The set-theoretic Yang-Baxter equation and skew bracoids

Isabel Martin-Lyons

joint work with Paul Truman

Keele University, UK

Discrete Mathematics Seminar Series
13^{th} of December 2023

The Plan

Previously on Distrete Mathematics of Keele...

A fortnight ago we were introduced to three things:

- solutions to the (set theoretic) Yang-Baxter equation,
- skew braces,
- subgroups of the holomorph.

You may remember that skew braces line up with solutions and subgroups with specific properties. Today, we will see how we can relax these properties and what we can put in place of the skew brace. We'll also briefly look at how we might go about finding these things.

Outline

Outline

1. Recap
2. How do we generalise the skew brace?
3. Connecting the dots

The Yang-Baxter Equation

Definition

A *solution to the set-theoretic Yang-Baxter equation* (hereafter simply a *solution*) is a non-empty set G, together with a map $r : G \times G \to G \times G$ satisfying

$$(r \times 1)(1 \times r)(r \times 1) = (1 \times r)(r \times 1)(1 \times r)$$

as functions on $G \times G \times G$.

Given a solution r on G, for all $x, y \in G$ we will frequently write

$$r(x, y) = (\lambda_x(y), \rho_y(x));$$

so that we have family of maps $\lambda_x : G \to G$ and a family of maps $\rho_y : G \to G$.

Properties of the Solution

Suppose G with r is a solution and write $r(x, y) = (\lambda_x(y), \rho_y(x))$.

We say this solution is:

- *bijective* if r is bijective;
- *involutive* if $r^2 = id$;
- *left non-degenerate* if λ_x is bijective for all $x \in G$;
- *right non-degenerate* if ρ_y is bijective for all $y \in G$;
- *non-degenerate* if r is both left and right non-degenerate.

Example

- The trivial solution $r(x, y) = (x, y)$ is bijective and degenerate.
- The twist solution $r(x, y) = (y, x)$ is bijective and non-degenerate.

Skew braces

Definition (Guarnieri and Vendramin, 2017)

A *skew brace* is a set G endowed with two binary operations $\cdot$ and $\star$ such that:

- $(G, \cdot)$ and $(G, \star)$ are groups;
- writing $\bar{x}$ for the inverse of x with respect to $\star$, we have

$$x \cdot (y \star z) = (x \cdot y) \star \bar{x} \star (x \cdot z)$$

  for all $x, y, z \in G$.

The thing we will generalise to here is quite a different beast!

The Holomorph

Definition

The Holomorph of a group $(G, \star)$ is the semidirect product

$$\mathrm{Hol}_\star(G) = (G, \star) \rtimes \mathrm{Aut}_\star(G).$$

The elements of $\mathrm{Hol}_\star(G)$ are pairs (x, α), with $x \in G$ and $\alpha \in \mathrm{Aut}_\star(G)$, and multiplication is given by

$$(x, \alpha)(y, \beta) = (x \star \alpha(y), \alpha\beta).$$

The holomorph as an actor

The holomorph (and therefore its subgroups) come with an action on the group from which it came, given by

$$(x, \alpha)y = x \star \alpha(y).$$

Things means we can ask if a subgroup of the holomorph $A \subseteq \mathrm{Hol}_\star(G)$ acts

- *transitively*, i.e. for all $x, y \in G$ there exists $(z, \alpha) \in A$ such that $(z, \alpha)x = y$;
- *regularly*, i.e. acts transitively and $|A| = |G|$.

We say that $A \subseteq \mathrm{Hol}_\star(G)$ is *transitive* (resp. *regular*) if it acts transitively (resp. regularly).

Examples

Examples

Take $(G, \star)$ to be the cyclic group of order n, with generator η.

- We could simply and take $G \rtimes id$, this would give us a regular subgroup.
- We could add in the inversion map ι to give $G \rtimes \langle \iota \rangle$, we then have merely a transitive subgroup.
- If we know that n is the product of odd primes pq, then we have $\langle \eta^q, (\eta^p, \alpha) \rangle$ is a regular subgroup where α is an automorphism of $\langle \eta^q \rangle$ of order a power of q. [Darlington, 2023]

The λ-function of a skew brace

Definition/Proposition (Guarnieri and Vendramin, 2017)

Let $(G, \star, \cdot)$ be a skew brace. Define the map $\lambda : G \to \mathrm{Perm}(G)$, taking $x \mapsto \lambda_x$, by

$$\lambda_x(y) = \bar{x} \star (x \cdot y).$$

Then,

- λ is in fact a group homomorphism, i.e. $\lambda_{xy} = \lambda_x \lambda_y$;
- $\lambda(G) \subseteq \mathrm{Aut}(G)$.

