Opposite skew left braces, Hopf-Galois theory, and solutions to the Yang-Baxter equation

Alan Koch

Agnes Scott College

March 16, 2019

Outline

Definition

A *skew left brace* is a set B with two binary operations $\cdot, \circ$ such that

1. $(B, \cdot)$ is a group;
2. $(B, \circ)$ is a group;
3. for all $x, y, z \in B$ we have

$$x \circ (y \cdot z) = (x \circ y) \cdot x^{-1} \cdot (x \circ z) \qquad \text{(brace relation)}$$

where x^{-1} is the inverse in $(B, \cdot)$.

Notation:

- Write $\mathfrak{B} = (B, \cdot, \circ)$.
- Write xy for $x \cdot y$ when appropriate.
- For brevity, “brace” = “skew left brace” here.
- Denote the inverse of x in $(B, \circ)$ by $\overline{x}$.
- $e \in B$ denotes the identity (note $xe = x \circ e = x$).

Example (Trivial Brace)

Let $(B, \cdot)$ be a group.

Define $x \circ y = xy$.

Then
$$(x \circ y)x^{-1}(x \circ z) = (xy)z = x(yz) = x \circ (yz)$$
and so $\mathfrak{B} := (B, \cdot, \circ)$ is a brace.

Example (Almost the Trivial Brace)

Let $(B, \cdot)$ be a group.

Define $x \circ y = yx$.

Then

$$\begin{aligned}(x \circ y)x^{-1}(x \circ z) &= (yx)x^{-1}(zx) \\ &= (yz)x \\ &= x \circ (yz).\end{aligned}$$

Thus, $\mathfrak{B} := (B, \cdot, \circ)$ is a brace.

Let N, G be groups.

We say $\mathfrak{B} = (B, \cdot, \circ)$ is *of type* N, G if $(B, \cdot) \cong N$ and $(B, \circ) \cong G$.

Example (Type D_4, Q_8)

Let $(B, \cdot) = \{\langle \sigma, \tau \rangle : \sigma^4 = \tau^2 = \sigma\tau\sigma\tau = e\} \cong D_4$ and define

$$x \circ y = \begin{cases} xy & x \in \langle \sigma \rangle \text{ or } y \in \langle \sigma \rangle \\ \sigma^2 xy & x, y \notin \langle \sigma \rangle \end{cases} .$$

Then $(B, \circ) \cong Q_8$. (Note: $\tau \circ \tau = \sigma^2\tau^2 = \sigma^2$.)

Example (Type S_n, S_n with $n \geq 4$)

Fix $\tau \in A_n,\ |\tau| = 2$. Let $(B, \cdot) = S_n$, and define

$$\sigma \circ \pi = \begin{cases} \sigma\pi & \sigma \in A_n \\ \sigma\tau\pi\tau & \sigma \notin A_n \end{cases}.$$

Then $(B, \circ) \cong S_n$.

Connection with Hopf-Galois theory

Let L/K be a finite Galois extension of fields, $(G, *) = \text{Gal}(L/K)$.

Greither-Pareigis (1987). There is a one-to-one correspondence between regular subgroups $N \leq \text{Perm}(G)$ which are normalized by G (acting by left regular representation) and Hopf-Galois structures on L/K.

Let $(N, \cdot) \leq \text{Perm}(G)$ be a regular subgroup normalized by G. Let $a : N \to G$ be the bijection given by $a(\eta) = \eta[1_G]$. Define

$$\eta \circ \pi = a^{-1}(a(\eta) * a(\pi)), \ \eta, \pi \in N.$$

Then $(N, \cdot, \circ)$ is a brace, and $(N, \circ) \cong (G, *)$.

The correspondence $[(N, \cdot) \leq \text{Perm}(G)] \mapsto (N, \cdot, \circ), \ (N, \circ) \cong G$ is onto the set of finite braces but not one-to-one.

Outline

Construction of the opposite

Let $\mathfrak{B} = (B, \cdot, \circ)$ be a brace. Define a new operation, $\circ'$, on B by

$$x \circ' y = \left(x^{-1} \circ y^{-1}\right)^{-1}, \; x, y \in B.$$

Since

$$\begin{aligned} x \circ' (y \circ' z) &= x \circ' \left(y^{-1} \circ z^{-1}\right)^{-1} \\ &= \left(x^{-1} \circ y^{-1} \circ z^{-1}\right)^{-1} \\ &= (x \circ' y) \circ' z, \end{aligned}$$

$(B, \circ')$ is associative.

Also, $x \circ' e = (x^{-1} \circ e)^{-1} = (x^{-1})^{-1} = x$ shows $e \in B$ is the identity.

