From the YBE to the Left Braces

Ivan Lau
(Joint Work with Patrick Kinnear and Dora Puljić)

University of Edinburgh

Groups, Rings and Associated Structures 2019
June 9-15 2019, Spa, Belgium

Small Challenge

Find **all** matrices $R \in \mathbb{C}^{4\times 4}$ which satisfy

$$\boxed{(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)}$$

where I is the identity matrix on $\mathbb{C}^{2\times 2}$.

Reminder on **Kronecker product** $\otimes$: For $S \in \mathbb{C}^{k\times m}$, $T \in \mathbb{C}^{l\times n}$
$S \otimes T$ is the block matrix $\in \mathbb{C}^{kl\times mn}$

$$S \otimes T = \begin{bmatrix} s_{11}T & \dots & s_{1m}T \\ \vdots & \ddots & \vdots \\ s_{k1}T & \dots & s_{km}T \end{bmatrix}.$$

In particular, $R \otimes I$ and $I \otimes R$ are both $\mathbb{C}^{8\times 8}$.

Small Challenge

Find **all** matrices $R \in \mathbb{C}^{4\times 4}$ which satisfy

$$\boxed{(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)}$$

where I is the identity matrix on $\mathbb{C}^{2\times 2}$.

Naive approach: Introduce **16 variables** for the entries of R and try matching the LHS and the RHS for each entry.

$$R = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ x_9 & x_{10} & x_{11} & x_{12} \\ x_{13} & x_{14} & x_{15} & x_{16} \end{bmatrix}$$

Small Challenge

Find **all** matrices $R \in \mathbb{C}^{4\times 4}$ which satisfy

$$\boxed{(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)}$$

where I is the identity matrix on $\mathbb{C}^{2\times 2}$.

Naive approach: Introduce **16 variables** for the entries of R and try matching the LHS and the RHS for each entry.

Problem: Matching each entry is equivalent to solving a **multivariate cubic polynomial**. Matching all **64 entries** is equivalent to **solving 64 cubic polynomials in 16 variables!**

Solved by (Hietarinta 1993) with the help of a **computer**!

Grand Challenge: YBE and the R-matrix

Find **all** matrices $R \in \mathbb{C}^{n^2 \times n^2}$ which satisfy

$$\boxed{(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)}$$

where I is the identity matrix on $\mathbb{C}^{n \times n}$.

Naive approach: solve n^6 cubic polynomials in n^4 variables.

Still open for $n \geq 3$.

The equation

$$\boxed{(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)}$$

is called the Yang-Baxter equation (YBE). Matrices R that satisfy YBE are called ***R*-matrices**.

(Drinfeld 1992): Set-theoretic Solutions

Let X be a non-empty set. Let $r\colon X^2 \to X^2$ be a bijective map.

We write $r \times \mathrm{id}$ as the map $X^3 \to X^3$ such that

$$(r \times \mathrm{id})(x, y, z) = \big(r\,(x, y), z\big).$$

Similarly,

$$(\mathrm{id} \times r)(x, y, z) = \Big(x, r(y, z)\Big).$$

The pair (X, r) is a **set-theoretic solution** of the YBE if it satisfies

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

Observe the similarity to the YBE:

$$\boxed{(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R).}$$

Example: Flip Map

Let X be a non-empty set. We define $r\colon X^2 \to X^2$ to be the map $r(x,y) = (y,x)$ for all $x, y \in X$.

