indecomposable solutions

(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

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

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

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

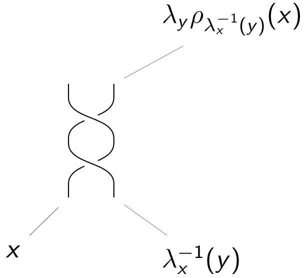
$$\rho_x = \begin{cases} (3\ 4) & \text{if } x = 1, 2 \\ (1\ 2) & \text{if } x = 3, 4. \end{cases}$$

  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 $\{3, 4\}$.

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-indecomposable solutions

Definition. Let (X, r) be a solution. Then (X, r) is derived-indecomposable if its derived solution is indecomposable.

Fact. Let (X, r) be a solution. If (X, r) is derived-indecomposable, then (X, r) is indecomposable.

Remarks.

- If (X, r) is involutive, then $s(x, y) = (y, x)$. Hence, there is a unique involutive derived-indecomposable solution, namely when $|X| = 1$.
- There are plenty of examples of (non-involutive) derived-indecomposable solutions (see for instance the Appendix of Lebed & Vendramin, 2019).

Derived-indecomposable solutions

Definition. Let (X, r) be a solution. Then (X, r) is derived-indecomposable if its derived solution is indecomposable.

Fact. Let (X, r) be a solution. If (X, r) is derived-indecomposable, then (X, r) is indecomposable.

Remarks.

- If (X, r) is involutive, then $s(x, y) = (y, x)$. Hence, there is a unique involutive derived-indecomposable solution, namely when $|X| = 1$.
- There are plenty of examples of (non-involutive) derived-indecomposable solutions (see for instance the Appendix of Lebed & Vendramin, 2019).

Derived-indecomposable solutions

Definition. Let (X, r) be a solution. Then (X, r) is derived-indecomposable if its derived solution is indecomposable.

Fact. Let (X, r) be a solution. If (X, r) is derived-indecomposable, then (X, r) is indecomposable.

Remarks.

- If (X, r) is involutive, then $s(x, y) = (y, x)$. Hence, there is a unique involutive derived-indecomposable solution, namely when $|X| = 1$.
- There are plenty of examples of (non-involutive) derived-indecomposable solutions (see for instance the Appendix of Lebed & Vendramin, 2019).

Derived-indecomposable solutions

- Also, in the non-involutive involutive case, indecomposable doesn't imply derived-indecomposable.

Example. Let $X = \{1, 2, 3, 4\}$. Consider

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

It is to see that $r(x, y) = (\lambda_x(y), \rho_y(x))$ is indecomposable but $s(x, y) = (y, \sigma_y(x))$ where $\sigma_y = \begin{cases} (3\ 4) & \text{if } x = 1, 2 \\ (1\ 2) & \text{if } y = 3, 4. \end{cases}$ is decomposable.

Derived-indecomposable solutions

- Also, in the non-involutive involutive case, indecomposable doesn't imply derived-indecomposable.

Example. Let $X = \{1, 2, 3, 4\}$. Consider

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

It is to see that $r(x, y) = (\lambda_x(y), \rho_y(x))$ is indecomposable but $s(x, y) = (y, \sigma_y(x))$ where $\sigma_y = \begin{cases} (3\ 4) & \text{if } x = 1, 2 \\ (1\ 2) & \text{if } y = 3, 4. \end{cases}$ is decomposable.

Skew braces

Let B be a set with two binary operations $+$ and $\circ$ such that

- $(B, +)$ and $(B, \circ)$ are groups (not necessarily abelian)
- for any $a, b, c \in B$ it holds

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

Skew braces & solutions to the YBE

Let $(B, +, \circ)$ be a skew brace, then the map $r : B \times B \to B \times B$ defined by

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

is a solution.

Skew braces & solutions to the YBE

Let (X, r) be a solution. Then there is a unique skew brace structure over the structure group

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

such that $r_{G(X,r)}(\iota \times \iota) = (\iota \times \iota)r$, where $\iota : X \to G(X, r)$ is the canonical map.

$$\begin{array}{ccc} X \times X & \xrightarrow{\iota \times \iota} & G(X,r) \times G(X,r) \\ \downarrow r & & \downarrow r_{G(X,r)} \\ X \times X & \xrightarrow{\iota \times \iota} & G(X,r) \times G(X,r) \end{array}$$

Question. Given a solution (X, r), can we find a property of $G(X, r)$ that helps us to detect if (X, r) is derived-indecomposable?

Skew braces with property (BS)

Definition. A skew brace B has property (BS) if there exists a positive integer n s.t.

$$\sup\{|(B,+):\mathrm{Fix}^r(x)\cap \mathrm{C}_x^+|, |(B,\circ):\mathrm{Fix}^l(x)\cap \mathrm{C}_x^\circ|\}\leq n.$$

where

$$\mathrm{Fix}^r(x)=\{b\colon x\circ b=x+b\},$$
$$\mathrm{Fix}^r(x)=\{b\colon b\circ x=b+x\}$$

and C_x^+ and C_x° are the centralizers of x in $(B,+)$ and $(B,\circ)$ respectively.