Finally, $x \circ' \overline{x^{-1}}^{-1} = \left(x^{-1} \circ \overline{x^{-1}}\right)^{-1} = e^{-1} = e$, so $(B, \circ')$ is a group.

$x \circ' y = \left(x^{-1} \circ y^{-1}\right)^{-1}$

Claim: $\mathfrak{B}' := (B, \cdot, \circ')$ is a brace.

For all $x, y, z \in B$ we have:

$$\begin{aligned}
x \circ' (yz) &= \left(x^{-1} \circ (yz)^{-1}\right)^{-1} \\
&= \left(x^{-1} \circ (z^{-1}y^{-1})\right)^{-1} \\
&= \left((x^{-1} \circ z^{-1})x(x^{-1} \circ y^{-1})\right)^{-1} \\
&= \left(x^{-1} \circ y^{-1}\right)^{-1} x^{-1} \left(x^{-1} \circ z^{-1}\right)^{-1} \\
&= (x \circ' y)x^{-1}(x \circ' z).
\end{aligned}$$

We call $\mathfrak{B}'$ the *opposite brace* to $\mathfrak{B}$.

$x \circ' y = \left(x^{-1} \circ y^{-1}\right)^{-1}$

Properties:

- $\mathfrak{B}'' := (\mathfrak{B}')' = \mathfrak{B}$.
- $(B, \circ) \cong (B, \circ')$ by the "inverse" map $x \mapsto x^{-1}$.
- If $(B, \cdot)$ is abelian, then $\mathfrak{B}' \cong \mathfrak{B}$.
- $\mathfrak{B}$ and $\mathfrak{B}'$ are of the same type.
- The identity $x \circ' y = x(x^{-1} \circ y)x$ holds.
- In general, $\left(\overline{x^{-1}}\right)^{-1} \neq \overline{x}$, i.e., the inverses under $\circ$ and $\circ'$ do not coincide.

Motivation: connection with Hopf-Galois theory II

Let L/K be a finite Galois extension of fields, $G = \mathrm{Gal}(L/K)$, and let $N \leq \mathrm{Perm}(G)$ be regular and normalized by G.

Let

$$N^{\mathrm{opp}} = \mathrm{Cent}_{\mathrm{Perm}(G)}(N) = \{\tau \in \mathrm{Perm}(G) : \eta\tau = \tau\eta \text{ for all } \eta \in N\}.$$

Then $N^{\mathrm{opp}} \leq \mathrm{Perm}\, G$ is regular and normalized by G, hence N^{opp} gives rise to a Hopf-Galois structure on L/K.

If $\mathfrak{B}$ is the brace corresponding to N, then turns out that the brace corresponding to N^{opp} is $\mathfrak{B}'$.

Outline

Example (Trivial Brace)

Let $\mathfrak{B} = (B, \cdot, \circ)$, $x \circ y = xy$.

Then

$$x \circ' y = x(x^{-1} \circ y)x = x(x^{-1} y)x = yx$$

and so $(B, \circ') = (B, \circ)^{\mathrm{opp}}$.

Note $\mathfrak{B}$ was the first example in this talk, $\mathfrak{B}'$ was the second.

Example (Type D_4, Q_8)

Let $(B, \cdot) = \{\langle \sigma, \tau \rangle : \sigma^4 = \tau^2 = \sigma\tau\sigma\tau = e\} \cong D_4$ with

$$x \circ y = \begin{cases} xy & x \in \langle \sigma \rangle \text{ or } y \in \langle \sigma \rangle \\ \sigma^2 xy & x, y \notin \langle \sigma \rangle \end{cases}.$$

Then

$$x \circ' y = \begin{cases} yx & x \in \langle \sigma \rangle \text{ or } y \in \langle \sigma \rangle \\ \sigma^2 yx & x, y \notin \langle \sigma \rangle \end{cases}.$$

Example (Type $S_n, S_n,\ n \geq 4$)

Fix $\tau \in A_n,\ |\tau| = 2$. Let $(B, \cdot) = S_n$ and

$$\sigma \circ \pi = \begin{cases} \sigma\pi & \sigma \in A_n \\ \sigma\tau\pi\tau & \sigma \notin A_n \end{cases}.$$

Then

$$\sigma \circ' \pi = \begin{cases} \pi\sigma & \sigma \in A_n \\ \tau\pi\tau\sigma & \sigma \notin A_n \end{cases}.$$

Outline

1. Solving the Yang-Baxter Equation

Braces were developed to provide set-theoretic solutions to the Yang-Baxter Equation.

A *set-theoretic solution* to the YBE is a set B together with a function $r : B \times B \to B \times B$ such that

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}$$

where $r_{ij} : B \times B \times B \to B \times B \times B$ is obtained by applying r to the i^{th} and j^{th} factors, $i < j$.

