On the number of quaternionic and dihedral braces

Fabio Ferri

joint with Nigel Byott

20th June 2023

Braces

Braces

Definition

Let A be a set with two operation $+$ and $\circ$ such that $(A, +)$ is an abelian group and $(A, \circ)$ is a group. $(A, +, \circ)$ is called (left) *brace* if $x \circ (y + z) = (x \circ y) - x + (x \circ z)$.

Braces

Definition

Let A be a set with two operation $+$ and $\circ$ such that $(A, +)$ is an abelian group and $(A, \circ)$ is a group. $(A, +, \circ)$ is called (left) *brace* if $x \circ (y + z) = (x \circ y) - x + (x \circ z)$.

Why are they important?

Braces

Definition

Let A be a set with two operation $+$ and $\circ$ such that $(A, +)$ is an abelian group and $(A, \circ)$ is a group. $(A, +, \circ)$ is called (left) *brace* if $x \circ (y + z) = (x \circ y) - x + (x \circ z)$.

Why are they important?

- They provide non-degenerate involutive solutions of the Yang–Baxter equation.

Braces

Definition

Let A be a set with two operation $+$ and $\circ$ such that $(A, +)$ is an abelian group and $(A, \circ)$ is a group. $(A, +, \circ)$ is called (left) *brace* if $x \circ (y + z) = (x \circ y) - x + (x \circ z)$.

Why are they important?

- They provide non-degenerate involutive solutions of the Yang–Baxter equation.
- There is a (non-bijective) correspondence between braces of additive group N and multiplicative group G with the Hopf–Galois structures of type N on a Galois extension of Galois group G.

Braces

Definition

Let A be a set with two operation $+$ and $\circ$ such that $(A, +)$ is an abelian group and $(A, \circ)$ is a group. $(A, +, \circ)$ is called (left) *brace* if $x \circ (y + z) = (x \circ y) - x + (x \circ z)$.

Why are they important?

- They provide non-degenerate involutive solutions of the Yang–Baxter equation.
- There is a (non-bijective) correspondence between braces of additive group N and multiplicative group G with the Hopf–Galois structures of type N on a Galois extension of Galois group G. Ideas from Greither/Pareigis and Byott, originally meant for Hopf–Galois structures, allow us to count and classify (skew) braces.

A conjecture by Guarnieri and Vendramin

A conjecture by Guarnieri and Vendramin

Conjecture

Let $m \geq 3$ be an integer and let $q(4m)$ be the number of isomorphism classes of left braces with multiplicative group isomorphic to Q_{4m}. Then

$$q(4m) = \begin{cases} 2 & \textit{if } 2 \nmid m \\ 6 & \textit{if } 2 \mid\mid m \\ 9 & \textit{if } 4 \mid\mid m \\ 7 & \textit{if } 8 \mid m. \end{cases}$$

A conjecture by Guarnieri and Vendramin

Conjecture

Let $m \geq 3$ be an integer and let $q(4m)$ be the number of isomorphism classes of left braces with multiplicative group isomorphic to Q_{4m}. Then

$$q(4m) = \begin{cases} 2 & \text{if } 2 \nmid m \\ 6 & \text{if } 2 \mid\mid m \\ 9 & \text{if } 4 \mid\mid m \\ 7 & \text{if } 8 \mid m. \end{cases}$$

Rump (2020) proved the conjecture when m is a power of 2.

A conjecture by Guarnieri and Vendramin

Conjecture

Let $m \geq 3$ be an integer and let $q(4m)$ be the number of isomorphism classes of left braces with multiplicative group isomorphic to Q_{4m}. Then

$$q(4m) = \begin{cases} 2 & \textit{if } 2 \nmid m \\ 6 & \textit{if } 2 \mid\mid m \\ 9 & \textit{if } 4 \mid\mid m \\ 7 & \textit{if } 8 \mid m. \end{cases}$$

Rump (2020) proved the conjecture when m is a power of 2.
We will prove the conjecture in full generality with explicit methods.
Furthermore, we will prove the analogous result for dihedral groups.

Preliminary material pt I

Preliminary material pt I

Theorem

Let G be a finite group and let N be a finite abelian group such that $|N| = |G|$. Then the number of isomorphism classes of braces with additive group N and multiplicative group G is equal to the number of conjugacy classes of regular subgroups of $\mathrm{Hol}(N) = N \rtimes \mathsf{Aut}(N)$ isomorphic to G.

