On solutions of the set-theoretic Yang-Baxter equation subjected to a choice of elements

Bernard Rybołowicz
Joint work with Anastasia Doikou

Heriot-Watt University

Blankenberge 2023

Set-theoretic Yang-Baxter equation

Definition

Let X be a set. We say that $r : X \times X \to X \times X$ is a *solution of the set-theoretic Yang-Baxter equation (solution)* if

$$(r \times id)(id \times r)(r \times id) = (id \times r)(r \times id)(id \times r), \quad (a, b) \mapsto (\sigma_a(b), \tau_b(a)).$$

Set-theoretic Yang-Baxter equation

Definition

Let X be a set. We say that $r : X \times X \to X \times X$ is a *solution of the set-theoretic Yang-Baxter equation (solution)* if

$$(r \times id)(id \times r)(r \times id) = (id \times r)(r \times id)(id \times r), \quad (a, b) \mapsto (\sigma_a(b), \tau_b(a)).$$

- We say that r is involutive if $r^2 = id$.

Set-theoretic Yang-Baxter equation

Definition

Let X be a set. We say that $r : X \times X \to X \times X$ is a *solution of the set-theoretic Yang-Baxter equation (solution)* if

$$(r \times id)(id \times r)(r \times id) = (id \times r)(r \times id)(id \times r), \quad (a, b) \mapsto (\sigma_a(b), \tau_b(a)).$$

- We say that r is involutive if $r^2 = id$.
- We say that r is non-degenerate if σ_a and τ_a are bijections for all $a \in X$.

Skew braces

Definition

A *skew brace* is a triple $(B, +, \circ)$ such that $(B, +)$ and $(B, \circ)$ are groups, and for all $a, b, c \in B$,

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

Skew braces

Definition

A *skew brace* is a triple $(B, +, \circ)$ such that $(B, +)$ and $(B, \circ)$ are groups, and for all $a, b, c \in B$,

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

- If additionally, $(B, +)$ is abelian, we say that $(B, +, \circ)$ is a brace

Skew braces

Definition

A *skew brace* is a triple $(B, +, \circ)$ such that $(B, +)$ and $(B, \circ)$ are groups, and for all $a, b, c \in B$,

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

- If additionally, $(B, +)$ is abelian, we say that $(B, +, \circ)$ is a brace
- If additionally, for all $a, b, c \in B$ $(b + c) \circ a = b \circ a - a + c \circ a$, we say that $(B, +, \circ)$ is two-sided.

Skew braces

Definition

A *skew brace* is a triple $(B, +, \circ)$ such that $(B, +)$ and $(B, \circ)$ are groups, and for all $a, b, c \in B$,

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

- If additionally, $(B, +)$ is abelian, we say that $(B, +, \circ)$ is a brace
- If additionally, for all $a, b, c \in B$ $(b + c) \circ a = b \circ a - a + c \circ a$, we say that $(B, +, \circ)$ is two-sided.

Remark

If $(B, +, \circ)$ is a two-sided brace, then $(B, +, *)$ is a radical ring, where $a * b := a \circ b - a - b$.

Rump theorem

Theorem (Wolfgang Rump)

Let $(B, +, \circ)$ *be a brace. Then the following map:*

$$r(a, b) := (-a + a \circ b, (-a + a \circ b)^{-1} \circ a \circ b)$$

is a non-degenerate involutive solution. Moreover, for any involutive solution r *on* X*, there exists a brace* G *and an injective emebedding* $\iota : X \to G$ *such that* $r_G|_{\iota(X)\times\iota(X)} \cong r$*.*

Rump theorem

Theorem (Wolfgang Rump)

Let $(B, +, \circ)$ be a brace. Then the following map:

$$r(a, b) := (-a + a \circ b, (-a + a \circ b)^{-1} \circ a \circ b)$$

is a non-degenerate involutive solution. Moreover, for any involutive solution r on X, there exists a brace G and an injective emebedding $\iota : X \to G$ such that $r_G|_{\iota(X)\times\iota(X)} \cong r$.