We call this map the λ-*function* of the skew brace.

This is central to producing both a solution and a subgroup of the holomorph from a skew brace.

Skew brace to solution

Theorem (Lu, Yan, and Zhu, 2000)

Let G be a group and suppose we have functions $\lambda : G \to \mathrm{Perm}(G)$ and $\rho : G \to \mathrm{Perm}(G)$ such that for all $x, y \in G$ we have

- $\lambda_{xy} = \lambda_x \lambda_y$ (i.e. λ is a homomorphism);
- $\rho_{xy} = \rho_y \rho_x$ (i.e. ρ is an anti-homomorphism);
- $\lambda_x(y)\rho_y(x) = xy$.

Let $r(x, y) = (\lambda_x(y), \rho_y(x))$, then G with r is a bijective non-degenerate solution.

Theorem (Childs, 2022)

Let $(G, \star, \cdot)$ be a skew brace and consider the map $r(x, y) = (\lambda_x(y), \rho_y(x))$ where λ is simply the $\lambda-$function of the skew brace and $\rho_y(x) := \lambda_x(y)^{-1}xy$. Then G with r is a bijective non-degenerate solution.

Skew braces and the holomorph

Theorem (Guarnieri and Vendramin, 2017)

Given a group $(G, \star)$, there is a bijection between operations $\cdot$ on G such that $(G, \star, \cdot)$ is a skew brace and regular subgroups of $\mathrm{Hol}_\star(G)$

Sketch Proof.

Given a skew brace $(G, \star, \cdot)$, the subset $A := \{(x, \lambda_x) \mid x \in G\}$ of $\mathrm{Hol}_\star(G)$ is in fact a regular subgroup.

Conversely, given a regular subgroup A of $\mathrm{Hol}_\star(G)$ we have a bijection $a : (x, \alpha) \mapsto (x, \alpha)e = x$. We can use this to define an operation in G given by

$$x \cdot y := a^{-1}(x)y,$$

under which $(G, \star, \cdot)$ is a skew brace. □

Outline

Skew Bracoids

Definition

A *skew bracoid* is a 5-tuple $(G, \cdot, N, \star, \odot)$, where $(G, \cdot)$ and $(N, \star)$ are groups and $\odot$ is a transitive action of G on N for which

$$x \odot (\eta \star \mu) = (x \odot \eta) \star (x \odot e_N)^{-1} \star (x \odot \mu),$$

for all $x \in G$ and $\eta, \mu \in N$.

- We will frequently write $(G, N, \odot)$, for $(G, \cdot, N, \star, \odot)$.
- We will refer to $(N, \star)$ as the additive group and $(G, \cdot)$ as the multiplicative or acting group.

Examples

Examples

- Any skew brace $(G, \star, \cdot)$, is also a skew bracoid $(G, \cdot, G, \star, \odot)$ where the action $x \odot y := x \cdot y$.
- Let $d, n \in \mathbb{N}$ such that $d|n$. Take $G = \langle r, s \mid r^n = s^2 = e, srs^{-1} = r^{-1} \rangle \cong D_n$ and $N = \langle \eta \rangle \cong C_d$. Then we get a skew bracoid $(G, N, \odot)$ for $\odot$ given by

$$r^i s^j \odot \eta^k = \eta^{i+(-1)^j k}.$$

The λ-function of a skew bracoid

Definition/Proposition

Let $(G, N, \odot)$ be a skew bracoid. Define the map $\lambda : G \to \mathrm{Perm}(N)$, taking $x \mapsto \lambda_x$, by

$$\lambda_x(\eta) = (x \odot e_N)^{-1}(x \odot \eta).$$

Then,

- λ is in fact a group homomorphism, i.e. $\lambda_{xy} = \lambda_x \lambda_y$;
- $\lambda(G) \subseteq \mathrm{Aut}(N)$.

We call this map the λ-*function* of the skew bracoid.

Examples of $\lambda-$functions

Examples

- If we have a skew bracoid $(G, \cdot, G, \star, \odot)$ then its $\lambda-$function is precisely what we would have got by viewing it as the skew brace $(G, \star, \cdot)$.
- In the $G = \langle r, s \rangle \cong D_n$ acting on $N = \langle \eta \rangle \cong C_d$ example we have

$$\begin{aligned} \lambda_{r^i s^j}(\eta^k) &= (r^i s^j \odot e)^{-1}(r^i s^j \odot \eta^k) \\ &= (\eta^i)^{-1}\eta^{i+(-1)^j k} \\ &= \eta^{(-1)^j k}. \end{aligned}$$

This is either inversion, when s is present, or the identity on N.

