Analyzing indecomposable involutive set-theoretic solutions to the Yang-Baxter equation through the displacement group

Marco Castelli

Università del Salento

Advances in Group Theory and Applications, Napoli, 27-06-2025

Basic definitions

The Yang-Baxter equation is a basic equation of the statistical mechanics that arose from Yang's work in 1967 and Baxter's one in 1972. In 1992, Drinfel'd suggested studying the special class of set-theoretic solutions.

Definition

A pair (X, r), where X is a non-empty set and $r : X \times X \to X \times X$ is a map, is a set-theoretic solution of the Yang-Baxter equation if

$$(r \times id_X)(id_X \times r)(r \times id_X) = (id_X \times r)(r \times id_X)(id_X \times r).$$

Basic definitions

The Yang-Baxter equation is a basic equation of the statistical mechanics that arose from Yang's work in 1967 and Baxter's one in 1972. In 1992, Drinfel'd suggested studying the special class of set-theoretic solutions.

Definition

A pair (X, r), where X is a non-empty set and $r : X \times X \to X \times X$ is a map, is a set-theoretic solution of the Yang-Baxter equation if

$$(r \times id_X)(id_X \times r)(r \times id_X) = (id_X \times r)(r \times id_X)(id_X \times r).$$

Basic definitions

From now on, a set-theoretic solution will be simply called a *solution*. If (X, r) is a solution and $x \in X$, we can define the maps $\lambda_x, \rho_x : X \longrightarrow X$ by $r(x, y) = (\lambda_x(y), \rho_y(x))$.

A solution (X, r) is said to be

- *involutive* if $r^2 = id_{X \times X}$
- *non-degenerate* if $\lambda_x, \rho_x \in Sym(X)$ for all $x \in X$

if, in addition, r is bijective

- *decomposable* if there is a partition of X into non-empty disjoint sets X_1, X_2 such that $r(X_i, X_i) \subseteq X_i \times X_i$ for $i = 1, 2$
- *indecomposable* if it is not decomposable.

Basic definitions

From now on, a set-theoretic solution will be simply called a *solution*. If (X, r) is a solution and $x \in X$, we can define the maps $\lambda_x, \rho_x : X \longrightarrow X$ by $r(x, y) = (\lambda_x(y), \rho_y(x))$.
A solution (X, r) is said to be

- *involutive* if $r^2 = id_{X \times X}$
- *non-degenerate* if $\lambda_x, \rho_x \in Sym(X)$ for all $x \in X$

if, in addition, r is bijective

- *decomposable* if there is a partition of X into non-empty disjoint sets X_1, X_2 such that $r(X_i, X_i) \subseteq X_i \times X_i$ for $i = 1, 2$
- *indecomposable* if it is not decomposable.

Basic definitions

Example

- (X, r) *with* $r(x, y) := (f(y), g(x))$ *with* $f, g : X \to X$ *commuting bijective maps.*

Definition (Etingof, Schedler Soloviev (1999) - Rump (2019))

Let (X, r) be a finite involutive non-degenerate solution.

- *The subgroup of $Sym(X)$ generated by the set $\{\lambda_x | x \in X\}$ will be denoted by $\mathcal{G}(X)$, and will be called Yang-Baxter group.*
- *The subgroup of $Sym(X)$ generated by the set $\{\lambda_x^{-1}\lambda_y | x, y \in X\}$ will be denoted by $Dis(X)$, and will be called displacement group.*

Basic definitions

Example

- (X, r) *with* $r(x, y) := (f(y), g(x))$ *with* $f, g : X \to X$ *commuting bijective maps.*

Definition (Etingof, Schedler Soloviev (1999) - Rump (2019))

Let (X, r) *be a finite involutive non-degenerate solution.*

- *The subgroup of* $Sym(X)$ *generated by the set* $\{\lambda_x | x \in X\}$ *will be denoted by* $\mathcal{G}(X)$*, and will be called Yang-Baxter group.*
- *The subgroup of* $Sym(X)$ *generated by the set* $\{\lambda_x^{-1}\lambda_y | x, y \in X\}$ *will be denoted by* $Dis(X)$*, and will be called displacement group.*

Indecomposability of solutions

Theorem (Etingof, Schedler, Soloviev (1999))

An involutive non-degenerate solution (X, r) is indecomposable if and only if $\mathcal{G}(X)$ acts transitively on X.

Proposition

The orbits with respect to $\mathcal{G}(X)$ provide smaller solutions.

Convention

Every solution (X, r) will be assumed to be involutive and non-degenerate. Moreover, even if not specified, X will be assumed to be a finite set.

