Skew left braces and the Yang-Baxter equation

Lindsay N. Childs

Abstract. We give a self-contained, notation-friendly proof that a skew left brace yields a solution of the Yang-Baxter equation.

Contents

1. Introduction 649
2. The proof 650
References 654

1. Introduction

A skew left brace is a set $B = (B, \circ, \cdot)$ with two group operations that satisfy the single compatibility condition: for all $x, y, z$ in $B$,

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

The inverse of $x$ in $(B, \circ)$ is denoted $\bar{x}$ and in $(B, \cdot)$ by $x^{-1}$. One easily checks from (#) that the two groups $(B, \circ)$ and $(B, \cdot)$ share a common identity element, $1$. (Let $x = z = 1$, and $y = 1$, in (#).)

Skew left braces were first defined by Guarneri and Vendramin in [GV17], generalizing the concept of left brace, a concept defined by W. Rump [Ru07] as a generalization of a radical ring.

The primary motivation behind the concept of a brace, and subsequently a skew brace, was to construct algebraic structures that yield set-theoretic solutions of the Yang-Baxter equation. Such a solution is a function $R : B \times B \to B \times B$ on a set $B$ that satisfies the equation

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

for all $a, b, c$ in $B$. This equation has been a question of considerable interest among algebraists since 1990 (motivated by [Dr92]). Solutions of the YBE have been constructed in various settings during the past 25 years (e.g. [LYZ00], [Ru07], [CJO14], [BCJ16]), but the only general descriptions of how a skew left brace yields a solution to the YBE appear in [GV17] and [Ba18].

Received February 6, 2024.

2010 Mathematics Subject Classification. 16T25, 16-02.

Key words and phrases. skew left brace, solution of the Yang-Baxter equation.
Beyond their connection to the YBE, skew braces have also been shown in [SV18] to be very closely related to Hopf-Galois structures on Galois extensions of fields—see, for example, [CGK...21] and [ST23].

Skew braces and their role in giving solutions to the YBE were recently introduced to a broad American audience by Vendramin in [Ve24], adapted from a longer survey article [Ve23]. The latter refers only to [GV17] for the proof that a skew brace yields a solution of the YBE. But the proof in [GV17] is not self-contained—it refers to braiding operators, from [LYZ00], and does not explicitly mention Proposition 2.4, below, which is central to the proof.

The referee pointed out that [Ba16], hence [Ba18], gives a self-contained proof of the skew brace-YBE connection that includes Proposition 2.4. But the proofs in [GV17] and [Ba18] involve notation for functions of functions that require multiple layers of subscripts whose complexity obscures what is going on.

This note presents a straightforward, entirely self-contained and notation-friendly proof that a skew left brace yields a solution of the form

$$R : B \times B \to B \times B$$

for all $x, y$ in $B$,

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

Then for all $x, y$ in $B$, $\sigma_x$ and $\tau_y$ are one-to-one maps from $B$ to $B$, and by definition of $\tau_y(x)$, $\sigma_x(y) \circ \tau_y(x) = \sigma_x(y) \circ (\sigma_x(y) \circ x) = x \circ y$. Define

$$R : B \times B \to B \times B$$

by

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

for all $a, b$ in $B$. Note that if $R(a, b) = (s, t)$, then $s \circ t = \sigma_a(b) \circ \tau_b(a) = a \circ b$.

We will prove:
Theorem 2.1. 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 Yang-Baxter equation: for all $a, b, c$ in $B$,

\[(R \times 1)(1 \times R)(a, b, c) = (1 \times R)(R \times 1)(a, b, c).
\]

Since $\sigma_a$ and $\tau_b$ are one-to-one maps from $B$ to $B$ for all $a, b$ in $B$, the solution $R$ of the Yang-Baxter equation is nondegenerate.

Proof. Given a skew brace $B(\circ, \cdot)$, for $x, y$ in $B$ the maps $\sigma_x(y) = x^{-1} \cdot (x \circ y)$ and $\tau_y(x) = \tau_x(y) \circ x \circ y$ satisfy the following two properties for all $x, y, z$ in $B$, as we show below:

(i): $\sigma$ is a homomorphism from $(B, \circ)$ to $\text{Perm}(B)$:

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

(ii): $\tau$ is an anti-homomorphism from $(B, \circ)$ to $\text{Perm}(B)$:

\[\tau_{z \circ y}(x) = \tau_y(\tau_z(x)).\]

Beside these two properties, the only other property we need is the property noted above:

(iii) if $u, v = (\sigma_u(v), \tau_u(u)) = (y, z)$, then $uv = yz$.