A simple example: let B be any set, $r(x, y) = (y, x)$.

Then

$$r_{12}r_{23}r_{12}(x, y, z) = (z, y, x) = r_{23}r_{12}r_{23}(x, y, z).$$

and the YBE holds.

A slightly more interesting example.

Let B be a group, and let $r(x, y) = (y, y^{-1}xy)$.

Then:

$$\begin{aligned}
r_{12}r_{23}r_{12}(x, y, z) &= r_{12}r_{23}(y, y^{-1}xy, z) \\
&= r_{12}(y, z, z^{-1}y^{-1}xyz) \\
&= (z, z^{-1}yz, (yz)^{-1}x(yz)) \\
r_{23}r_{12}r_{23}(x, y, z) &= r_{23}r_{12}(x, z, z^{-1}yz) \\
&= r_{23}(z, z^{-1}xz, z^{-1}yz) \\
&= (z, z^{-1}yz, z^{-1}y^{-1}zz^{-1}xzz^{-1}yz) \\
&= (z, z^{-1}yz, (yz)^{-1}x(yz)).
\end{aligned}$$

Why (skew left) braces matter

Let $\mathfrak{B}$ be a brace.

Then

$$r(x,y) = (x^{-1}(x\circ y), \overline{x^{-1}(x\circ y)} \circ x \circ y)$$

is a (non-degenerate) set-theoretic solution to YBE.

Example (Trivial Brace)

Let $\mathfrak{B} = (B, \cdot, \cdot)$. Then $r(x,y) = (y, y^{-1}xy)$, as above.

$r(x, y) = (x^{-1}(x \circ y), \overline{x^{-1}(x \circ y)} \circ x \circ y)$

Example (Type D_4, Q_8)

Let $(B, \cdot) \cong D_4$,

$$x \circ y = \begin{cases} xy & x \in \langle\sigma\rangle \text{ or } y \in \langle\sigma\rangle \\ \sigma^2 xy & x, y \notin \langle\sigma\rangle \end{cases} .$$

Then

$$r(x, y) = \begin{cases} (y, y^{-1}xy) & x \in \langle\sigma\rangle \text{ or } y \in \langle\sigma\rangle \\ (\sigma^2 y, \sigma^2 y^{-1}xy) & x, y \notin \langle\sigma\rangle \end{cases} .$$

Using opposites

Proposition

If $\mathfrak{B} = (B, \cdot, \circ)$ *is a brace, then*

$$r(x,y) = (x^{-1}(x \circ y), \overline{x^{-1}(x \circ y)} \circ x \circ y)$$

$$r'(x,y) = (x^{-1}(x \circ' y), \left(\overline{(x^{-1}(x \circ' y))^{-1}}\right)^{-1} \circ' x \circ' y)$$

are set-theoretic solutions to the Yang-Baxter equation.

Note that since $x \circ' y = x(x^{-1} \circ y)x$,

$$r'(x,y) = \left(w, \left(\overline{w^{-1}}\right)^{-1} \left(\overline{w^{-1}} \circ xw\right) \left(\overline{w^{-1}}\right)^{-1}\right)$$

where $w = (x^{-1} \circ y)x$.

Example: type D_4, Q_8

Let $(B,\cdot) = \{\langle \sigma, \tau \rangle : \sigma^4 = \tau^2 = \sigma\tau\sigma\tau = e\} \cong D_4$ and

$$x \circ y = \begin{cases} xy & x \in \langle \sigma \rangle \text{ or } y \in \langle \sigma \rangle \\ \sigma^2 xy & x, y \notin \langle \sigma \rangle \end{cases},$$

$$x \circ' y = \begin{cases} yx & x \in \langle \sigma \rangle \text{ or } y \in \langle \sigma \rangle \\ \sigma^2 yx & x, y \notin \langle \sigma \rangle \end{cases}.$$

Then

$$r(x,y) = \begin{cases} (y, y^{-1}xy) & x \in \langle \sigma \rangle \text{ or } y \in \langle \sigma \rangle \\ (\sigma^2 y, \sigma^2 y^{-1} xy) & x, y \notin \langle \sigma \rangle \end{cases},$$

$$r'(x,y) = \begin{cases} (x^{-1}yx, x) & x \in \langle \sigma \rangle \text{ or } y \in \langle \sigma \rangle \\ (\sigma^2 x^{-1} yx, \sigma^2 x) & x, y \notin \langle \sigma \rangle \end{cases}.$$

2. The Hopf-Galois correspondence

Suppose we have a Hopf Galois structure on a Galois extension L/K, consisting of a K-Hopf algebra H and an action of H on L satisfying certain properties.

Then some, not necessarily all, intermediate fields can be found by considering the “fixed fields" of the action of H restricted to a sub-Hopf algebra.

