

Hopf-Galois Theory and the Yang-Baxter Equation

Kayvan Nejabati Zenouz¹

University of Edinburgh

MAXIMALS algebra seminar

May 15, 2018

¹Email: knejabat@ed.ac.uk website: <http://www.maths.ed.ac.uk/~knejabat/>

Acknowledgements

**This research was partially supported
by the ERC Advanced grant 320974**

Aim of this talk is to give an overview of

The Yang-Baxter Equation

and its connection to

Hopf-Galois Theory

through

Skew Braces

**Skew braces provide solutions of the
Yang-Baxter equation**

The Yang-Baxter Equation

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

Nowadays the Yang-Baxter equation is studied in **quantum group theory** and has applications in **integrable systems**, **knot theory**, **tensor categories**, and other areas.

For a vector space V , the YBE is a matrix equation for elements of $GL(V \otimes V)$.

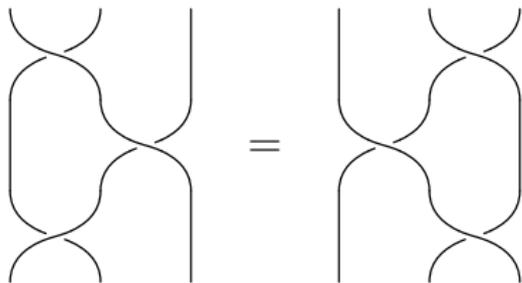
The Yang-Baxter Equation

An element $R \in GL(V \otimes V)$ is said to satisfy **the Yang-Baxter equation** if

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

holds.

This equation can be represented by the picture



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 (Set-theoretic solution of the YBE)

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

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

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

Set-Theoretic Yang-Baxter Equation

Examples

Let X be a nonempty set.

- 1 (Trivial solution) The map $r(x, y) = (y, x)$.
- 2 (Permutations solutions) Let $f, g : X \rightarrow X$ 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

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

gives a solution.

Structure Group of (X, r)

Definition (Structure Group)

Let (X, r) be a non-degenerate solution of the YBE. The **structure group** of (X, r) is defined by

$$G(X, r) = \langle X \mid xy = f_x(y)g_y(x) \text{ for all } x, y \in X \rangle.$$

Example

For (X, r) the trivial solution, i.e., $r(x, y) = (y, x)$

$$G(X, r) = \mathbb{Z}^X.$$

It is known that $G(X, r)$ is in general **abelian-by-finite**.

Skew Braces

Definition (Skew Brace)

A (left) **skew brace** is a triple (B, \oplus, \odot) which consists of a set B together with two operations \oplus and \odot such 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 .

Interesting for ring theorists:

$$0 = 1.$$

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 .

- (B, \oplus) is called the **additive group**.
- (B, \odot) is called the **multiplicative group**.

Skew Braces: History I

Example

Any group (B, \oplus) with

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

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

A skew brace (B, \oplus, \odot) is called a **brace** if (B, \oplus) is abelian.

Braces were introduced by Rump [Rum07a] to **generalise radical rings**.

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

Skew Braces: History II

Skew braces were introduced by Guarnieri and Vendramin [GV17] and **generalise braces**.

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

Their connection to **ring theory** and **Hopf-Galois structures** was studied by Byott, Konovalov, Smoktunowicz, and Vendramin [SV18, KSV18].

Skew Braces and the YBE

Theorem (L. Guarnieri and L. Vendramin)

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

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

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

Furthermore, for every non-degenerate solution of YBE (X, r) , the **structure group** $G(X, r)$ can be given a skew braces structure in a unique way.

Skew braces parametrise Hopf-Galois structures on a field extension

Hopf-Galois Theory

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: Motivations

For simplicity we assume L/K is a **Galois extension** of fields with Galois group G .

Normal Basis Theorem

L is a free $K[G]$ -module of rank one.

- Assume L/K is an extension of global or local fields (e.g., extensions of \mathbb{Q} or \mathbb{Q}_p).
- Denote by \mathcal{O}_L and \mathcal{O}_K the rings of integers of L and K , respectively.
- Then \mathcal{O}_L is also a module over $\mathcal{O}_K[G]$.
- Can \mathcal{O}_L be free over $\mathcal{O}_K[G]$?

... No in general.

