The Yang-Baxter Equation and Hopf-Galois Theory via Skew Braces

Kayvan Nejabati Zenouz[1]

Oxford Brookes University

Hopf Algebras and Galois Module Theory Conference
University of Nebraska Omaha

May 28, 2019

[1]Email: knejabati-zenouz@brookes.ac.uk website: www.nejabatiz.com

Contents

1. Introduction
2. The Yang-Baxter Equation
3. Skew Braces
   - Skew Braces and the YBE
   - Relation to Rings
4. Hopf-Galois Theory
   - Hopf-Galois Structures
5. Hopf-Galois Structures and Skew Braces
   - Automorphism Groups of Skew Braces
6. Classification of Hopf-Galois Structures and Skew Braces
   - Strategy for the Proofs
7. Skew Braces of Semi-direct Product Type
8. Scopes and Work in Progress

Outline

Introduction to

The Yang-Baxter Equation

and its connection to

Hopf-Galois Theory

via

Skew Braces

Classification of

Hopf-Galois Structures and Skew Braces of order p^3

The Yang-Baxter Equation

For a vector space V, an element

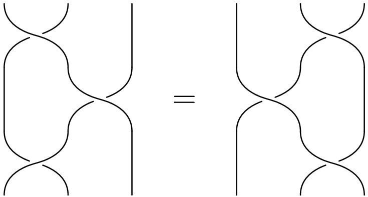
$$R \in \mathrm{GL}(V \otimes V)$$

is said to satisfy the **Yang-Baxter equation (YBE)** if

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)$$

holds.

This equation can be depicted by



The Yang-Baxter Equation

The **Yang-Baxter equation** appeared in work of Yang and Baxter in **statistical mechanics** and **mathematical physics**.

Nowadays the Yang-Baxter equation has a central role in **quantum group theory** with applications in

integrable systems

knot theory

tensor categories

Set-Theoretic Yang-Baxter Equation

In 1992 Drinfeld suggested studying the **simplest class of solutions** arising from the **set-theoretic** version of this equation.

Definition

Let X be a nonempty set and

$$\begin{aligned} r: X \times X &\longrightarrow X \times X \\ (x, y) &\longmapsto (f_x(y), g_y(x)) \end{aligned}$$

a bijection. Then (X, r) is a **set-theoretic solution** of YBE if

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r)$$

holds. The solution (X, r) is called **non-degenerate** if $f_x, g_x \in \mathrm{Perm}(X)$ for all $x \in X$ and **involutive** if $r^2 = \mathrm{id}$.

Examples

Let X be a nonempty set.

1. The map $r(x, y) = (y, x)$.
2. Let $f, g : X \longrightarrow X$ be bijections with $fg = gf$. Then

$$r(x, y) = (f(y), g(x))$$

   gives a non-degenerate solution, which is involutive if and only if $f = g^{-1}$.
3. For any group structure on X the map

$$r(x, y) = (y, yxy^{-1}).$$

4. If $(R, +, \cdot)$ is a radical ring with circle operation $a \circ b = a + ab + b$ then $r(x, y) = (xy + y, (xy + y)^{\circ -1} \circ x \circ y)$.

Skew Braces

Definition

A (left) **skew brace** is a triple $(B, \oplus, \odot)$ which consists of a set B together with two operations $\oplus$ and $\odot$ so that $(B, \oplus)$ and $(B, \odot)$ are groups such that for all $a, b, c \in B$:

$$a \odot (b \oplus c) = (a \odot b) \ominus a \oplus (a \odot c),$$

where $\ominus a$ is the inverse of a with respect to the operation $\oplus$.

Remark

A skew brace is called **two-sided** if

$$(b \oplus c) \odot a = (b \odot a) \ominus a \oplus (c \odot a).$$

Interesting for ring theorists: $0 = 1$.

Skew Braces

Example

Any group $(B, \oplus)$ with

$$a \odot b = a \oplus b \quad \text{(similarly with } a \odot b = b \oplus a\text{)}$$

is a skew brace. This is the **trivial** skew brace structure.