Let $\mathfrak{B} = (B, \cdot, \circ)$ be the corresponding brace.

Recently, Childs has established a connection between the intermediate fields found above with “$\circ$-stable subgroups" of $(B, \cdot)$.

A subgroup $C \leq (B, \cdot)$ is $\circ$-*stable* if $(x \circ c)x^{-1} \in C$ for all $x \in B, c \in C$.

Additionally, Bachiller defines a *left ideal* of $\mathfrak{B}$ to be a subgroup $C \leq (B, \cdot)$ such that $x^{-1}(x \circ c) \in C$ for all $x \in B, c \in C$.

These are opposite substructures.

$\circ'$-stable: $(x \circ' c)x^{-1} \in C$; left ideal: $x^{-1}(x \circ c) \in C$

Proposition

$C \le (B, \cdot)$ is a left ideal of $\mathfrak{B}$ if and only if C is $\circ'$-stable.

Proof. (sketch)

$$\begin{aligned}(x \circ' c)x^{-1} &= \left(x(x^{-1} \circ c)x\right) x^{-1} \\ &= x(x^{-1} \circ c),\end{aligned}$$

So $(x \circ' c)x^{-1} \in C$ iff $(x^{-1})^{-1}(x^{-1} \circ c) \in C$ for all $x \in B, c \in C$.

Thus, the intermediate fields corresponding to $N \le \mathrm{Perm}(G)$ can be identified using the left ideals of the opposite brace.

Outline

Let $B = \mathrm{GL}_3(\mathbb{F}_2)$, and let

$$H = \left\{ A \in \mathrm{GL}_3(\mathbb{F}_2) : A \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right\}, \; C = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \; K = \langle C \rangle.$$

Then every $X \in GL_3(\mathbb{F}_2)$ factors uniquely into AC^i for $A \in H$, $0 \leq i \leq 6$.

Define

$$(A_1 C^i) \circ (A_2 C^j) = A_1 A_2 C^{i+j}, \; A_1, A_2 \in H.$$

Then $(B, \circ) \cong H \times K \cong S_4 \times C_7$ and $\mathfrak{B} = (B, \cdot, \circ)$ is a brace.

In all previous brace examples, $\left(\overline{x^{-1}}\right)^{-1} = \overline{x}$, that is, the inverses under $\circ$ and $\circ'$ coincide.

Here, let

$$X = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Then

$$\overline{X} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \left(\overline{X^{-1}}\right)^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

$(A_1 C^i) \circ (A_2 C^j) = A_1 A_2 C^{i+j}$

Let

$$X = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \; Y = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Then

$$r(X, Y) = \left(\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \right)$$

$$r'(X, Y) = \left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \right)$$

In all previous brace examples, $r'(x, y) = TrT(x, y)$, where $T : B \times B \to B \times B$ is the twist map, but...

$(A_1 C^i) \circ (A_2 C^j) = A_1 A_2 C^{i+j}$

$$r(X, Y) = \left(\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \right)$$

$$r'(X, Y) = \left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \right)$$

$$TrT(x, y) = \left(\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \right)$$

...shows this is not true in general.

Outline

$r' \neq TrT$

Question. If one is given the value of $r(x, y)$ for some x, y, is $r'(x, y)$ easy to deduce without looking at the corresponding brace?

Isomorphism?

Let $\mathfrak{B} = (B, \cdot, \circ)$. If $(B, \cdot)$ is abelian, then $x \mapsto x^{-1} : \mathfrak{B} \to \mathfrak{B}'$ is an isomorphism of braces.

Question. Can $\mathfrak{B} \cong \mathfrak{B}'$ if $(B, \cdot)$ nonabelian? (We conjecture "no".)

Proposition (Goodnight-Stordy). If there exist $x, y \in B$ with $xy \neq yx$ and either $x \circ y = xy$ or $x \circ y = yx$ then $\mathfrak{B} \not\cong \mathfrak{B}'$.

The $x \circ y = xy$ or yx property appears in each of our examples:

Trivial Brace: $x \circ y = xy$

Type D_4, Q_8 : $x \circ y = \begin{cases} xy & x \in \langle\sigma\rangle \text{ or } y \in \langle\sigma\rangle \\ \sigma^2 xy & x, y \notin \langle\sigma\rangle \end{cases}$

Type S_n, S_n : $\sigma \circ \pi = \begin{cases} \sigma\pi & \sigma \in A_n \\ \sigma\tau\pi\tau & \sigma \notin A_n \end{cases}$

Type $\mathrm{GL}_3(\mathbb{F}_2), (S_4 \times C_7)$: $(A_1 C^i) \circ (A_2 C^j) = A_1 A_2 C^{i+j}$.

Thank you.