Hopf-Galois Structures

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

Definition (Hopf-Galois structure)

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

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

is an isomorphism.

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

Hopf-Galois Structures: Application

- Suppose H endows L/K with a Hopf-Galois structure.
- Define the associated order of \mathcal{O}_L in H by

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

- Is \mathcal{O}_L be free over \mathfrak{A}_H ?
... Sometimes and depends on H .

Hopf-Galois Structures:

A Theorem of Greither and Pareigis

Theorem (Greither and Pareigis [GP87])

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

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

Notation: The *isomorphism type* of N is known as the **type** of the Hopf-Galois structure.

Hopf-Galois Structures: Byott's Translation

Problem

The group $\text{Perm}(G)$ 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

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

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

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

Hopf-Galois Structures: Byott's Translation

Using Byott's translation one can show that

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

Byott found cases where \mathcal{O}_L is **free** over \mathfrak{A}_H for some H which gives a non-classical Hopf-Galois structure on L/K , but **not free** over $\mathfrak{A}_{K[G]}$.

Hopf-Galois Structures and Skew Braces

Question

How are Hopf-Galois structures related to skew braces?

Skew braces parametrise Hopf-Galois structures.

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

Hopf-Galois Structures and Skew Braces

Kayvan Nejabati Zenouz

University of Edinburgh

MAXIMALS algebar seminar

May 15, 2018

¹Email: knejabat@ed.ac.uk website: <http://www.maths.ed.ac.uk/~knejabat/>

Overview

Aim of this talk:

Explain the connection between Hopf-Galois structures and skew braces

Look at results relating to classification

From Skew Braces to Hopf-Galois Structures

- Suppose (B, \oplus, \odot) is a skew brace.
- The map

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

is a regular embedding.

- The skew brace property implies that $\text{Im } d$ is normalised by the left translations.
- Fix L/K with Galois group (B, \odot) .
- Thus $L[\text{Im } d]^{(B, \odot)}$ endows L/K with a Hopf-Galois structure of type (B, \oplus) .

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

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

- 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

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

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

following Hopf-Galois structures on L/K

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

Upshot: Automorphism Groups of Skew Braces

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

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

using this observation we find

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

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

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

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

Classification of Hopf-Galois Structures and Skew Braces: Theoretical

Hopf-Galois structures

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

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

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 $(a, b) \mapsto a \odot b$.

Skew Braces and Regular Subgroups of Holomorph Correspondence

Bachiller, Byott, Vendramin:

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

Another Characterisation of Automorphism Group

We find

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

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

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

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

Skew Braces: Some Results

- ◆ Rump (2007) classified **cyclic braces** [Rum07b].
- ◆ Bachiller (2015) classified **braces of order p^3** [Bac15].
- ◆ Bachiller, Cedo, Jespers, Okninski (2017) **matched products of braces**.
- ◆ Guarnieri, Vendramin (2017) made conjectures using **computer assisted results** about certain skew braces [GV17].
- ◆ NZ (2018) **skew braces of order p^3** [NZ18b, NZ18a].
- ◆ Skew braces with **non-trivial annihilator** [CCS18].
- ◆ Dietzel studied **braces of order p^2q** [Die18].

Hopf-Galois Structures: Some Results

- ◆ Byott (1996) showed if $|G| = n$, then L/K a **unique Hopf-Galois structure** iff $\gcd(n, \phi(n)) = 1$ [Byo96].
- ◆ Kohl (1998) classified Hopf-Galois structures for $G = C_{p^n}$ for a prime $p > 2$ [Koh98]: there are p^{n-1} , all are of cyclic type. Byott (2007) studies $G = C_{2^n}$ case [Byo07].
- ◆ Byott (1996, 2004) studied the problem for $|G| = p^2, pq$, also when G is a **nonabelian simple group** [Byo96, Byo04].
- ◆ Carnahan and Childs (1999, 2005) studied Hopf-Galois structures for $G = C_p^n$ and $G = S_n$ [CC99].
- ◆ Alabadi and Byott (2017) studied the problem for $|G|$ is **squarefree** [AB18].
- ◆ NZ (2018) Hopf-Galois structures for $|G| = p^3$ [NZ18b].

