Opposite braces and their applications

Alan Koch

Agnes Scott College

May 28, 2019

Joint work with:

Pa Tru

Outline

Yang-Baxter Equation

A *set-theoretic solution* to the Yang-Baxter equation is a set B and a function $R : B \times B \to B \times B$ such that

$$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23}$$

holds, where $R_{ij} : B \times B \times B \to B \times B \times B$ is R applied to the i^{th} and j^{th} factors.

Example

Let B be any set, and $R(x,y) = (y,x),\ x,y \in B$.

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

$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23}$

Example

Let B be any group, $R(x,y) = (y, y^{-1}xy)$.

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

Note that if B is abelian, then this is the previous example.

$R^{(1)}(x,y)=(y,x),\ R^{(2)}(x,y)=(y,y^{-1}xy)$

Let R be a solution to the YBE, and write

$$R(x,y)=(\sigma_x(y),\sigma_y(x)).$$

We say R is:

- *non-degenerate* if $\sigma_x,\sigma_y : B\to B$ are bijections.
- *involutive* if $R^2=1_B$.

Both examples above are non-degenerate, $R^{(1)}$ is involutive, but

$$R^{(2)}(R^{(2)}(x,y))=R^{(2)}(y,y^{-1}xy)=(y^{-1}xy,y^{-1}x^{-1}yxy),$$

so $R^{(2)}$ is not involutive unless B is abelian.

(Skew left) braces

Skew left braces can be used to construct non-degenerate solutions to the YBE.

A *skew left brace* is a triple $\mathfrak{B} = (B, \cdot, \circ)$ where

- $(B, \cdot)$ is a group: the inverse to x is x^{-1} and we write $x \cdot y$ as xy unless it creates confusion.
- $(B, \circ)$ is a group: the inverse to x is $\overline{x}$.
- For all $x, y, z \in B$ the following identity holds, which we call the *brace relation*:

$$x \circ (yz) = (x \circ y)x^{-1}(x \circ z).$$

In this talk, we will abbreviate “skew left brace” with “brace”.

Fact. The groups $(B, \cdot)$ and $(B, \circ)$ share the same identity 1_B.

Notation, notation

There does not yet appear to be a uniform notation:

- Guarnieri and Vendramin, 2016 (arXiv): $(B, \cdot, \circ)$.
- Bachiller, 2016 (arXiv): $(B, \star, \cdot)$.
- Childs, 2017 (NYJM): $(G, \cdot, \circ)$.
- Smoktunowicz, Vendramin, and Byott, 2017 (arXiv): $(A, \cdot, \circ)$.
- Zenouz, 2018 (arXiv): $(B, \oplus, \odot)$.
- Vendramin, 2018 (arXiv): $(B, +, \circ)$.
- Konovalov, Smoktunowicz, and Vendramin, 2018 (arXiv): $(A, \circ, +)$, which puts the operations in reverse order.
- Childs, 2019 (arXiv): $(G, \circ, \star)$ order of the operations irrelevant (bi-skew braces–coming tomorrow!).

Some examples:

- $(B, \cdot)$ any group, $x \circ y = xy$. We call this "the" *trivial brace*.
- $(B, \cdot)$ any group, $x \circ y = yx$. We call this "the" *almost trivial brace*.
- $(B, \cdot) = S_n,\ n \geq 4,\ \tau \in A_n,\ \tau^2 = 1$, and

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

  Note $(B, \circ) \cong S_n$.
- $(B, \cdot) = \langle r, s : r^4 = s^2 = rsrs = 1 \rangle \cong D_4$ with

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

  Note $(B, \circ) \cong Q_8$.

Connection to the Yang-Baxter Equation

A brace $\mathfrak{B} = (B, \cdot, \circ)$ gives a non-degenerate set-theoretic solution to the YBE: for $x, y \in B$,

$$R_{\mathfrak{B}}(x, y) = \left(x^{-1}(x \circ y), \overline{x^{-1}(x \circ y)} \circ x \circ y\right).$$

Exercise: $R_{\mathfrak{B}}$ is involutive iff $(B, \cdot)$ is abelian.

