Some Counting Problems for Hopf-Galois Structures

Nigel Byott

University of Exeter, UK

Omaha, 27 May 2016

Joint work with Ali Bilal

In view of Griff's instruction to include work-in-progress and wild speculations, rather than just polished results, I will talk about 4 counting problems:

- one we have solved (and are writing up);
- one we are working on (we have a method but not yet an answer);
- one we probably can't solve in general;
- one where we have a strategy that *might* work.

The set-up: Hopf-Galois Structures

Let N/K be a finite Galois extension of fields, with $\Gamma = \mathrm{Gal}(N/K)$.

A *Hopf-Galois structure* (HGS) on N/K consists of a Hopf algebra H over K and a "nice" K-linear action of H on N (basic example: $H = K[\Gamma]$):

- the action is compatible with the multiplication on N:

$$\alpha \cdot (xy) = \mathrm{mult}\left(\Delta(\alpha) \cdot (x \otimes y)\right),$$

$$\alpha \cdot 1 = \epsilon(\alpha) 1 \text{ for all } \alpha \in K[G],\ x, y \in N,$$

  where Δ is the comultiplication and ϵ the augmentation;
- ("Galois", i.e. non-degeneracy, condition): the following map is bijective:

$$\theta : N \otimes_K H \longrightarrow \mathrm{End}_K N, \quad \theta(x \otimes h)(y) = x(h \cdot y).$$

In particular, this means $\dim_K H = [N : K]$ and H acts faithfully on N.

The set-up: Classifying Hopf-Galois Structures

Greither and Pareigis (1987) showed the Hopf-Galois structures correspond bijectively to subgroups G of the (large) group $\mathrm{Perm}(\Gamma)$ which are **regular** (i.e. given $x, y \in \Gamma$ there is a unique $g \in G$ with $g \cdot x = y$) and are normalised by $\lambda(\Gamma)$, the left translations by Γ.

Counting the Hopf-Galois structures then becomes a combinatorial question in group theory, which we can approach in two ways:

(1) work directly in $\mathrm{Perm}(\Gamma)$;

(2) turn around the relation between Γ and G (the "holomorph approach").

Set-up: The holomorph approach

Hopf-Galois structures correspond to equivalence classes of regular embeddings

$$\Gamma \longrightarrow \mathrm{Hol}(G) \subseteq \mathrm{Perm}(G),$$

where G is an abstract group with $|G| = |\Gamma|$, and

$$\mathrm{Hol}(G) = \lambda(G) \rtimes \mathrm{Aut}(G).$$

Two embeddings are deemed to be equivalent if they are conjugate by an element of $\mathrm{Aut}(G)$.

The **type** of the HGS is (the isomorphism class of) G.

To count HGS using the holomorph approach, we need either

(i) a manageable classification of all groups G with $|G| = |\Gamma|$, or

(ii) a group-theoretic reason why only a few such G are relevant.

Some Examples

(i) For $\Gamma = C_{p^r}$ with p an odd prime, there are p^{r-1} Hopf-Galois structures, all with $G = C_{p^r}$ [Kohl, 1998].

(ii) For $\Gamma = C_{2^r}$ with $r \geq 3$, there are 2^{r-2} HGS for each of $G = C_{2^r}$, Q_{2^r}, D_{2^r} [B, 2007].

(iii) For Γ a nonabelian simple group, there are two HGS, both with $G = \Gamma$ [B, 2004]

(iv) Results are also known for all groups of order n where:

- $n = pq$, with $p > q$ prime [B, 2004];
- $n = 2pq = p(p-1)$ where p and $q = (p-1)/2$ are odd primes (so p is a safeprime) [Childs, 2003, 2012; Kohl 2013];
- $n = pqr$ where $p > q > r > 2$ are primes and $p, q \equiv 1 \pmod{r}$, $p \not\equiv 1 \pmod{q}$ [Kohl, 2015].

Problem 1: $\Gamma = C_n$ with n squarefree

We consider cyclic extensions of degree n, where n is squarefree (with arbitrary many prime factors).

Definition

A **C-group** is a finite group, all of whose Sylow subgroups are cyclic.

Any group of squarefree order is a C-group.

It is a standard result that a C-group must be metacyclic. In principle, this gives a classification of C-groups.

This was made explicit by Murty & Murty (1984).

Theorem (Murty & Murty)

(i) *Any C-group of order n (not necessarily squarefree) has the form*

$$G(e,d,k) := \{\sigma,\tau \ : \ \sigma^e = 1 = \tau^d, \tau\sigma\tau^{-1} = \sigma^k\}$$

where $ed = n$, $\gcd(e,d) = 1$ and $k \in \mathbb{Z}_e^\times$ has order d.

