Counting Quaternion and Dihedral Braces and the Associated Hopf-Galois Structures

Nigel Byott (University of Exeter)

joint work with Fabio Ferri

(funded by EPSRC grants EP/V005995/1 and EP/W52265X/1)

Omaha (virtually), 29 May 2024

Introduction

Conjecture: Guarnieri & Vendramin (2017):
Let $m \geq 3$ and let $q(4m)$ be the number of braces B whose multiplicative group $(B, \circ)$ is a generalised quaternion group of order $4m$. Then

$$q(4m) = \begin{cases} 2 & \text{if } m \text{ is odd}, \\ 7 & \text{if } m \equiv 0 \pmod 8, \\ 9 & \text{if } m \equiv 4 \pmod 8, \\ 6 & \text{if } m \equiv 2 \pmod 8 \text{ or } m \equiv 6 \pmod 8. \end{cases}$$

Introduction

Conjecture: Guarnieri & Vendramin (2017):
Let $m \geq 3$ and let $q(4m)$ be the number of braces B whose multiplicative group $(B, \circ)$ is a generalised quaternion group of order $4m$. Then

$$q(4m) = \begin{cases} 2 & \text{if } m \text{ is odd,} \\ 7 & \text{if } m \equiv 0 \pmod 8, \\ 9 & \text{if } m \equiv 4 \pmod 8, \\ 6 & \text{if } m \equiv 2 \pmod 8 \text{ or } m \equiv 6 \pmod 8. \end{cases}$$

Some remarks:
(1) This is about (classical) **braces**, i.e. the additive group is abelian
(2) Rump (2020) gave a partial proof, showing $q(2^n) = 7$ for $n \geq 5$.
(3) The "odd part" of m does not make a difference to $q(4m)$. Why?
(4) What about dihedral braces? What about Hopf-Galois structures?

Introduction

Conjecture: Guarnieri & Vendramin (2017):
Let $m \geq 3$ and let $q(4m)$ be the number of braces B whose multiplicative group $(B, \circ)$ is a generalised quaternion group of order $4m$. Then

$$q(4m) = \begin{cases} 2 & \text{if } m \text{ is odd,} \\ 7 & \text{if } m \equiv 0 \pmod 8, \\ 9 & \text{if } m \equiv 4 \pmod 8, \\ 6 & \text{if } m \equiv 2 \pmod 8 \text{ or } m \equiv 6 \pmod 8. \end{cases}$$

Some remarks:
(1) This is about (classical) **braces**, i.e. the additive group is abelian
(2) Rump (2020) gave a partial proof, showing $q(2^n) = 7$ for $n \geq 5$.
(3) The "odd part" of m does not make a difference to $q(4m)$. Why?
(4) What about dihedral braces? What about Hopf-Galois structures?

I will outline a full proof of the conjecture, with corresponding results for dihedral braces and for Hopf-Galois structures: details in the preprint B+Ferri (2024).

Counting braces and HGS via regular subgroups

If $(B, +, \circ)$ is a brace, we can embed $(B, \circ)$ into $\mathrm{Hol}(B, +) = B \rtimes \mathrm{Aut}(B)$ as a regular subgroup by $b \mapsto (b, \lambda_b)$ with $\lambda_b(c) = -b + b \circ c$.

Conversely, if G is a regular subgroup in $\mathrm{Hol}(N)$ for an abelian group $(N, +)$, write g_η for the unique element of G moving 0_N to η. Then B becomes a brace where $g_{\eta \circ \eta'} = g_\eta g'_\eta$. Two regular subgroups give isomorphic braces if they are conjugate by an element of $\mathrm{Aut}(N)$.

Counting braces and HGS via regular subgroups

If $(B, +, \circ)$ is a brace, we can embed $(B, \circ)$ into $\mathrm{Hol}(B, +) = B \rtimes \mathrm{Aut}(B)$ as a regular subgroup by $b \mapsto (b, \lambda_b)$ with $\lambda_b(c) = -b + b \circ c$. Conversely, if G is a regular subgroup in $\mathrm{Hol}(N)$ for an abelian group $(N, +)$, write g_η for the unique element of G moving 0_N to η. Then B becomes a brace where $g_{\eta \circ \eta'} = g_\eta g'_\eta$. Two regular subgroups give isomorphic braces if they are conjugate by an element of $\mathrm{Aut}(N)$.

