Counting Hopf Galois Structures on Non-abelian Galois Field Extensions

Scott Carnahan, California Institute of Technology
Lindsay Childs, Department of Mathematics, University at Albany
November 30, 1998

Let L be a field which is a Galois extension of the field K with Galois group G. Greither and Pareigis [GP87] showed that for many G there exist K-Hopf algebras H other than the group ring KG which make L into an H-Hopf Galois extension of K (or a Galois H^*-object in the sense of Chase and Sweedler [CS69]). Using Galois descent they translated the problem of determining the Hopf Galois structures on L/K into one which depends only on the Galois group G. By this translation, they showed, for example, that any Galois extension with non-abelian G admits at least one non-classical Hopf Galois structure. Byott [By96] further translated the problem to a more amenable group-theoretic problem, and showed that a Galois extension L/K of fields with group G has a unique Hopf Galois structure, namely that by KG, iff n, the order of G, is a Burnside number, that is, is coprime to $\phi(n)$, Euler's phi-function of n. (This implies that G is cyclic of square-free order.)

The observation of Greither and Pareigis is the only one in the literature to this point which gives any information on the number of Hopf Galois structures on Galois field extensions for G non-abelian.

The purpose of this paper is to make a start at determining the number of Hopf Galois structures on L/K for some non-abelian Galois groups G.

Before stating our results, we need to describe Byott's counting formula.

Let n be the order of G, and let N be an abstract group with cardinality n. Let λ, resp. $\rho : N \to Perm(N)$ be the maps given by sending η to left translation by η, resp. right translation by the inverse of η. The holomorph of N, $Hol(N) \subset Perm(N)$, is the normalizer of $\lambda(N)$ in $Perm(N)$: then $Hol(N) = \rho(N) \cdot Aut(N)$. The number of Hopf Galois structures

$$H \otimes L \to L$$

for K-Hopf algebras H such that $L \otimes H \cong LN$, is equal to the number of equivalence classes of embeddings

$$\beta : G \to Hol(N)$$

such that the stabilizer in G of the identity element of the set N is trivial (i.e. β is *regular*), where the equivalence relation is given by $\beta \sim \beta'$ iff $\beta' = C(\delta) \circ \beta$ for some $\delta \in Aut(N)$, where $C(\delta)$ is conjugation by δ . If we denote the number of equivalence classes of regular embeddings of G into $Hol(N)$ by $e(G,N)$, then the number of Hopf Galois structures on a Galois extension with group G is the sum, over the set of isomorphism classes of groups N of cardinality n, of $e(G,N)$.

For some groups, $e(G,N) = 0$ for N not isomorphic to G. This is true for G is cyclic of prime power order, because the holomorph of any non-cyclic group of order p^n has no elements of order p^n ([Ko 98]). This suggests that to seek non-trivial Hopf Galois

structures, the most promising place to start is to look for regular embeddings of the Galois group G into $Hol(G)$, up to equivalence by $Aut(G)$.

In this paper we examine $e(G,G)$ for G a symmetric or alternating group ($n \geq 4$). For $K = \mathbb{Q}$, these include the Galois groups of "most" polynomials of degree n. It turns out that the case G simple is essentially the same as for G alternating, $n \geq 5$. We show:

Theorem. *For G simple, $e(G,G) = 2$;*
For the symmetric group S_n, $n \geq 4$,

$$e(S_n, S_n) = 2 \sum_{k=0}^{\lfloor n/4 \rfloor} \frac{n!}{(n-4k)!2^{2k}(2k)!}.$$

For the alternating group $A_4, e(A_4, A_4) = 10$.

We also get a lower bound on $e(S_n, N)$ for $N = A_n \times C_2$, $n \geq 5$, which yields

Theorem. *A Galois extension L/K with Galois group S_n has at least $(n!)^{1/2}$ Hopf Galois structures.*

Our approach to counting $e(G,G)$ is to "unwind" regular embeddings

$$\beta : G \to Hol(G) = G \cdot Aut(G)$$

by showing that for the groups we consider, β maps to $G \cdot Inn(G) \cong G \times G$, hence can be described via the maps $\beta_i : G \to G$ arising from composition with the projection maps $\pi_i : G \times G \to G$, $i = 1, 2$. The equivalence relation on $e(G,G)$ and regularity then allow us to assume that one of β_1, β_2 is the identity. This makes counting $e(G,G)$ feasible.