For any $x, y, z \in X$,

$$\begin{aligned}(r\times \mathrm{id})(\mathrm{id}\times r)(r\times \mathrm{id})(x,y,z) &= (r\times \mathrm{id})(\mathrm{id}\times r)(y,x,z)\\ &= (r\times \mathrm{id})(y,z,x)\\ &= (z,y,x).\end{aligned}$$

Similarly,

$$\begin{aligned}(\mathrm{id}\times r)(r\times \mathrm{id})(\mathrm{id}\times r)(x,y,z) &= (\mathrm{id}\times r)(r\times \mathrm{id})(x,z,y)\\ &= (\mathrm{id}\times r)(z,x,y)\\ &= (z,y,x).\end{aligned}$$

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

Constructing R-matrix from Set-theoretic Solution

Example: We construct the R-matrix from $r(x,y) = (y,x)$ on $X = \{x_1, x_2\}$. Consider
$r(x_1, x_1) = (x_1, x_1) \implies R_{11}^{11} = 1$,
$r(x_1, x_2) = (x_2, x_1) \implies R_{12}^{21} = 1 \dots$

$$R = \begin{array}{c} \\ 11 \\ 12 \\ 21 \\ 22 \end{array} \begin{array}{c} \begin{array}{cccc} 11 & 12 & 21 & 22 \end{array} \\ \begin{bmatrix} R_{11}^{11} & R_{11}^{12} & R_{11}^{21} & R_{11}^{22} \\ R_{12}^{11} & R_{12}^{12} & R_{12}^{21} & R_{12}^{22} \\ R_{21}^{11} & R_{21}^{12} & R_{21}^{21} & R_{21}^{22} \\ R_{22}^{11} & R_{22}^{12} & R_{22}^{21} & R_{22}^{22} \end{bmatrix} \end{array} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Constructing R-matrix from Set-theoretic Solution

Example: We construct the R-matrix from $r(x, y) = (y, x)$ on $X = \{x_1, x_2\}$. Consider
$r(x_1, x_1) = (x_1, x_1) \implies R^{11}_{11} = 1,$
$r(x_1, x_2) = (x_2, x_1) \implies R^{21}_{12} = 1 \ldots$

$$R = \begin{array}{c|cccc} & 11 & 12 & 21 & 22 \\ \hline 11 & R^{11}_{11} & R^{12}_{11} & R^{21}_{11} & R^{22}_{11} \\ 12 & R^{11}_{12} & R^{12}_{12} & R^{21}_{12} & R^{22}_{12} \\ 21 & R^{11}_{21} & R^{12}_{21} & R^{21}_{21} & R^{22}_{21} \\ 22 & R^{11}_{22} & R^{12}_{22} & R^{21}_{22} & R^{22}_{22} \end{array} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

General case: Given a solution (X, r) where $X = \{x_1, \ldots, x_n\}$. Construct an $n^2 \times n^2$ R-matrix with indices $11, 12, \ldots, 1n$, $21, \ldots, 2n$, $\ldots, n1, \ldots, nn$ such that $R^{kl}_{ij} = 1$ if $r(x_i, x_j) = (x_k, x_l)$, and 0 otherwise.

Non-degenerate Involutive Set-theoretic Solution

We say a solution (X, r) is **involutive** if $r^2 = \mathrm{id}_{X^2}$, i.e.

$$\text{for all } x, y \in X, r\big(r(x, y)\big) = (x, y).$$

Write $r(x, y) = \big(f(x, y), g(x, y)\big)$ where $f(x, -), g(-, y)$ are maps $X \to X$. We say (X, r) is **non-degenerate** if

$$\text{for all } x, y \in X, f(x, -), g(-, y) \text{ are bijective.}$$

Notation: We will denote non-degenerate involutive set-theoretic solutions of YBE by **solutions** for convenience.

Entering Left Braces

Introduced in (Rump 2007) to help study solutions of the YBE. A left brace is a triple $(B, +, \circ)$ satisfying axioms

(B1) $(B, +)$ is an abelian group;

(B2) $(B, \circ)$ is a group;

(B3) $a \circ (b + c) + a = a \circ b + a \circ c$.

Example: Define $(B, +) = (\mathbb{Z}_p, +)$. Define $(B, \circ)$ such that

$$a \circ b = a + b.$$

Call this a **trivial brace**.

Left Braces Yield Solutions

Notation: Write b^{-1} as the inverse of b in $(B, \circ)$.

