Yang–Baxter equation and a congruence of biracks

Přemysl Jedlička
with Agata Pilitowska and Anna Zamojska-Dzienio

Department of Mathematics
Faculty of Engineering (former Technical Faculty)
Czech University of Life Sciences (former Czech University of Agriculture) in Prague

Budapest, 10^{th} July 2019

Faculty of Engineering

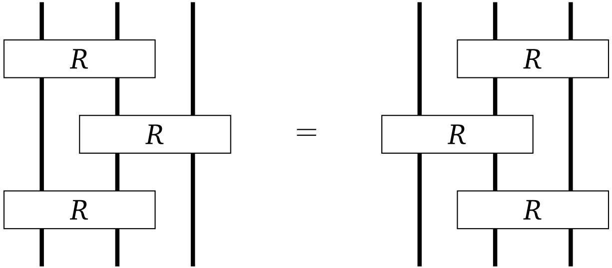
CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Yang–Baxter equation

Definition

Let V be a vector space. A homomorphism $R : V \otimes V \to V \otimes V$ is called a *solution of Yang–Baxter equation* if it satisfies

$$(R \otimes \mathrm{id}_V)(\mathrm{id}_V \otimes R)(R \otimes \mathrm{id}_V) = (\mathrm{id}_V \otimes R)(R \otimes \mathrm{id}_V)(\mathrm{id}_V \otimes R).$$



Set-theoretic solutions

Definition

Let X be a set. A mapping $r : X \times X \to X \times X$ is called a *set-theoretic solution of Yang–Baxter equation* if it satisfies

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

Examples

- Let $(S, \cdot)$ be an idempotent semigroup. Then
$$r : (a, b) \mapsto (a, a \cdot b)$$
is a set-theoretic solution on S.
- Let $(L, \vee, \wedge)$ be a distributive lattice. Then
$$r : (a, b) \mapsto (a \wedge b, a \vee b)$$
is an idempotent (that means $r^2 = r$) set-theoretic solution on L.

Set-theoretic solutions

Definition

Let X be a set. A mapping $r : X \times X \to X \times X$ is called a *set-theoretic solution of Yang–Baxter equation* if it satisfies

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

Examples

- Let $(S, \cdot)$ be an idempotent semigroup. Then
$$r : (a, b) \mapsto (a, a \cdot b)$$
is a set-theoretic solution on S.
- Let $(L, \vee, \wedge)$ be a distributive lattice. Then
$$r : (a, b) \mapsto (a \wedge b, a \vee b)$$
is an idempotent (that means $r^2 = r$) set-theoretic solution on L.

Non-degenerate solutions

Definition

A solution $r:(x,y)\mapsto(\sigma_x(y),\tau_y(x))$ is called *non-degenerate* if σ_x and τ_y are bijections, for all $x,y\in X$.

Fact

If a solution r is non-degenerate then r is a bijection of X^2.

Example

Let $(G,\cdot)$ be a group. Then

$$r_1:(a,b)\mapsto(a^{-1}ba,a)$$
$$r_2:(a,b)\mapsto(ab^{-1}a^{-1},ab^2)$$

are both non-degenerate solutions.

Non-degenerate solutions

Definition

A solution $r : (x,y) \mapsto (\sigma_x(y), \tau_y(x))$ is called *non-degenerate* if σ_x and τ_y are bijections, for all $x, y \in X$.

Fact

If a solution r is non-degenerate then r is a bijection of X^2.

Example

Let $(G, \cdot)$ be a group. Then

$$r_1 : (a,b) \mapsto (a^{-1}ba, a)$$
$$r_2 : (a,b) \mapsto (ab^{-1}a^{-1}, ab^2)$$

are both non-degenerate solutions.

Non-degenerate solutions

Definition

A solution $r : (x,y) \mapsto (\sigma_x(y), \tau_y(x))$ is called *non-degenerate* if σ_x and τ_y are bijections, for all $x, y \in X$.

Fact

If a solution r is non-degenerate then r is a bijection of X^2.

Example

Let $(G, \cdot)$ be a group. Then

$$r_1 : (a,b) \mapsto (a^{-1}ba, a)$$
$$r_2 : (a,b) \mapsto (ab^{-1}a^{-1}, ab^2)$$

are both non-degenerate solutions.

Involutive solutions

Definition

A solution r is called *involutive* if $r^2 = \mathrm{id}_{X^2}$.

Observation

If $r = (\sigma_x, \tau_y)$ *is involutive then* $\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x)$.