Normalized embeddings

We begin with the unwinding.

Let G be a finite group, $S = Aut(G)$ and

$$\beta : G \to Hol(G) = G \cdot Aut(G) = G \cdot S$$

be a regular embedding.

Let

$$\gamma : Hol(G) \to S \cdot Inn(S) = Hol(S)$$

by $\gamma(\eta\alpha) = C(\eta)C(\alpha)$, where $C(\eta), \eta \in G$ is the inner automorphism of G given by conjugation by η, and similarly for $C(\alpha)$. To see that γ is a homomorphism is routine, using that for any $\delta \in Aut(G), \eta \in G$,

$$\delta \cdot C(\eta) \cdot \delta^{-1} = C(\delta(\eta))$$

in $Aut(G)$.

Let $j : S \cdot Inn(S) \to S \times S$ by $j(\alpha C(\beta)) = (\alpha\beta, \beta)$; then j is an isomorphism with inverse $i : S \times S \to S \cdot Inn(S)$ by $i(\sigma, \tau) = \sigma\tau^{-1}C(\tau)$.

Let $\pi_i : S \times S \to S$ be the projections: $\pi_i(\sigma_1, \sigma_2) = \sigma_i$, $i = 1, 2$. Let $\hat{\beta}_i = \pi_i j\gamma\beta : G \to S$, homomorphisms.

If $\beta(\tau) = \sigma\alpha$ with τ, σ in G, α in $S = Aut(G)$, then

$$\begin{aligned} j\gamma\beta(\tau) &= j\gamma(\sigma\alpha) \\ &= j(C(\sigma)C(\alpha)) \\ &= (C(\sigma)\alpha, \alpha) \end{aligned}$$

So $\hat{\beta}_1(\tau) = C(\sigma)\alpha$, $\hat{\beta}_2(\tau) = \alpha$. Thus $\hat{\beta}_2$ is the composition of β with the quotient map from $Hol(G)$ to $Aut(G)$. We have, then,

Lemma 1. *$\beta(G) \subset G \cdot Inn(G)$ iff $\hat{\beta}_1(G) \subset Inn(G)$ iff $\hat{\beta}_2(G) \subset Inn(G)$. If these inclusions hold then there exist homomorphisms $\beta_i : G \to G$, $i = 1, 2$, such that*

$$\beta(\tau) = \beta_1(\tau)\beta_2(\tau^{-1})C(\beta_2(\tau)).$$

Proof The first equivalences are clear from the definitions of $\hat{\beta}_i$.

Suppose $\beta(G) \subset Inn(G)$. Then we can write

$$\beta(\tau) = \sigma\rho^{-1}C(\rho)$$

for some σ, ρ in G. Then $\hat{\beta}_1(\tau) = C(\sigma\rho^{-1})C(\rho) = C(\sigma)$ and $\hat{\beta}_2(\tau) = C(\rho)$. Define

$$\beta_i : G \to G$$

by $\beta_1(\tau) = \sigma$, $\beta_2(\tau) = \rho$. Then

$$\beta(\tau) = \beta_1(\tau)\beta_2(\tau^{-1})C(\beta_2(\tau)).$$

□

Lemma 2. *Suppose $\beta(G) \subset G \cdot Inn(G)$. If β_i is 1-1 for $i = 1$ or 2, then there is some $\delta \in Aut(G)$ so that in $Hol(G)$, $\delta^{-1}\beta(\tau)\delta = \beta'(\tau)$ where $\beta'_i(\tau) = \tau$.*

Proof Let $\beta(\tau) = \sigma\rho^{-1}C(\rho)$. For $\delta \in Aut(G)$, let

$$\beta'(\tau) = \delta^{-1}\beta(\tau)\delta = \delta^{-1}\sigma\rho^{-1}C(\rho)\delta = \delta^{-1}(\sigma)\delta^{-1}(\rho^{-1})C(\delta^{-1}(\rho)).$$

Then $\beta'_1(\tau) = \delta^{-1}(\sigma)$ and $\beta'_2(\tau) = \delta^{-1}(\rho)$. If β_1 is 1-1, let $\delta = \beta_1$, then $\sigma = \beta_1(\tau)$ and $\hat{\beta}_1(\tau) = \tau$; if β_2 is 1-1, let $\delta = \beta_2$, then $\rho = \beta_2(\tau)$ and $\hat{\beta}_2(\tau) = \tau$. □

Thus if $\beta(G) \subset G \cdot Inn(G)$ and β_1 is 1-1, we can assume that for all $\tau \in G$,

$$\beta(\tau) = \tau\rho^{-1}C(\rho) \tag{1}$$

for some $\rho \in G$; or if β_2 is 1-1, we can assume that for all $\tau \in G$,

$$\beta(\tau) = \sigma\tau^{-1}C(\tau) \tag{2}$$

for some $\sigma \in G$.