- This result was further generalise by L. Guarnieri and L. Vendramin to the case of skew braces and non-degenerate solutions.

Definition

Let B be a skew brace. A *right distributor* of B is a subset

$$\mathcal{D}_r(B) := \{z \in B \mid \forall a, b \in B \ (a+b) \circ z = a \circ z - z + b \circ z\}$$

Definition

Let B be a skew brace. A *right distributor* of B is a subset

$$\mathcal{D}_r(B) := \{z \in B \mid \forall a, b \in B \ (a + b) \circ z = a \circ z - z + b \circ z\}$$

Theorem

Let B be a skew brace, then for any $z \in \mathcal{D}_r(B)$, the following maps

$$r_z(a, b) := (\sigma_a^z(b), \tau_b^z(a)) = (a \circ b - a \circ z + z, (a \circ b - a \circ z + z)^{-1} \circ a \circ b)$$

$$\check{r}_z(a, b) := (\check{\sigma}_a^z(b), \check{\tau}_b^z(a)) = (-a \circ z + a \circ b \circ z, (-a \circ z + a \circ b \circ z)^{-1} \circ a \circ b)$$

are non-degenerate solutions. Moreover, $\check{r}_{z^{-1}} = r_z^{-1}$.

Affinity and parameter

Remark

Let B be a brace and $z \in \mathcal{D}_r(B)$, then for any ideal I of B,

$$r_z|_{(I+z)\times(I+z)}$$

is a non-degenerate solution.

Those solutions correspond to particular congruence classes.

Examples

Example (1)

Let us consider a triple $(\mathrm{Odd} := \left\{\frac{2n+1}{2k+1} \mid n, k \in \mathbb{Z}\right\}, +_1, \circ)$ where $(a, b) \xrightarrow{+_1} a - 1 + b$ and $(a, b) \xrightarrow{\circ} a \cdot b$. The triple $(\mathrm{Odd}, +_1, \circ)$ is a brace and the solution r_z is involutive if and only if for all $a \in B$

$$(z-1)\cdot(1-a) = 0.$$

Therefore, for all $z \neq 1$, $\check{r}_z$ is non-involutive. Moreover, $r_z = r_w$ if and only if if $z = w$.

Examples

Example (2)

Let us consider a ring $\mathbb{Z}/8\mathbb{Z}$. A triple

$$\left(\mathrm{OM} := \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in \{1,3,5,7\},\ b, c \in \{0,2,4,6\}\right\}, +_{\mathbb{I}}, \circ\right)$$

is a brace, where $(A, B) \xmapsto{+_{\mathbb{I}}} A - \mathbb{I} + B$, $(A, B) \xmapsto{\circ} A \cdot B$. Moreover one can easily check that two solutions $\check{r}_A$ and $\check{r}_B$ are equal if and only if $(D - \mathbb{I}) \cdot (B - A) = 0 \pmod 8$ $\forall D \in \mathrm{OM}$.

The Lemma

Lemma

Let B be a skew brace and $z \in \mathcal{D}_r(B)$. Then the map

$$\tau^z : (B, \circ) \to \mathrm{Aut}(B), \quad a \mapsto \tau_a^z$$

is a group action if and only if for all $a \in B$ $a \circ z = z + a$.

The Lemma

Lemma

Let B be a skew brace and $z \in \mathcal{D}_r(B)$. Then the map

$$\tau^z : (B, \circ) \to \mathrm{Aut}(B), \quad a \mapsto \tau_a^z$$

is a group action if and only if for all $a \in B$ $a \circ z = z + a$.

Theorem

Let B be a brace, then if there exists $a \in B$ such that $a \circ z \neq z + a$ and $z \in \mathcal{D}_r(B)$, then r_z is not isomorphic with any solution (with parameter 1) coming from skew braces.

