Degree-weighted Normal Covers of Symmetric and Alternating Groups

Luca Blanchi

June 2026

Abstract

Let G be a finite group. A normal cover of G is a family of proper subgroups $H_i < G$ such that the union of their conjugates is all of G. The usual normal covering number counts the number of conjugacy classes of subgroups used. We study the degree-weighted variant

$$\beta(G) = \min \sum_i [G : H_i],$$

where the minimum is taken over normal covers by proper subgroups. Equivalently, $\beta(G)$ is the minimum degree of a finite G-set Ω such that every element of G fixes some point of Ω, while G has no global fixed point on Ω. We also study the faithful version $\beta_{\text{faith}}(G)$, where the G-action is required to be faithful.

This invariant is a degree-weighted analogue of the normal covering number and of the invariant $s(G)$ appearing in the theory of intersective polynomials. In that setting, $s(G)$ records the minimum number of irreducible factors forced by group theory; $\beta_{\text{faith}}(G)$ records instead the minimum possible total permutation degree.

We prove that, for all sufficiently large odd n,

$$\beta_{\text{faith}}(S_n) = 2^{n-1} + 1,$$

and classify the optimal covers. For even n, we prove the second-order estimate

$$\beta_{\text{faith}}(S_n) = \frac{1}{2}\binom{n}{n/2} + \Theta\left(\binom{n}{\lfloor n/3 \rfloor}\right).$$

For alternating groups of even degree, we prove the exact formula

$$\beta_{\text{faith}}(A_{2m}) = \sum_{\substack{1 \le k < m \\ k \text{ odd}}} \binom{2m}{k} + \frac{1}{2}\binom{2m}{m}$$

for all sufficiently large m, and classify the optimal covers. Equivalently,

$$\beta_{\text{faith}}(A_{2m}) = \begin{cases} 2^{2m-2}, & m \text{ odd}, \\ 2^{2m-2} + \frac{1}{2}\binom{2m}{m}, & m \text{ even}. \end{cases}$$

For n odd composite, with $q = P^-(n)$ the smallest prime divisor of n, we prove

$$\beta_{\text{faith}}(A_n) \sim \frac{n!}{((n/q)!)^q q!}.$$

For $n = p$ prime,

$$\beta_{\text{faith}}(A_p) = (1 + o(1))c_p,$$

where

$$c_p = \min\{[A_p : H] : H < A_p,\ H \text{ contains a } p\text{-cycle}\},$$

and

$$\log \beta_{\mathrm{faith}}(A_p) = p \log p - p + O((\log p)^2).$$

The proofs combine a dual certificate for weighted set cover, slack identities, elementary cycle-type arguments, comparisons among imprimitive wreath products, and standard bounds for primitive permutation groups.

1 Introduction

Let G be a finite group. A normal cover of G is a family of proper subgroups $H_1, \ldots, H_r < G$ such that

$$G = \bigcup_{i=1}^{r} \bigcup_{g \in G} g H_i g^{-1}.$$

The normal covering number $\gamma(G)$ is the minimum possible number r, or equivalently the minimum number of conjugacy classes of proper subgroups needed. Normal covers of finite groups, and especially of symmetric and alternating groups, have been studied extensively.

In arithmetic applications, especially in the theory of intersective polynomials, one is often interested in covers by proper subgroups whose cores intersect trivially. Bubboloni and Sonn define an invariant $s(G)$ as the minimum number of proper subgroups whose conjugates cover G and whose total core intersection is trivial. This gives a group-theoretic lower bound for the number of irreducible factors of an intersective polynomial with Galois group G.

The present paper studies the degree-weighted analogue. Instead of assigning cost 1 to a subgroup H, we assign cost

$$[G : H],$$

the degree of the transitive permutation representation $G \curvearrowright G/H$. Thus the cost of a family H_i is

$$\sum_i [G : H_i].$$

This is the total degree of the associated finite G-set. In arithmetic language, it is the degree of the corresponding finite etale algebra, or the total degree of the corresponding product of irreducible factors.