We now show that this description is valid for the groups under consideration.

If G is simple, then, since $Aut(G)/Inn(G)$ is solvable by Schreier's conjecture [Go82, p. 55], $\beta_i : G \to Aut(G)$ maps to $Inn(G)$.

If $G = S_n$, $n \geq 4, n \neq 6$ then $Aut(G) = Inn(G)$.

If $G = S_6$ and $\hat{\beta}_i$ is 1-1, then $\hat{\beta}_i(G) \subset Inn(G)$ since $Inn(S_6)$ is the unique subgroup of $Aut(S_6)$ of index 2 isomorphic to S_6 [LL93].

If $G = A_4$ and $\hat{\beta}_i : A_4 \to Aut(A_4) \cong S_4$, then the image of $\hat{\beta}_i$ is contained in $Inn(A_4)$: the composite

$$A_4 \to S_4 \to S_4/A_4$$

is trivial because A_4 has no subgroups of index 2.

Thus for the groups of interest in this paper, if $\hat{\beta}_i$ is 1-1, then we can assume that β has the form (1) or (2).

We now examine these groups.

Simple Groups

Theorem 4. *If G is simple, then $e(G,G) = 2$.*

Proof Since G is simple, β_i is either 1-1 or trivial.

Case 1 Suppose both β_1 and β_2 are 1-1. Then we can assume

$$\beta(\tau) = \tau\beta_2(\tau^{-1})C(\beta_2(\tau)).$$

Now β is regular iff the function $f : \tau \mapsto \tau\beta_2(\tau^{-1})$ from G to G is 1-1. But f is 1-1 iff the automorphism β_2 is fixed-point free. Since G is non-abelian and simple, G has no fixed-point free automorphisms, another consequence of the classification of finite simple groups [Go82, p. 55]. Thus Case 1 yields no regular embeddings of G into $Hol(G)$.

Case 2 β_1 1-1, β_2 is trivial. Then we can assume β_1 is the identity, and then $\beta(\tau) = \beta_1(\tau) = \tau$, which is regular.

Case 3 β_2 1-1, β_1 is trivial. Then we can assume β_2 is the identity, and then $\beta(\tau) = \tau^{-1}C(\tau)$ which is regular. Since the case β_1 is trivial, β_2 is trivial gives no regular embeddings, we have a total of 2 regular embeddings, as we wished to show. □

Symmetric Groups

Let $G = S_n$ for $n \geq 5$. In this section we compute $e(G,G)$.

Theorem 5. *e(G, G) = two times the number of even permutations in S_n of order dividing 2.*

Proof Let $\beta : G \to Hol(G)$ be a regular embedding and $\hat{\beta}_i : G \to Aut(G)$ be the corresponding projections. If $\hat{\beta}_i$ is 1-1, then $\hat{\beta}(G)$ is either $Aut(G) = Inn(G)$ if $n \neq 6$, or a subgroup of index 2 in $Aut(G)$ if $n = 6$. In that case, $\hat{\beta}(G) = Inn(G)$, as noted above.

Let $A = A_n$ be the alternating group. The restriction of $\hat{\beta}_i$ to A is a homomorphism from A to $Aut(G)$; since $Inn(A)$ is a normal subgroup of $Aut(G)$ and the quotient group has order at most 4, $\hat{\beta}_i$ must map into $Inn(A)$. Hence $\hat{\beta}_i$ restricted to A is either 1-1 or trivial. If both $\hat{\beta}_1$ and $\hat{\beta}_2$ are both trivial on A, then β is trivial on A, so is not regular. Thus at least one of $\hat{\beta}_i$ is 1-1, and we can assume that for all σ in G,

$$\beta(\sigma) = \beta_1(\sigma)\beta_2(\sigma^{-1})C(\beta_2(\sigma))$$

by Lemma 1.

Since β is regular, the stabilizer of the identity element of G is trivial, which means that if $\beta_1(\sigma) = \beta_2(\sigma)$, then $\sigma = 1$.

