How to construct a database of Hopf-Galois Structures of small degree.

Andrew Darlington

Thursday 3rd August 2023

University of Exeter

Finding HGS

L/K separable (but not necessarily normal) of degree n, E Galois closure, $G := \mathrm{Gal}(E/K)$, $G' := \mathrm{Gal}(E/L)$.

- [GP87]: Let $X := G/G'$.

  $$\text{HGS on } L/K \longleftrightarrow \text{ subgroups } N < \mathrm{Perm}(X)$$

  s.t. N regular & normalised by $\lambda(G)$ where $\lambda(g)(hG') := (gh)G'$ for all $g, h \in G$.
- [Byo96]:

  $$\text{HGS of type } N \longleftrightarrow \text{ subgroups } G < \mathrm{Hol}(N)$$

  s.t. G transitive.

  Note: G_1, G_2 transitive subgroups of $\mathrm{Hol}(N)$ correspond to the *same HGS* if and only if they are isomorphic as permutation groups (i.e. $G_1 \overset{\phi}{\cong} G_2$ such that $\phi(G_1') = G_2'$, stabilisers are preserved).

Finding HGS

$e(G,N) := \#$HGS of type N with $\mathrm{Gal}(E/K) \cong G$,
$e'(G,N) := \#$transitive subgroups of $\mathrm{Hol}(N)$ isomorphic to G,
$\mathrm{Aut}(G,G') := \{\alpha \in \mathrm{Aut}(G) \mid \alpha(G') = G'\}$.

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

Question: Can we use a computer to find all HGS on extensions of low degree?

Known results: Galois

Let L/K be Galois. Then we look for **regular** subgroups G in $\mathrm{Hol}(N)$, so we restrict $|G| = |N|$. Also $G' = \{1_G\}$, so $\mathrm{Aut}(G, G') = \mathrm{Aut}(G)$.

So, given a positive integer n, we can use GAP to:

1) List all groups N_i of order n. Then for each i:
2) Compute $\mathrm{Hol}(N_i)$.
3) Find the subgroups G_j of $\mathrm{Hol}(N_i)$ such that $|G_j| = n$ and G_j acts transitively on N_i.
4) Find when two subgroups G_{j_1}, G_{j_2} are isomorphic as permutation groups.
5) Sum up $e(G_j, N_i)$.

Known results: Galois

- In [SV18], Byott and Vendramin use MAGMA to compute the number of Hopf-Galois structures on Galois extensions of degree up to 46.
- Vendramin (in [GV17]) has also used MAGMA/GAP to enumerate skew braces of order up to 1000, with several people filling in the gaps (such as for orders 32, 64, etc.). Recall that two regular subgroups G_1, G_2 of $\mathrm{Hol}(N)$ yield isomorphic skew braces iff they are conjugate by an element of $\mathrm{Aut}(N)$.

Going to non-Galois

Now let L/K be a separable (but not necessarily normal) extension of degree n. If we still wish to use the $\mathrm{Hol}(N)$ approach,

- We now no longer have a bound on the size of the transitive subgroups of $\mathrm{Hol}(N)$ (apart from $|\mathrm{Hol}(N)|$).
- We no longer have that $\mathrm{Aut}(G, G') = \mathrm{Aut}(G)$, meaning we need to know more than just the size of the automorphism group.
- We also now must take into account that the relevant isomorphism between two transitive subgroups G_1, G_2 of $\mathrm{Hol}(N)$ must also give an isomorphism of $\mathrm{Stab}_{G_i}(1_N)$.

Known results: separable

• Crespo and Salguero in [CS20] give a full classification up to degree 11 using MAGMA and directly using Greither-Pareigis.

They use Butler and McKay's classification of transitive permutation groups of degree up to 11. [BM83].

• In the sequel, [CS21], they give a full classification (also using MAGMA) up to degree 31. Here they use Byott's translation and look at transitive subgroups of $\mathrm{Hol}(N)$.