Preliminary material pt I

Theorem

Let G be a finite group and let N be a finite abelian group such that $|N| = |G|$. Then the number of isomorphism classes of braces with additive group N and multiplicative group G is equal to the number of conjugacy classes of regular subgroups of $\mathrm{Hol}(N) = N \rtimes \mathsf{Aut}(N)$ isomorphic to G.

Lemma

Let $N = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$. Then an element of $\mathrm{Hol}(N)$ can be represented as

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix},$$

where A is a matrix in $(p^{\max\{0,a_i-a_j\}}(\mathbb{Z}/p^{a_r}\mathbb{Z}))_{1\leq i,j\leq n}$ whose reduction is in $\mathrm{GL}_r(\mathbb{F}_p)$ and $v \in N$. Precisely, we need to quotient by $(p^{a_i}(\mathbb{Z}/p^{a_r}\mathbb{Z}))_{i,j}$.

Preliminary material pt II

Preliminary material pt II

$$n \geq 2:$$

$$G = Q_{2^n s} = \langle x, y : x^{2^{n-1}s} = 1, yx = x^{-1}y, y^2 = x^{2^{n-2}s} \rangle$$

or

$$G = D_{2^n s} = \langle x, y : x^{2^{n-1}s} = 1, yx = x^{-1}y, y^2 = 1 \rangle$$

Preliminary material pt II

$$n \geq 2 :$$

$$G = Q_{2^n s} = \langle x, y : x^{2^{n-1}s} = 1, yx = x^{-1}y, y^2 = x^{2^{n-2}s} \rangle$$

or

$$G = D_{2^n s} = \langle x, y : x^{2^{n-1}s} = 1, yx = x^{-1}y, y^2 = 1 \rangle$$

Lemma

The 2-Sylow subgroups of G are quaternionic or dihedral, respectively. If G_2 is any 2-Sylow subgroup of G, we can write $G \cong C_s \rtimes G_2$. There is only one possible subgroup of G of order s, which is normal and generated by $x^{2^{n-1}}$.

2-power case: a restriction on the possible additive groups

2-power case: a restriction on the possible additive groups

Proposition

Let $n \geq 5$. Then there is no quaternionic or dihedral left brace of type C_2^n.

2-power case: a restriction on the possible additive groups

Proposition

Let $n \geq 5$. Then there is no quaternionic or dihedral left brace of type C_2^n.

Proof.

No element of order 2^{n-1} in $\mathrm{GL}_{n+1}(\mathbb{F}_2)$. □

2-power case: a restriction on the possible additive groups

Proposition

Let $n \geq 5$. Then there is no quaternionic or dihedral left brace of type C_2^n.

Proof.

No element of order 2^{n-1} in $\mathrm{GL}_{n+1}(\mathbb{F}_2)$. $\square$

Lemma

Let X be a matrix of 2-power order in $\mathrm{Mat}_{r+1}(\mathbb{Z}/2^d\mathbb{Z})$. Then $X^{2^{t+d-1}} = I$, where $t = \lceil \log_2(r+1) \rceil$.

2-power case: a restriction on the possible additive groups

Proposition

Let $n \geq 5$. Then there is no quaternionic or dihedral left brace of type C_2^n.

Proof.

No element of order 2^{n-1} in $\mathrm{GL}_{n+1}(\mathbb{F}_2)$. $\square$

Lemma

Let X be a matrix of 2-power order in $\mathrm{Mat}_{r+1}(\mathbb{Z}/2^d\mathbb{Z})$. Then $X^{2^{t+d-1}} = I$, where $t = \lceil \log_2(r+1) \rceil$.

- C_{2^n} for $n \geq 2$;
- $C_2 \times C_{2^{n-1}}$ for $n \geq 2$;
- $C_4 \times C_{2^{n-2}}$ for $n \geq 4$;
- $C_2 \times C_2 \times C_{2^{n-2}}$ for $n \geq 3$;
- $C_2 \times C_2 \times C_2 \times C_{2^{n-3}}$ for $n \geq 4$.

Type C_{2^n}, $n \geq 4$

Type C_{2^n}, $n \geq 4$

$$X = \begin{pmatrix} \alpha & v \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} \beta & w \\ 0 & 1 \end{pmatrix}$$

with $\alpha, \beta \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ and $v, w \in \mathbb{Z}/2^n\mathbb{Z}$ with the following relations: $X^{2^{n-1}} = I$, $X^{2^{n-2}} \neq I$, $YX = X^{-1}Y$ and either $Y^2 = X^{2^{n-2}}$ or $Y^2 = I$.