The Hopf-Galois structures on a Galois extension L/K with Galois group G correspond (via the Greither-Pareigis theorem) to regular subgroups N in $\mathrm{Perm}(G)$ normalised by the left translations $\lambda(G)$. We call N the *type* of the Hopf-Galois structure. Transporting the structure of G to N, we find that the number of Hopf-Galois structures on L/K of type N is

$$\frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} \times \big(\text{Number of regular subgroups} \cong G \text{ in } \mathrm{Hol}(N)\big).$$

Counting braces and HGS via regular subgroups

If $(B, +, \circ)$ is a brace, we can embed $(B, \circ)$ into $\mathrm{Hol}(B, +) = B \rtimes \mathrm{Aut}(B)$ as a regular subgroup by $b \mapsto (b, \lambda_b)$ with $\lambda_b(c) = -b + b \circ c$. Conversely, if G is a regular subgroup in $\mathrm{Hol}(N)$ for an abelian group $(N, +)$, write g_η for the unique element of G moving 0_N to η. Then B becomes a brace where $g_{\eta \circ \eta'} = g_\eta g'_\eta$. Two regular subgroups give isomorphic braces if they are conjugate by an element of $\mathrm{Aut}(N)$.

The Hopf-Galois structures on a Galois extension L/K with Galois group G correspond (via the Greither-Pareigis theorem) to regular subgroups N in $\mathrm{Perm}(G)$ normalised by the left translations $\lambda(G)$. We call N the *type* of the Hopf-Galois structure. Transporting the structure of G to N, we find that the number of Hopf-Galois structures on L/K of type N is

$$\frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} \times \big(\text{Number of regular subgroups} \cong G \text{ in } \mathrm{Hol}(N)\big).$$

So we will be interested in quaternion/dihedral regular subgroups in $\mathrm{Hol}(N)$ for an abelian group N.

The 2-power case

Recall (Featherstonhaugh): *If p prime and $r < p$ then $\mathrm{Hol}(C_p^r)$ contains no element of order p^2.*

The 2-power case

Recall (Featherstonhaugh): *If p prime and $r < p$ then $\mathrm{Hol}(C_p^r)$ contains no element of order p^2.*

A generalisation of this is:

Lemma: *Let N be a finite abelian p-group of rank r and exponent p^d. If $\mathrm{Hol}(N)$ contains an element of order p^k then $k < \lceil \log_p(r+1) \rceil + d$.*

The 2-power case

Recall (Featherstonhaugh): *If p prime and $r < p$ then $\mathrm{Hol}(C_p^r)$ contains no element of order p^2.*

A generalisation of this is:

Lemma: *Let N be a finite abelian p-group of rank r and exponent p^d. If $\mathrm{Hol}(N)$ contains an element of order p^k then $k < \lceil \log_p(r+1) \rceil + d$.*

Since a quaternion or dihedral group of order 2^n contains an element of order 2^{n-1}, we deduce:

Corollary: *Let N be an abelian group of order 2^n with $n \geq 2$. Suppose that there is a regular quaternion or dihedral subgroup of $\mathrm{Hol}(N)$. Then N must be one of the following groups:*

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

Omitting small values of n, we look for regular quaternion/dihedral subgroups in $\mathrm{Hol}(N)$ for each N, and obtain the following counts.

G	N		# regular subgroups	# braces	# HGS
Q_{2^n} or D_{2^n}	C_{2^n}	$n \geq 4$	1	1	2^{n-2}
Q_{2^n} or D_{2^n}	$C_2 \times C_{2^{n-1}}$	$n \geq 5$	8	6	2^{n+1}

with no regular quaternion/dihedral subgroups for $N = C_4 \times C_{2^{n-2}}$, $C_2 \times C_2 \times C_{2^{n-2}}$ or $C_2 \times C_2 \times C_2 \times C_{2^{n-3}}$ when $n \geq 5$.