Example (trivial brace)

$$R_{\mathfrak{B}}(x, y) = (y, y^{-1}xy).$$

Example (almost trivial brace)

$$R_{\mathfrak{B}}(x, y) = (x^{-1}yx, y).$$

Connection with Hopf-Galois theory

Hopf-Galois structures on Galois field extensions give braces, and conversely.

Let $(G, *_G)$ be the Galois group of an extension L/K, let $N \leq \mathrm{Perm}(G)$ be regular and G-stable (i.e., normalized by conjugation by $\lambda(G) \leq \mathrm{Perm}(G)$).

Let $a : N \to G$ be the bijection given by $a(\eta) = \eta[1_G]$.

Define, for $\eta, \pi \in N$,

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

Set $B = N$. Then $\mathfrak{B} := (B, \cdot, \circ)$ is a brace with $(B, \cdot) = N$, and $(B, \circ) \cong (G, *_G)$ via the isomorphism a.

Alternatively

Given $(G, *_G), (N, *_N)$ as above, let $(B, \circ) = (G, *_G)$ and define

$$g \cdot h = a(a^{-1}(g) *_N a^{-1}(h)).$$

Then $\mathfrak{B}_{\text{alt}} := (B, \cdot, \circ)$ is a brace with $(B, \circ) = (G, *_G)$, and $(B, \cdot) \cong (N, *_N)$ via the isomorphism a^{-1}.

In fact, the map $a : \mathfrak{B} \to \mathfrak{B}_{\text{alt}}$ is a brace isomorphism (bijection, preserves both operations).

HGS give braces

The correspondence

$$\{\text{Hopf-Galois structures on } L/K\} \to \{\text{Braces } (B,\cdot,\circ) \text{ with } (B,\circ)\cong G\}$$

is surjective but not injective.

Given a regular, G-stable subgroup $N \leq \mathrm{Perm}(G)$, denote its corresponding brace by $\mathfrak{B}(N)$.

Outline

Motivation

Let L/K be Galois, group G.

Let $N \leq \text{Perm}(G)$ be regular and G-stable.

Then N induces a Hopf-Galois structure on L/K.

Additionally, let

$$N' = \text{Cent}_{\text{Perm}(G)}(N) = \{\eta' \in \text{Perm}(G) : \eta'\eta = \eta\eta' \text{ for all } \eta \in N\}.$$

Then $N' \cong N$ is regular and G-stable, giving a HGS on L/K, different from the HGS that N gives if N is nonabelian.

Question. How do $\mathfrak{B}(N)$ and $\mathfrak{B}(N')$ compare?

Comparing braces

Recall [Greither-Pareigis]: $N' = \{\phi_\eta : \eta \in N\}$, where $\eta[g] = \mu_g[\eta[1_G]]$ and $\mu_g \in N$ is uniquely determined by $\mu_g[1] = g$.

Also, $\phi_\eta \phi_\pi = \phi_{\pi\eta}$, and the map: $\eta \mapsto \phi_{\eta^{-1}} : N \to N'$ is an isomorphism.

Let $a' : N' \to G$ be the bijection $\phi_\eta \mapsto \phi_\eta[1_G]$. Then

$$a'(\phi_\eta) = \phi_\eta[1_G] = \mu_1[\eta[1_G]] = \eta[1_G] = a(\eta).$$

$a'(\phi_\eta) = a(\eta)$

Then

$$\begin{aligned}\phi_\eta \circ' \phi_\pi &:= (a')^{-1}\left(a'(\phi_\eta) *_G a'(\phi_\pi)\right) \\ &= (a')^{-1}(a(\eta) *_G a(\pi)) \\ &= (a')^{-1}(a(\eta \circ \pi)) \\ &= \phi_{\eta\circ\pi}.\end{aligned}$$

Then $\mathfrak{B}(N') = (N', \cdot_{N'}, \circ')$.