Notation

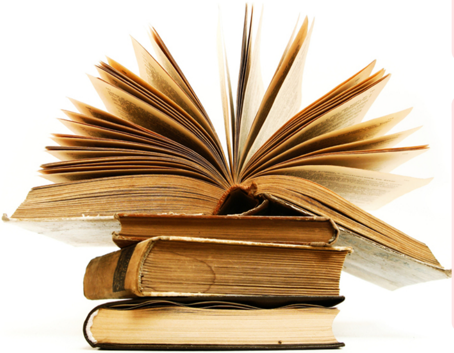
- We call a skew brace $(B, \oplus, \odot)$ such that $(B, \oplus) \cong N$ and $(B, \odot) \cong G$ a G-skew brace of **type** N.
- A skew brace $(B, \oplus, \odot)$ is called a **brace** if $(B, \oplus)$ is abelian, i.e., a skew brace of abelian type.

Braces were introduced by Rump in 2007 as a **generalisation of radical rings**. They provide *non-degenerate, involutive* **set-theoretic solutions of the YBE**.

Skew Braces: History

Skew braces generalise braces and were introduced by Guarnieri and Vendramin in 2017.

They provide *non-degenerate* **set-theoretic solutions of the Yang-Baxter equation**.



Their connection to **ring theory** and **Hopf-Galois structures** was studied by Bachiller, Byott, Smoktunowicz, and Vendramin.

Theorem (L. Guarnieri and L. Vendramin)

Let $(B, \oplus, \odot)$ be a skew brace. Then the map

$$\begin{aligned} r_B : B \times B &\longrightarrow B \times B \\ (a, b) &\longmapsto \big(\ominus a \oplus (a \odot b), (\ominus a \oplus (a \odot b))^{-1} \odot a \odot b\big) \end{aligned}$$

is a non-degenerate set-theoretic solution of the YBE, which is involutive if and only if $(B, \oplus, \odot)$ is a brace.

Relation to Rings

- Given a skew brace $(B, \oplus, \odot)$ define

$$a \otimes b = \ominus a \oplus (a \odot b) \ominus b.$$

  Cedo, Konovalov, Vendramin, Smoktunowicz (2018) study $(B, \oplus, \otimes)$ using ring theoretic methods.
- However, if B is a **two-sided brace**, then $(B, \oplus, \otimes)$ is a **radical ring**.
- Conversely, if $(B, \oplus, \otimes)$ is a **radical ring**, then $(B, \oplus, \circ)$, where

$$a \circ b = a \oplus a \otimes b \oplus b$$

  is a **two-sided brace**.

Two aims in developing the theory:

Galois theory for **inseparable extensions** of fields

Studying **rings of integers** of extensions of **number fields**

Hopf-Galois Structures

Hopf-Galois structures are K-Hopf algebras together with an action on L.

Definition

A **Hopf-Galois structure** on L/K consists of a finite dimensional cocommutative K-*Hopf algebra* H together with an action on L such that the R-module homomorphism

$$\begin{aligned} j : & L \otimes_K H \longrightarrow \mathrm{End}_K(L) \\ & s \otimes h \longmapsto (t \longmapsto sh(t)) \text{ for } s, t \in L,\ h \in H \end{aligned}$$

is an isomorphism.

The **group algebra** $K[G]$ endows L/K with the classical Hopf-Galois structure.

Hopf-Galois Structures: Application

- Assume L/K is a **Galois extension** of (local/global) fields with **Galois group** G.
- Suppose H endows L/K with a Hopf-Galois structure.
- Define the associated order of $\mathcal{O}_L$ in H by

$$\mathfrak{A}_H = \{\alpha \in H \mid \alpha(\mathcal{O}_L) \subseteq \mathcal{O}_L\}.$$

- Can $\mathcal{O}_L$ be free over $\mathfrak{A}_H$?
- How to find Hopf-Galois structures?

Hopf-Galois Structures: A Theorem of Greither and Pareigis

Theorem (Greither and Pareigis)

Hopf-Galois structures on L/K correspond bijectively to regular subgroups of $\mathrm{Perm}(G)$ *which are normalised by the image of* G*, as left translations, inside* $\mathrm{Perm}(G)$.