(ii) *$G(e,d,k) \cong G(e',d',k')$ if and only if $e = e'$, $d = d'$, and $\langle k \rangle = \langle k' \rangle$ (as subgroups of $\mathbb{Z}_e^\times$).*

Corollary (Hölder, 1895)

For n squarefree, the number of groups of order n (up to isomorphism) is

$$\sum_{ed=n} \frac{1}{\varphi(d)} \prod_{q \mid d} \left(q^{v(q,e)} - 1 \right),$$

where the product is over primes q dividing d, and $v(q,e)$ is the number of primes $p \mid e$ with $p \equiv 1 \pmod{q}$.

Our main result is:

Theorem (B+B)

On a cyclic field extension of squarefree degree n:

(i) *The number of Hopf-Galois structures of type $G = G(e, d, k)$ is*

$$2^{\omega(g)}\varphi(d),$$

where

$$g = \frac{e}{\gcd(e, k-1)},$$

and $\omega(g)$ is the number of (distinct) prime factors of g.
In particular, Hopf-Galois structures of all possible types occur.

(ii) *The total number of Hopf-Galois structures is*

$$\sum_{dgz=n} 2^{\omega(g)}\mu(z)\prod_{q|d}\left(q^{v(q,g)} - 1\right),$$

where μ is the Möbius function: $\mu(z) = (-1)^{\omega(z)}$ for z squarefree.

Some properties of G:

Let $G = G(e,d,k) = \{\sigma, \tau \ : \ \sigma^e = 1 = \tau^d, \tau\sigma\tau^{-1} = \sigma^k\}$.
Set $z = \gcd(e, k-1)$, so $e = gz$.

- the centre of G is $Z(G) = \langle \sigma^g \rangle \cong C_z$.
- Hence $n = de = dgz$ has 3 sorts of prime factors p:
  - p is "active" if $p \mid d$;
  - p is "passive" (acted upon) if $p \mid g$;
  - p is "central" if $p \mid z$.
- G has commutator subgroup $[G, G] = \langle \sigma^z \rangle \cong C_g$.
- We have the power formula (when τ occurs to power 1)

$$(\sigma^a\tau)^j = \sigma^{aS(k,j)}\tau^j \text{ where } S(k,j) = \sum_{i=0}^{j-1} k^i.$$

$\mathrm{Aut}(G)$ and $\mathrm{Hol}(G)$

$$\mathrm{Aut}(G) = \langle \theta \rangle \rtimes \{\phi_s : s \in \mathbb{Z}_e^\times\} \cong C_g \rtimes \mathbb{Z}_e^\times,$$

where

$$\theta(\sigma) = \sigma, \quad \theta(\tau) = \sigma^z \tau;$$

$$\phi_s(\sigma) = \sigma^s, \quad \phi_s(\tau) = \tau.$$

Note that all automorphisms preserve the exponent on τ.

We may write an element $x \in \mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ as

$$x = [\alpha, \lambda] = [\sigma^a \tau^b, \theta^c \phi_s] \text{ with } a \in \mathbb{Z}_e, b \in \mathbb{Z}_d, c \in \mathbb{Z}_g, s \in \mathbb{Z}_e^\times,$$

where

$$\alpha = \sigma^a \tau^b \in G, \qquad \lambda = \theta^c \phi_s \in \mathrm{Aut}(G).$$

Multiplication in $\mathrm{Hol}(G)$ is given by

$$[\alpha, \lambda][\alpha', \lambda'] = [\alpha\lambda(\alpha'), \lambda\lambda'].$$

In particular, even though the projection map

$$\mathrm{Hol}(G) \longrightarrow G, \qquad x \mapsto \alpha$$

is not a group homomorphism in general, the projection map

$$\mathrm{Hol}(G) \longrightarrow \langle \tau \rangle = C_d, \qquad x \mapsto \tau^b$$

is a group homomorphism.

Now fix $b = 1$, and consider

$$x = [\sigma^a \tau, \theta^c \phi_s] \in \mathrm{Hol}(G), \text{ with } a \in \mathbb{Z}_e, \ c \in \mathbb{Z}_g, \ s \in \mathbb{Z}_e^\times.$$

Then we have the power formula

$$x^j = [\sigma^{aS(sk,j)+czkT(k,s,j)} \tau^j, \theta^{cS(s,j)} \phi_{s^j}],$$

where

$$T(k,s,0) = 0, \qquad T(k,s,j) = \sum_{h=0}^{j-1} S(s,h) k^{h-1} \text{ for } j \geq 1.$$

To count Hopf-Galois structures of type $G = G(e,d,k)$ on our cyclic extension, we determine the triples $(a,c,s) \in \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e^\times$ for which

$$x = [\sigma^a \tau, \theta^c \phi_s]$$

generates a regular cyclic subgroup of $\mathrm{Hol}(G)$, i.e.

$$x^n = \mathrm{id}_{\mathrm{Hol}(G)} \text{ and } \langle x \rangle \cdot \mathrm{id}_G = G.$$

Examining $S(k,j)$, $T(k,s,j)$ mod p for each prime $p \mid e$, and taking into account the special cases $s \equiv 1$ and $sk \equiv 1$, we find this happens if and only if

- for each prime $p \mid z$, we have $s \equiv 1 \pmod{p}$ and $p \nmid a$;
- for each prime $p \mid g$, we have either
  - $s \equiv 1 \pmod{p}$, $p \nmid c$, or
  - $s \equiv k^{-1} \pmod{p}$, $p \nmid (a(s-1) + cz)$.