These three properties suffice to show that $R$ satisfies

\[(R \times 1)(1 \times R)(R \times 1)(a, b, c) = (1 \times R)(R \times 1)(1 \times R)(a, b, c) \quad (*),
\]

for all $a, b, c$ in $B$, as follows.

The left side of (*) is:

\[(R \times 1)(1 \times R)(R \times 1)(a, b, c) = (R \times 1)(1 \times R)(d, e, c) = (R \times 1)(d, f, g) = (h, k, g)
\]

where

\[d = \sigma_d(b), \quad e = \tau_d(a), \quad \text{so} \quad a \circ b = d \circ e,
\]

and

\[f = \sigma_f(c), \quad g = \tau_c(e), \quad \text{so} \quad e \circ c = f \circ g,
\]

The right side of (*) is:

\[(1 \times R)(R \times 1)(1 \times R)(a, b, c) = (1 \times R)(R \times 1)(a, q, r) = (1 \times R)(s, t, r) = (s, v, w),
\]

where

\[q = \sigma_q(c), \quad r = \tau_q(b), \quad \text{so} \quad b \circ c = q \circ r,
\]

and

\[s = \sigma_s(q), \quad t = \tau_q(a), \quad \text{so} \quad a \circ q = s \circ t,
\]

and

\[v = \sigma_v(r), \quad w = \tau_q(t), \quad \text{so} \quad t \circ r = v \circ w.
\]

We want to show that $(h, k, g) = (s, v, w)$.

To show that $h = s$ uses property (i): $\sigma_{y \circ z}(x) = \sigma_y(\sigma_z(x))$, as follows:

\[s = \sigma_s(q) = \sigma_d(\sigma_b(c)) = \sigma_{a \circ b}(c);
\]

\[h = \sigma_d(f) = \sigma_d(\sigma_c(c)) = \sigma_{d \circ o}(c);
\]
and
\[ doe = \sigma_d(b)\sigma_b(a) = a\circ b. \]

So
\[ h = \sigma_{doe}(c) = \sigma_{aob}(c) = s. \]

To show that \( w = g \) uses property (ii): \( \tau_{zoq}(x) = \tau_y(\tau_z(x)), \) as follows:
\[ g = \tau_c(e) = \tau_c(\tau_b(a)) = \tau_{boc}(a); \]
\[ w = \tau_r(t) = \tau_r(\tau_q(a)) = \tau_{qor}(a) \]

and
\[ q\circ r = \sigma_b(c)\tau_c(b) = b\circ c. \]

So
\[ w = \tau_{qor}(a) = \tau_{boc}(a) = g. \]

Finally, to show that \( k = v \) we just use property (iii) many times, that for any \( u,v, \) if \( R(u,v) = (m,n), \) then \( mon = uov: \)

The left side of equation (*) is \((h,k,g)\); the right side is \((s,v,w)\), and using all of the equalities above, we have that
\[ s\circ v\circ w = a\circ b\circ c = h\circ k\circ g. \]

For
\[ s\circ(v\circ w) = s\circ(\sigma_r(t)\sigma_r(t)) = s\circ(t\circ r) \]
\[ = (s\circ t)\circ r = (\sigma_d(\sigma_q(a))\sigma_r(a))\circ r = (a\circ q)\circ r \]
\[ = a\circ(\sigma_b(c)\sigma_c(b) = a\circ b\circ c); \]

while
\[ (a\circ b)\circ c = (\sigma_d(b)\sigma_b(a))\circ c = (d\circ e)\circ c \]
\[ = d\circ(e\circ c) = d\circ(\sigma_x(c)\sigma_e(e)) = d\circ(f\circ g) \]
\[ = (d\circ f)\circ g = (\sigma_d(f)\sigma_f(d))\circ g = (h\circ k)\circ g. \]