Now β_i restricted to A is also regular since β is regular on G: for $\sigma \in A$, $\beta_1(\sigma) = \beta_2(\sigma)$ only for $\sigma = 1$. Hence for some i, β_i is 1-1 on A, hence 1-1 on G. Thus we can assume β has one of the following forms:

$$\beta(\sigma) = \sigma\beta_2(\sigma^{-1})C(\beta_2(\sigma)),$$

or

$$\beta(\sigma) = \beta_1(\sigma)\sigma^{-1}C(\sigma).$$

Since β on A is a regular embedding, if β_1 is the identity, then β_2 is trivial on A, and similarly if β_2 is the identity. If β_i is trivial on A, then β_i maps every odd permutation to a single element τ of S of order dividing 2, and is trivial on all even permutations.

Thus there exists an element τ of S so that for all $\sigma \in G$, $\beta(\sigma)$ has one of the two following forms:

- $\beta(\sigma) = \sigma\tau^{-1}C(\tau)$ for σ odd, $\beta(\sigma) = \sigma$ for σ even; or
- $\beta(\sigma) = \tau\sigma^{-1}C(\sigma)$ for σ odd, $\beta(\sigma) = \sigma^{-1}C(\sigma)$ for σ even.

where τ is a fixed element of S of order dividing 2. (Hence $\tau = \tau^{-1}$.)

The only further restriction on τ is that it must be even, for if τ were odd, then $\sigma\tau$ would be even for all odd σ in G, and so $\beta(G)e_G$ would be a subset of A and β would not be

regular. On the other hand, if τ is even, then $\{\sigma\tau|\sigma \text{ odd}\}$ contains all odd permutations of S, and $\{\sigma|\sigma \text{ even}\}$, resp $\{\sigma^{-1}|\sigma \text{ even}\}$ contains all even permutations of G, and so in either case β is regular.

Thus to determine $e(G,G)$ it suffices to observe that if $\beta(\sigma) = \sigma\tau^{-1}C(\tau)$ for σ odd, $\beta(\sigma) = \sigma$ for σ even, or $\beta(\sigma) = \tau\sigma^{-1}C(\sigma)$ for σ odd, $\beta(\sigma) = \sigma^{-1}C(\sigma)$ for σ even, and β' is similarly of one of those two forms for some $\tau' \neq \tau$, then β and β' are not equivalent: that is, there exists no element δ of $Aut(G)$ so that $\delta\beta(\sigma)\delta^{-1} = \beta'(\sigma)$ for all σ. We have three cases.

Case I. $\beta(\sigma) = \sigma\tau^{-1}C(\tau)$ for σ odd, $\beta(\sigma) = \sigma$ for σ even; $\beta'(\sigma) = \tau'\sigma^{-1}C(\sigma)$ for σ odd, $\beta'(\sigma) = \sigma^{-1}C(\sigma)$ for σ even. Then for all σ even,

$$\delta\sigma\delta^{-1} = \sigma^{-1}C(\sigma)$$

or

$$\delta(\sigma) = \sigma^{-1}C(\sigma).$$

This never holds for $\sigma \neq 1$.

The other two cases are similar:

Case II. $\beta(\sigma) = \sigma\tau^{-1}C(\tau)$ for σ odd, $\beta(\sigma) = \sigma$ for σ even; $\beta'(\sigma) = \sigma{\tau'}^{-1}C(\tau')$ for σ odd, $\beta'(\sigma) = \sigma$ for σ even. Then for all σ even,

$$\delta\sigma\delta^{-1} = \sigma,$$

or

$$\delta(\sigma) = \sigma.$$

Case III. $\beta(\sigma) = \tau\sigma^{-1}C(\sigma)$ for σ odd, $\beta(\sigma) = \sigma^{-1}C(\sigma)$ for σ even; $\beta'(\sigma) = \tau'\sigma^{-1}C(\sigma)$ for σ odd, $\beta'(\sigma) = \sigma^{-1}C(\sigma)$ for σ even. Then for all σ even,

$$\delta\sigma^{-1}C(\sigma)\delta^{-1} = \sigma^{-1}C(\sigma)$$

or

$$\delta(\sigma^{-1})C(\delta(\sigma^{-1})) = \sigma^{-1}C(\sigma),$$

hence $\delta(\sigma) = \sigma$ for all even σ.