Type C_{2^n}, $n \geq 4$

$$X = \begin{pmatrix} \alpha & v \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} \beta & w \\ 0 & 1 \end{pmatrix}$$

with $\alpha, \beta \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ and $v, w \in \mathbb{Z}/2^n\mathbb{Z}$ with the following relations: $X^{2^{n-1}} = I$, $X^{2^{n-2}} \neq I$, $YX = X^{-1}Y$ and either $Y^2 = X^{2^{n-2}}$ or $Y^2 = I$.
We can only have

$$X = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} -1 + 2^{n-1} & 1 \\ 0 & 1 \end{pmatrix}$$

or

$$X = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Type $C_2 \times C_{2^{n-1}}$, $n \geq 5$

Type $C_2 \times C_{2^{n-1}}$, $n \geq 5$

$$X = \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} B & w \\ 0 & 1 \end{pmatrix}$$

with $v = (v_1, v_2)^\top$ such that $v_1 \in \mathbb{Z}/2\mathbb{Z}$ and $v_2 \in \mathbb{Z}/2^{n-1}\mathbb{Z}$ (analogously for w), A and B are matrices in

$$\begin{pmatrix} 1 & \mathbb{Z}/2\mathbb{Z} \\ 2^{n-2}(\mathbb{Z}/2\mathbb{Z}) & (\mathbb{Z}/2^{n-1}\mathbb{Z})^\times \end{pmatrix},$$

and which satisfy $X^{2^{n-1}} = I$, $X^{2^{n-2}} \neq I$, $YX = X^{-1}Y$ and either $Y^2 = X^{2^{n-2}}$ or $Y^2 = I$.

Type $C_2 \times C_{2^{n-1}}$, $n \geq 5$

$$X = \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} B & w \\ 0 & 1 \end{pmatrix}$$

with $v = (v_1, v_2)^\top$ such that $v_1 \in \mathbb{Z}/2\mathbb{Z}$ and $v_2 \in \mathbb{Z}/2^{n-1}\mathbb{Z}$ (analogously for w), A and B are matrices in

$$\begin{pmatrix} 1 & \mathbb{Z}/2\mathbb{Z} \\ 2^{n-2}(\mathbb{Z}/2\mathbb{Z}) & (\mathbb{Z}/2^{n-1}\mathbb{Z})^\times \end{pmatrix},$$

and which satisfy $X^{2^{n-1}} = I$, $X^{2^{n-2}} \neq I$, $YX = X^{-1}Y$ and either $Y^2 = X^{2^{n-2}}$ or $Y^2 = I$. Modulo conjugation we can assume $v_1 = 0, v_2 = 1, w_1 = 1, w_2 = 0$.

Type $C_2 \times C_{2^{n-1}}$, $n \geq 5$

$$X = \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} B & w \\ 0 & 1 \end{pmatrix}$$

with $v = (v_1, v_2)^\top$ such that $v_1 \in \mathbb{Z}/2\mathbb{Z}$ and $v_2 \in \mathbb{Z}/2^{n-1}\mathbb{Z}$ (analogously for w), A and B are matrices in

$$\begin{pmatrix} 1 & \mathbb{Z}/2\mathbb{Z} \\ 2^{n-2}(\mathbb{Z}/2\mathbb{Z}) & (\mathbb{Z}/2^{n-1}\mathbb{Z})^\times \end{pmatrix},$$

and which satisfy $X^{2^{n-1}} = I$, $X^{2^{n-2}} \neq I$, $YX = X^{-1}Y$ and either $Y^2 = X^{2^{n-2}}$ or $Y^2 = I$. Modulo conjugation we can assume $v_1 = 0, v_2 = 1, w_1 = 1, w_2 = 0$. We find eight subgroups in each case, which will lie in six conjugacy classes.

On the non-2-power case

On the non-2-power case

$G \cong C_s \rtimes G_2$ is quaternionic or dihedral. $N \cong N_s \times N_2$ is abelian. We are looking for regular embeddings $G \to \mathrm{Hol}(N) \cong \mathrm{Hol}(N_s) \times \mathrm{Hol}(N_2)$.

On the non-2-power case

$G \cong C_s \rtimes G_2$ is quaternionic or dihedral. $N \cong N_s \times N_2$ is abelian. We are looking for regular embeddings $G \to \mathrm{Hol}(N) \cong \mathrm{Hol}(N_s) \times \mathrm{Hol}(N_2)$.
The map $G \to \mathrm{Hol}(N_2)$ is trivial on C_s. This and Schur-Zassenhaus tell us that the brace structure on N is a semidirect product of N_s and N_2.