So \( s\circ v\circ w = h\circ k\circ g. \) Since \( w = g, \) and \( h = s \) in the group \((B,\circ), \) it follows that \( k = u. \) Given properties (i) and (ii), that completes the proof. \( \square \)

To prove properties (i) and (ii) we need the following consequence of the compatibility condition (\#) for a skew brace (c.f. [GV17], Lemma 1.7 (2)):

**Lemma 2.2.** For all \( a, b \) in \( B, \) \( a^{-1} \cdot (a\circ b^{-1}) \cdot a^{-1} = (a\circ b)^{-1}. \)

**Proof.** The compatibility condition (\#) 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
\[ x \cdot (x\circ y)^{-1} \cdot (x\circ(y \cdot z)) = x\circ z \]
or
\[ x\circ z = x \cdot (x\circ y)^{-1} \cdot (x\circ(y \cdot z)). \]

Set \( x = a, y = b, z = b^{-1} \) to get
\[ a\circ b^{-1} = a \cdot (a\circ b)^{-1} \cdot a, \]
or
\[
a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1} = (a \circ b)^{-1}.
\]

Here is property (i): it is Proposition 1.9 (2) of [GV17].

**Proposition 2.3.** For all \(x, y, z\) in \(B\),
\[
\sigma_{x \circ y}(z) = \sigma_x(\sigma_y(z)).
\]

**Proof.** (from [GV17]) The right side of
\[
\sigma_{x \circ y}(z) = \sigma_x(\sigma_y(z))
\]
is
\[
\sigma_x(\sigma_y(z)) = x^{-1} \cdot (x \circ \sigma_y(z))
\]
\[
= x^{-1} \cdot (x \circ (y^{-1} \cdot (y \circ z)))
\]
\[
= x^{-1} \cdot (x \circ y^{-1}) \cdot x^{-1} \cdot (x \circ y \circ z) \quad \text{(by (#))}
\]
By Lemma 2.2, this is
\[
= (x \circ y)^{-1} \cdot (x \circ y \circ z)
\]
\[
= \sigma_{x \circ y}(z).
\]

(We note that [GV17] proves that given a set \(B\) with two group operations, \(\cdot\) and \(\circ\), and \(\sigma_x(y) = x^{-1} \cdot (x \circ y)\), then for all \(x, y, z\) in \(B\),
\[
\sigma_x(\sigma_y(z)) = \sigma_{x \circ y}(z)
\]
if and only if the compatibility condition (\#) holds, if and only if \(B\) is a skew left brace: see Proposition 1.9 of [GV17].)

Finally, we prove property (ii):

**Proposition 2.4.** \(\tau\) is an anti-homomorphism from \((B, \circ)\) to \(\text{Perm}(B)\): for all \(x, y, z\) in \(B\),
\[
\tau_{x \circ y}(x) = \tau_x(\tau_y(x)).
\]

**Proof.** We begin with the definition of \(\sigma_x(q)\):
\[
x^{-1} \cdot (x \circ y) = \sigma_x(y)
\]
Rearrange the equation and use that \(x \circ y = \sigma_x(y) \circ \tau_y(x)\), to get:
\[
\sigma_x(y)^{-1} \cdot x^{-1} = (\sigma_x(y) \circ \tau_y(x))^{-1}
\]
Apply the Lemma 2.2 formula, \((a \circ b)^{-1} = a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1}\) to the right side, to get:
\[
\sigma_x(y)^{-1} \cdot x^{-1} = \sigma_x(y)^{-1} \cdot (\sigma_x(y) \circ \tau_y(x)^{-1}) \cdot \sigma_x(y)^{-1}
\]
Cancel \(\sigma_x(y)^{-1}\) on the left and multiply both sides by \((x \circ y \circ z)\) on the right:
\[
x^{-1} \cdot (x \circ y \circ z) = (\sigma_x(y) \circ \tau_y(x)^{-1}) \cdot \sigma_x(y)^{-1} \cdot (x \circ y \circ z)
\]
Apply the definition of $\sigma$ to the left side and use that $x \circ y = \sigma_x(y) \circ \tau_y(x)$ on the right side:

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

Apply the skew brace formula (#) to the right side:

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

Use the definition of $\sigma$ on the far right side:

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

Take the $\circ$-inverse of both sides, and multiply both sides by $\circ x \circ y \circ z$:

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

Use the definition of $\tau$: $\tau_b(a) = \sigma_a(b) \circ a \circ b$ on the right side:

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

then on both sides:

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

So $\tau$ is an anti-homomorphism on $(B, \circ)$.