Theorem (Rump 2007): Let B be a left brace. Define a map $r_B \colon B^2 \to B^2$ as

$$r_B(a, b) = (a \circ b - a, z \circ a - z)$$

where $z = (a \circ b - a)^{-1}$. Then (B, r_B) is a solution of the YBE.

Significance: Left braces give us solutions!
Notation: We call the pair (B, r_B) the **associated** solution of B.
Example: Any trivial brace. Note that the associated r is flip map.

$$r(a, b) = (a + b - a, b^{-1} + a - b^{-1}) = (b, a).$$

Finding all Left Braces $\Longrightarrow$ Finding all Solutions

Theorem (Cedó, Gateva-Ivanova & Smoktunowicz 2017): Let (X, r) be a finite solution of the YBE. Then we can construct a (finite) left brace $B \supseteq X$ such that its associated map $r_B \colon B^2 \to B^2$ satisfies

$$r_{B|_{X^2}} = r.$$

Significance: Any finite solution (X, r) is embedded in some finite left brace (B, r_B)!

Finding all Left Braces $\implies$ Finding all Solutions

Theorem (Cedó, Gateva-Ivanova & Smoktunowicz 2017): Let (X, r) be a finite solution of the YBE. Then we can construct a (finite) left brace $B \supseteq X$ such that its associated map $r_B \colon B^2 \to B^2$ satisfies

$$r_{B|_{X^2}} = r.$$

Significance: Any finite solution (X, r) is embedded in some finite left brace (B, r_B)!

(Cedó, Jespers & Del Rio 2010): The task of finding all finite solutions can be broken down into two sub-problems:

Problem 1: Classify **all** finite left braces.

Problem 2: For each left brace B, classify **all** embedded subsolutions $(X, r_{B|_{X^2}})$.

Finding all Left Braces $\Longrightarrow$ Finding all Solutions

Theorem (Cedó, Gateva-Ivanova & Smoktunowicz 2017): Let (X, r) be a finite solution of the YBE. Then we can construct a (finite) left brace $B \supseteq X$ such that its associated map $r_B \colon B^2 \to B^2$ satisfies

$$r_{B|_{X^2}} = r.$$

Significance: Any finite solution (X, r) is embedded in some finite left brace (B, r_B)!

(Cedó, Jespers & Del Rio 2010): The task of finding all finite solutions can be broken down into two sub-problems:

Problem 1: Classify **all** finite left braces.

Problem 2: For each left brace B, classify **all** embedded subsolutions $(X, r_{B|_{X^2}})$.

Problem 2 is solved by (Bachiller, Cedó & Jespers 2016)!
$\therefore$ Finding all solutions is reduced to Problem 1!

Braces: Crossover of Groups and Rings (I)

- A left brace $(B, +, \circ)$ relates two groups $(B, +)$ and $(B, \circ)$ through
$$a \circ (b + c) + a = a \circ b + a \circ c.$$
- A left brace $(B, +, \circ)$ can be equipped with the operation $*$ defined by
$$a * b = a \circ b - a - b.$$
It can be checked that $*$ is left-distributive over $+$. That is,
$$a * (b + c) = a * b + a * c$$
for $a, b, c \in B$. Then $(B, +, *)$ satisfies all ring axioms except
    - Right-distributivity
    - Associativity

  Intuitively, you can say $(B, +, *)$ is "like" a Jacobson radical ring with these two axioms being relaxed.

Good Artists Copy, Great Artists Steal? (I)

Basic definitions with analogues in group or ring theory:

- Subbrace
- Morphisms
- Ideals
- Left/Right Ideals
- Quotient braces
- Direct Product
- Semidirect Product

Good Artists Copy, Great Artists Steal? (II)

Well-studied concepts with analogues in group or ring theory:

