Classifying bidihedral skew braces
Part I: constraints and necessary conditions

Paul Truman

Keele University, UK

Hopf algebras and Galois module theory

Agnes Scott College, May 2026

Overview

- Joint work with Alan Koch.

Aim

Classify skew braces $(G, \bullet, \circ)$ in which $G^\bullet \cong G^\circ \cong D_n$ for some n. We call such skew braces **bidihedral**. In this talk we will focus on the conditions and constraints that a bidihedral skew brace must satisfy.

- Skew braces, γ-functions, ideals
- An important ideal $(H, \bullet, \circ)$ in a bidihedral skew brace $(G, \bullet, \circ)$
- If $(G, \bullet, \circ)$ is bidihedral and H° is cyclic then ...
- If $(G, \bullet, \circ)$ is bidihedral and H° is dihedral then ...

Our favourite circle of ideas

Let G, N be finite groups of the same order.

There are correspondences between:

- Regular subgroups of $\mathrm{Perm}(G)$ isomorphic to N and normalized by $\lambda(G)$;
- Regular subgroups of $\mathrm{Hol}(N)$ isomorphic to G;
- Hopf-Galois structures of type N on a G-Galois extension;
- Skew braces with multiplicative group isomorphic to G and additive group isomorphic to N.

It is natural to classify or enumerate the possibilities for given combinations of G and N.

For instance: what if $G \cong N \cong D_n$ (order $2n$)?

A bidihedral classification

Theorem (Kohl, 2020)

Let $n \in \mathbb{N}$, let $K_n = \{k \in \mathbb{Z}_n \mid k^2 \equiv 1 \pmod{n}\}$, and let $\kappa_n = |K_n|$. Then the number of Hopf-Galois structures of type D_n on a D_n-Galois extension is

$$\begin{cases} \kappa_n & \text{if } n \equiv 1,3,5,7 \pmod 8 \\ (n+1)\,\kappa_n & \text{if } n \equiv 2,6 \pmod 8 \\ \left(\frac{n}{2}+1\right)\,\kappa_n & \text{if } n \equiv 4 \pmod 8 \\ \left(\frac{n}{2}+2\right)\,\kappa_n & \text{if } n \equiv 0 \pmod 8. \end{cases}$$

We seek the equivalent classification of skew braces.

Why not extract information from Kohl's results?

Skew braces and their γ-functions

Definition

A **Skew (left) brace** is a triple $(G, \bullet, \circ)$ in which $G^\bullet$ and G° are groups and

$$x \circ (yz) = (x \circ y)x^{-1}(x \circ z) \text{ for all } x, y, z \in G.$$

Here x^{-1} denotes the inverse of x in $G^\bullet$.

The two group structures in a skew brace share the same identity element $e \in G$, but inverse may differ: the inverse of x in G° is denoted $\overline{x}$.

If $(G, \bullet, \circ)$ is a skew brace then for each $x \in G$ the function defined by $\gamma_x(y) = x^{-1}(x \circ y)$ is an automorphism of $G^\bullet$.

The function $x \mapsto \gamma_x$ is a homomorphism from G° into $\mathrm{Aut}(G^\bullet)$, called the γ-**function** of the skew brace.

An ideal situation

The γ-function of a skew brace relates the two operations: we have

$$x \circ y = x\gamma_x(y).$$

Hence the γ-function determines $\circ$.

It can also be used to characterize substructures such as **ideals** (kernels of skew brace homomorphisms):

A subset H of G is an ideal if and only if

- $\gamma_x(y) \in H$ for all $x \in G$ and $y \in H$;
- $H^\bullet \trianglelefteq G^\bullet$;
- $H^\circ \trianglelefteq G^\circ$.

If H satisfies the first condition and is a subgroup with respect to one operation then it is a subgroup with respect to the other.

Still have to check normality!

An important ideal in a bidihedral skew brace

Let $G = (G, \bullet, \circ)$ be a bidihedral skew brace of order $2n$, and write

$$G^\bullet = \langle r, s \mid r^n = s^2 = e,\ srs^{-1} = r^{-1} \rangle.$$

Proposition

Let $H = \langle r \rangle_\bullet$. Then H is an ideal of G.

Proof.

