Skew left braces and the Yang-Baxter equation

Lindsay N. Childs
University at Albany
Albany, NY 12222

June 1, 2022

What the talk is about

In this expository talk I want to describe how a skew left brace yields a solution of the Yang-Baxter equation.
A skew (left) brace is a set $B = (B, \circ, \cdot)$ with two group operations that satisfy the single compatibility condition

$$(\#) \quad a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c)$$

If $(B, \cdot)$ is abelian then a skew brace is called a brace. The inverse of a in $(B, \circ)$ is denoted $\overline{a}$ and in $(B, \cdot)$ by a^{-1}. One easily checks from (#) that the two groups $(B, \circ)$ and $(B, \cdot)$ share a common identity element, 1.

The YBE

Braces were first defined by W. Rump [Ru07] to yield set-theoretic solutions of the Yang-Baxter equation. The latter has been a question of considerable interest among algebraists since 1990 (Drin'feld's ICM talk).
Skew left braces were defined by Guarneri and Vendramin [GV17] to yield more general solutions of the YBE, and the appendix by Byott and Vendramin in [SV18] quantified the relationship between skew braces and Hopf-Galois structures.
So classifying Hopf Galois structures relates to classifying solutions of the YBE.

[Om21]

[Om21] = L. Childs, C. Greither, K. Keating, A. Koch, T. Kohl, P. Truman, R. Underwood, Hopf Algebras and Galois Module Theory, AMS Math. Surveys and Monographs 260 (November, 2021).

Skew braces show up in five of the 15 chapters. But Yang-Baxter equations were barely noted in [Om21], and in fact, the term "Yang-Baxter equation" was omitted from the index of [Om21]. (For the record, "Yang-Baxter equation" appears on pages 4 and 14 of [Om21].)

Given the original motivation for braces, an appendix to the book showing how a skew brace yields a solution to the YBE would have been nice. "Better late than never:" these slides will be posted on Paul's website.

So I looked at some of the published solutions...

... and got frustrated.

Why so?

Published solutions

Solutions of the YBE have been described in various settings for over 20 years (e. g. J. Lu, M. Yan, Y. Zhu [LYZ03], Rump [Ru07], F. Cedo, E. Jespers, J. Okninski [CJO14]).

When I looked for proofs on how a skew left brace yields a solution to the YBE, I found Guarnieri and Vendramin [GV17], the paper that first defined skew left braces, and Bachiller [Ba18]. (Smoktunowicz and Vendramin [SV18] simply refers back to [GV17].) But those papers, like the earlier ones, were notationally challenging, and most were not self-contained, but instead referred to previously defined concepts and results for part of their discussion.

So what to do?

So I decided to try to construct a self-contained proof I could understand.

This talk is the result of that effort.

The maps σ and τ

To start, given a skew brace $B = (B, \circ, \cdot)$, following [GV17], define $\sigma_a : B \to B$ by

$$\sigma_a(b) = a^{-1}(a \circ b).$$

($\sigma_a(b)$ is often denoted by $\lambda_a(b)$ or $\gamma_a(b)$ in the skew brace literature). Define

$$\tau_b(a) = \overline{\sigma_a(b)} \circ a \circ b.$$

In other words, $\tau_b(a)$ is defined to be the function so that $\sigma_a(b) \circ \tau_b(a) = a \circ b$. ([GV17] defines $\tau_b(a)$ much differently, but eventually shows that it coincides with our definition.)