Every K-Hopf algebra which endows L/K with a Hopf-Galois structure is of the form $L[N]^G$ for some regular subgroup $N \subseteq \mathrm{Perm}(G)$ normalised by the left translations.

Hopf-Galois Structures: Byott's Translation

Problem

The group $\mathrm{Perm}(G)$ can be large.

Instead of working with groups of permutations, work with *holomorphs*.

Theorem (Byott 1996)

Let G and N be finite groups. There exists a bijection between the sets

$$\mathcal{N} = \{\alpha : N \hookrightarrow \mathrm{Perm}(G) \mid \alpha(N) \textit{ is regular and normalised by } G\}$$

$$\mathcal{G} = \{\beta : G \hookrightarrow \mathrm{Hol}(N) \mid \beta(G) \textit{ is regular}\},$$

where $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$.

Enumerating Hopf-Galois Structures (Byott)

Using Byott's translation one can show that

$$\sharp\text{HGS on } L/K \text{ of type } N = \frac{|\mathrm{Aut}\,(G)|}{|\mathrm{Aut}\,(N)|}\,|\{H \subseteq \mathrm{Hol}(N) \text{ regular with } H \cong G\}|\,.$$

Hopf-Galois Structures: Some Results

- Byott (1996) showed if $|G| = n$, then L/K a **unique Hopf-Galois structure** iff $\gcd(n, \phi(n)) = 1$.
- Kohl (1998, 2019) classified Hopf-Galois structures for $G = C_{p^n}, D_n$ for a prime $p > 2$.
- Byott (1996, 2004) studied the problem for $|G| = p^2, pq$, also when G is a **nonabelian simple group**.
- Carnahan and Childs (1999, 2005) studied Hopf-Galois structures for $G = C_p^n$ and $G = S_n$.
- Alabadi and Byott (2017) studied the problem for $|G|$ is **squarefree**.
- Nejabati Zenouz (2018) Hopf-Galois structures for $|G| = p^3$ where p is a prime number.
- Crespo and Salguero extensions of degree $C_{p^n} \rtimes C_D$, Samways cyclic extensions, and Tsang S_n-extensions.

Hopf-Galois Structures of Order p^3 for $p > 3$

Theorem 1 [cf. NZ18, Jan 2018]

The number of Hopf-Galois structures on L/K of type N, $e(G, N)$, is given by

$e(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	$C_p^2 \rtimes C_p$	$C_{p^2} \rtimes C_p$
C_{p^3}	p^2	-	-	-	-
$C_{p^2} \times C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$
C_p^3	-	-	$(p^4+p^3-1)p^2$	$(p^3-1)(p^2+p-1)p^2$	-
$C_p^2 \rtimes C_p$	-	-	$(p^2+p-1)p^2$	$(2p^3-3p+1)p^2$	-
$C_{p^2} \rtimes C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$

Column $C_p^2 \rtimes C_p$ J. Algebra [cf. NZ19, Apr 2019]. Cases $p = 2, 3$ are also treated.

Remark

Note $p^2 \mid e(G, N)$ and

$$|\mathrm{Aut}(N)|\, e(G, N) = |\mathrm{Aut}(G)|\, e(N, G).$$

Hopf-Galois Structures and Skew Braces

Question

How are Hopf-Galois structures related to skew braces?

Skew braces parametrise Hopf-Galois structures.

$$\left\{\begin{array}{c}\text{isomorphism classes}\\ \text{of } G\text{-skew braces,}\\ \text{i.e., with } (B,\odot)\cong G\end{array}\right\} \overset{\text{bij}}{\leftrightsquigarrow} \left\{\begin{array}{c}\text{classes of certain regular}\\ \text{subgroups of Perm(G) under}\\ \text{conjugation by elements of}\\ \mathrm{Aut}(G)\end{array}\right\}$$

From Skew Braces to Hopf-Galois Structures

- Suppose $(B, \oplus, \odot)$ is a skew brace.
- Then $(B, \oplus)$ acts on $(B, \odot)$ and we find

$$
\begin{aligned}
d : (B, \oplus) &\longrightarrow \operatorname{Perm}(B, \odot) \\
a &\longmapsto (d_a : \ b \longmapsto a \oplus b)
\end{aligned}
$$

  which is a regular embedding.
- The skew brace property implies that $\operatorname{Im} d$ is normalised by the left translations.
- Fix L/K with Galois group $(B, \odot)$.
- Thus $L[\operatorname{Im} d]^{(B,\odot)}$ endows L/K with a Hopf-Galois structure of type $(B, \oplus)$.
- Isomorphic skew braces correspond to conjugate regular subgroups.