Example

If $\sigma_{\sigma_x(y)} = \sigma_y = \tau_y^{-1}$ then (σ_x, τ_y) is an involutive solution.

Example

σ	1	2	3
1	1	2	3
2	1	2	3
3	2	1	3

τ	1	2	3
1	1	1	2
2	2	2	1
3	3	3	3

Involutive solutions

Definition

A solution r is called *involutive* if $r^2 = \mathrm{id}_{X^2}$.

Observation

If $r = (\sigma_x, \tau_y)$ *is involutive then* $\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x)$.

Example

If $\sigma_{\sigma_x(y)} = \sigma_y = \tau_y^{-1}$ then (σ_x, τ_y) is an involutive solution.

Example

σ	1	2	3
1	1	2	3
2	1	2	3
3	2	1	3

τ	1	2	3
1	1	1	2
2	2	2	1
3	3	3	3

Vocabulary

universal algebra setting	STSYBE setting
support of a solution	quadratic set
identity	condition
idempotent	square-free
subsolution	restricted solution
(left) ideal	(left) invariant subset
projection algebra	trivial solution
congruence	equivalence such that the blocks form a solution

Retraction relation

Definition

Let $r = (\sigma_x, \tau_y)$ be an involutive solution on a set X. We define a relation $\sim$ on X as

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y.$$

Definition

Let r be an involutive solution on a set X. We denote by $\mathrm{Ret}(X)$ the factor solution $X/\sim$.

Conjecture [T. Gateva-Ivanova]

Let r be a finite involutive solution satisfying $\sigma_x(x) = \tau_x(x) = x$. Then there exists $k \in \mathbb{N}$ such that $|\mathrm{Ret}^k(X)| = 1$.

Retraction relation

Definition

Let $r = (\sigma_x, \tau_y)$ be an involutive solution on a set X. We define a relation $\sim$ on X as

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y.$$

Definition

Let r be an involutive solution on a set X. We denote by $\mathrm{Ret}(X)$ the factor solution $X/\sim$.

Conjecture [T. Gateva-Ivanova]

Let r be a finite involutive solution satisfying $\sigma_x(x) = \tau_x(x) = x$. Then there exists $k \in \mathbb{N}$ such that $|\mathrm{Ret}^k(X)| = 1$.

Retraction relation

Definition

Let $r = (\sigma_x, \tau_y)$ be an involutive solution on a set X. We define a relation $\sim$ on X as

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y.$$

Definition

Let r be an involutive solution on a set X. We denote by $\mathrm{Ret}(X)$ the factor solution $X/\sim$.

Conjecture [T. Gateva-Ivanova]

Let r be a finite involutive solution satisfying $\sigma_x(x) = \tau_x(x) = x$. Then there exists $k \in \mathbb{N}$ such that $|\mathrm{Ret}^k(X)| = 1$.

Retraction is a congruence

Theorem (P. Etingof, T. Schedler, A. Soloviev)

Let r be an involutive solution on a finite set X. Then there is a well-defined involutive solution on the set $X/\sim$.

Sketch of the proof.

- Define a group $G = \langle X;\ xy = \sigma_x(y)\tau_y(x)\rangle$.
- Show that $x \neq y$, for all $x, y \in G$.
- Prove that $f : x \mapsto \sigma_x$ is a group homomorphism.
- Clearly $x \sim y$ if and only if $f(x) = f(y)$.
- The group $G/\operatorname{Ker} f$ belongs to the solution $X/\sim$. □

Retraction is a congruence

Theorem (P. Etingof, T. Schedler, A. Soloviev)

Let r be an involutive solution on a finite set X. Then there is a well-defined involutive solution on the set $X/\sim$.

Sketch of the proof.

- Define a group $G = \langle X;\ xy = \sigma_x(y)\tau_y(x)\rangle$.
- Show that $x \neq y$, for all $x, y \in G$.
- Prove that $f : x \mapsto \sigma_x$ is a group homomorphism.
- Clearly $x \sim y$ if and only if $f(x) = f(y)$.
- The group $G/\operatorname{Ker} f$ belongs to the solution $X/\sim$. □