Clearly $H^\bullet \leq G^\bullet$; in fact it is characteristic.

Hence $\gamma_x(y) \in H$ for all $x \in G$ and $y \in H$, and $H^\bullet \trianglelefteq G^\bullet$.

It follows that $H^\circ \leq G^\circ$. Since it has index 2, it is normal. □

- $(H, \bullet, \circ)$ is an ideal of G with $H^\bullet$ cyclic and H° cyclic or dihedral.
- Strategy: apply existing classification results to H and investigate additional constraints arising from the fact that H embeds and an ideal in G.

The case H° cyclic

Proposition (Rump, 2007)

The circle operations on $H^\bullet$ such that $(H, \bullet, \circ)$ is a skew brace with H° cyclic are precisely

$$r^i \circ r^j = r^{i+j+dij}$$

where

- d divides n;
- every prime number dividing n also divides d;
- if $4 \mid n$ then $4 \mid d$.

H° cyclic: constraints on the γ-function

Recall: $r^i \circ r^j = r^{i+j+dij}$ with $d \mid n$, $p \mid d$ for all $p \mid n$, and $4 \mid d$ if $4 \mid n$.

Question

What additional constraints arise from the fact that H is embedded as an ideal in G?

- H° is also the rotations in G°, and is generated by r.
- Hence s is a reflection in G°, and G° is generated by r and s.
- The γ-function of $(G, \bullet, \circ)$ is determined by

$$\gamma_r(r),\ \gamma_r(s),\ \gamma_s(r),\ \gamma_s(s).$$

H° cyclic: constraints on the γ-function

Recall: $r^i \circ r^j = r^{i+j+dij}$ with $d \mid n$, $p \mid d$ for all $p \mid n$, and $4 \mid d$ if $4 \mid n$.

Lemma

$\gamma_r(r) = r^{1+d}$.

Proof.

From the definition we have $\gamma_r(r) = r^{-1}(r^{1+1+d}) = r^{1+d}$. □

Lemma

$\gamma_s(s) = s$.

Proof.

Recall that s is a reflection in both $G^\bullet$ and G°.

From the definition we have $\gamma_s(s) = s^{-1}(s \circ s) = s^{-1}e = s$. □

H° cyclic: constraints on the γ-function

Lemma

$\gamma_s(r) = r^k$ *with* $k^2 \equiv 1 \pmod{n}$.

Proof.

We have $\gamma_s(r) = r^k$ for some k coprime to n, but

$$\gamma_s^2(r) = \gamma_{s\circ s}(r) = \gamma_e(r) = r,$$

so in fact $k^2 \equiv 1 \pmod{n}$. □

- We still need to determine $\gamma_r(s)$.
- Before we do this, we derive some constraints on d.

H° cyclic: constraints on d

Lemma

$$d = \begin{cases} n \text{ or } n/2 & \text{if } n \equiv 0 \pmod 8 \\ n & \text{otherwise.} \end{cases}$$

Recall $d \mid n$, $p \mid n \Rightarrow p \mid d$, $4 \mid n \Rightarrow 4 \mid d$.

Proof.

We have $s \circ r = \overline{r} \circ s$, so $\gamma_s\gamma_r(r) = \gamma_{s\circ r}(r) = \gamma_{\overline{r}\circ s}(r) = \gamma_r^{-1}\gamma_s(r)$.

Thus $r^{k(1+d)} = r^{k(1+d)^{-1}}$, so $(1+d)^2 \equiv 1 \pmod n$.

Hence $d(d+2) \equiv 0 \pmod n$.

Write $n = 2^\ell m$ with m odd.

Then $d \equiv 0 \pmod m$, and $d \equiv 0 \pmod{2^\ell}$ unless $\ell \geq 3$, when $d \equiv 2^{\ell-1} \pmod{2^\ell}$ is also possible. □

H° cyclic: final constraint on the γ-function

Recall: $d = n$ or $n/2$,

$\gamma_r(r) = r^{1+d}$, $\gamma_s(s) = s$, $\gamma_s(r) = r^k$ with $k^2 \equiv 1 \pmod{n}$.

Lemma

$\gamma_r(s) = r^{(1+d)k-1}s$.

Proof.

From the definition we have $\gamma_r(s) = r^{-1}(r \circ s) = r^{-1}(s \circ \overline{r})$.