References

[Ba16] Bachiller, David. Study of the algebraic structure of left braces and the Yang–Baxter equation. Ph.D. thesis, Universitat Autonoma de Barcelona, 2016. 650

[Ba18] Bachiller, David. Solutions of the Yang–Baxter equation associated to skew left braces, with applications to racks. J. Knot Theory Ramifications 27 (2018), no. 8, 185005, 36 pp. MR3835326, Zbl 1461.16040, arXiv:1611.08138, doi:10.1142/S0218216518500554, 649, 650

[BCJ16] Bachiller, David; Cedó, Ferran; Jespers, Eric. Solutions of the Yang–Baxter equation associated with a left brace. J. Algebra 463 (2016), 80–102. MR3527540, Zbl 1348.16027, arXiv:1503.02814, doi:10.1016/j.jalgebra.2016.05.024, 649

[CJO14] Cedó, Ferran; Jespers, Eric; Okniński, Jan. Braces and the Yang–Baxter equation. Comm. Math. Phys. 327 (2014), no. 1, 101–116. MR3179933, Zbl 1287.81062, arXiv:1205.3587, doi:10.1007/s00220-014-1935-y, 649

[CGK...21] Childs, Lindsay N.; Greither, Cornelius; Keating, Kevin P.; Koch, Alan; Kohl, Timothy; Truman, Paul J.; Underwood, Robert G. Hopf algebras and Galois module theory. Mathematical Surveys and Monographs, 260. American Mathematical Society, Providence, RI, 2021. vii+31 pp. ISBN:978-1-4704-6516-2. MR4390798, Zbl 1489.16001, doi:10.1090/surv/260, 650

[Dr92] Drinfel’d, Vladimir G. On some unsolved problems in quantum group theory. Quantum Groups (Leningrad, 1990), 1–8. Lecture Notes in Math., 1510. Springer-Verlag, Berlin, 1992. ISBN:3-540-55305-3. MR1183474, Zbl 0765.17014, doi:10.1007/BFb0101175, 649

[GV17] Guarnieri, L.; Vendramin, Leandro. Skew braces and the Yang–Baxter equation. Math. Comp 86 (2017), no. 307, 2519–2534.; MR3647970, Zbl 1371.16037, arXiv:1511.03171, doi:10.1090/mcom/3161, 649, 650, 652, 653

[LYZ00] Lu, Jiang-Hua; Yan, Min; Zhu, Yong-Chang. On the set-theoretical Yang–Baxter equation. Duke Math. J. 104 (2000), no. 1, 1–18. MR1769723, Zbl 0960.16043, doi:10.1215/S0012-7094-00-10411-5, 649, 650
Rump, Wolfgang. Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra* **307** (2007), no. 1, 153–170. MR2278047, Zbl 1115.16022, doi:10.1016/j.jalgebra.2006.03.040.

Smoktunowicz, Agata; Vendramin, Leandro. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra* **2** (2018), no. 1, 47–86. MR3763907, Zbl 1416.16037, arXiv:1705.06958, doi:10.4171/JCA/2-1-3.

Stefanello, Lorenzo; Trappeniers, Senne. On the connection between Hopf–Galois structures and skew braces. *Bull. Lond. Math. Soc.* **55** (2023), no. 4, 1726–1748. MR4623681, Zbl 07738097, arXiv:2206.07610v4, doi:10.1112/blms.12815.

Vendramin, Leandro. Skew braces: a brief survey. Preprint, 2023.

Ve23 Vendramin, Leandro. What is ... a skew brace?. *Notices Amer. Math. Soc.* **71** (2024), no. 1, 65–67. MR4693602.

(Lindsay N. Childs) Department of Mathematics and Statistics, University at Albany, Albany, NY 12222, USA

lchilds@albany.edu

This paper is available via [http://nyjm.albany.edu/j/2024/30-29.html](http://nyjm.albany.edu/j/2024/30-29.html).