The set theoretic Yang-Baxter equation and the structure of skew braces

Paul Truman

Keele University, UK

Braiding new ground, Maynooth University,
17$^{\text{th}}$ September 2026

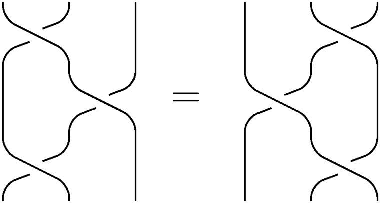
Overview

Aim

Introduce skew braces as an algebraic framework for studying solutions to the set-theoretic Yang-Baxter equation. Illustrate how properties of skew braces are reflected in the corresponding solutions, and present new results on substructures / decompositions of skew braces.

- The braid equation
- Solutions from groups and skew braces
- Internal structure and substructures of skew braces
- Skew braces of order pq revisited

The braid equation (or Yang-Baxter equation)



- Often expressed in terms of a linear transformation R of a tensor product of vector spaces $V \otimes V$. We require that

$$(R \otimes 1)(1 \otimes R)(R \otimes 1) = (1 \otimes R)(R \otimes 1)(1 \otimes R).$$

- We shall study the *set theoretic* version: a (nonempty) set G and a map $r : G \times G \to G \times G$ such that

$$(r \times 1)(1 \times r)(r \times 1) = (1 \times r)(r \times 1)(1 \times r).$$

Notation and terminology

- A solution $r : G \times G \to G \times G$ is called *bijective* if r is a bijection, and *involutive* if $r^2 = \mathrm{id}$.
- We write $r(x, y) = (\lambda_x(y), \rho_y(x))$.
- A solution is called
  - *left nondegenerate* if each λ_x is bijective;
  - *right nondegenerate* if each ρ_y is bijective;
  - *nondegenerate* if it is both left and right nondegenerate.

Example

The trivial solution $r(x, y) = (x, y)$ has $\lambda_x(y) = x$ and $\rho_y(x) = y$. This solution is involutive and degenerate.
The twist solution $r(x, y) = (y, x)$ has $\lambda_x(y) = y$ and $\rho_y(x) = x$. This solution is involutive and nondegenerate.

- Particular interest in finding bijective nondegenerate solutions.

Group-Theoretic Solutions?

Theorem (Lu, Yan, Zhu (2000))

Let G be a group. Suppose that we have functions $\lambda : G \to \mathrm{Perm}(G)$ and $\rho : G \to \mathrm{Perm}(G)$ such that:

- $\lambda_{xy} = \lambda_x \lambda_y$ *(i.e. λ is a homomorphism);*
- $\rho_{xy} = \rho_y \rho_x$ *(i.e. ρ is an anti-homomorphism);*
- $\lambda_x(y)\rho_y(x) = xy$.

Then

$$r(x, y) = (\lambda_x(y), \rho_y(x))$$

is a nondegenerate bijective solution.

Skew braces

Definition (Guarnieri and Vendramin, 2017)

A *(left) skew brace* is a set G together with two binary operations $\bullet$ and $\circ$ such that

- $(G, \bullet)$ and $(G, \circ)$ are groups;
- $x \circ (y \bullet z) = (x \circ y) \bullet x^{-1} \bullet (x \circ z)$ for all $x, y, z \in G$, where x^{-1} denotes the inverse of x with respect to $\bullet$.

- A skew brace in which $(G, \bullet)$ is abelian is called a *brace*. These objects were introduced by Rump in 2007.
- The groups $(G, \bullet)$ and $(G, \circ)$ are called the *additive group* and *multiplicative group* of the skew brace.
- These groups share the same identity element, but $x^{-1} \neq \overline{x}$ in general.

Examples of Skew braces

Example

Let $(G, \bullet)$ be a group and define $x \circ y = xy$. Then $(G, \bullet, \circ)$ is a skew brace, called the *trivial skew brace* on G.

Example

Let $(G, \bullet)$ be a group and define $x \circ y = yx$. Then $(G, \bullet, \circ)$ is a skew brace, called the *almost trivial skew brace* on G.

Example

Consider $(\mathbb{Z}_{2n}, +)$ and define $\circ$ by $x \circ y = x + (-1)^x y$. Then $(\mathbb{Z}_{2n}, \circ) \cong D_n$ and $(\mathbb{Z}_{2n}, +, \circ)$ is a skew brace.

Skew braces produce $\lambda - \rho$ pairs

Theorem (Guarnieri and Vendramin, 2017)

Given a skew brace $(G, \bullet, \circ)$ *define*

- $\lambda : G \to \mathrm{Perm}(G)$ *by* $\lambda_x(y) = x^{-1}(x \circ y)$
- $\rho : G \to \mathrm{Perm}(G)$ *by* $\rho_y(x) = \overline{\lambda_x(y)} \circ x \circ y$.