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

Theorem 1 [NZ18b]

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

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

Remark

Note

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

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

Theorem 2 [NZ18b]

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	-	-	$(p^4 + p^3 - 1)p^2$	$(p^3 - 1)(p^2 + p - 1)p^2$	-
$C_p^2 \rtimes C_p$	-	-	$(p^2 + p - 1)p^2$	$(2p^3 - 3p + 1)p^2$	-
$C_{p^2} \rtimes C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$

Remark

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

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

Strategy for the Proof

For each group N of order p^3

- determine $\text{Aut}(N)$
- classify regular subgroups of $\text{Hol}(N)$ according to the size of their image under the natural projection

$$\text{Hol}(N) \longrightarrow \text{Aut}(N),$$

- find conjugation formula by elements of $\text{Aut}(N)$ inside $\text{Hol}(N)$.

Skew Braces of C_{p^n} type

Example

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

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

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

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

We also have

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

Scopes

- 1 Determine the structure group of these skew braces
- 2 Study the arithmetic invariants of Hopf-Galois structures corresponding to a skew brace.
- 3 Some methods can be used to study skew braces of type $(C_{p^e} \times C_{p^f}) \rtimes C_{p^g}$ for natural numbers e, f, g .
- 4 Study skew braces whose type is an extension of two abelian groups. Does the pattern

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

still hold?

Thank you for your attention!

Selected References I

- [AB18] Ali A. Alabdali and Nigel P. Byott. Counting Hopf-Galois structures on cyclic field extensions of squarefree degree. *Journal of Algebra*, 493:1–19, 2018.
- [Bac15] David Bachiller. Classification of braces of order p^3 . *J. Pure Appl. Algebra*, 219(8):3568–3603, 2015.
- [Byo96] N. P. Byott. Uniqueness of Hopf-Galois structure for separable field extensions. *Comm. Algebra*, 24(10):3217–3228, 1996.
- [Byo04] Nigel P. Byott. Hopf-Galois structures on Galois field extensions of degree pq . *J. Pure Appl. Algebra*, 188(1-3):45–57, 2004.
- [Byo07] Nigel P. Byott. Hopf-Galois structures on almost cyclic field extensions of 2-power degree. *J. Algebra*, 318(1):351–371, 2007.
- [CC99] Scott Carnahan and Lindsay Childs. Counting Hopf-Galois structures on non-abelian Galois field extensions. *J. Algebra*, 218(1):81–92, 1999.
- [CCS18] Francesco Catino, Ilaria Colazzo, and Paola Stefanelli. Skew left braces with non-trivial annihilator. *Journal of Algebra and Its Applications*, 2018.
- [Die18] C. Dietzel. Braces of order p^2q . *Preprint on ArXiv.org*, Feb 2018. <https://arxiv.org/pdf/1801.06911>.
- [GP87] Cornelius Greither and Bodo Pareigis. Hopf-Galois theory for separable field extensions. *J. Algebra*, 106(1):239–258, 1987.
- [GV17] L. Guarnieri and L. Vendramin. Skew braces and the Yang-Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.

Selected References II

- [Koh98] Timothy Kohl. Classification of the Hopf-Galois structures on prime power radical extensions. *J. Algebra*, 207(2):525–546, 1998.
- [KSV18] A. Konovalov, A Smoktunowicz, and L. Vendramin. On skew braces and their ideas. *Preprint on ArXiv.org*, April 2018. <https://arxiv.org/pdf/1804.04106>.
- [NZ18a] Kayvan Nejabati Zenouz. Skew braces and hopf-galois structures of heisenberg type. *Preprint on ArXiv.org*, April 2018. <https://arxiv.org/abs/1804.01360>.
- [NZ18b] Kayvan Nejabati Zenouz. *On Hopf-Galois Structures and Skew Braces of Order p^3* . The University of Exeter, PhD Thesis, Supervised by Prof N. Byott, Funded by EPSRC DTG, January 2018. <https://ore.exeter.ac.uk/repository/handle/10871/32248>.
- [Rum07a] Wolfgang Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007.
- [Rum07b] Wolfgang Rump. Classification of cyclic braces. *J. Pure Appl. Algebra*, 209(3):671–685, 2007.
- [SV18] A. Smoktunowicz and L. Vendramin. On skew braces (with an appendix by N. Byott and L. Vendramin). *Journal of combinatorial algebra*, 2018.