On the non-2-power case

$G \cong C_s \rtimes G_2$ is quaternionic or dihedral. $N \cong N_s \times N_2$ is abelian. We are looking for regular embeddings $G \to \mathrm{Hol}(N) \cong \mathrm{Hol}(N_s) \times \mathrm{Hol}(N_2)$.
The map $G \to \mathrm{Hol}(N_2)$ is trivial on C_s. This and Schur-Zassenhaus tell us that the brace structure on N is a semidirect product of N_s and N_2.
By a result of Kohl (1998), N_s is cyclic. Then the map $G \to \mathrm{Aut}(N_s)$ is trivial on C_s (N_s is a trivial brace). The following result refines Crespo, Gil-Muñoz, Rio, Vela (2022).

On the non-2-power case

$G \cong C_s \rtimes G_2$ is quaternionic or dihedral. $N \cong N_s \times N_2$ is abelian. We are looking for regular embeddings $G \to \mathrm{Hol}(N) \cong \mathrm{Hol}(N_s) \times \mathrm{Hol}(N_2)$.

The map $G \to \mathrm{Hol}(N_2)$ is trivial on C_s. This and Schur-Zassenhaus tell us that the brace structure on N is a semidirect product of N_s and N_2.

By a result of Kohl (1998), N_s is cyclic. Then the map $G \to \mathrm{Aut}(N_s)$ is trivial on C_s (N_s is a trivial brace). The following result refines Crespo, Gil-Muñoz, Rio, Vela (2022).

Theorem

Let Q be a quaternionic or dihedral group of order $2^n s$. Then the number of conjugacy classes of regular subgroups G of $\mathrm{Hol}(N)$ isomorphic to Q is equal to the number of classes (G_2, τ), where G_2 runs over the regular subgroups of $\mathrm{Hol}(N_2)$ isomorphic to Q_2, and τ runs over $\tau : G_2 \to \mathrm{Aut}(N_s)$ such that $N_s \rtimes_\tau G_2 \cong Q$ modulo: (G_2, τ) is equivalent to (G_2', τ') if $\tau(\cdot) = \tau'(g \cdot g^{-1})$ for $g \in \mathrm{Aut}(N_2) \subseteq \mathrm{Hol}(N_2)$.

The final result

The final result

In most cases (quaternionic with $3 \neq n \geq 2$ or dihedral with $n \geq 3$), there is only one such τ modulo conjugate. Otherwise, we only have to look at Q_{24} and D_{12}.

The final result

In most cases (quaternionic with $3 \neq n \geq 2$ or dihedral with $n \geq 3$), there is only one such τ modulo conjugate. Otherwise, we only have to look at Q_{24} and D_{12}.

Theorem

Let $m \geq 3$ be an integer, let $q(4m)$ be the number of isomorphism classes of left braces with multiplicative group isomorphic to Q_{4m} and let $d(4m)$ be the number of isomorphism classes of left braces with multiplicative group isomorphic to D_{4m}. Then

$$q(4m) = \begin{cases} 2 & \textit{if } 2 \nmid m \\ 6 & \textit{if } 2 \mid\mid m \\ 9 & \textit{if } 4 \mid\mid m \\ 7 & \textit{if } 8 \mid m \end{cases} \quad d(4m) = \begin{cases} 3 & \textit{if } 2 \nmid m \\ 8 & \textit{if } 2 \mid\mid m \\ 7 & \textit{if } 4 \mid\mid m \\ 7 & \textit{if } 8 \mid m. \end{cases}$$

Hopf–Galois structures

Hopf–Galois structures

Proposition

Let G *be a finite group and let* N *be a finite abelian group such that* $|N| = |G|$. *Then the number of Hopf–Galois structures with Galois group* G *and type* N *is equal to the number of regular subgroups of* $\mathrm{Hol}(N) = N \rtimes \mathsf{Aut}(N)$ *isomorphic to* G *times* $\frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|}$.

Hopf–Galois structures

Proposition

Let G be a finite group and let N be a finite abelian group such that $|N| = |G|$. Then the number of Hopf–Galois structures with Galois group G and type N is equal to the number of regular subgroups of $\mathrm{Hol}(N) = N \rtimes \mathsf{Aut}(N)$ isomorphic to G times $\frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|}$.

Both the proofs and the MAGMA computations can be refined in order to find the actual number of regular subgroups.

Thanks for the attention!