By identifying N' with N via the bijection $\phi_\eta \mapsto \eta$, we see that $\mathfrak{B}(N') \cong (N, \cdot', \circ)$ where

$$\eta \cdot' \pi = \pi\eta.$$

The opposite brace

Let $\mathfrak{B} = (B, \cdot, \circ)$ be any brace, and let

$$x \cdot' y = yx.$$

Then $\mathfrak{B}' := (B, \cdot', \circ)$ is called the *opposite brace* to $\mathfrak{B}$.

Note: it is easy to show that the brace relation holds on $\mathfrak{B}'$.

Historical note

In March, 2019 I gave a different definition for $\mathfrak{B}'$, call it $\mathfrak{B}^*$.

$\mathfrak{B}^* = (B, \cdot, \circ')$ where

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

One can show that the map $B \to B$ given by $x \mapsto x^{-1}$ is an isomorphism of braces $\mathfrak{B}^* \to \mathfrak{B}'$.

The May opposite is an easier reformulation of the March opposite.

Some properties

- $(\mathfrak{B}')' \cong \mathfrak{B}$.
- If $(B, \cdot)$ is abelian, $\mathfrak{B}' \cong \mathfrak{B}$.
- $(B, \cdot')$ has the same identity and inverses as $(B, \cdot)$.
- If $\phi : \mathfrak{B}_1 \to \mathfrak{B}_2$ is a morphism of braces, then it is also a morphism $\mathfrak{B}_1' \to \mathfrak{B}_2'$ of opposite braces since

$$\phi(x \cdot' y) = \phi(yx) = \phi(y)\phi(x) = \phi(x) \cdot' \phi(y).$$

A simple example

Suppose $\mathfrak{B} = (B, \cdot, \cdot)$ is the trivial brace.

Then $\mathfrak{B}' = (B, \cdot', \cdot)$ is isomorphic to the almost trivial brace $(B, \cdot, \cdot')$ by the inverse map $\iota : (B, \cdot, \cdot') \to (B, \cdot', \cdot),\ \iota(x) = x^{-1}$:

$$\iota(x \cdot y) = (x \cdot y)^{-1} = y^{-1} \cdot x^{-1} = \iota(x) \cdot' \iota(y)$$
$$\iota(x \circ y) = \iota(y \cdot x) = (y \cdot x)^{-1} = x^{-1} \cdot y^{-1} = \iota(x) \circ \iota(y).$$

Note. The regular subgroups of $\mathrm{Perm}(G)$ which produce $\mathfrak{B}$ and $\mathfrak{B}'$ are $\lambda(G)$ and $\rho(G)$ respectively.

Outline

Application #1: Back to YBE

If $\mathfrak{B}' \not\cong \mathfrak{B}$, a brace now gives two set-theoretic solutions to the YBE:

$$\begin{aligned} R_{\mathfrak{B}}(x,y) &= \left(x^{-1}(x\circ y), \overline{x^{-1}(x\circ y)}\circ x\circ y\right) \\ R_{\mathfrak{B}'}(x,y) &= \left(x^{-1}\cdot' (x\circ y), \overline{x^{-1}\cdot' (x\circ y)}\circ x\circ y\right) \\ &= \left((x\circ y)x^{-1}, \overline{(x\circ y)x^{-1}}\circ x\circ y\right). \end{aligned}$$

Example

Let $\mathfrak{B}$ be the trivial brace.
Then:

$$R_{\mathfrak{B}}(x,y) = (y, y^{-1}xy)$$
$$R_{\mathfrak{B}'}(x,y) = (xyx^{-1}, x).$$

Note. In this example, $R_{\mathfrak{B}}^{-1} = R_{\mathfrak{B}'}$.

Example

$(B,\cdot) = \langle r, s : r^4 = s^2 = rsrs = 1\rangle \cong D_4$ with

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

Then:

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

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

Remark. It takes more work, but it can be shown that $R_{\mathfrak{B}}^{-1} = R_{\mathfrak{B}'}$.

But...