From Hopf-Galois Structures to Skew Braces

- Suppose H endows L/K with a Hopf-Galois structure.
- Then $H = L[N]^{(B,\odot)}$ for some $N \subseteq \text{Perm}\,(B, \odot)$ which is a regular subgroup normalised the left translations.
- N is a regular subgroup, implies that we have a bijection

$$\begin{aligned} \phi : & N \longrightarrow (B, \odot) \\ & n \longmapsto n \cdot 1. \end{aligned}$$

- Define

$$a \oplus b = \phi\left(\phi^{-1}(a)\,\phi^{-1}(b)\right) \text{ for } a, b \in (B, \odot)\,.$$

- N is normalised by the left translations implies that $(B, \oplus, \odot)$ is a skew brace of type N corresponding to H.

Skew Braces and Hopf-Galois Structures Correspondence

$$\left\{\begin{array}{c}\text{isomorphism classes}\\ \text{of } G\text{-skew braces,}\\ \text{i.e., with } (B,\odot)\cong G\end{array}\right\} \overset{\text{bij}}{\leftrightsquigarrow} \left\{\begin{array}{c}\text{classes of Hopf-Galois structures}\\ \text{on } L/K \text{ under } L[N_1]^G \sim L[N_2]^G\\ \text{if } N_2=\alpha N_1\alpha^{-1} \text{ for some}\\ \alpha\in\operatorname{Aut}(G)\end{array}\right\}$$

i.e., if $(B,\oplus,\odot)$ is a skew brace of type, then we get the

following Hopf-Galois structures on L/K

$$\left\{L[\alpha\,(\operatorname{Im} d)\,\alpha^{-1}]^{(B,\odot)} \mid \alpha\in\operatorname{Aut}(B,\odot)\right\}.$$

Upshot: Automorphism Groups of Skew Braces

Automorphism Groups [cf. NZ19, Apr 2019, Corollary 2.3]

In particular, if $f : (B, \oplus, \odot) \longrightarrow (B, \oplus, \odot)$ is an automorphism, then we have

$$\begin{array}{ccc} (B, \oplus) & \xhookrightarrow{\;d\;} & \operatorname{Perm}(B, \odot) \\ \wr\big\downarrow f & & \wr\big\downarrow C_f \\ (B, \oplus) & \xhookrightarrow{\;d\;} & \operatorname{Perm}(B, \odot)\,; \end{array}$$

using this observation we find

$$\operatorname{Aut}_{\mathcal{B}r}(B, \oplus, \odot) \cong \left\{ \alpha \in \operatorname{Aut}(B, \odot) \mid \alpha\,(\operatorname{Im} d)\,\alpha^{-1} \subseteq \operatorname{Im} d \right\}.$$

Classification of Hopf-Galois Structures and Skew Braces: Theoretical

Classifying Skew Braces

To find the non-isomorphic G-skew braces of type N classify elements of the set

$$\mathcal{S}(G, N) = \{H \subseteq \operatorname{Perm}(G) \mid H \text{ is regular, NLT, } H \cong N\},$$

and extract a maximal subset whose elements are not conjugate by any element of $\operatorname{Aut}(G)$.

Classification of Hopf-Galois Structures and Skew Braces: Theoretical

Hopf-Galois Structures Parametrised by Skew Braces [cf. NZ19, Corollary 2.4]

Denote by B_G^N the isomorphism class of a G-skew brace of type N given by $(B, \oplus, \odot)$. Then the number of Hopf-Galois structures on L/K of type N is given by

$$e(G, N) = \sum_{B_G^N} \frac{|\mathrm{Aut}\,(G)|}{|\mathrm{Aut}_{\mathcal{B}r}\,(B_G^N)|}.$$

Classification of Hopf-Galois Structures and Skew Braces: Practical

Again we would like to work with **holomorphs** instead of the **permutation groups**.