Other way

Let us start with:

Other way

Let us start with:

- group $(G, \circ)$,

Other way

Let us start with:

- group $(G, \circ)$,
- some fixed parameter $z \in G$,

Other way

Let us start with:

- group $(G, \circ)$,
- some fixed parameter $z \in G$,
- a solution $r_z : G \times G \to G \times G$, $r_z(a, b) = (\sigma_a^z(b), \tau_b^z(a))$,

Other way

Let us start with:

- group $(G, \circ)$,
- some fixed parameter $z \in G$,
- a solution $r_z : G \times G \to G \times G$, $r_z(a, b) = (\sigma_a^z(b), \tau_b^z(a))$,
- $a \circ b = \sigma_a^z(b) \circ \tau_b^z(a)$.

Other way

Let us start with:

- group $(G, \circ)$,
- some fixed parameter $z \in G$,
- a solution $r_z : G \times G \to G \times G$, $r_z(a, b) = (\sigma_a^z(b), \tau_b^z(a))$,
- $a \circ b = \sigma_a^z(b) \circ \tau_b^z(a)$.

Then we can define a binary operation

$$y + x := x \circ \sigma_{x^{-1}}^z(y \circ z) \circ z^{-1}$$

Other way

Let us start with:

- group $(G, \circ)$,
- some fixed parameter $z \in G$,
- a solution $r_z : G \times G \to G \times G$, $r_z(a,b) = (\sigma^z_a(b), \tau^z_b(a))$,
- $a \circ b = \sigma^z_a(b) \circ \tau^z_b(a)$.

Then we can define a binary operation

$$y + x := x \circ \sigma^z_{x^{-1}}(y \circ z) \circ z^{-1}$$

Remark

The operation + is associative if and only if for all $x, y, c \in X$,

$$\sigma^z_{c^{-1}}(y \circ z^{-1} \circ \sigma^z_{z \circ y^{-1}}(x)) = \sigma^z_{c^{-1}}(y) \circ z^{-1} \circ \sigma^z_{(c \circ \sigma^z_{c^{-1}}(y) \circ z^{-1})^{-1}}(x).$$

Other way

Let us start with:

- group $(G, \circ)$,
- some fixed parameter $z \in G$,
- a solution $r_z : G \times G \to G \times G$, $r_z(a,b) = (\sigma^z_a(b), \tau^z_b(a))$,
- $a \circ b = \sigma^z_a(b) \circ \tau^z_b(a)$.

Then we can define a binary operation

$$y + x := x \circ \sigma^z_{x^{-1}}(y \circ z) \circ z^{-1}$$

Remark

The operation $+$ is associative if and only if for all $x, y, c \in X$,

$$\sigma^z_{c^{-1}}(y \circ z^{-1} \circ \sigma^z_{z \circ y^{-1}}(x)) = \sigma^z_{c^{-1}}(y) \circ z^{-1} \circ \sigma^z_{(c \circ \sigma^z_{c^{-1}}(y) \circ z^{-1})^{-1}}(x).$$

In general it is not associative, but if it is, then $(G, +)$ is a group.

From solution to near brace

Theorem

(A) *The pair* $(X, +)$ *is a group.*

(B) *There exists* $\phi : X \to X$ *such that for all* $a, b, c \in X$
$a \circ (b + c) = a \circ b + \phi(a) + a \circ c.$

(C) *For* $z \in X$ *appearing in* $\sigma_x^z(y)$ *there exist* $\widehat{\phi} : X \to X$ *such that for all* $a, b \in X$ $(a + b) \circ z = a \circ z + \widehat{\phi}(z) + b \circ z.$

(D) *The neutral element* 0 *of* $(X, +)$ *has a left and right distributivity.*

From solution to near brace

Theorem

(A) *The pair* $(X,+)$ *is a group.*

(B) *There exists* $\phi : X \to X$ *such that for all* $a,b,c \in X$
$a \circ (b+c) = a \circ b + \phi(a) + a \circ c.$

(C) *For* $z \in X$ *appearing in* $\sigma_x^z(y)$ *there exist* $\widehat{\phi} : X \to X$ *such that for all* $a,b \in X$ $(a+b) \circ z = a \circ z + \widehat{\phi}(z) + b \circ z.$

(D) *The neutral element* 0 *of* $(X,+)$ *has a left and right distributivity.*

Then for all $a,b,c \in X$ *the following statements hold:*

1. $\phi(a) = -a \circ 0$ *and* $\widehat{\phi}(z) = -0 \circ z$,
2. $\sigma_a^z(b) = (a \circ b \circ z^{-1} - a \circ 0 + 1) \circ z = a \circ b - a \circ 0 \circ z + z.$
3. $a - a \circ 0 = 1$ *and (i)* $0 \circ 0 = -1$ *(ii)* $1 + 1 = 0^{-1}$.