Solving the YBE

A solution in the skew brace B of the Yang-Baxter equation is a function $R : B \times B \to B \times B$ that satisfies: for all a, b, c in B,

$$(**): \quad (R \times id)(id \times R)(R \times id)(a, b, c) = (id \times R)(R \times id)(id \times R)(a, b, c).$$

We consider the function $R : B \times B \to B \times B$ defined by

$$R(a, b) = (\sigma_a(b), \tau_b(a))$$

with $\sigma_a(b) = a^{-1}(a \circ b)$ and $\tau_b(a) = \overline{\sigma_a(b)} \circ a \circ b$. The choice of τ implies that the proposed solution has the essential property that for all a, b in B, if $R(a, b) = (s, t)$, then

$$s \circ t = \sigma_a(b) \circ \tau_b(a) = a \circ b.$$

The Theorem

We prove:

Theorem

If B is a skew left brace and $R : B \times B \to B \times B$ is defined by $R(a,b) = (\sigma_a(b), \tau_b(a))$ for a, b in B, then R is a solution of the YBE: that is,

$$(**): \quad (R\times id)(id\times R)(R\times id)(a,b,c) = (id\times R)(R\times id)(id\times R)(a,b,c).$$

The left side

$$(**): \quad (R\times id)(id\times R)(R\times id)(a,b,c) = (id\times R)(R\times id)(id\times R)(a,b,c).$$

The left side of (**) is:

$$\begin{aligned}
&(R\times id)(id\times R)(R\times id)(a,b,c)\\
&\qquad = (R\times id)(id\times R)(\sigma_a(b),\tau_b(a),c)\\
&\qquad = (R\times id)(id\times R)(d,e,c)\\
&\qquad = (R\times id)(d,\sigma_e(c),\tau_c(e))\\
&\qquad = (R\times id)(d,f,g)\\
&\qquad = (\sigma_d(f),\tau_f(d),g)\\
&\qquad = (h,k,g)
\end{aligned}$$

where $d=\sigma_a(b), e=\tau_b(a); f=\sigma_e(c), g=\tau_c(e); h=\sigma_d(f), k=\tau_f(d)$.

The right side

$$(**): \quad (R\times id)(id\times R)(R\times id)(a,b,c) = (id\times R)(R\times id)(id\times R)(a,b,c).$$

Similarly, the right side of (**) is:

$$\begin{aligned}
&(1\times R)(R\times 1)(1\times R)(a,b,c)\\
&\qquad = (1\times R)(R\times 1)(a,\sigma_b(c),\tau_c(b))\\
&\qquad = (1\times R)(R\times 1)(a,q,r)\\
&\qquad = (1\times R)(\sigma_a(q),\tau_q(a),r)\\
&\qquad = (1\times R)(s,t,r)\\
&\qquad = (s,\sigma_t(r),\tau_r(t))\\
&\qquad = (s,v,w).
\end{aligned}$$

where $q=\sigma_b(c), r=\tau_c(b); s=\sigma_a(q), t=\tau_q(a); v=\sigma_t(r), w=\tau_r(t)$.

To recapitulate: show $(h, k, g) = (s, v, w)$

We want to show that $(h, k, g) = (s, v, w)$ where $d = \sigma_a(b), e = \tau_b(a); f = \sigma_e(c), g = \tau_c(e); h = \sigma_d(f), k = \tau_f(d)$, $q = \sigma_b(c), r = \tau_c(b); s = \sigma_a(q), t = \tau_q(a); v = \sigma_t(r), w = \tau_r(t)$, all connected by the fact that

$$\sigma_x(y) \circ \tau_y(x) = x \circ y :$$

$$b \circ c = \sigma_b(c) \circ \tau_c(b) = q \circ r,$$
$$a \circ q = \sigma_a(q) \circ \tau_q(a) = s \circ t,$$
$$t \circ r = \sigma_t(r) \circ \tau_r(t) = v \circ w$$
$$a \circ b = \sigma_a(b) \circ \tau_b(a) = d \circ e,$$
$$a \circ q = \sigma_a(q) \circ \tau_q(a) = s \circ t,$$
$$t \circ r = \sigma_t(r) \circ \tau_r(t) = v \circ w;$$

To show $(h, k, g) = (s, v, w)$: $h = s$

To try to show that $h = s$, we have:

$$s = \sigma_a(q) = \sigma_a(\sigma_b(c)) \text{ and } h = \sigma_d(f) = \sigma_d(\sigma_e(c)).$$