For a skew brace $(B, \oplus, \odot)$ consider the action of $(B, \odot)$ on $(B, \oplus)$ by $(a, b) \longmapsto a \odot b$. This yeilds to a map

$$\begin{aligned} m : (B, \odot) &\longrightarrow \mathrm{Hol}\,(B, \oplus) \\ a &\longmapsto (m_a : b \longmapsto a \odot b) \end{aligned}$$

which is a regular embedding.

Skew Braces and Regular Subgroups of Holomorph Correspondence

Bachiller, Byott, Vendramin:

$$\left\{\begin{array}{c}\text{isomorphism classes}\\ \text{of skew braces of}\\ \text{type } N\text{, i.e., with}\\ (B,\oplus)\cong N\end{array}\right\} \overset{\text{bij}}{\leftrightsquigarrow} \left\{\begin{array}{c}\text{classes of regular subgroup of}\\ \mathrm{Hol}(N) \text{ under } H_1 \sim H_2 \text{ if}\\ H_2 = \alpha H_1 \alpha^{-1} \text{ for some}\\ \alpha \in \mathrm{Aut}(N)\end{array}\right\}$$

Another Characterisation of Automorphism Group [cf. NZ18, Jan 2018, Theorem 2.3.8, p 29]

We find

$$\mathrm{Aut}_{\mathcal{B}r}\left(B,\oplus,\odot\right) \cong \left\{\alpha \in \mathrm{Aut}\left(B,\oplus\right) \mid \alpha\left(\mathrm{Im}\, m\right)\alpha^{-1} \subseteq \mathrm{Im}\, m\right\}.$$

Classifying Skew Braces and Hopf-Galois Structures

Skew braces

To find the non-isomorphic G-skew braces of type N for a fixed N, classify elements of the set

$$\mathcal{S}'(G, N) = \{H \subseteq \mathrm{Hol}\,(N) \mid H \text{ is regular}, \; H \cong G\},$$

and extract a maximal subset whose elements are not conjugate by any element of $\mathrm{Aut}\,(N)$.

Skew Braces: Some Results

- Rump (2007) classified **cyclic braces**.
- Bachiller (2015) classified **braces of order** p^3.
- Bachiller, Cedo, Jespers, Okninski (2017) **matched products of braces**.
- Guarnieri, Vendramin (2017, 2018) conjectures using **computer assisted results** and **Problems on skew left braces**.
- Nejabati Zenouz (2018) **skew braces of order** p^3.
- Catino, Colazzo, and Stefanelli (2017, 2018) **semi-braces** and skew braces with **non-trivial *annihilator***.
- Dietzel (2018) **braces of order** p^2q.
- Childs (2018, 2019) **correspondence** and **bi-skew braces**.
- Timur Nasybullov (2018), **two-sided skew braces**.
- Koch and Truman (2019), **Opposite braces** and **isomorphism correspondence**.

Skew Braces of Order p^3 for $p > 3$

Theorem 2 [cf. NZ18, Jan 2018]

The number of G-skew braces of type N, $\widetilde{e}(G,N)$, is given by

$\widetilde{e}(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	$C_p^2 \rtimes C_p$	$C_{p^2} \rtimes C_p$
C_{p^3}	3	-	-	-	-
$C_{p^2} \times C_p$	-	9	-	-	$4p+1$
C_p^3	-	-	5	$2p+1$	-
$C_p^2 \rtimes C_p$	-	-	$2p+1$	$2p^2-p+3$	-
$C_{p^2} \rtimes C_p$	-	$4p+1$	-	-	$4p^2-3p-1$

Column $C_p^2 \rtimes C_p$ and automorphism groups [cf. NZ19, Apr 2019].