Main structures: Cycle sets

"How to solve the QYBE? Construct a cycle set!" (W. Rump)

Definition (Rump (2007))

A set X with a binary operation $\cdot$ is a non-degenerate cycle set if $(X,\cdot)$ is a left quasigroup, i.e. each left multiplication $\sigma_x : X \to X, y \mapsto x\cdot y$ is bijective, and

- *the equality $(x\cdot y)\cdot(x\cdot z) = (y\cdot x)\cdot(y\cdot z)$ holds for all $x, y, z \in X$*
- *the map $x \mapsto x\cdot x$ is bijective*

Example

- *X a set, $\alpha \in Sym(X)$ and $x\cdot y := \alpha(y)$ (this is called trivial cycle set).*

Correspondence cycle sets-solutions

Theorem (Rump (2007))

Involutive non-degenerate solutions bijectively correspond to non-degenerate cycle sets, and the correspondence is given by

$$(X, \cdot\,) \longrightarrow r(x,y) := (\sigma_x^{-1}(y), \sigma_x^{-1}(y)\cdot x)$$

$$(X, r) \longrightarrow x\cdot y := \lambda_x^{-1}(y)$$

Of course, indecomposable solutions corresponds to indecomposable cycle sets.

Studying indecomposable cycle sets

Definition

A cycle set X is said to be simple if its only epimorphic images are X and the trivial cycle set of size 1.

Theorem (Vendramin (2016) + C., Catino, Pinto (2019))

Let $(X, *), (Y, \cdot)$ be indecomposable cycle sets and $p : X \to Y$ an epimorphism. Then, X is isomorphic to a cycle set on $Y \times S$ given by

$$(y, s) \bullet (w, t) := (y \cdot w, \alpha_{(y,s,w)}(t))$$

for all $(y, s), (w, t) \in Y \times S$, where α is a "suitable" map.

Therefore, the first main step in the study of indecomposable cycle sets is the study of the simple ones.

Studying indecomposable cycle sets

Definition

A cycle set X is said to be simple if its only epimorphic images are X and the trivial cycle set of size 1.

Theorem (Vendramin (2016) + C., Catino, Pinto (2019))

Let $(X,*), (Y,\cdot)$ be indecomposable cycle sets and $p : X \to Y$ an epimorphism. Then, X is isomorphic to a cycle set on $Y \times S$ given by

$$(y,s) \bullet (w,t) := (y \cdot w, \alpha_{(y,s,w)}(t))$$

for all $(y,s),(w,t) \in Y \times S$, where α is a "suitable" map.

Therefore, the first main step in the study of indecomposable cycle sets is the study of the simple ones.

Main structures: Braces

Definition (Rump (2007), Cedó, Jespers, Okniński (2014))

A triple $(B, +, \circ)$ is a brace if $(B, +)$ is an abelian group, $(B, \circ)$ a group and $a \circ (b + c) = a \circ b - a + a \circ c$ for all $a, b, c \in B$.

Definition (Rump (2007), Cedó, Jespers, Okniński (2014))

Let B be a brace. A subgroup I of $(B, +)$ is an ideal if

- *I is a normal subgroup of $(B, \circ)$*
- *$\lambda_a(I) \subseteq I$ for all $a \in B$, where $\lambda_a(x) = -a + a \circ x$.*

Main structures: Braces

Definition (Rump (2007), Cedó, Jespers, Okniński (2014))

A triple $(B, +, \circ)$ is a brace if $(B, +)$ is an abelian group, $(B, \circ)$ a group and $a \circ (b + c) = a \circ b - a + a \circ c$ for all $a, b, c \in B$.

Definition (Rump (2007), Cedó, Jespers, Okniński (2014))

Let B be a brace. A subgroup I of $(B, +)$ is an ideal if

- *I is a normal subgroup of $(B, \circ)$*
- *$\lambda_a(I) \subseteq I$ for all $a \in B$, where $\lambda_a(x) = -a + a \circ x$.*

Braces and indecomposable cycle sets

Let X be an indecomposable cycle set.

Proposition (Cedó, Jespers, Okniński (2014))

The associated permutation group $\mathcal{G}(X)$ has a brace structure, where the $\circ$ operation is the usual composition of maps.

Proposition (Rump (2019))

The displacement group $Dis(X)$ is an ideal of the brace $\mathcal{G}(X)$.

Proposition (Rump (2019))

The orbits of an ideal I of $\mathcal{G}(X)$ provide a cycle set structure X/I such that $X \to X/I$, $x \mapsto [x]_I$ is an epimorphism of cycle sets.