To finish both case II and case III, we note that if $\delta = C(\pi)$ for some $\pi \in S_n$ and δ fixes all of A_n then $\pi = 1$; if δ is an outer automorphism, then $n = 6$ and the centralizer of δ in $Aut(S_6)$ contains $Inn(A_6)$, so has order ≥ 360: but any outer automorphism of S_6 has centralizer of order dividing 20, by [LL93, Proposition 2.3]. Therefore δ is trivial and $\tau = \tau'$.

Thus $e(G,G)$ is twice the number of even permutations in S of order dividing 2, as we wished to show $\square$

Corollary 6.

$$e(G,G) = 2\sum_{k=0}^{\lfloor n/4 \rfloor} \frac{n!}{(n-4k)!2^{2k}(2k)!}$$

Proof Any permutation of A_n of order dividing 2 is the product of an even number of disjoint transpositions. To find all products of $2k$ disjoint transpositions for $0 \leq k \leq n/4$, pick two numbers from the original n, then two from the remaining $n-2$ numbers, then two from the remaining, etc.: the number of choices is $\binom{n}{2} \cdot \binom{n-2}{2} \cdot \ldots \cdot \binom{n-(4k-2)}{2}$. That gives $\frac{n!}{(n-4k)!2^{2k}}$ choices. But since the order of the $2k$ transpositions doesn't matter, we divide by $(2k)!$. The result is the number of ways of choosing an element which is a product of $2k$ disjoint transpositions. □

The groups A_4 and S_4

Theorem 7. *$e(A_4,A_4) = 10$ and $e(S_4,S_4) = 8$.*

The proofs are similar to those above. For both groups, Lemma 1 applies, so for $A = A_4$ we have three cases for possible embeddings:

1. β_1 is 1-1, β_2 is 1-1;
2. β_1 is 1-1, $|\beta_2(A)|$ divides 3;
3. $|\beta_1(A)|$ divides 3, β_2 is 1-1.

Case 1 gives no embeddings, as before.

For *Case 2*, if β_1 is 1-1, then we can assume that β has the form

$$\beta(\sigma) = \sigma\beta_2(\sigma^{-1})C(\beta_2(\sigma))$$

for all σ in A_4; then β is regular iff the map

$$f : \sigma \mapsto \sigma\beta_2(\sigma^{-1})$$

is 1-1. If β_2 is trivial, then β is regular. If β_2 has kernel V_4, then f is 1-1 on V_4. Fix a τ of order 3, then β_2 is determined by $\beta_2(\tau)$. Now $\tau\beta_2(\tau^{-1})$ cannot be in V_4, or else f is not 1-1. Thus $\beta_2(\tau)$ must be in the same coset modulo V_4 as τ. There are then four choices for $\beta_2(\tau)$, and each gives a regular embedding. Thus we have five regular embeddings from case 2.

Case 3 is similar to Case 2.

Since $Aut(A_4) = Inn(S_4)$, it is a routine computation similar to that for S_n above that the 10 regular embeddings are all non-equivalent. We leave details to the reader. Similar arguments give the result for S_4.

Computing $e(G,N)$ for $N \ncong G$

To count the number of Hopf Galois structures on a Galois extension L/K with Galois group G, we need to know not only $e(G,G)$ but also $e(G,N)$ for groups N not isomorphic to G but of the same cardinality as G. This is a non-trivial task: for example, if $G = S_6$, a group of order 720, there are 839 such groups N to be checked [GAP97].

For simple groups the task is made easier by the following observation:

Lemma 8. *If G is simple, N is a group not isomorphic to G but of the same cardinality, and $e(G,N) \neq 0$, then G embeds in $O(N) = Aut(N)/Inn(N)$*

Proof Let $\beta : G \to Hol(N) = N \cdot Aut(N)$ be a regular map. Consider the composition

$$\rho\pi\beta : G \to N \cdot Aut(N) \to Aut(N) \to O(N).$$

If $\pi\beta = 0$ then β yields an isomorphism from G to N since β is regular. Thus $\pi\beta$ is 1-1. If $\rho\pi\beta = 0$ then $\pi\beta$ maps G onto $Inn(N) \cong N$. Thus $\rho\pi\beta$ is 1-1. □