Remark

Note

$$\widetilde{e}(G,N) = \widetilde{e}(N,G).$$

Strategy for the Proofs of Theorems 1 & 2

- For each group N of order p^3 determine $\mathrm{Aut}(N)$.

$$\mathrm{Aut}(C_{p^3}) \cong C_{p^2} \times C_{p-1},\ \mathrm{Aut}(C_p^3) \cong \mathrm{GL}_3(\mathbb{F}_p),$$

$$\mathrm{Aut}(C_p^2 \rtimes C_p) \cong C_p^2 \rtimes \mathrm{GL}_2(\mathbb{F}_p),$$

$$1 \longrightarrow C_p^2 \longrightarrow \mathrm{Aut}(C_{p^2} \times C_p) \longrightarrow \mathrm{UP}_2(\mathbb{F}_p) \longrightarrow 1,$$

$$1 \longrightarrow C_p^2 \longrightarrow \mathrm{Aut}(C_{p^2} \rtimes C_p) \longrightarrow \mathrm{UP}_2^1(\mathbb{F}_p) \longrightarrow 1.$$

- Classify regular subgroups of $\mathrm{Hol}(N)$ according to the size of their image under the natural projection

$$\mathrm{Hol}(N) \longrightarrow \mathrm{Aut}(N).$$

- To find **skew braces** study conjugation formula by elements of $\mathrm{Aut}(N)$ inside $\mathrm{Hol}(N)$.

Example

Let $p > 2$, $n > 1$, and $C_{p^n} = \left\langle \sigma \mid \sigma^{p^n} = 1 \right\rangle$. Then

$$\mathrm{Hol}\left(C_{p^n}\right) = \langle \sigma \rangle \rtimes \langle \beta, \gamma \rangle$$

with $\beta(\sigma) = \sigma^{p+1}$. Then the *trivial* (skew) brace is $\langle \sigma \rangle$, and the *nontrivial* (skew) braces are given by

$$\left\langle \sigma \beta^{p^m} \right\rangle \cong C_{p^n} \text{ for } m = 0, ..., n-2.$$

We also have

$$\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \sigma \beta^{p^m} \right\rangle\right) = \left\langle \beta^{p^{n-m-2}} \right\rangle \text{ for } m = 0, ..., n-2.$$

Skew Braces of Semi-direct Product Type

Question

How general is the pattern $\widetilde{e}(G,N)=\widetilde{e}(N,G)$?

Proposition 4.6.12 [cf. NZ18, Jan 2018, p. 130]

Let P and Q be groups. Suppose $\alpha,\beta : Q \longrightarrow \mathrm{Aut}(P)$ are group homomorphisms such that $\mathrm{Im}\,\beta$ is an abelian group and $[\mathrm{Im}\,\alpha, \mathrm{Im}\,\beta]=1$.

1. We can form an $(P \rtimes_\alpha Q)$-skew brace of type $P \rtimes_\beta Q$.
2. And an $(P \rtimes_\beta Q^{\mathrm{op}})$-skew brace of type $P \rtimes_\alpha Q$.

What is the relationship between $\widetilde{e}(G,N)$ and $\widetilde{e}(N,G)$ for N which is a general extensions of two groups?

Scopes and Work in Progress

1. Work in progress: classify skew braces and Hopf-Galois structures of type $C_{p^n} \rtimes C_p$.
2. Study the Galois module theoretic invariants of Hopf-Galois structures corresponding to a skew brace.
3. Extend results to study skew braces of type $\left(C_{p^e} \times C_{p^f}\right) \rtimes C_{p^g}$ for natural numbers e, f, g.
4. Study skew braces whose type is an extension of two abelian groups. Does the pattern

$$\widetilde{e}(G, N) = \widetilde{e}(N, G)$$

still hold?

Thank you for your attention!

Selected References I

[NZ18] Kayvan Nejabati Zenouz. On Hopf-Galois Structures and Skew Braces of Order p^3. *The University of Exeter, PhD Thesis, Funded by EPSRC DTG*, January 2018. https://ore.exeter.ac.uk/repository/handle/10871/32248.

[NZ19] Kayvan Nejabati Zenouz. Skew Braces and Hopf-Galois Structures of Heisenberg Type. *Journal of Algebra*, 524:187–225, April 2019. https://doi.org/10.1016/j.jalgebra.2019.01.012.