Braces and indecomposable cycle sets

Let X be an indecomposable cycle set.

Proposition (Cedó, Jespers, Okniński (2014))

The associated permutation group $\mathcal{G}(X)$ has a brace structure, where the $\circ$ operation is the usual composition of maps.

Proposition (Rump (2019))

The displacement group $Dis(X)$ is an ideal of the brace $\mathcal{G}(X)$.

Proposition (Rump (2019))

The orbits of an ideal I of $\mathcal{G}(X)$ provide a cycle set structure X/I such that $X \to X/I$, $x \mapsto [x]_I$ is an epimorphism of cycle sets.

Braces and indecomposable cycle sets

Let X be an indecomposable cycle set.

Proposition (Cedó, Jespers, Okniński (2014))

The associated permutation group $\mathcal{G}(X)$ has a brace structure, where the $\circ$ operation is the usual composition of maps.

Proposition (Rump (2019))

The displacement group $Dis(X)$ is an ideal of the brace $\mathcal{G}(X)$.

Proposition (Rump (2019))

The orbits of an ideal I of $\mathcal{G}(X)$ provide a cycle set structure X/I such that $X \to X/I$, $x \mapsto [x]_I$ is an epimorphism of cycle sets.

How to detect indecomposable simple cycle sets?

Let X be an indecomposable cycle set.

Theorem (C. (2022))

X is a simple cycle set if and only if $|X| = p$, for some prime number p, or $Dis(X)$ is the unique minimal ideal of the brace $\mathcal{G}(X)$ and it acts transitively on X.

In 2024, Colazzo, Jespers, Kubat and Van Antwerpen provided an extension of the previous theorem to non-involutive solutions.

How to detect indecomposable simple cycle sets?

Let X be an indecomposable cycle set.

Theorem (C. (2022))

X is a simple cycle set if and only if $|X| = p$, for some prime number p, or $Dis(X)$ is the unique minimal ideal of the brace $\mathcal{G}(X)$ and it acts transitively on X.

In 2024, Colazzo, Jespers, Kubat and Van Antwerpen provided an extension of the previous theorem to non-involutive solutions.

Classification results

- Indecomposable simple cycle sets of size ≤ 9 (Vendramin)
- Every indecomposable cycle set of prime order p is simple and is isomorphic $(\mathbb{Z}/p\mathbb{Z}, \cdot\,)$ with $x \cdot y := y + 1$ (Etingof, Schedler and Soloviev (1999))
- Classified indecomposable simple cycle sets of size p^2 (Dietzel, Properzi and Trappeniers (2024))

Classification results

- Indecomposable simple cycle sets of size ≤ 9 (Vendramin)
- Every indecomposable cycle set of prime order p is simple and is isomorphic $(\mathbb{Z}/p\mathbb{Z}, \cdot\,)$ with $x \cdot y := y + 1$ (Etingof, Schedler and Soloviev (1999))
- Classified indecomposable simple cycle sets of size p^2 (Dietzel, Properzi and Trappeniers (2024))

Classification results

- Indecomposable simple cycle sets of size ≤ 9 (Vendramin)
- Every indecomposable cycle set of prime order p is simple and is isomorphic $(\mathbb{Z}/p\mathbb{Z}, \cdot)$ with $x \cdot y := y + 1$ (Etingof, Schedler and Soloviev (1999))
- Classified indecomposable simple cycle sets of size p^2 (Dietzel, Properzi and Trappeniers (2024))

Examples/classification results

- Constructed indecomposable simple cycle sets of size p^t, n^2, $m^2 n$ with p a prime number and $m, n, t > 1$ (Cedó, Okniński (2021-2024))

as obstruction results

- If $|X|$ is square-free and X is simple $\Rightarrow |X| = p$ (Cedó, Okniński (2022))
- If $Dis(X)$ is cyclic and X is simple $\Rightarrow |X| = p$ (Bonatto, C. 2025)

Examples/classification results

- Constructed indecomposable simple cycle sets of size p^t, n^2, m^2n with p a prime number and $m, n, t > 1$ (Cedó, Okniński (2021-2024))

as obstruction results

- If $|X|$ is square-free and X is simple $\Rightarrow |X| = p$ (Cedó, Okniński (2022))
- If $Dis(X)$ is cyclic and X is simple $\Rightarrow |X| = p$ (Bonatto, C. 2025)

