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

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)$$

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 $\mathbb{C}^{kl \times mn}$

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

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

\[
(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)
\]

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

Naive approach: Introduce \textbf{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 $R \in \mathbb{C}^{4\times4}$ which satisfy

\[(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)\]

where $I$ is the identity matrix on $\mathbb{C}^{2\times2}$.

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

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)$$

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

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)$$

is called the Yang-Baxter equation (YBE). Matrices $R$ that satisfy YBE are called $R$-matrices.
Let $X$ be a non-empty set. Let $r : X^2 \to X^2$ be a bijective map.

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

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

Similarly,

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

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

$$(r \times \text{id})(\text{id} \times r)(r \times \text{id}) = (\text{id} \times r)(r \times \text{id})(\text{id} \times r).$$

Observe the similarity to the YBE:

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R).$$
Example: Flip Map

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

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

$$(r \times \text{id})(\text{id} \times r)(r \times \text{id})(x, y, z) = (r \times \text{id})(\text{id} \times r)(y, x, z)$$

$$= (r \times \text{id})(y, z, x)$$

$$= (z, y, x).$$

Similarly,

$$(\text{id} \times r)(r \times \text{id})(\text{id} \times r)(x, y, z) = (\text{id} \times r)(r \times \text{id})(x, z, y)$$

$$= (\text{id} \times r)(z, x, y)$$

$$= (z, y, x).$$

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

$r(x_1, x_1) = (x_1, x_1) \implies R_{11}^{11} = 1,$
$r(x_1, x_2) = (x_2, x_1) \implies R_{12}^{21} = 1$...

\[
R = \begin{bmatrix}
R_{11}^{11} & R_{11}^{12} & R_{11}^{21} & R_{11}^{22} \\
R_{12}^{11} & R_{12}^{12} & R_{12}^{21} & R_{12}^{22} \\
R_{21}^{11} & R_{21}^{12} & R_{21}^{21} & R_{21}^{22} \\
R_{22}^{11} & R_{22}^{12} & R_{22}^{21} & R_{22}^{22}
\end{bmatrix}
= \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]
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

- $r(x_1, x_1) = (x_1, x_1) \implies R_{11}^{11} = 1,$
- $r(x_1, x_2) = (x_2, x_1) \implies R_{21}^{21} = 1 . . .$

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

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 $R_{ij}^{kl} = 1$ if $r(x_i, x_j) = (x_k, x_l)$, and 0 otherwise.
We say a solution \((X, r)\) is **involutive** if \(r^2 = \text{id}_X\), i.e.

\[
\text{for all } x, y \in X, \quad r(r(x, y)) = (x, y).
\]

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

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

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 $r_B: B^2 \to B^2$ 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 $\implies$ 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 $r_B : B^2 \to B^2$ 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 $r_B : B^2 \to B^2$ 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 $(X, r_B|_{X^2})$. 

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 \(r_B : B^2 \to B^2\) 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)!
\[
\therefore \text{Finding all solutions is reduced to Problem 1!}
\]
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 \(\ast\) defined by
  \[
  a \ast b = a \circ b - a - b.
  \]
  It can be checked that \(\ast\) is left-distributive over \(+\). That is,
  \[
  a \ast (b + c) = a \ast b + a \ast c
  \]
  for \(a, b, c \in B\). Then \((B, +, \ast)\) satisfies all ring axioms except
  - Right-distributivity
  - Associativity

Intuitively, you can say \((B, +, \ast)\) is “like” a Jacobson radical ring with these two axioms being relaxed.
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 \( I \ast J = 0 \) for \( I, J \) ideals of \( B \), then one of \( I, J \) is zero

- **Semiprime**: if \( I \ast I = 0 \) 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**: \( (b \ast (b \ast \ldots (b \ast (b \ast (b \ast b) \ldots) = 0 \)

- **Right nil**: \( (\cdots (b \ast b) \ast b) \cdots \ast b) \ast b) = 0 \)

- **Nilpotent**: there is \( n \in \mathbb{N} \) such that \( B^n = \{0\} \)

- **Left nilpotent**: \( (B \ast (B \ast \ldots (B \ast (B \ast (B \ast B) \ldots) = \{0\} \)

- **Right nilpotent**: \( (\cdots (B \ast B) \ast B) \ast B) \cdots \ast B) \ast B) = \{0\} \)

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

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

\[(B, +, *) \text{ right-distributive} \implies (B, +, *) \text{ is a ring} \text{ (Rump 2007).}\]

\[(B, +, *) \text{ associative} \implies (B, +, *) \text{ is a ring} \text{ (Lau 2018).}\]
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!