Then:

- λ *is a homomorphism;*
- ρ *is an anti-homomorphism;*
- $\lambda_x(y) \circ \rho_y(x) = x \circ y$.

Therefore $r : G \times G \to G \times G$ *defined by*

$$r(x, y) = (\lambda_x(y), \rho_y(x))$$

is a nondegenerate bijective solution.

Solutions from skew braces

Example

Let $(G, \bullet, \circ)$ be a trivial skew brace. Then $\overline{x} = x^{-1}$, $\lambda_x(y) = x^{-1}(xy) = y$, and $\rho_y(x) = y^{-1}xy$. The corresponding solution is $r(x, y) = (y, y^{-1}xy)$.

Example

Let $(G, \bullet, \circ)$ be an almost trivial skew brace. Then $\overline{x} = x^{-1}$, $\lambda_x(y) = x^{-1}(x \circ y) = x^{-1}yx$, and $\rho_y(x) = x$. The corresponding solution is $r(x, y) = (x^{-1}yx, x)$.

Example

For the skew brace $(\mathbb{Z}_{2n}, +, \circ)$ with $x \circ y = x + (-1)^x y$, we have
$\lambda_x(y) = (-1)^x y$ and $\rho_y(x) = (-1)^y x$.
The corresponding solution is $r(x, y) = ((-1)^x y, (-1)^y x)$.

Involutive and inverse solutions

Recall that a solution r is called *involutive* if $r^2 = \mathrm{id}$.

Proposition

Given a skew brace $(G, \bullet, \circ)$, the corresponding solution is involutive if and only if $(G, \bullet)$ is abelian.

Theorem (Koch and T., 2020)

Given a skew brace $(G, \bullet, \circ)$ *define* $\bullet^{opp}$ *by*

$$x \bullet^{opp} y = y \bullet x.$$

Then $(G, \bullet^{opp}, \circ)$ *is a skew brace, called the opposite of the original skew brace. Furthermore, the solutions corresponding to these two skew braces are mutually inverse.*

Classifying skew braces

An *isomorphism* of skew braces is a bijective map that respects both operations. Isomorphic skew braces produce solutions that are isomorphic in a natural sense.

It is natural to try to classify skew braces up to isomorphism. For example, by order:

- p, p^2, p^3 (p a prime)
- pq with p, q distinct primes
- p^2q with p, q distinct primes
- squarefree

Or by properties of the multiplicative / additive group:

- simple multiplicative group
- both groups cyclic
- both groups dihedral

More on the λ-function

Recall that given a skew brace $(G, \bullet, \circ)$ there is a homomorphism $\lambda : (G, \circ) \to \mathrm{Perm}(G)$ defined by $\lambda_x(y) = x^{-1}(x \circ y)$.

- In fact $\lambda_x \in \mathrm{Aut}(G, \bullet)$ for each $x \in G$.
- The λ-function of a skew brace translates between the two group structures: we have

$$x \circ y = x\lambda_x(y) \text{ for all } x, y \in G.$$

- In terms of left regular representations we have

$$\mathcal{L}_\circ(x) = \mathcal{L}_\bullet(x)\lambda_x \text{ for each } x \in G.$$

- Thus

$$\mathcal{L}_\circ(G) \subseteq \mathcal{L}_\bullet(G)\lambda(G) \cong (G, \bullet) \rtimes \lambda(G).$$

Substructures of skew braces

Definition

A *subskew brace* of a skew brace $(G, \bullet, \circ)$ is a subset H of G that is a subgroup with respect to both operations.

- A subgroup with respect to either operation is a subskew brace if and only if $\lambda_x(y) \in H$ for all $x, y \in H$.
- A subskew brace H is called a *left ideal* if $\lambda_x(y) \in H$ for all $x \in G$ and all $y \in H$.
- A left ideal is called an *ideal* if it is normal with respect to both operations.

Question

For which divisors d of $|G|$ does $(G, \bullet, \circ)$ necessarily have a substructure of order d?

Low hanging fruit

Recall that $\lambda_x \in \mathrm{Aut}(G, \bullet)$ for each $x \in G$ and that $\lambda : (G, \circ) \to \mathrm{Aut}(G, \bullet)$ is a homomorphism.

Hence $(G, \circ)$ acts on the set of subgroups of $(G, \bullet)$ of a given order by $H \mapsto \lambda_x(H)$.

Proposition

Suppose that $(G, \bullet)$ has a unique subgroup of a particular order. Then this subgroup is a left ideal of $(G, \bullet, \circ)$, hence a subskew brace.

Corollary

Suppose that $(G, \bullet)$ is nilpotent. Then each Sylow subgroup of $(G, \bullet)$ is a left ideal of $(G, \bullet, \circ)$.

Sylow's first theorem for skew braces

Theorem (T.)