Suppose we know that σ is a homomorphism from $(B, \circ)$ to $\mathrm{Perm}(B)$: that is,

$$\sigma_x(\sigma_y(z)) = \sigma_{x \circ y}(z),$$

Then

$$h = \sigma_d(\sigma_e(c)) = \sigma_{d \circ e}(c),$$

and

$$s = \sigma_a(q) = \sigma_a(\sigma_b(c)) = \sigma_{a \circ b}(c).$$

Since $\sigma_a(b) = d$ and $\tau_b(a) = e$, it follows that

$$d \circ e = \sigma_a(b) \circ \tau_b(a) = a \circ b,$$

and so

$$h = \sigma_{d \circ e}(c) = \sigma_{a \circ b}(c) = s.$$

Done!

So we need...

So for the left-most components of the YB equation to be =, it suffices that

$$\sigma_x(\sigma_y(z)) = \sigma_{x\circ y}(z).$$

for all x, y, z in B.

To show $(h, k, g) = (s, v, w)$: $w = g$

The right side goes the same way. To show that $w = g$, we have

$$g = \tau_c(e) = \tau_c(\tau_b(a)) \text{ and } w = \tau_r(t) = \tau_r(\tau_q(a))$$

If we know that $\tau_y(\tau_z(x)) = \tau_{z\circ y}(x)$, that is, τ is an anti-homomorphism on $(B, \circ)$, then

$$g = \tau_c(\tau_b(a)) = \tau_{b\circ c}(a),$$

$$w = \tau_r(\tau_q(a)) = \tau_{q\circ r}(a),$$

and

$$q \circ r = \sigma_b(c) \circ \tau_c(b) = b \circ c.$$

So

$$w = \tau_{q\circ r}(a) = \tau_{b\circ c}(a) = g.$$

So we need...

So for the right-most components of the YB equation to be =, it suffices that

$$\tau_z(\tau_y(x)) = \tau_{y\circ z}(x)$$

for all x, y, z in B.

To show $(h, k, g) = (s, v, w)$: $k = v$

Finally, given that $g = w$ and $h = s$, we have

$$\begin{aligned} a \circ b \circ c &= a \circ \sigma_b(c) \circ \tau_c(b) = a \circ q \circ r, \\ &= \sigma_a(q) \circ \tau_q(a) \circ r = s \circ t \circ r, \\ &= s \circ \sigma_t(r) \circ \tau_r(t) = s \circ v \circ w \end{aligned}$$

and also

$$\begin{aligned} a \circ b \circ c &= \sigma_a(b) \circ \tau_b(a) \circ c = d \circ e \circ c, \\ &= d \circ \sigma_e(c) \circ \tau_c(e) = d \circ f \circ g\ . \\ &= \sigma_d(f) \circ \tau_f(d) \circ g = h \circ k \circ g \end{aligned}$$

So $h \circ k \circ g = a \circ b \circ c = s \circ v \circ w$.
Since $h = s$ and $g = w$, we get $k = v$. Done.

The key facts needed in the proof:

We're left to prove

$$(i): \ \sigma_a(\sigma_b(c)) = \sigma_{a\circ b}(c)$$

and

$$(ii): \ \tau_k(\tau_h(g)) = \tau_{h\circ k}(g).$$

Both need the following result (c.f. [GV17], Lemma 1.7 (2)):

Lemma. For all a, b in a skew brace B,

$$a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1} = (a \circ b)^{-1}.$$

This result is proved in [GV17].