Omitting small values of n, we look for regular quaternion/dihedral subgroups in $\mathrm{Hol}(N)$ for each N, and obtain the following counts.

G	N		# regular subgroups	# braces	# HGS
Q_{2^n} or D_{2^n}	C_{2^n}	$n \geq 4$	1	1	2^{n-2}
Q_{2^n} or D_{2^n}	$C_2 \times C_{2^{n-1}}$	$n \geq 5$	8	6	2^{n+1}

with no regular quaternion/dihedral subgroups for $N = C_4 \times C_{2^{n-2}}$, $C_2 \times C_2 \times C_{2^{n-2}}$ or $C_2 \times C_2 \times C_2 \times C_{2^{n-3}}$ when $n \geq 5$.

For $n = 3$ and $n = 4$, we used MAGMA:

G	N	# reg subgp	# braces	# HGS
Q_8	C_8	1	1	6
Q_8	$C_2 \times C_4$	2	1	6
Q_8	$C_2 \times C_2 \times C_2$	14	1	2
D_8	C_8	1	1	2
D_8	$C_2 \times C_4$	14	5	14
D_8	$C_2 \times C_2 \times C_2$	126	2	6
Q_{16}	C_{16}	1	1	4
Q_{16}	$C_2 \times C_8$	8	4	16
Q_{16}	$C_4 \times C_4$	48	2	16
Q_{16}	$C_2 \times C_2 \times C_4$	48	1	8
Q_{16}	$C_2 \times C_2 \times C_2 \times C_2$	5040	1	8
D_{16}	C_{16}	1	1	4
D_{16}	$C_2 \times C_8$	16	6	32
D_{16}	$C_4 \times C_4$	0	0	0
D_{16}	$C_2 \times C_2 \times C_4$	0	0	0
D_{16}	$C_2 \times C_2 \times C_2 \times C_2$	0	0	0

The general (i.e. non-2-power) case:

Let $n \geq 2$, $s \geq 3$ with s odd, and let $(N, +)$ be an abelian group of order $2^n s$. Then we have canonical decompositions

$$N = N_s \times N_2 = \{(a, b) : a \in N_s, b \in N_2\},$$

$$\mathrm{Hol}(N) = \mathrm{Hol}(N_s) \times \mathrm{Hol}(N_2)$$

where $|N_s| = s$, $|N_2| = 2^n$.

The general (i.e. non-2-power) case:

Let $n \geq 2$, $s \geq 3$ with s odd, and let $(N, +)$ be an abelian group of order $2^n s$. Then we have canonical decompositions

$$N = N_s \times N_2 = \{(a, b) : a \in N_s, b \in N_2\},$$

$$\mathrm{Hol}(N) = \mathrm{Hol}(N_s) \times \mathrm{Hol}(N_2)$$

where $|N_s| = s$, $|N_2| = 2^n$.

Let $G = \{(\eta, \lambda_\eta) : \eta \in N\}$ be a regular quaternion/dihedral subgroup of $\mathrm{Hol}(N)$. Then G determines an operation $\circ$ on N so that $(N, +, \circ)$ is a quaternion/dihedral brace.

The general (i.e. non-2-power) case:

Let $n \geq 2$, $s \geq 3$ with s odd, and let $(N, +)$ be an abelian group of order $2^n s$. Then we have canonical decompositions

$$N = N_s \times N_2 = \{(a, b) : a \in N_s, b \in N_2\},$$

$$\mathrm{Hol}(N) = \mathrm{Hol}(N_s) \times \mathrm{Hol}(N_2)$$

where $|N_s| = s$, $|N_2| = 2^n$.

Let $G = \{(\eta, \lambda_\eta) : \eta \in N\}$ be a regular quaternion/dihedral subgroup of $\mathrm{Hol}(N)$. Then G determines an operation $\circ$ on N so that $(N, +, \circ)$ is a quaternion/dihedral brace.

Then $G_s := \{(\eta, \lambda_\eta) : \eta \in N_s\}$ is a subgroup of G of order s and (because G is quaternion/dihedral) must be normal in G and cyclic. The image of G_s in $\mathrm{Hol}(N_s)$ is a regular subgroup of $\mathrm{Hol}(N_s)$, and gives rise to an operation $\circ_s$ on N_s making $(N_s, +, \circ_s)$ into a brace. It turns out that $\circ_s = +$, so we get the trivial brace structure on N_s and $(N_s, +)$ is also cyclic. Further, G_s acts trivially on N_2.