Near braces

Definition

A *near brace* is a set B together with two group operations $+, \circ : B \times B \to B$, the first is called addition and the second is called multiplication, such that $\forall a, b, c \in B$,

$$a \circ (b + c) = a \circ b - a \circ 0 + a \circ c,$$

and $a - a \circ 0 = -a \circ 0 + a = 1$. We denote by 0 the neutral element of the $(B, +)$ group and by 1 the neutral element of the $(B, \circ)$ group. We say that a near brace B is an abelian near brace if $+$ is abelian.

Near braces

Definition

A *near brace* is a set B together with two group operations $+, \circ : B \times B \to B$, the first is called addition and the second is called multiplication, such that $\forall a, b, c \in B$,

$$a \circ (b + c) = a \circ b - a \circ 0 + a \circ c,$$

and $a - a \circ 0 = -a \circ 0 + a = 1$. We denote by 0 the neutral element of the $(B, +)$ group and by 1 the neutral element of the $(B, \circ)$ group. We say that a near brace B is an abelian near brace if $+$ is abelian.

Example

Let $(B, \circ)$ be a group with neutral element 1 and define $a + b := a \circ \kappa^{-1} \circ b$, where $1 \neq \kappa \in B$ is an element of the center of $(B, \circ)$. Then $(B, \circ, +)$ is a near brace with neutral element $0 = \kappa$, and we call it the trivial near brace. **Thanks Paola!**

Solutions with more parameters

Theorem

Let $(B, \circ, +)$ *be a near brace and* $z \in B$ *such that* $\exists\ c_{1,2} \in B, \forall a, b, c \in B,\ (a - b + c) \circ z_i = a \circ z_i - b \circ z_i + c \circ z_i$, $i \in \{1, 2\}$, $a \circ z_2 \circ z_1 - a \circ \xi = c_1$ *and* $-a \circ \xi + a \circ z_1 \circ z_2 = c_2$. *We define a map* $\check{r} : B \times B \to B \times B$ *given by*

$$\check{r}(a, b) = (\sigma^p_a(b), \tau^p_b(a)),$$

where $\sigma^p_a(b) = a \circ b \circ z_1 - a \circ \xi + z_2$, $\tau^p_b(a) = \sigma^p_a(b)^{-1} \circ a \circ b$. *The pair* $(B, \check{r})$ *is a solution.*

Solutions with more parameters

Theorem

Let $(B, \circ, +)$ be a near brace and $z \in B$ such that $\exists\ c_{1,2} \in B, \forall a, b, c \in B$, $(a - b + c) \circ z_i = a \circ z_i - b \circ z_i + c \circ z_i$, $i \in \{1, 2\}$, $a \circ z_2 \circ z_1 - a \circ \xi = c_1$ and $-a \circ \xi + a \circ z_1 \circ z_2 = c_2$. We define a map $\check{r} : B \times B \to B \times B$ given by

$$\check{r}(a, b) = (\sigma_a^p(b), \tau_b^p(a)),$$

where $\sigma_a^p(b) = a \circ b \circ z_1 - a \circ \xi + z_2$, $\tau_b^p(a) = \sigma_a^p(b)^{-1} \circ a \circ b$. The pair $(B, \check{r})$ is a solution.

Example

- $z_1 = 1, z_2 = \xi$
- $z_1 \circ z_2 = \xi, \quad z_i \in Z(B, \circ)$

How restrictive are those parameters?