Proof that $a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1} = (a \circ b)^{-1}$

The defining equation (#) for a skew brace is that for all x, y, z in B,

$$x \circ (y \cdot z) = (x \circ y) \cdot x^{-1} \cdot (x \circ z),$$

hence

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

Set $x = a, y = b, z = b^{-1}$ to get

$$a \circ b^{-1} = a \cdot (a \circ b)^{-1}) \cdot (a \circ 1),$$

or our desired formula:

$$a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1} = (a \circ b)^{-1}.$$

For a, b, c in B, $\sigma_{a\circ b}(c) = \sigma_a(\sigma_b(c))$

Here is a proof, from Proposition 1.9 of [GV17] (5 steps):
Start with the definition of σ:

$$\sigma_a(\sigma_b(c)) = a^{-1} \cdot (a \circ \sigma_b(c))$$

Then use the definition again:

$$\sigma_a(\sigma_b(c)) = a^{-1} \cdot (a \circ (b^{-1} \cdot (b \circ c)))$$

Then use the skew brace relation (#):

$$\sigma_a(\sigma_b(c)) = a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1} \cdot (a \circ b \circ c)$$

Then apply the Lemma:

$$\sigma_a(\sigma_b(c)) = (a \circ b)^{-1} \cdot (a \circ b \circ c)$$

Then use the definition of σ on the right side:

$$\sigma_a(\sigma_b(c)) = \sigma_{a\circ b}(c).$$

Done.

A converse

We note that [GV17] proves that given a set B with two group operations, $\cdot$ and $\circ$, and $\sigma_a(b) = a^{-1} \cdot (a \circ b)$, then for all a, b, c in B,

$$\sigma_a(\sigma_b(c)) = \sigma_{a \circ b}(c)$$

if and only if the compatibility condition $(\#)$ holds, if and only if B is a skew left brace: see Proposition 1.9 of [GV17].

τ is an antihomorphism

The only thing left to do is to prove that τ is an anti-homomorphism from $(B, \circ)$ to $\mathrm{Perm}(B)$:

$$\tau_{h \circ k}(g) = \tau_k(\tau_h(g)).$$

This is a bit more complicated (13 steps).

Proof of Prop. 2: τ is an antihomomorphism on $(B, \circ)$

We begin with the definition of $\sigma_g(h)$:

$$g^{-1} \cdot (g \circ h) = \sigma_g(h)$$

Rearrange the equation:

$$\sigma_g(h))^{-1} \cdot g^{-1} = (g \circ h)^{-1}$$

Use that $\sigma_g(h) \circ \tau_h(g) = g \circ h$, to get:

$$\sigma_g(h)^{-1} \cdot g^{-1} = (\sigma_g(h) \circ \tau_h(g))^{-1}$$

Apply the Lemma formula: $(a \circ b)^{-1} = a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1})$ to the right side, to get:

$$\sigma_g(h)^{-1} \cdot g^{-1} = \sigma_g(h)^{-1} \cdot (\sigma_g(h) \circ \tau_h(g)^{-1}) \cdot \sigma_g(h)^{-1}$$

proof of Prop. 2 ctd.

We have

$$\sigma_g(h)^{-1} \cdot g^{-1} = \sigma_g(h)^{-1} \cdot (\sigma_g(h) \circ \tau_h(g)^{-1}) \cdot \sigma_g(h)^{-1},$$

Cancel $\sigma_g(h)^{-1}$ on the left:

$$g^{-1} = (\sigma_g(h) \circ \tau_h(g)^{-1}) \cdot \sigma_g(h)^{-1}$$

Multiply both sides by $\cdot(g \circ h \circ k)$:

$$g^{-1} \cdot (g \circ h \circ k) = (\sigma_g(h) \circ \tau_h(g)^{-1}) \cdot \sigma_g(h)^{-1} \cdot (g \circ h \circ k)$$

Apply the definition of σ to the left side:

$$\sigma_g(h \circ k) = (\sigma_g(h) \circ \tau_h(g)^{-1}) \cdot \sigma_g(h)^{-1} \cdot (g \circ h \circ k)$$

Use that $g \circ h = \sigma_g(h) \circ \tau_h(g)$ on the right side:

$$\sigma_g(h \circ k) = (\sigma_g(h) \circ \tau_h(g)^{-1}) \cdot \sigma_g(h)^{-1} \cdot (\sigma_g(h) \circ \tau_h(g) \circ k)$$

proof of Prop. 2 ctd.