- **Solvable**: there exists a sequence of ideals $\{0\} = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = B$ with B_i/B_{i-1} trivial
- **Prime**: if $I * J = 0$ for I, J ideals of B, then one of I, J is zero
- **Semiprime**: if $I * I = 0$ for I an ideal of B, then $I = \{0\}$
- ~~**Nil**: for all $b \in B$, there is $n \in \mathbb{N}$ such that $b^n = 0$~~
- **Left nil**: $(b * (b * \dots (b * (b * (b * b) \dots) = 0$
- **Right nil**: $(\cdots (b * b) * b) * b) \cdots * b) * b) = 0$
- ~~**Nilpotent**: there is $n \in \mathbb{N}$ such that $B^n = \{0\}$~~
- **Left nilpotent**: $(B * (B * \dots (B * (B * (B * B) \dots) = \{0\}$
- **Right nilpotent**: $(\cdots (B * B) * B) * B) \cdots * B) * B) = \{0\}$

Solvable important for classification of **groups.**
(Semi) prime, nil, nilpotent important for classification of **rings.**
Analogues important for classification of **left braces?**

Good Artists Copy, Great Artists Steal? (III)

- A semiprime **ring** R is a subdirect product of prime **rings**. (Wedderburn–Artin Theorem)
- A semiprime **left brace** B is a subdirect product of prime **left braces** (Konovalov, Smoktunowicz & Vendramin 2018).

Statement in **rings** $\implies$ Analogous statement in **left braces**?

- **Groups** G, H are solvable if and only if their semidirect product is solvable.
- **Left braces** G, H are solvable if and only if their semidirect product is solvable (**new result**).

Statement in **groups** $\implies$ Analogous statement in **left braces**?

Too Good to be True

Problem: Ring-theoretic techniques may not work as they often rely on right-distributivity or/and associativity of $*$.

Recall: Left brace is like Jacobson radical ring but with right-distributivity and associativity of $*$ relaxed.

General questions: To what extent can we mimic? If so, is it straightforward or tricky? If not, why?

Right Distributivity vs Associativity

Recall: Left brace is like Jacobson radical ring but with right-distributivity or associativity of $*$ relaxed.

Question: Are **both** of these axioms essential for a left brace to be a ring?

Answer: **Exactly one** is sufficient.

$(B, +, *)$ right-distributive $\implies$ $(B, +, *)$ is a ring (Rump 2007).

$(B, +, *)$ associative $\implies$ $(B, +, *)$ is a ring (Lau 2018).

Probabilistic and Combinatorial Brace Theory?

5/8 Theorem in Probabilistic Group Theory: **Randomly** choose two elements of a finite group. If the probability that they commute is bigger than 5/8, the group is abelian!

Approximate subgroup in Arithmetic Combinatorics: Finite subsets that are **almost** closed under products/ behaves like a subgroup "up to a constant error".

Any similar interesting and meaningful concept/statements for Left Braces?

Thank you for listening!

References I

Bachiller, D., Cedó, F. & Jespers, E. (2016), 'Solutions of the Yang–Baxter equation associated with a left brace', Journal of Algebra **463**, 80 – 102.

Cedó, F., Gateva-Ivanova, T. & Smoktunowicz, A. (2017), 'On the Yang–Baxter equation and left nilpotent left braces', Journal of Pure and Applied Algebra **221**(4), 751–756.

Cedó, F., Jespers, E. & Del Rio, A. (2010), 'Involutive Yang-Baxter groups', Transactions of the American Mathematical Society **362**(5), 2541–2558.

Drinfeld, V. (1992), On some unsolved problems in quantum group theory, in P. P. Kulish, ed., 'Quantum Groups', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–8.

Hietarinta, J. (1993), 'Solving the two-dimensional constant quantum Yang-Baxter equation', Journal of Mathematical Physics **34**, 1725–1756.

References II

Konovalov, A., Smoktunowicz, A. & Vendramin, L. (2018), 'On skew braces and their ideals', Experimental Mathematics pp. 1–10.

Lau, I. (2018), 'Left Brace With The Operation $*$ Associative Is A Two-sided Brace', arXiv: 1811.04894v2 [math.RA] .

Rump, W. (2007), 'Braces, radical rings, and the quantum Yang-Baxter equation', Journal of Algebra **307**(1), 153 – 170.