Theorem again

Lemma

Let B be a skew brace and $z \in \mathcal{D}_r(B)$. Then the map

$$\tau^z : (B, \circ) \to \mathrm{Aut}(B), \quad a \mapsto \tau_a^z$$

is a group action if and only if for all $a \in B$ $a \circ z = z + a$.

Theorem

Let B be a brace, then if there exists $a \in B$ such that $a \circ z \neq z + a$ and $z \in \mathcal{D}_r(B)$, then r_z is not isomorphic with any solution (with parameter 1) coming from skew braces.

Proof of the theorem

Let us assume that r_1 is isomorphic to r_z, for some skew brace S. Then there exists a bijection $f : S \to B$ such that,

$$\begin{aligned}(f \times f)r_1 &= r_z(f \times f)\\ f(a \circ b - a) &= f(a) \circ f(b) - f(a) \circ z + z\\ f((\sigma_a(b))^{-1} \circ a \circ b) &= \sigma^z_{f(a)}(f(b))^{-1} \circ f(a) \circ f(b)\end{aligned}$$

Observe that for $b = 1$, we get that

$$f(1) = f(a) \circ f(1) - f(a) \circ z + z \implies -f(a) \circ f(1) + f(1) = -f(a) \circ z + z$$

Thus $\sigma^z = \sigma^{f(1)}$ and $\check{r}_{f(1)} = \check{r}_z$. Moreover, $f(1)$ is the center of the group $(B, \circ)$ as

$$\begin{aligned}f(a) = f(\tau_1(a)) = \tau^z_{f(1)}(f(a)) &= \sigma^z_{f(a)}(f(1))^{-1} \circ f(a) \circ f(1)\\ &= f(\sigma_a(1))^{-1} \circ f(a) \circ f(1) = f(1)^{-1} \circ f(a) \circ f(1),\end{aligned}$$

and since f is surjective $f(1)$ is in the center of $(B, \circ)$.

Proof

Further, for all $a \in S$

$$f(a) = f(\sigma_1(a)) = \sigma_{f(1)}^{f(1)}(f(a)) = f(1) \circ f(a) - f(1)^2 + f(1),$$

and $-f(1) \circ f(a) + f(a) = -f(1)^2 + f(1)$, which for $f(a) = 1$ gives $f(1)^2 = f(1) + f(1)$. By simple substitution we get $-f(1) \circ f(a) + f(a) = -f(1)$, and thus $f(a) + f(1) = f(1) \circ f(a) = f(a) \circ f(1)$. Finally, since $f(1) + f(a) = f(a) + f(1) = f(a) \circ f(1)$, we get that $\tau^{f(1)} = \tau^z$ is a group action. This contradicts with the assumption that τ^z was not a group action.

Proof

Further, for all $a \in S$

$$f(a) = f(\sigma_1(a)) = \sigma_{f(1)}^{f(1)}(f(a)) = f(1) \circ f(a) - f(1)^2 + f(1),$$

and $-f(1) \circ f(a) + f(a) = -f(1)^2 + f(1)$, which for $f(a) = 1$ gives $f(1)^2 = f(1) + f(1)$. By simple substitution we get $-f(1) \circ f(a) + f(a) = -f(1)$, and thus $f(a) + f(1) = f(1) \circ f(a) = f(a) \circ f(1)$. Finally, since $f(1) + f(a) = f(a) + f(1) = f(a) \circ f(1)$, we get that $\tau^{f(1)} = \tau^z$ is a group action. This contradicts with the assumption that τ^z was not a group action.

Example

Let us consider a two-sided brace $U(\mathbb{Z}/16\mathbb{Z})$. Observe that in this case $\check{r}_7$ is not equivalent to $\check{r}_1$ as $5 - 1 + 7 = 11 \pmod{16}$ and $5 \circ 7 = 3 \pmod{16}$. One can easily compute that

$$\tau_{15}^7(5) = 5 \pmod{16} \quad \& \quad \tau_3^7 \tau_5^7(5) = 13 \pmod{16}.$$

Thank you