Recall $(B, \cdot) = S_n,\ n \geq 4,\ \tau \in A_n,\ \tau^2 = 1$, and

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

Suppose $\tau = (12)(34)$. Then

$$R_{\mathfrak{B}'} R_{\mathfrak{B}}((12),(123)) = R_{\mathfrak{B}'}((142),(24)) = ((24),(132))$$

So $R_{\mathfrak{B}}^{-1} \neq R_{\mathfrak{B}'}$ in general.

Application #2: Back to HGS

Let L/K be Galois, group G, and suppose H is a Hopf algebra which acts on L such that L/K is a Hopf-Galois extension.

Then each sub-Hopf algebra of H corresponds to an intermediate field of L/K.

This assignment is injective, but not necessarily surjective [Greither-Pareigis].

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

Last year, in Omaha, Lindsay discussed the image of this correspondence using "$\circ$-stable subgroups" of the $\mathfrak{B}$.

$\circ$-stable subgroups: What Lindsay did

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

$$(x \circ c)x^{-1} \in C.$$

A $\circ$-stable subgroup C of $(B, \cdot)$ is also a subgroup of $(B, \circ)$, so $(C, \cdot, \circ)$ is a sub-brace of $\mathfrak{B}$.

Sub-Hopf algebras, hence the intermediate fields obtained via H, are in 1-1 correspondence with $\circ$-stable subgroups.

Left ideals: What Bachiller did

A subgroup $D \leq (B, \cdot)$ is a *left ideal* if, for all $d \in D, x \in B$,

$$x^{-1}(x \circ d) \in D.$$

A left ideal is also a subgroup of $(B, \circ)$, hence a sub-brace.

People seem to care about these–for example, there's a "YangBaxter" GAP package with commands such as LeftIdeals, which computes all of the left ideals of a given brace.

Clearly:

Proposition

C is a $\circ$-stable subgroup in $\mathfrak{B}$ iff it is a left ideal in $\mathfrak{B}'$.

Wild idea.
If we were to re-define the brace corresponding to $(N, *_N) \leq \text{Perm}(G)$ to have dot operation

$$\eta \cdot \pi = \pi *_N \eta$$

and the circle operation as before, then the left ideals would give the intermediate fields directly.

Outline

Abelian case

We say $\mathfrak{B} = (B, \cdot, \circ)$ is *abelian* if $(B, \cdot)$ is abelian. (Called a "left brace" in the literature.)

If $\mathfrak{B}$ is abelian, then the identity map is an isomorphism $(B, \cdot) \to (B, \cdot')$ which respects $\circ$.

Hence $\mathfrak{B}' \cong \mathfrak{B}$.

More generally (i.e., $\mathfrak{B}$ not necessarily abelian), whenever $\mathfrak{B}' \cong \mathfrak{B}$ we say $\mathfrak{B}$ is *self-opposite*.

If $\mathfrak{B}$ is self-opposite:

1. Only one solution to YBE.
2. Intermediate fields found using left ideals.

Question. Are there non-abelian self-opposite braces?

Yes.

Let $(G, \cdot)$ be any group.

Let $B = G \times G$ and define

$$(x_1, x_2) \circ (y_1, y_2) = (x_1 y_1, y_2 x_2).$$

It is easy to show $(B, \cdot, \circ)$ is a brace and that

$$T : B \to B, \ T(x_1, x_2) = (x_2, x_1)$$

is a brace isomorphism $\mathfrak{B}' \to \mathfrak{B}$.

More generally, for any brace $\mathfrak{B}$ we have

$$(\mathfrak{B} \times \mathfrak{B}')' \cong \mathfrak{B}' \times \mathfrak{B} \cong \mathfrak{B} \times \mathfrak{B}'.$$

When is $\mathfrak{B}$ self-opposite?

One strategy: compute $\text{Aut}(B, \circ)$, and for each $\varphi \in \text{Aut}(B, \circ)$ determine whether $\varphi(xy) = \varphi(y)\varphi(x)$.