For G simple, this greatly restricts the possible $N \ncong G$ for which $e(G,N) \neq 0$. For simple G with $|G| \leq 1000$ the only case we found where G embeds in $O(N)$ for $N \ncong G$ is $G = GL_3(\mathbb{F}_2), N = C_2^3 \times K$ of order 168, where K is any group of order 21. But then, since C_2^3 and K are characteristic subgroups of N, $Hol(N) \cong Hol(C_2^3) \times Hol(K)$. If $\beta : G \to Hol(N)$ were regular, then $G \to Hol(K)$ would be non-trivial, and hence G would embed in $Hol(K)$. However, if $K = C_7 \cdot C_3$ is non-abelian, then $Aut(K) = Hol(C_7)$ so $Hol(K)$ has order $21 \cdot 42$, while if $K = C_{21}$, then $Aut(K) = C_{12}$ and $Hol(K)$ has order $21 \cdot 12$ [**Correction** May 3, 2004: $Aut(K) = C_6 \times C_2$, which has the same order]. Hence in neither case does G embed in $Hol(K)$.

By contrast, we have

Theorem 9. *Let $n \geq 5$ and $N = A_n \times C_2$. Then $e(S_n,N) =$ the number of odd permutations of S_n of order 2.*

Proof Both C_2 and A_n are characteristic subgroups of N: C_2 is characteristic because C_2 is the center of N. A_n is in fact fully invariant: any endomorphism α of N takes A_n to itself, for if π is the projection of N onto C_2, then $\pi\alpha = 0$. Since $N = A_n \times C_2$ and both factors are characteristic,

$$Hol(N) = Hol(A_n) \times Hol(C_2) = (A_n \cdot Aut(A_n)) \times C_2.$$

Now $Aut(A_n) = Aut(S_n) = Inn(S_n)$ for $n \neq 6$, a theorem of Hölder (c.f. [Ro82], p. 399), and $Aut(A_6) = Aut(S_6)$ by [LL93], Theorem 4.6.

Suppose $\beta : S_n \to (A_n \cdot Aut(A_n)) \times C_2$ is regular. Then the maps obtained by following β by the two projections,

$$\beta_a : S_n \to A_n \cdot Aut(A_n)$$

and

$$\beta_b : S_n \to C_2$$

are both regular. Thus β_b is onto, has kernel A_n, and is unique.

For σ in S_n let $\beta_a(\sigma) = \eta\alpha$, where $\eta \in A_n$, $\alpha \in Aut(A_n)$. If we compose β_a with the map

$$j\gamma : A_n \cdot Aut(A_n) \to Aut(A_n) \times Aut(A_n)$$

followed by the projection maps onto $Aut(A_n)$ we obtain maps

$$\hat{\beta}_i : S_n \to Aut(A_n) = Aut(S_n)$$

by $\hat{\beta}_1(\sigma) = C(\eta)\alpha$, $\hat{\beta}_2(\sigma) = \alpha$.

If $n = 6$ then at least one of $\hat{\beta}_1$ and $\hat{\beta}_2$ is 1-1. Otherwise, both have kernel containing A_6, and so β is not 1-1. But if $\hat{\beta}$ is 1-1, then $\hat{\beta}_i$ maps onto $Inn(S_6)$ as noted below Lemma 2. If $n \neq 6$ then $Aut(S_n) = Inn(S_n)$. Hence for all n, $\alpha = C(\tau)$ for some $\tau \in S_n$, so $\hat{\beta}_i$ yields $\beta_i : S_n \to S_n$ where $\beta_1(\sigma) = \eta\tau, \beta_2(\sigma) = \tau$ with $\eta \in A_n, \tau \in S_n$, and

$$\beta_a(\sigma) = \beta_1(\sigma)\beta_2(\sigma^{-1})C(\beta_2(\sigma)) \in A_n \cdot Inn(S_n).$$

If β_1 is 1-1, then by Lemma 2 there is some $\delta \in Aut(S_n) = Aut(A_n)$ so that $\delta^{-1}(\beta_a(\sigma))\delta = \beta(\sigma)$ with $\beta_1(\sigma) = \sigma$. Hence we can assume that $\beta_a(\sigma) = \sigma\tau^{-1}C(\tau)$ for $\tau = \beta_2(\sigma)$. Similarly if β_2 is 1-1.