For this, they use Hulpke's classification of transitive permutation groups of degree up to 31. [Hul05].

Known results: separable

In each paper, they also compute:

- The number of almost classically Galois extensions of each degree.
- The number of HGS for which the Hopf-Galois correspondence is bijective.
- The number of Hopf algebra isomorphism classes..

Our approach

The transitive permutation groups of degree up to 48 are now known ([HRT22]) but we want to use MAGMA to directly compute the transitive subgroups of $\mathrm{Hol}(N)$.

We note that MAGMA is more efficient than GAP for these problems due to the way it finds transitive subgroups. It is also a little more efficient in general when dealing with permutation groups.

Our (initial) approach

For a given ("small") positive integer n:

- MAGMA knows the list $\{N_i\}$ of groups of order n.
- Compute the subgroups of $\mathrm{Hol}(N_i)$ which have order divisible by n and which are transitive on N_i. (MAGMA computes these up to conjugacy).
- If we sum over all transitive subrgoups, we don't need to compute $e'(G, N)$.
- We compute $|\mathrm{Aut}(G, G')|$. **Note:** MAGMA doesn't deal with this very well, and so we have used the same code used in [CS21] to compute this.

Our results

- We compute #HGS of each type (at the moment)
- With an older version of the current code, we have obtained results for separable extensions of degree up to 63, within a very reasonable amount of time (currently missing out degrees $32, 48, 50, 54, 56$).
- The code appears to be able to deal with degrees for which there aren't 'too many' groups for, or where the size of the holomorph is less than around 300000.

Our results (confirming previous)

Degree	Types	#HGS
2	1	1
3	1	2
4	2	10
5	1	3
6	2	15
7	1	4
8	5	348
9	2	38
10	2	27
11	1	4
12	5	249
13	1	6
14	2	32
15	1	8
16	14	49913

Degree	Types	#HGS
17	1	5
18	5	881
19	1	6
20	5	434
21	2	78
22	2	36
23	1	4
24	15	14908
25	2	106
26	2	58
27	5	6699
28	4	388
29	1	6
30	4	479
31	1	8

Our results (extending)

Degree	Types	#HGS
33	1	10
34	2	59
35	1	16
36	14	16512
37	1	9
38	2	57
39	2	133
40	14	29534
41	1	8
42	6	1041
43	1	8
44	4	466
45	2	166

Degree	Types	#HGS
46	2	48
47	1	4
49	2	200
51	1	14
52	5	1023
53	1	6
55	2	192
57	2	169
58	2	74
59	1	4
61	1	12
62	2	82
63	4	1875

Looking ahead

- We will hopefully be able to extend the results of [CS21] by computing the number of a.c.g. extensions, and looking into when the Galois correspondence is bijective.
- Once a more extensive list is obtained, we should be able to make conjectures and prove more general results about HGS (much like in [CS20] and [CS21]).
- Can we adapt this code to finding and counting skew bracoids of small order?

Thank You!

Questions?

References i

- Gregory Butler and John McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), no. 8, 863–911. MR 695893
- N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228. MR 1402555
- Teresa Crespo and Marta Salguero, *Computation of Hopf Galois structures on low degree separable extensions and classification of those for degrees p^2 and $2p$*, Publ. Mat. **64** (2020), no. 1, 121–141. MR 4047559

References ii

——— , *Computation of Hopf Galois structures on separable extensions and classification of those for degree twice an odd prime power*, Journal of Algebra and Its Applications **20** (2021), no. 04, 2150049.

Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476

L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. **86** (2017), no. 307, 2519–2534. MR 3647970

- Derek Holt, Gordon Royle, and Gareth Tracey, *The transitive groups of degree 48 and some applications*, J. Algebra **607** (2022), 372–386. MR 4441332
- Alexander Hulpke, *Constructing transitive permutation groups*, J. Symbolic Comput. **39** (2005), no. 1, 1–30. MR 2168238
- Agata Smoktunowicz and Leandro Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), no. 1, 47–86. MR 3763907