Example

For $n \geq 4,\ n \neq 6$, let $\mathfrak{B} = (B, \cdot, \circ)$ with $(B, \cdot) = S_n$ and

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

All automorphisms of $(B, \circ) \cong S_n$ are inner. Let $\varphi(\sigma) = \gamma\sigma\gamma^{-1},\ \gamma \in S_n$. Then

$$\begin{aligned} \varphi((123) \cdot (12)) &= \varphi((13)) = \gamma(13)\gamma^{-1} \\ \varphi((123)) \cdot' \varphi((12)) &= (\gamma(12)\gamma^{-1}) \cdot' (\gamma(123)\gamma^{-1}) \\ &= (\gamma(123)\gamma^{-1}) \cdot (\gamma(12)\gamma^{-1}) = \gamma(23)\gamma^{-1}, \end{aligned}$$

so φ is not an isomorphism $\mathfrak{B} \to \mathfrak{B}'$ and $\mathfrak{B}$ is not self-opposite.

Self opposite investigation: L-pairs and R-pairs

We say $(x, y) \in B \times B$ is an *L-pair* of $\mathfrak{B}$ if $x \circ y = xy$, equivalently, y is fixed by the bijection $\mathcal{L}_x$ given by

$$\mathcal{L}_x(y) = x^{-1}(x \circ y).$$

Similarly, if $x \circ y = yx$ we call (x, y) an R-pair of $\mathfrak{B}$.

Clearly, an L-pair of $\mathfrak{B}$ is an R-pair of $\mathfrak{B}'$ and vice versa.

Thus, if $\mathfrak{B}$ is self-opposite, $|\mathcal{L}| = |\mathcal{R}|$.

An example

As before, let $(B,\cdot) = \langle r, s : r^4 = s^2 = rsrs = 1\rangle \cong D_4$ with

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

Then $|\mathcal{L}| = 48$ (trivial computation).

What is $|\mathcal{R}|$?

- $r^i \circ r^j = r^{i+j} = r^j r^i$ for all i, j: 16 pairs
- $r^i \circ r^j s = r^{i+j} s = r^j s r^i$ iff i is even: 8 pairs
- $r^i s \circ r^j = r^{i-j} s = r^j r^i s$ iff j is even: 8 pairs
- $r^i s \circ r^j s = r^{2+i-j} = r^j s r^i s$ iff $i \not\equiv j \pmod 2$: 8 pairs.

So $|\mathcal{R}| = 40$ and $\mathfrak{B}$ is not self-opposite.

Outline

$n-1$ Questions

1. Is there an elegant way to relate $R_{\mathfrak{B}}$ and $R_{\mathfrak{B}'}$?
   Elegant: Given $R_{\mathfrak{B}}(x,y) = (u,v)$, a nice formula to $R_{\mathfrak{B}'}(x,y)$ in terms of u and v.
   (Failed conjecture: $R_{\mathfrak{B}'} = TR_{\mathfrak{B}}T,\ T(x,y) = (y,x)$.)
   Best I have right now: $R_{\mathfrak{B}'}(x,y) = (u \circ v)x^{-1}, \overline{(u \circ v)x^{-1}} \circ u \circ v)$.
2. Can we develop "nice" necessary and sufficient conditions to determine whether $\mathfrak{B}$ is self-opposite?
3. Do Hopf Galois structures which correspond to self-opposite braces have interesting properties?
   (For example: if $\mathfrak{B}$ is self-opposite, intermediate fields correspond to left ideals.)
4. Is there any value to the "classic" definition of opposite, $\mathfrak{B}^*$?
   Philosophically:

$$\mathfrak{B}, \mathfrak{B}': \text{ fix } G, \text{ vary } N.$$
$$\mathfrak{B}, \mathfrak{B}^*: \text{ fix } N, \text{ vary } G.$$

Last question

5. The construction of $\mathfrak{B}'$ was motivated to understand the opposite HGS given by N'–specifically, the Hopf algebra structure of $L[N']^G$. What insight does $\mathfrak{B}'$ give us?

We'll talk about this again on Thursday.

Thank you.