The weighted invariant behaves differently from the usual normal covering number. In the unweighted problem for S_n and A_n, one is led to additive-combinatorial questions about partitions of n. In the weighted problem, the first-order behavior is governed by expensive cycle classes, such as n-cycles and two-cycle classes $(k, n-k)$. A residual partition problem still appears in the second-order behavior of $\beta_{\mathrm{faith}}(S_{2m})$.

The main proof method is a dual certificate. Given nonnegative weights on conjugacy classes, if every proper subgroup H sees total class-weight at most $[G : H]$, then the total weight gives a lower bound for $\beta(G)$. In the extremal cases we study, the dual certificates are sharp. Their slack identities give not only values of β_{faith}, but also rigidity of the optimal covers.

2 Definitions

Let G be a finite group. A finite G-set Ω is called a fixed-point cover if

$$\Omega^g \neq \varnothing \qquad \text{for every } g \in G.$$

It is called blind if, in addition,

$$\Omega^G = \varnothing.$$

It is called faithfully blind if the action of G on Ω is faithful.

Define

$$\beta(G) = \min\{|\Omega| : \Omega \text{ is a blind finite } G\text{-set}\},$$

and

$$\beta_{\text{faith}}(G) = \min\{|\Omega| : \Omega \text{ is a faithfully blind finite } G\text{-set}\}.$$

Every finite G-set decomposes as a disjoint union of transitive G-sets:

$$\Omega = \bigsqcup_i G/H_i.$$

For $g \in G$,

$$(G/H_i)^g \neq \varnothing$$

if and only if

$$g \in xH_ix^{-1}$$

for some $x \in G$. Therefore Ω is a fixed-point cover if and only if

$$G = \bigcup_i \bigcup_{x\in G} xH_ix^{-1}.$$

Moreover,

$$(G/H_i)^G \neq \varnothing$$

if and only if $H_i = G$. Thus Ω is blind if and only if all H_i are proper and their conjugates cover G.

The kernel of the action of G on G/H_i is

$$\mathrm{Core}_G(H_i) = \bigcap_{x\in G} xH_ix^{-1}.$$

Hence the kernel of the action on

$$\bigsqcup_i G/H_i$$

is

$$\bigcap_i \mathrm{Core}_G(H_i).$$

Thus

$$\beta(G) = \min\left\{\sum_i [G : H_i] : H_i < G,\ G = \bigcup_i \bigcup_{x\in G} xH_ix^{-1}\right\},$$

and

$$\beta_{\mathrm{faith}}(G) = \min\left\{\sum_i [G : H_i] : H_i < G,\ G = \bigcup_i \bigcup_{x\in G} xH_ix^{-1}, \bigcap_i \mathrm{Core}_G(H_i) = 1\right\}.$$

For A_n, $n \geq 5$, the group is simple, so every proper subgroup has trivial core. Therefore

$$\beta_{\mathrm{faith}}(A_n) = \beta(A_n).$$

For S_n, $n \geq 5$, the same equality holds.

Lemma 2.1. For $n \geq 5$,

$$\beta_{\mathrm{faith}}(S_n) = \beta(S_n).$$

Proof.
Let $H_1, \ldots, H_r$ be a normal cover of S_n by proper subgroups. Since the cover must contain odd permutations, at least one H_i is not contained in A_n. The core of this H_i cannot be A_n, and cannot be S_n because H_i is proper. Since the only nontrivial proper normal subgroup of S_n, for $n \geq 5$, is A_n, this core is trivial. Hence the total core intersection is trivial. □

3 Cycle classes and elementary subgroup facts

We use standard cycle-type notation. A class of S_n is described by a partition of n. We write (a, b) for the class of permutations with two cycles of lengths a and b.

Recall that a conjugacy class of S_n splits into two classes in A_n if and only if all cycle lengths are odd and pairwise distinct.