Definition of a birack

Definition

A *birack* is an algebra $(X, \circ, \bullet, \backslash, /)$ that satisfies

$$x\backslash(x \circ y) = y, \qquad (x \bullet y)/y = x,$$

$$x \circ (x\backslash y) = y, \qquad (x/y) \bullet y = x,$$

$$x \circ (y \circ z) = (x \circ y) \circ ((x \bullet y) \circ z),$$

$$(x \circ y) \bullet ((x \bullet y) \circ z) = (x \bullet (y \circ z)) \circ (y \bullet z),$$

$$(x \bullet y) \bullet z = (x \bullet (y \circ z)) \bullet (y \bullet z),$$

A birack is said to be *involutive* if it satisfies

$$(x \circ y) \circ (x \bullet y) = x, \qquad (x \circ y) \bullet (x \bullet y) = y.$$

Observation

If $(X, \circ, \bullet, \backslash, /)$ is a birack then $(x \circ y, x \bullet y)$ is a solution. Conversely, if (σ, τ) is a solution then, by setting $x \circ y = \sigma_x(y)$, $x \bullet y = \tau_y(x)$, $x\backslash y = \sigma_x^{-1}(y)$ and $x/y = \tau_y^{-1}(x)$, we obtain a birack.

Retraction relation of biracks

Definition

Let $(X, \circ, \bullet, \backslash, /)$ be a birack. We define a relation $\sim$ on X as follows:

$$x \sim y \text{ if and only if } x \circ z = y \circ z, \text{ for all } z \in X.$$

Theorem (P. Etingof, T. Schedler, A. Soloviev)

If a birack is finite and involutive then $\sim$ is a congruence.

Proposition (P. J., A. P., A. Z.-D.)

If $\circ$ is left distributive, i.e., $x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$, then $\sim$ is a congruence.

Fact

There exists a birack, for which $\sim$ is not a congruence.

Retraction relation of biracks

Definition

Let $(X, \circ, \bullet, \backslash, /)$ be a birack. We define a relation $\sim$ on X as follows:

$$x \sim y \text{ if and only if } x \circ z = y \circ z, \text{ for all } z \in X.$$

Theorem (P. Etingof, T. Schedler, A. Soloviev)

If a birack is finite and involutive then $\sim$ is a congruence.

Proposition (P. J., A. P., A. Z.-D.)

If $\circ$ is left distributive, i.e., $x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$, then $\sim$ is a congruence.

Fact

There exists a birack, for which $\sim$ is not a congruence.

Retraction relation of biracks

Definition

Let $(X, \circ, \bullet, \backslash, /)$ be a birack. We define a relation $\sim$ on X as follows:

$$x \sim y \text{ if and only if } x \circ z = y \circ z, \text{ for all } z \in X.$$

Theorem (P. Etingof, T. Schedler, A. Soloviev)

If a birack is finite and involutive then $\sim$ is a congruence.

Proposition (P. J., A. P., A. Z.-D.)

If $\circ$ is left distributive, i.e., $x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$, then $\sim$ is a congruence.

Fact

There exists a birack, for which $\sim$ is not a congruence.

Retraction relation of biracks

Definition

Let $(X, \circ, \bullet, \backslash, /)$ be a birack. We define a relation $\sim$ on X as follows:

$$x \sim y \text{ if and only if } x \circ z = y \circ z, \text{ for all } z \in X.$$

Theorem (P. Etingof, T. Schedler, A. Soloviev)

If a birack is finite and involutive then $\sim$ is a congruence.

Proposition (P. J., A. P., A. Z.-D.)

If $\circ$ is left distributive, i.e., $x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$, then $\sim$ is a congruence.

Fact

There exists a birack, for which $\sim$ is not a congruence.

Retraction congruence of biracks

Definition

Let $(X, \circ, \bullet, \backslash, /)$ be a birack. We define a relation $\approx$ on X as follows:

$$x \approx y \text{ if and only if } x \circ z = y \circ z \text{ and } z \bullet x = z \bullet y, \text{ for all } z \in X.$$

Theorem (P. J., A. P., A. Z.-D.)

$\approx$ is a congruence of every birack.

Proof.

For each $x \approx x'$, $y \approx y'$ and $z \in X$, we prove

$$(x \circ y) \circ z = (x' \circ y') \circ z \qquad z \bullet (x \circ y) = z \bullet (x' \circ y')$$
$$(x \bullet y) \circ z = (x' \bullet y') \circ z \qquad z \bullet (x \bullet y) = z \bullet (x' \bullet y')$$
$$(x \backslash y) \circ z = (x' \backslash y') \circ z \qquad z \bullet (x \backslash y) = z \bullet (x' \backslash y')$$
$$(x / y) \circ z = (x' / y') \circ z \qquad z \bullet (x / y) = z \bullet (x' / y')$$

□

Retraction congruence of biracks

Definition

Let $(X, \circ, \bullet, \backslash, /)$ be a birack. We define a relation $\approx$ on X as follows:

$$x \approx y \text{ if and only if } x \circ z = y \circ z \text{ and } z \bullet x = z \bullet y, \text{ for all } z \in X.$$

Theorem (P. J., A. P., A. Z.-D.)