Derived-indecomposable solutions & Skew braces with property (BS)

Theorem. If a solution $(X.r)$ is derived indecomposable, then the $G(X,r)$ has the property (BS).

Theorem. A skew brace has property (BS) if and only if $[B,B]_+$ and $B*B=\mathrm{gr}(a*b\colon a,b\in B)_+$, where $a*b=-a+a\circ b-b$, are finite.

Derived-indecomposable solutions & Skew braces with property (BS)

Theorem. If a solution $(X.r)$ is derived indecomposable, then the $G(X,r)$ has the property (BS).

Theorem. A skew brace has property (BS) if and only if $[B,B]_+$ and $B*B = \mathrm{gr}(a*b\colon a,b \in B)_+$, where $a*b = -a + a\circ b - b$, are finite.

Skew braces with property (S)

Definition. A skew brace B has property (S) if $|(B,+) : \mathrm{Fix}^r(x) \cap \mathrm{C}_x^+|$ and $|(B,\circ) : \mathrm{Fix}^l(x) \cap \mathrm{C}_x^\circ|$ are finite.

- Skew braces with property (BS) are skew braces with property (S).
- Every skew brace B s.t. $|B/\operatorname{Ann}(B)| < \infty$ has property (S).
  $\operatorname{Ann}(B) = \{x \colon x \circ y = x + y\} \cap Z(B,+) \cap Z(B,\circ)$.

Theorem. Let (X, r) be a solution s.t. $G(X, r)$ is a skew brace with property (S). Then (X, r) is indecomposable if and only if (X, r) is derived-indecomposable.

Facts.

- Let B be a skew brace with property (S). TFAE
  (i) B is finitely generated (as a skew brace),
  (ii) $(B,+)$ is finitely generated,
  (iii) $(B,+)$ is finitely generated.

- Let B be a skew brace with property (S). Then
  1. $T_+(B) = T_\circ(B)$,
  2. $T_+(B)$ is an ideal of B,
  3. $T_+(B/T_+(B)) = \{0\}$,
  4. if B is finitely generated then $T_+(B)$ is finite.

Facts.

- Let B be a skew brace with property (S). TFAE
  (i) B is finitely generated (as a skew brace),
  (ii) $(B, +)$ is finitely generated,
  (iii) $(B, +)$ is finitely generated.

- Let B be a skew brace with property (S). Then
  1. $T_+(B) = T_\circ(B)$,
  2. $T_+(B)$ is an ideal of B,
  3. $T_+(B/T_+(B)) = \{0\}$,
  4. if B is finitely generated then $T_+(B)$ is finite.

Facts.

- If B is a periodic skew brace with property (S) (i.e. $T_+(B) = (B, +)$, then
  1. B is locally finite (i.e. every finitely generated sub-skew brace of B is finite),
  2. If B is finitely generated then B is finite,
  3. If B is finitely generated then $B/\operatorname{Ann}(B)$ is finite.

- Let B be a skew brace with property (S). Then B can be embedded in the direct product of a trivial brace C and a periodic skew brace D. Moreover, C and D are homomorphic images of B.

Facts.

- If B is a periodic skew brace with property (S) (i.e. $T_+(B) = (B, +)$, then
  1. B is locally finite (i.e. every finitely generated sub-skew brace of B is finite),
  2. If B is finitely generated then B is finite,
  3. If B is finitely generated then $B/\operatorname{Ann}(B)$ is finite.

- Let B be a skew brace with property (S). Then B can be embedded in the direct product of a trivial brace C and a periodic skew brace D. Moreover, C and D are homomorphic images of B.

Questions

Question 1. Let B be a skew brace and consider the set $F(B)$ of all elements X of B such that $|(B,+) : \mathrm{Fix}^r(x) \cap \mathrm{C}_x^+|$ and $|(B,\circ) : \mathrm{Fix}^l(x) \cap \mathrm{C}_x^\circ|$ are finite. Is $F(B)$ an ideal?

The answer is affirmative for two-sided braces.

Question 2. Let B be a periodic skew brace with property (S). Is it true that any finitely generated ideal of B is finite?

Questions

Question 1. Let B be a skew brace and consider the set $F(B)$ of all elements X of B such that $|(B,+) : \mathrm{Fix}^r(x) \cap \mathrm{C}_x^+|$ and $|(B,\circ) : \mathrm{Fix}^l(x) \cap \mathrm{C}_x^\circ|$ are finite. Is $F(B)$ an ideal?

The answer is affirmative for two-sided braces.

Question 2. Let B be a periodic skew brace with property (S). Is it true that any finitely generated ideal of B is finite?

Thank you!!!