Outline

The restriction needed for a solution

Here we have to add in those restrictions. Let $(G, N, \odot)$ be a skew bracoid and let $S = \mathrm{Stab}_G(e_N)$. We require that there is a complement H to S in G, so that G decomposes in an exact factorisation $G = HS$ (i.e. all $x \in G$ can be written as a product of some $h \in H$ and some $s \in S$, and $H \cap S = e$).

With this assumption we see

- Since $G = HS$ and G acts transitively on N we know that

$$N = G \odot e_N = HS \odot e_N = H \odot e_N,$$

  so that H acts transitively on N as well.
- Also, $|G| = |H||S|$ as $G = HS$ and $|G| = |N||S|$ by the Orbit-Stabiliser theorem so $|H| = |N|$. This means H acts regularly on N and the map $b : h \mapsto h \odot e_N$ is a bijection.

In our example

Example

Consider our $G = \langle r, s \rangle \cong D_n$ acting on $N = \langle \eta \rangle \cong C_n$ example, note that we have fixed $d = n$. Here

$$r^i s^j \odot e_N = \eta^{i+(-1)^j \cdot 0} = \eta^i,$$

so $S := \mathrm{Stab}_G(e_N) = \langle s \rangle$.

Let $R := \langle r \rangle$, then given the presentation of G we know $G = RS$. Hence we are in the required case.

See also that here $b : r^i \mapsto \eta^i$.

What we need to get a solution

The result of Lu, Yan, and Zhu works in a more general setting than previously stated.

Theorem

Given functions $\lambda : G \to \mathrm{Map}(G)$ and $\rho : G \to \mathrm{Map}(G)$ such that for all $x, y \in G$ we have

- $\lambda_{xy} = \lambda_x \lambda_y$ (i.e. λ is a homomorphism);
- $\rho_{xy} = \rho_y \rho_x$ (i.e. ρ is an anti-homomorphism);
- $\lambda_x(y)\rho_y(x) = xy$.

Let $r(x, y) = (\lambda_x(y), \rho_y(x))$, then G with r is a solution.

Skew bracoid to solution

Let $(G, N, \odot)$ be a skew bracoid with $G = HS$, where $S = \mathrm{Stab}_G(e_N)$. We will sketch how we can use the structure of a skew bracoid (of this form) to give a solution on the acting group. We have to reconcile the fact the $\lambda-$function maps into $\mathrm{Aut}(N)$. For this we use the bijection $b : H \to N$ given by $h \mapsto h \odot e_N$.

Proposition (Colazzo, Koch, M-L, and Truman, soon?)

Define the map $\hat{\lambda} : G \to \mathrm{Map}(G)$ by $\hat{\lambda}_x(y) = b^{-1}\lambda_x(y \odot e_N)$. Then for all $x, y \in G$,

- $\hat{\lambda}_{xy} = \hat{\lambda}_x\hat{\lambda}_y$,
- $\hat{\lambda}_x(G) = H$.

Skew bracoid to solution

We can define ρ from this $\hat{\lambda}$ in exactly the same way as before.

Proposition (Colazzo, Koch, M-L, and Truman, soon?)

Define the map $\rho : G \to \mathrm{Map}(G)$ by $\rho_y(x) := \hat{\lambda}_x(y)^{-1}xy$, where $\hat{\lambda}$ is as on the previous slide. Then for all $x, y \in G$,

- $\rho_{xy} = \rho_y \rho_x$,
- $\rho_x(G) = G$.

Hence we get a left-degenerate, right non-degenerate solution!

Running Example

Example

In our running example

$$\begin{aligned}\hat{\lambda}_{r^i s^j}(r^k s^\ell) &= b^{-1}\lambda_{r^i s^j}(\eta^k) \\ &= b^{-1}(\eta^{(-1)^j k}) \\ &= r^{(-1)^j k}.\end{aligned}$$

From this we get

$$\begin{aligned}\rho_{r^k s^\ell}(r^i s^j) &= \hat{\lambda}_{r^i s^j}(r^k s^\ell)^{-1} r^i s^j r^k s^\ell \\ &= r^{(-1)^j k} r^{i+(-1)^j k} s^{j+\ell} \\ &= r^i s^{j+\ell}.\end{aligned}$$

Hence $r(r^i s^j, r^k s^\ell) = (r^{(-1)^j k}, r^i s^{j+\ell})$ is a solution.