Likewise, let $G_2 := \{(\eta, \lambda_\eta) : \eta \in N_2\}$. This is a Sylow 2-subgroup of G distinguished by the fact that $G < \mathrm{Hol}(N)$. The image H of G_2 in $\mathrm{Hol}(N_2)$ is a regular quaternion/dihedral subgroup which determines an operation $\circ_H$ on N_2, making $(N_2, +, \circ_H)$ into a brace.

Likewise, let $G_2 := \{(\eta, \lambda_\eta) : \eta \in N_2\}$. This is a Sylow 2-subgroup of G distinguished by the fact that $G < \mathrm{Hol}(N)$. The image H of G_2 in $\mathrm{Hol}(N_2)$ is a regular quaternion/dihedral subgroup which determines an operation $\circ_H$ on N_2, making $(N_2, +, \circ_H)$ into a brace.

For each regular quaternion/dihedral subgroup H of $\mathrm{Hol}(N_2)$, let T_H be the set of all homomorphisms

$$\tau : (N_2, \circ_H) \to \mathrm{Aut}(N_s)$$

such that $N_s \rtimes_\tau (N_2, \circ_H)$ is a quaternion/dihedral group. Then, along with H, our group G gives rise to an element $\tau \in T_H$.

Likewise, let $G_2 := \{(\eta, \lambda_\eta) : \eta \in N_2\}$. This is a Sylow 2-subgroup of G distinguished by the fact that $G < \mathrm{Hol}(N)$. The image H of G_2 in $\mathrm{Hol}(N_2)$ is a regular quaternion/dihedral subgroup which determines an operation $\circ_H$ on N_2, making $(N_2, +, \circ_H)$ into a brace.

For each regular quaternion/dihedral subgroup H of $\mathrm{Hol}(N_2)$, let T_H be the set of all homomorphisms

$$\tau : (N_2, \circ_H) \to \mathrm{Aut}(N_s)$$

such that $N_s \rtimes_\tau (N_2, \circ_H)$ is a quaternion/dihedral group. Then, along with H, our group G gives rise to an element $\tau \in T_H$.

Lemma: *There is a bijection between regular quaterion/dihedral subgroups G in $\mathrm{Hol}(N)$ and pairs (H, τ) with $\tau \in T_H$. If G corresponds to (H, τ) and $\alpha \in \mathrm{Aut}(N_s)$, $\beta \in \mathrm{Aut}(N_2)$, then $(\alpha, \beta)G(\alpha, \beta)^{-1}$ corresponds to $(\beta H \beta^{-1}, \beta \cdot \tau)$ where $(\beta \cdot \tau)_b = \tau_{\beta^{-1}(b)}$.*

Likewise, let $G_2 := \{(\eta, \lambda_\eta) : \eta \in N_2\}$. This is a Sylow 2-subgroup of G distinguished by the fact that $G < \mathrm{Hol}(N)$. The image H of G_2 in $\mathrm{Hol}(N_2)$ is a regular quaternion/dihedral subgroup which determines an operation $\circ_H$ on N_2, making $(N_2, +, \circ_H)$ into a brace.

For each regular quaternion/dihedral subgroup H of $\mathrm{Hol}(N_2)$, let T_H be the set of all homomorphisms

$$\tau : (N_2, \circ_H) \to \mathrm{Aut}(N_s)$$

such that $N_s \rtimes_\tau (N_2, \circ_H)$ is a quaternion/dihedral group. Then, along with H, our group G gives rise to an element $\tau \in T_H$.