We have

$$\sigma_g(h \circ k) = (\sigma_g(h) \circ \tau_h(g)^{-1}) \cdot \sigma_g(h)^{-1} \cdot (\sigma_g(h) \circ \tau_h(g) \circ k)$$

Apply the skew brace formula (#) (in reverse):

$$\sigma_g(h \circ k) = (\sigma_g(h) \circ (\tau_h(g)^{-1} \cdot (\tau_h(g) \circ k))$$

Use the definition of σ on the far right side:

$$\sigma_g(h \circ k) = \sigma_g(h) \circ \sigma_{\tau_h(g)}(k)$$

Take the $\circ$-inverse of both sides:

$$\overline{\sigma_g(h \circ k)} = \overline{\sigma_{\tau_h(g)}(k)} \circ \overline{\sigma_g(h)}$$

proof of Prop. 2 ctd.

We have

$$\overline{\sigma_g(h \circ k)} = \overline{\sigma_{\tau_h(g)}(k)} \circ \overline{\sigma_g(h)}$$

Multiply both sides by $\circ g \circ h \circ k$:

$$\overline{\sigma_g(h \circ k)} \circ g \circ h \circ k = \overline{\sigma_{\tau_h(g)}(k)} \circ (\overline{\sigma_g(h)} \circ g \circ h) \circ k$$

Use the definition of τ on the right side:

$$\overline{\sigma_g(h \circ k)} \circ g \circ (h \circ k) = \overline{\sigma_{\tau_h(g)}(k)} \circ \tau_h(g) \circ k$$

On both sides use the definition of τ: $\tau_b(a) = \overline{\sigma_a(b)} \circ a \circ b$:

$$\tau_{h \circ k}(g) = \tau_k(\tau_h(g))$$

So τ is an anti-homomorphism on $(B, \circ)$. Done!

Where to read the details:

See http://arxiv.org/abs/2205.07287

References

[Ba18] D. Bachiller, Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks, J. Knot Theory and its Ramifications 27 (2018).

[Ch22] L. Childs, Skew left braces and the Yang-Baxter equation, http://arxiv.org/abs/2205.07287

[CJO14] F. Cedo, E. Jespers, J. Okninski, Braces and the Yang-Baxter equation, Comm. Math. Physica 327 (2014), 101–116.

[Ge92] V. G. Drinfel'd, On some unsolved problems in quantum group theory, Lecture Notes in Math. vol 1510, Springer, Berlin, 1992, 1–6.

[GV17] L. Guarneri, L. Ventramin, Skew braces and the Yang-Baxter equation, Math. Comp 86 (2017), 2519–2534.

References

[LYZ03] J. Lu, M. Yan, Y. Zhu, On the set-theoretical Yang-Baxter equation, Duke Math. J. 104 (2000), 153–170.

[Om21] L. Childs, C. Greither, K. Keating, A. Koch, T. Kohl, P. Truman, R. G. Underwood. Hopf Algebras and Galois Module Theory, AMS Math. Surveys and Monographs 260 (2021).

[Ru07] W. Rump, Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra 307 (2007), 153–170.

[SV18] A. Smoktunowicz, L. Vendramin, On skew braces, with an appendix by N. Byott and L. Vendramin, J. Comb. Algebra 2 (2018),47–86.

Finally, I want to thank Griff Elder for these conferences. I've attended them each year for the past 11 years, one in Exeter, ten in Omaha, and they have had an enormously positive impact on my research activity in mathematics and, I suspect, on the research activity of all the regular attendees. I'm hopeful that we can look forward to these conferences in the coming years, to continue to motivate all of us.

Thank you!