So the number of suitable x is

$$\left(\prod_{p \mid z} (p-1) \right) \left(\prod_{p \mid g} 2p(p-1) \right) = 2^{\omega(g)} g \varphi(e).$$

Hence

$$\begin{aligned}
\#\text{ HGS of type } G(e,d,k) &= \frac{\#\text{ suitable } x}{\#\text{ generators } x \text{ per subgroup}} \times \frac{|\mathrm{Aut}(C_n)|}{|\mathrm{Aut}(G)|} \\
&= \frac{2^{\omega(g)} g\varphi(e)}{\varphi(e)} \times \frac{\varphi(n)}{g\varphi(e)} \\
&= 2^{\omega(g)}\varphi(d).
\end{aligned}$$

To find the total number of HGS, we sum over isomorphism types of $G(e,d,k)$. For a given factorisation $n = ed = gzd$, we need the number of subgroups $\langle k \rangle \subseteq \mathbb{Z}_e^\times$ of order d such that $\gcd(e, k-1) = z$.

The number of subgroups with $z \mid \gcd(e, k-1)$ is

$$\frac{1}{\varphi(d)} \prod_{q \mid d} (q^{v(q,g)} - 1).$$

Using Möbius inversion, we find the total number of HGS is

$$\sum_{dgz=n} 2^{\omega(g)} \mu(z) \prod_{q \mid d} \left(q^{v(q,g)} - 1 \right).$$

Problem 2: Arbitrary Γ of squarefree order

This is work in progress: we have a strategy but not yet an answer!

Fix $G = G(e,d,k)$ and $G' = G(\epsilon,\delta,\kappa)$ of squarefree order n.

Inside $\mathrm{Hol}(G)$, we try to count regular copies of G'. This will enable us to count HGS of type G on a Galois extension with group $\Gamma = G'$.

As before, set

$$z = \gcd(e, k-1), \qquad e = gz;$$

and similarly

$$\zeta = \gcd(\epsilon, \kappa - 1), \qquad \epsilon = \gamma\zeta.$$

Useful Observation: $[G', G'] \cong C_\gamma$ is a semiregular subgroup of $\mathrm{Hol}(G)$ contained in $[\mathrm{Hol}(G), \mathrm{Hol}(G)]$, so it is in the kernel of the projection homomorphism $\mathrm{Hol}(G) \longrightarrow \langle\tau\rangle = C_d$. Hence it acts on $\langle\sigma\rangle \cong C_e$, so

$$\gamma \mid e, \text{ or, equivalently } d \mid \delta\zeta.$$

So some combinations of G and G' give no HGS.

Now G' contains a cyclic subgroup $C_\delta \times C_\zeta$ of order $\delta\zeta$. This will have a generator of the form

$$x = [\sigma^a \tau, \theta^c \phi_s] \in \mathrm{Hol}(G),$$

(where τ occurs to power 1). Look for a complementary generator

$$y = [\sigma^{a'}, \theta^{c'} \phi_{s'}]$$

(where τ does not occur).

We need to count pairs (x, y), i.e. sextuples (a, c, s, a', c', s'), such that

- $x^{\zeta\delta} = \mathrm{id}_{\mathrm{Hol}(G)}$;
- $\langle x^d \rangle \cdot \mathrm{id}_G$ has size $\delta\zeta/d$.
- $y^\gamma = \mathrm{id}_{\mathrm{Hol}(G)}$, and the orbits of $\langle y \rangle$ on $\langle \sigma \rangle$ all have size γ;
- $xyx^{-1} = y^\kappa$.

Then $\langle x, y \rangle$ is a regular copy of G', and every regular copy arises this way (up to replacing κ by another generator of the same cyclic subgroup of $\mathbb{Z}_\epsilon^\times$).

It turns out that $s = 1$, but counting the quintuples (a, c, a', c', s') is difficult since among the primes $p \mid \gamma$ there are various special cases (depending on the choice of s'), e.g.

- $s' \equiv 1 \pmod{p}$;
- $s' \equiv k^{-1} \pmod{p}$;
- $s' \equiv \kappa \pmod{p}$;
- $s' \equiv k^{-1} \equiv \kappa \pmod{p}$;

all with different restrictions on a, c, a', c'.