If both β_1 and β_2 are 1-1, we can assume $\beta_1(\sigma) = \sigma$ and β_2 is an automorphism of S_n. For β_a to be regular, the function $f : S_n \to A_n$, $f(\sigma) = \sigma\beta_2(\sigma^{-1})$, must be surjective. Let η be in the image of f. Then $\sigma_1\beta_2(\sigma_1^{-1}) = \eta = \sigma_2\beta_2(\sigma_2^{-1})$ iff $\sigma_2^{-1}\sigma_1$ is fixed by the automorphism β_2, and so the cardinality of the preimage of any $\eta \in A_n$ is equal to the cardinality of the set $B(\beta_2)$ of fixed points of β_2. If β_2 is inner, conjugation by $\pi \in S_n$, then $|B(\beta_2)|$ is easily seen to be at least 3 for any π. If $n = 6$ and β_2 is an outer automorphism of S_6, then $|B(\beta_2)| \geq 4$ by [LL93] (see page 290, top). Hence if both β_1 and β_2 are 1-1, then β_a cannot be regular.

Thus if β_a is regular, exactly one of β_1 and β_2 is 1-1, and the other map is therefore trivial on A_n and maps any odd permutation to a fixed permutation τ of order 2 in S_n. Thus β_a either has the form

$$\beta_a(\sigma) = \sigma\tau^{-1}C(\tau) \text{ for } \sigma \text{ odd},$$
$$\beta_a(\sigma) = \sigma \text{ for } \sigma \text{ even},$$

or

$$\beta_a(\sigma) = \tau\sigma^{-1}C(\sigma) \text{ for } \sigma \text{ odd},$$
$$\beta_a(\sigma) = \sigma^{-1}C(\sigma) \text{ for } \sigma \text{ even}.$$

Since $\beta_a : S_n \to A_n \cdot Inn(S_n)$, τ must be odd. As in the proof of Theorem 5, both cases give distinct embeddings β for all odd τ of order 2, and so the number of regular embeddings of S_n into $A_n \cdot Inn(S_n)$ is equal to twice the number of odd permutations in S_n of order 2. □

The same argument as for Corollary 6 gives

Corollary 10. *For $n \geq 5$,*

$$e(S_n, A_n \times C_2) = 2\sum_{k=0}^{\infty} \frac{n!}{(n-4k-2)!2^{2k+1}(2k+1)!}.$$

Corollary 11. *If L/K is a Galois extension with Galois group S_n, $n \geq 5$, then the number of Hopf Galois structures on L/K is at least $(n!)^{1/2}$.*

Proof The sums of Corollaries 6 and 11 add up to

$$2\sum_{j=0}^{\infty} \frac{n!}{(n-2j)!2^j j!}.$$

For $n = 2k+2$, the term for $j = k$ is

$$\frac{(2k+2)!}{2!2^k k!};$$

for $n = 2k+1$ the term for $j = k$ is

$$\frac{(2k+1)!}{2^k k!}.$$

Each of these terms is easily seen to be $\geq (n!)^{1/2}$. □

Note that by Stirling's formula, $(n!)^{1/2} \geq (2\pi)^{1/4} n^{1/4} (\frac{n}{e})^{n/2}$. Finally, we remark that by a now familiar argument, $e(S_6, M_{10}) = 72$, so a lower bound for the number of Hopf Galois structures on L/K with Galois group S_6 is 224.

This research was partially supported by National Security Agency research grant #MDA9049710114.

References

[By96] N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions,* Comm. Algebra **24** (1996), 3217-3228, 3705.

[CS69] S. Chase, M. E. Sweedler *Hopf Algebras and Galois Theory,* Springer Lecture Notes in Mathematics *97* (1969)

[GAP97] *GAP–Groups, Algorithms and Programming* The GAP group, Lehrstuhl D fur Mathematik, RWTH Aachen, Germany, and School of Mathematical and Computational Sciences, U. St. Andrews, Scotland *Version 3.4.4* (1997)

[Go82] D. Gorenstein *Finite Simple Groups, An Introduction to Their Classification,* Plenum Press, New York and London (1982)

[GP87] C. Greither, B. Pareigis *Hopf Galois theory for separable field extensions,* J. Algebra *106* (1987), 239-258.

[Ko98] T. Kohl *Classification of the Hopf Galois structures on prime power radical extensions,* J. Algebra *207* (1998), 525-546.

[LL93] T. Y. Lam, D. B. Leep *Combinatorial structure on the automorphism group of* S_6 Expositiones Math *11* (1993), 289-308.

[Ro82] D. J. S. Robinson *A Course in the Theory of Groups* Springer Verlag, New York (1982)