$\approx$ is a congruence of every birack.

Proof.

For each $x \approx x'$, $y \approx y'$ and $z \in X$, we prove

$$(x \circ y) \circ z = (x' \circ y') \circ z \qquad z \bullet (x \circ y) = z \bullet (x' \circ y')$$
$$(x \bullet y) \circ z = (x' \bullet y') \circ z \qquad z \bullet (x \bullet y) = z \bullet (x' \bullet y')$$
$$(x \backslash y) \circ z = (x' \backslash y') \circ z \qquad z \bullet (x \backslash y) = z \bullet (x' \backslash y')$$
$$(x / y) \circ z = (x' / y') \circ z \qquad z \bullet (x / y) = z \bullet (x' / y')$$

□

Retraction congruence of biracks

Definition

Let $(X, \circ, \bullet, \backslash, /)$ be a birack. We define a relation $\approx$ on X as follows:

$$x \approx y \text{ if and only if } x \circ z = y \circ z \text{ and } z \bullet x = z \bullet y, \text{ for all } z \in X.$$

Theorem (P. J., A. P., A. Z.-D.)

$\approx$ is a congruence of every birack.

Proof.

For each $x \approx x'$, $y \approx y'$ and $z \in X$, we prove

$$\begin{aligned} (x \circ y) \circ z &= (x' \circ y') \circ z & \qquad z \bullet (x \circ y) &= z \bullet (x' \circ y') \\ (x \bullet y) \circ z &= (x' \bullet y') \circ z & \qquad z \bullet (x \bullet y) &= z \bullet (x' \bullet y') \\ (x \backslash y) \circ z &= (x' \backslash y') \circ z & \qquad z \bullet (x \backslash y) &= z \bullet (x' \backslash y') \\ (x / y) \circ z &= (x' / y') \circ z & \qquad z \bullet (x / y) &= z \bullet (x' / y') \end{aligned}$$

□

Identities of retracts

Proposition (T. Gateva-Ivanova)

Let $(X, \circ, \bullet, \backslash, /)$ *be an involutive birack and let* $k \in \mathbb{N}$. *Then* $|\mathrm{Ret}^k(X)| = 1$ *if and only if*

$$(\cdots(x_1 \circ x_2) \circ \cdots) \circ x_k) \circ y = (\cdots(x_1' \circ x_2) \circ \cdots) \circ x_k) \circ y,$$

for all $x_1, \ldots, x_k, y$ *and* $x_1' \in X$.

Open Problem

Find an equational basis for biracks satisfying $|\mathrm{Ret}^k(X)| = 1$.

For distributive biracks, see the talk of Anna!

Identities of retracts

Proposition (T. Gateva-Ivanova)

Let $(X, \circ, \bullet, \backslash, /)$ *be an involutive birack and let* $k \in \mathbb{N}$. *Then* $|\mathrm{Ret}^k(X)| = 1$ *if and only if*

$$(\cdots(x_1 \circ x_2) \circ \cdots) \circ x_k) \circ y = (\cdots(x_1' \circ x_2) \circ \cdots) \circ x_k) \circ y,$$

for all $x_1, \ldots, x_k, y$ *and* $x_1' \in X$.

Open Problem

Find an equational basis for biracks satisfying $|\mathrm{Ret}^k(X)| = 1$.

For distributive biracks, see the talk of Anna!

Identities of retracts

Proposition (T. Gateva-Ivanova)

Let $(X, \circ, \bullet, \backslash, /)$ *be an involutive birack and let* $k \in \mathbb{N}$. *Then* $|\mathrm{Ret}^k(X)| = 1$ *if and only if*

$$(\cdots(x_1 \circ x_2) \circ \cdots) \circ x_k) \circ y = (\cdots(x_1' \circ x_2) \circ \cdots) \circ x_k) \circ y,$$

for all $x_1, \ldots, x_k, y$ *and* $x_1' \in X$.

Open Problem

Find an equational basis for biracks satisfying $|\mathrm{Ret}^k(X)| = 1$.

For distributive biracks, see the talk of Anna!