Using the information we have derived about d, we find $\overline{r} = r^{-(1+d)}$.

Hence

$$\gamma_r(s) = r^{-1}(s \circ r^{-(1+d)}) = r^{-1}s\gamma_s(r)^{-(1+d)}.$$

We know $\gamma_s(r) = r^k$, so

$$\gamma_r(s) = r^{-1}sr^{-(1+d)k} = r^{(1+d)k-1}s.$$

Summary for H° cyclic

Let $(G, \bullet, \circ)$ be a bidihedral skew brace.

Write $G^\bullet = \langle r, s \rangle$, let $H = \langle r \rangle$, and suppose that H° is cyclic.

Then G° is also generated by r and s and

$$\begin{aligned}
\gamma_s(r) &= r^k \text{ with } k^2 \equiv 1 \pmod{n} \\
\gamma_s(s) &= s \\
\gamma_r(r) &= r^{1+d} \\
\gamma_r(s) &= r^{(1+d)k-1}s,
\end{aligned}$$

where

$$d = \begin{cases} n \text{ or } n/2 & \text{if } n \equiv 0 \pmod{8} \\ n & \text{otherwise.} \end{cases}$$

Question

Which of these can we realize? What are the isomorphism classes?

The case H° dihedral

Recall $|G| = 2n$; write $n = |H| = 2^\ell m$ with m odd. Suppose $\ell \geq 1$.

Proposition (Byott and Ferri, 2025)

A circle operation on $H^\bullet$ such that $(H, \bullet, \circ)$ is a skew brace with H° dihedral is given by

$$r^i \circ r^j = r^{i+(-1)^i j}. \tag{1}$$

If $\ell \neq 2$ then this is the only possibility.

If $\ell = 2$ then there are two further possibilities:

$$r^{4i_4+mi_m} \circ r^{4j_4+mj_m} = r^{4(i_4+(-1)^{\frac{i_m(i_m \pm 1)}{2}} j_4)+m(i_4+(-1)^{i_4} j_4)}. \tag{2}$$

Lemma

There is no bidihedral skew brace $(G, \bullet, \circ)$ of order $8m$ that yields either of the circle operations of type (2) on H.

The case H° dihedral

Lemma

There is no bidihedral skew brace $(G, \bullet, \circ)$ of order $8m$ such that

$$r^{4i_4+mi_m} \circ r^{4j_4+mj_m} = r^{4(i_4+(-1)^{\frac{i_m(i_m-1)}{2}}j_4)+m(i_4+(-1)^{i_4}j_4)}.$$

Proof.

If so, the element r^{4+m} has order $2m$ in G°.

Hence there exists $a \in G - H$ such that $a \circ a = r^{4+m}$.

Now consider $a \circ a \circ r^m$.

We have $a \circ a \circ r^m = r^{4+m} \circ r^m = r^4$.

But also, using $a \circ r^m = a\gamma_a(r)^m$, we find $a \circ a \circ r^m = r^4 r^{m(1+u^2)}$ for some $u \in \mathbb{Z}$.

Hence $m(1+u^2) \equiv 0 \pmod{4m}$, so $1+u^2 \equiv 0 \pmod 4$, a contradiction. $\square$

The case H° dihedral

The circle operation on H is $r^i \circ r^j = r^{i+(-1)^i j}$.

- We find that r is a reflection in H°; write $b = r$.
- We find that r^2 has order $n/2$ in H°.

  Hence there exists $a = r^\alpha s \in G$ such that $a \circ a = r^2$.
- Then a, b generate G° and $G^\bullet$ (for different reasons).
- As before, the skew brace $(G, \bullet, \circ)$ is determined by

$$\gamma_a(a),\ \gamma_a(b),\ \gamma_b(a),\ \gamma_b(b).$$

- We find:

$$\begin{aligned} \gamma_a(a) &= b^{-2}a, \quad & \gamma_a(b) &= b^k \text{ with } k^2 \equiv 1 \pmod{n}, \\ \gamma_b(a) &= b^{k-1}a, & \gamma_b(b) &= b^{-1}. \end{aligned}$$

Question

Which of these can we realize? What are the isomorphism classes?

Thank you for your attention.