Skew Bracoids in the Holomorph

Proposition

Let N be a group. We have a correspondence between

- skew bracoids $(G, N, \odot)$,
- and transitive subgroups A of $\mathrm{Hol}(N)$.

Sketch Proof.

Given a skew bracoid $(G, N, \odot)$, the subset $A := \{(x \odot e_N, \lambda_x) \mid x \in G\}$ of $\mathrm{Hol}(N)$ is in fact a transitive subgroup of $\mathrm{Hol}(N)$.

Conversely any transitive subgroup A of $\mathrm{Hol}(N)$ can be packaged up with N itself to form a skew bracoid $(A, N, \odot)$, with all the obvious operations. $\square$

An old friend

Example

Consider our favourite example, with $G \cong D_n$ and $N \cong C_n$. We are expecting to land on a transitive subgroup of $\mathrm{Hol}(N)$ isomorphic to G.

Following the sketch we take

$$\begin{aligned} A &= \{(r^i s^j \odot e_N, \lambda_{r^i s^j}) \mid r^i s^j \in G\} \\ &= \{(\eta^i, \lambda_{r^i s^j}) \mid 0 \le i < n, j = 0, 1\} \\ &= \{(\eta^i, \iota^j) \mid 0 \le i < n, j = 0, 1\} \\ &= N \rtimes \langle \iota \rangle. \end{aligned}$$

Which subgroups of the holomorph lead to solutions?

In the holomorph the stabiliser of the identity consists precisely of those elements with identity in the N position, i.e. elements like (e_N, α). So we are looking for $A \subseteq \mathrm{Hol}(N)$ with $A = BC$ where $C = A \cap (e_N, \mathrm{Aut}(N))$.

Observations

- By the same argument as for the $G = HS$ assumption, B must be a regular subgroup of $\mathrm{Hol}(N)$. Conversely, if we take some B with a subgroup of $\mathrm{Aut}(N)$, we will certainly get a transitive subgroup.
- It's not quite that simple because adding particular automorphisms to particular B's might lead to more purely automorphism elements.
- That said, there is a wealth of classifications of regular subgroups of the holomorph (e.g. [Byo04], [AB18], [CCD20]) so these could be extended to the transitive subgroups we care about, without the need to find all the transitive subgroups.

Further Questions

- Can we relax our condition on the skew bracoid further? (We think not, at least not without changing the approach considerably.)
- It is clear that our solution is in some sense a solution from a skew brace with some extra degenerate piece. Can we formalise this relationship?
- What qualitative information carries through these three settings? Are there properties that are significantly easier to prove in one setting?
- Is it finally time to start using GAP or Magma to get our hands on some more examples?

Thank you for your attention!

References I

L. Guarnieri and L. Vendramin. Skew braces and the Yang–Baxter equation. *Mathematics of Computation*, 86(307):2519–2534, 2017. ISSN 1088-6842. doi: 10.1090/mcom/3161. URL http://dx.doi.org/10.1090/mcom/3161.

Andrew Darlington. Hopf-Galois structures on separable field extensions of degree *pq*, 2023.

Jiang-Hua Lu, Min Yan, and Yong-Chang Zhu. On the set-theoretical Yang-Baxter equation. *Duke Mathematical Journal*, 104(1):1 – 18, 2000. doi: 10.1215/S0012-7094-00-10411-5. URL https://doi.org/10.1215/S0012-7094-00-10411-5.

Lindsay N. Childs. Skew left braces and the yang-baxter equation, 2022.

References II

Nigel P. Byott. Hopf–Galois structures on Galois field extensions of degree pq. *Journal of Pure and Applied Algebra*, 188(1):45–57, 2004. ISSN 0022-4049. doi: https://doi.org/10.1016/j.jpaa.2003.10.010. URL https://www.sciencedirect.com/science/article/pii/S0022404903002160.

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. ISSN 0021-8693. doi: https://doi.org/10.1016/j.jalgebra.2017.09.009. URL https://www.sciencedirect.com/science/article/pii/S0021869317304969.

E. Campedel, A. Caranti, and I. Del Corso. Hopf-Galois structures on extensions of degree p2q and skew braces of order p2q: The cyclic Sylow p-subgroup case. *Journal of Algebra*, 556:1165–1210, 2020. ISSN 0021-8693. doi: https://doi.org/10.1016/j.jalgebra.2020.04.009. URL https://www.sciencedirect.com/science/article/pii/S0021869320301770.