Problem 3: Non-normal extensions of squarefree degree

Hopf-Galois structures on separable (but not necessarily normal) extensions of squarefree degree n would correspond to transitive subgroups $H \subseteq \mathrm{Hol}(G)$ with $|G| = n$. Here H need not have squarefree order.

When do

$$H_1 \subseteq \mathrm{Hol}(G_1), \qquad H_2 \subseteq \mathrm{Hol}(G_2)$$

give HGS on *the same* field extension? This occurs if $H_1 \cong H_2$ as degree n permutation groups (not just as abstract groups).

These permutation groups are very special (e.g. they are soluble) but I don't know how to describe them without reference to G.

So we don't even have the language to formulate an answer in general.

However, it ought to be possible to analyse completely certain special cases, e.g.

- $n = pq$, with p, q prime and $p \equiv 1 \pmod{q}$;
- $\gcd(n, \varphi(n)) = 1$.
  [There should be at most one HGS; is the converse true?]

Problem 4: $\Gamma = C_n$ for arbitrary n (not squarefree)

Here is a strategy by which it *might* be possible to count all HGS on a cyclic extension L/K of arbitrary degree n.

We need to find regular *cyclic* subgroups $C \subseteq \mathrm{Hol}(G)$ where G is a group of order n. In general, we cannot hope to classify all such G, but we might be able to classify the relevant ones.

Let J be a characteristic subgroup of G, i.e. J is stable under all automorphisms of G. Then there is a canonical homomorphism $\mathrm{Hol}(G) \longrightarrow \mathrm{Hol}(G/J)$, via which C acts transitively on G/J.

Let $D \subset C$ be the stabiliser of $\mathrm{id}_{G/J}$. We have $D \lhd C$ since C is abelian, so D acts trivially on G/J. It follows that C/D acts *regularly* on G/J, and D acts regularly J.

So we have HGS of types G/J, J on the cyclic extensions N^D/K, N/N^D.

Repeating the argument, we can break up G into characteristically simple pieces, each arising as the type of a HGS on a cyclic extension.

These characteristically simple pieces must be soluble. (In fact, any HGS on an *abelian* extension has soluble type.) Hence each piece is elementary abelian of order p^r for some prime p and some $r \geq 1$.

But a cyclic extension of degree p^r can only have a HGS of elementary abelian type if $r = 1$ or if $p = 2$, $r = 2$.

So if a cyclic extension of degree n has a HGS of type G, then we have a chain of subgroups

$$\{id\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$$

in which each G_j is characteristic in G and each quotient $G_{j+1}/G_j \cong C_p$ (for some prime p) or $C_2 \times C_2$.

Definition

A finite group H is **supersoluble** it has a chain of subgroups

$$\{id\} = H_0 \lhd H_1 \lhd \cdots \lhd H_r = H$$

where each $H_j \lhd H$ (not just $H_j \lhd H_{j+1}$!) and each H_{j+1}/H_j is cyclic (WLOG of prime order).

We can rearrange these quotients into the “right order”:

Theorem (Zappa, 1941)

If H is supersoluble, there is a chain of subgroups as above such that each $|H_{j+1}/H_j|$ is prime and

$$|H_{j+1}/H_j| \geq |H_{j+2}/H_{j+1}|.$$

Suppose temporarily that $4 \nmid n$.

If our cyclic extension of degree n has a HGS of type G, then G cannot have a characteristically simple piece $C_2 \times C_2$, so G is supersoluble. Combining the quotients in Zappa's Theorem which correspond to the same prime, we get a chain of subgroups

$$\{id\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$$

in which G_{j+1}/G_j is a p_j-group, for primes $p_0 > p_1 > \ldots > p_{r-1}$.

Then the G_j are characteristic in G, so each quotient G_{j+1}/G_j occurs as the type of a HGS on a cyclic extension. Thus these quotients are cyclic.

This means that G is a C-group, and occurs in the classification of Murty & Murty.

So we should be able to proceed as in the squarefree cyclic case (but with more complicated congruence calculations) when $4 \nmid n$.

To handle the case $4 \mid n$, we would need to consider "weakly supersoluble" groups G with a chain of subgroups

$$\{id\} = H_0 \lhd H_1 \lhd \cdots \lhd H_r = H$$

such that each $H_j \lhd H$ and each $H_{j+1}/H_j \cong C_p$ or $C_2 \times C_2$.

However, in our case, each H_j is *characteristic* in H (not just normal).

We would need to prove a version of Zappa's Theorem for these, and to classify the (relevant) groups whose Sylow subgroups are either cyclic or D_{2^r} or Q_{2^r}; these groups will either be C-groups, or will have a characteristic C-subgroup of index 2 or 4.

Thank you!