Examples/classification results

- Constructed indecomposable simple cycle sets of size p^t, n^2, m^2n with p a prime number and $m, n, t > 1$ (Cedó, Okniński (2021-2024))

as obstruction results

- If $|X|$ is square-free and X is simple $\Rightarrow |X| = p$ (Cedó, Okniński (2022))
- If $Dis(X)$ is cyclic and X is simple $\Rightarrow |X| = p$ (Bonatto, C. 2025)

Affine cycle sets

Definition

An algebraic structure $(X, \cdot\,)$ *is said to be*

- *a quasigroup if the left multiplications (i.e.* $\sigma_x(y) := x \cdot y$*) and the right multiplications (i.e.* $\delta_x(y) := y \cdot x$*) are bijections*
- *an affine quasigroup if* X *can be endowed with an abelian group operation* $+$, $A, B \in Aut(X, +)$ *and* $c \in X$ *such that*

$$x \cdot y = A(x) + B(y) + c$$

  and we indicate it by $(X, +, A, B, c)$.
- *an affine cycle set if it has the structure of both a quasigroup and a cycle set.*

Affine simple cycle sets and the displacement group

Clearly, an affine cycle set X is indecomposable.

Propositions-Remarks (Bonatto, Kinyon, Stanovský, Vojtěchovský (2020))

- *An affine quasigroup $(X, +, A, B, c)$ is a cycle set if and only if $BA^{-1} - A^{-1}B = Id_X$.*
- *Let X be an affine cycle set. Then, X can be constructed as an affine quasigroup $(G, +, A, B, c)$ with $(G, +) \cong Dis(X)$.*

Lemma (Bonatto, C. (2025))

Let X be an affine simple cycle set. Then, $Dis(X) \cong \mathbb{Z}/p\mathbb{Z}^n$ for some n. Moreover, p divides n.

Affine simple cycle sets and the displacement group

Clearly, an affine cycle set X is indecomposable.

Propositions-Remarks (Bonatto, Kinyon, Stanovský, Vojtěchovský (2020))

- *An affine quasigroup $(X, +, A, B, c)$ is a cycle set if and only if $BA^{-1} - A^{-1}B = Id_X$.*
- *Let X be an affine cycle set. Then, X can be constructed as an affine quasigroup $(G, +, A, B, c)$ with $(G, +) \cong Dis(X)$.*

Lemma (Bonatto, C. (2025))

Let X be an affine simple cycle set. Then, $Dis(X) \cong \mathbb{Z}/p\mathbb{Z}^n$ for some n. Moreover, p divides n.

Affine simple cycle sets and the displacement group

Clearly, an affine cycle set X is indecomposable.

Propositions-Remarks (Bonatto, Kinyon, Stanovský, Vojtěchovský (2020))

- *An affine quasigroup $(X, +, A, B, c)$ is a cycle set if and only if $BA^{-1} - A^{-1}B = Id_X$.*
- *Let X be an affine cycle set. Then, X can be constructed as an affine quasigroup $(G, +, A, B, c)$ with $(G, +) \cong Dis(X)$.*

Lemma (Bonatto, C. (2025))

Let X be an affine simple cycle set. Then, $Dis(X) \cong \mathbb{Z}/p\mathbb{Z}^n$ for some n. Moreover, p divides n.

Affine simple cycle sets

Let A_1 be the first Weyl algebra over $\mathbb{Z}/p\mathbb{Z}$ generated by a and b.

Theorem (Bonatto, C. (2025))

Let p be a prime number and ρ be an irreducible representation with dimension n of A_1. Suppose that $\rho(a)$ and $\rho(b)$ are invertible, let $c \in (\mathbb{Z}/p\mathbb{Z})^n$ and set $A := \rho(b)^{-1}$ and $B := \rho(a)$. Then

$$((\mathbb{Z}/p\mathbb{Z})^n, +, A, B, c)$$

is a simple affine cycle set for every $c \in \mathbb{Z}/p\mathbb{Z}^n$.
Conversely, every affine simple cycle set can be constructed in this way.

Affine simple cycle sets of size p^p

Theorem (Bonatto, C. (2025))

Let p be a prime and X be an affine simple cycle set of size p^p. Then X is isomorphic to one of the following affine cycle sets:

$$((\mathbb{Z}/p\mathbb{Z})^p, +, M_\lambda^{-1}, M_\mu, (0, \dots, 0))$$

$$((\mathbb{Z}/p\mathbb{Z})^p, +, M_\lambda^{-1}, M_1, (1, 0, \dots, 0))$$

for $\mu, \lambda = 1, \dots, p-1$. In particular, there are $p^2 - p$ non-isomorphic affine simple cycle sets of size p^p.

Thank you!