Lemma: *There is a bijection between regular quaterion/dihedral subgroups G in $\mathrm{Hol}(N)$ and pairs (H, τ) with $\tau \in T_H$. If G corresponds to (H, τ) and $\alpha \in \mathrm{Aut}(N_s)$, $\beta \in \mathrm{Aut}(N_2)$, then $(\alpha, \beta)G(\alpha, \beta)^{-1}$ corresponds to $(\beta H \beta^{-1}, \beta \cdot \tau)$ where $(\beta \cdot \tau)_b = \tau_{\beta^{-1}(b)}$.*

$|T_H| = 1$ unless $H = Q_8$ or $D_4 = C_2 \times C_2$, when $|T_H| = 3$. (This is because Q_8 and $C_2 \times C_2$ have 3 subgroups of index 2.)

Putting these pieces together, if $H \neq Q_8$, $C_2 \times C_2$ then the correspondence $G \leftrightarrow H$ is bijective and we get the same number of regular subgroups/braces for odd $s \geq 3$ as for $s = 1$.

Putting these pieces together, if $H \neq Q_8$, $C_2 \times C_2$ then the correspondence $G \leftrightarrow H$ is bijective and we get the same number of regular subgroups/braces for odd $s \geq 3$ as for $s = 1$.

If $H = Q_8$ or $C_2 \times C_2$, we need to take into account the orbits of $\mathrm{Aut}(N_2)$ on T_H: these depend on N_2 but not on $s \geq 3$. So it suffices to check the cases Q_{24} and D_{12} in MAGMA.

N	Conditions	Quaternion braces	Dihedral braces
$C_s \times C_8$	$s \geq 3$ odd	2	1
$C_s \times C_2 \times C_4$	$s \geq 3$ odd	3	5
$C_s \times C_2 \times C_2 \times C_2$	$s \geq 3$ odd	1	2
C_8		1	1
$C_4 \times C_2$		1	5
$C_2 \times C_2 \times C_2$		1	2
$C_s \times C_4$	$s \geq 3$ odd	1	2
$C_s \times C_2 \times C_2$	$s \geq 3$ odd	1	1
C_4		1	1
$C_2 \times C_2$		1	1

Final count of braces

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

$$q(4m) = \begin{cases} 2 & \text{if } m \text{ is odd;} \\ 6 & \text{if } m \equiv 2 \pmod 4; \\ 9 & \text{if } m \equiv 4 \pmod 8; \\ 7 & \text{if } m \equiv 0 \pmod 8. \end{cases}$$

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

$$d(4m) = \begin{cases} 3 & \text{if } m \text{ is odd;} \\ 8 & \text{if } m \equiv 2 \pmod 4; \\ 7 & \text{if } m \equiv 4 \pmod 8; \\ 7 & \text{if } m \equiv 0 \pmod 8. \end{cases}$$

Final count of Hopf-Galois structures

When $H = Q_8$ or $C_2 \times C_2$, the extra factor 3 in the number of regular subgroups is compensated by a factor 3 in $|\mathrm{Aut}(H)|$ so we get the same formula (involving s) whether $s \geq 3$ or $s = 1$.

N	Conditions	G quaternion	G dihedral
$C_s \times C_{2^n}$	$n \geq 5$	$2^{n-2}s$	$2^{n-2}s$
$C_s \times C_2 \times C_{2^{n-1}}$	$n \geq 5$	$2^{n+1}s$	$2^{n+1}s$
$C_s \times C_{16}$		$4s$	$4s$
$C_s \times C_2 \times C_8$		$16s$	$32s$
$C_s \times C_4 \times C_4$		$16s$	0
$C_s \times C_2 \times C_2 \times C_4$		$8s$	0
$C_s \times C_2 \times C_2 \times C_2 \times C_2$		$8s$	0
$C_s \times C_8$		$6s$	$2s$
$C_s \times C_2 \times C_4$		$6s$	$14s$
$C_s \times C_2 \times C_2 \times C_2$		$2s$	$6s$
$C_s \times C_4$		s	$3s$
$C_s \times C_2 \times C_2$		s	s

References:

B. + F. Ferri (2024): *On the number of quaternion and dihedral braces and Hopf-Galois structures* `arXiv:2402.12547v2`

L. Guarnieri & L. Vendramin: *Skew braces and the Yang-Baxter equation*. Math. Comp. **86** (2017) no. 307, 2519–2534.

W. Rump: *Classification of the affine structures of a generalized quaternion group of order* ≥ 32. J. Group Theory **23** (2020) no. 5, 847–869.