Let $G = (G, \bullet, \circ)$ be a finite skew brace, let p be a prime number, and write $|G| = p^e m$ with $p \nmid m$. Then G has a subskew brace of order p^e.

Proof (sketch).

- Let $(B, \circ)$ be a Sylow p-subgroup of $(G, \circ)$.
- There exists a Sylow p-subgroup $(A, \bullet)$ of $(G, \bullet)$ such that $\lambda_y(A) = A$ for all $y \in B$.
- Hence $(A, \bullet) \rtimes \lambda(B)$ is a Sylow p-subgroup of $(G, \bullet) \rtimes \lambda(G)$.
- Hence $\mathcal{L}_\circ(B) \subseteq (g, \lambda_h)(A \rtimes \lambda(B))(g, \lambda_h)^{-1}$, so
$$\mathcal{L}_\circ(B)(g, \lambda_h) \subseteq (g, \lambda_h)(A \rtimes \lambda(B)).$$
- Evaluating each side at the identity we get $B \circ g \subseteq g\lambda_h(A)$, so $\overline{g} \circ B \circ g \subseteq \overline{g} \circ (g\lambda_h(A)) = (\overline{g} \circ g)(\overline{g})^{-1}(\overline{g} \circ \lambda_h(A)) = \lambda_{\overline{g}}\lambda_h(A)$. $\square$

Corollaries

Corollary

Let G be a finite skew brace with $|G| = p^e m$ with $p \nmid m$. Then G contains a subskew brace of each order p^r with $0 \leq r \leq e$.

Corollary

Let G be a finite skew brace and let p be a prime dividing $|G|$. Then G contains a subskew brace of order p.

Skew braces of order pq revisited

- Let $p > q$ be prime numbers

Proposition

If $p \not\equiv 1 \pmod{q}$ then up to isomorphism there is a unique skew brace of order pq, which is the trivial skew brace on the cyclic group of order pq.

- Now suppose $G = (G, \bullet, \circ)$ has order pq, with $p \equiv 1 \pmod{q}$.
- Each of $(G, \bullet)$ and $(G, \circ)$ is cyclic or metacyclic.
- G contains a subskew brace P of order p; in fact this is an ideal. It is trivial as a skew brace; write $P = \langle s \rangle$.
- G contains a subskew brace Q of order q, which is trivial as a skew brace; write $Q = \langle t \rangle$.

The case $(G, \bullet)$ cyclic

- Recall: P is ideal of order p; Q is subskew brace of order q.

Proposition

Up to isomorphism there are 2 skew braces of order pq with cyclic additive group.

Proof.

In this case Q is a left ideal of G.

Hence $G \cong P \rtimes_1^d Q$ where $d^q = 1 \in \mathbb{Z}_p^\times$ and

$$(s^i, t^u)(s^j, t^v) = (s^{i+j}, t^{u+v})$$
$$(s^i, t^u) \circ (s^j, t^v) = (s^{i+d^u j}, t^{u+v}).$$

If $d = 1$ then $(G, \circ)$ is cyclic.

If $d \neq 1$ then $(G, \circ)$ metacyclic; all choices isomorphic. $\square$

The case $(G, \bullet)$ metacyclic

- Recall: P is ideal of order p; Q is subskew brace of order q.

Proposition

Up to isomorphism there are q skew braces of order pq with metacyclic additive group such that Q is a left ideal.

Proof.

Since Q is a left ideal of G we have $G \cong P \rtimes_g^d Q$ where $d^q = g^q = 1 \in \mathbb{Z}_p^\times$ and

$$(s^i, t^u)(s^j, t^v) = (s^{i+g^u j}, t^{u+v})$$
$$(s^i, t^u) \circ (s^j, t^v) = (s^{i+d^u j}, t^{u+v}).$$

If $d = 1$ then $(G, \circ)$ is cyclic.

If $d \neq 1$ then $(G, \circ)$ metacyclic; all choices pairwise nonisomorphic. $\square$

The case $(G, \bullet)$ metacyclic

- Recall: Up to isomorphism there are q skew braces of order pq with metacyclic additive group such that Q is a left ideal.

Proposition

Suppose that G is a skew brace of order pq with $(G, \bullet)$ metacyclic. Then Q is a left ideal in exactly one of G or G^{opp}.

- The proof relies on the fact that $\lambda_t(t) = t$ and $\lambda_s(s) = s$, and examines possibilities for $\lambda_s(t)$ and $\lambda_t(s)$.

Corollary

Up to isomorphism there are $2q$ skew braces of order pq with metacyclic additive group.

Further questions

- Complements / Schur-Zassenhaus type results: already well underway!
- Revisit other classification results: skew braces of orders p^2q or pq^2? Of squarefree order?
- Back to counting: do the Sylow p-subskew braces of a skew brace form a single orbit under the action of some other group?
- Criteria for existence of left ideals of various orders: useful in Hopf-Galois theory.

Thank you for your attention.