Lemma 3.1. Let $H < S_n$ be intransitive. If H contains an element of cycle type $(a, n-a)$, then, after conjugacy,

$$H \leq S_a \times S_{n-a}.$$

Consequently,

$$[S_n : H] \geq \binom{n}{a}.$$

Similarly, if $H < A_n$ is intransitive and contains an element of type $(a, n-a)$, then, after conjugacy,

$$H \leq (S_a \times S_{n-a}) \cap A_n,$$

and

$$[A_n : H] \geq \binom{n}{a}.$$

Proof.

Let $x \in H$ have cycle type $(a, n-a)$. Since $x \in H$, each cycle support of x is contained in an H-orbit. Hence every H-orbit is a union of the two cycle supports of x. Since H is intransitive, it cannot have a single orbit containing both cycle supports. Therefore the H-orbits are exactly the two supports, of sizes a and $n-a$. The containment and index estimate follow. The A_n case is identical. $\square$

Lemma 3.2. Let n be even and let $k < n/2$ be odd. The S_n-class of cycle type $(k, n-k)$ splits into two A_n-classes. The subgroup

$$(S_k \times S_{n-k}) \cap A_n$$

meets both of them.

Proof.

The splitting criterion applies because k and $n-k$ are distinct odd integers. Let

$$M = S_k \times S_{n-k}.$$

Then M contains odd permutations. If $x \in M \cap A_n$ has type $(k, n-k)$, and $t \in M$ is odd, then

$$txt^{-1} \in M \cap A_n$$

has the same S_n-cycle type. Since conjugation by an odd element interchanges the two A_n-classes lying inside a split S_n-class, $M \cap A_n$ meets both classes. $\square$

Lemma 3.3. Let n be odd composite, let $q = P^-(n)$, and set

$$W_q = S_{n/q} \wr S_q$$

in its natural imprimitive action on n points. Then

$$W_q \cap A_n$$

meets both A_n-classes of n-cycles.

Proof.

The S_n-class of n-cycles splits in A_n, since n is odd. The wreath product W_q contains an n-cycle. It also contains odd permutations, for instance a transposition inside one block. If $c \in W_q \cap A_n$ is an n-cycle and $t \in W_q$ is odd, then

$$tct^{-1} \in W_q \cap A_n$$

is an n-cycle lying in the other A_n-class. $\square$

Lemma 3.4. Let p be an odd prime. If $H < A_p$ contains a p-cycle, then H meets both A_p-classes of p-cycles.

Proof.

Let $c \in H$ be a p-cycle. Then H contains every power c^a, $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. The two A_p-classes of p-cycles are distinguished by whether a is a quadratic residue or nonresidue modulo p. Hence the powers of c meet both classes. □

4 Dual certificates and slack

Let $\mathcal{C}(G)$ be the set of nonidentity conjugacy classes of G.

Proposition 4.1. Let $w : \mathcal{C}(G) \to \mathbb{R}_{\geq 0}$ satisfy

$$\sum_{\substack{C \in \mathcal{C}(G) \\ C \cap H \neq \varnothing}} w(C) \leq [G : H]$$

for every proper subgroup $H < G$. Then

$$\beta(G) \geq \sum_{C \in \mathcal{C}(G)} w(C).$$

If G is nonabelian simple, then the same lower bound holds for $\beta_{\mathrm{faith}}(G)$.

Proof.

Let $H_1, \ldots, H_r$ be a normal cover of G. Every nonidentity conjugacy class meets at least one H_i. Hence

$$\sum_C w(C) \leq \sum_{i=1}^{r} \sum_{\substack{C \\ C \cap H_i \neq \varnothing}} w(C) \leq \sum_{i=1}^{r} [G : H_i].$$

Taking the minimum over all normal covers gives the result. If G is simple, every proper subgroup has trivial core. □

Proposition 4.2. With w as in Proposition 4.1, put

$$w(H) = \sum_{\substack{C \\ C \cap H \neq \varnothing}} w(C)$$

and

$$\mathrm{slack}_w(H) = [G : H] - w(H).$$

If $\mathcal{H} = \{H_1, \ldots, H_r\}$ is a normal cover, define

$$\mathrm{overlap}_w(\mathcal{H}) = \sum_i w(H_i) - \sum_C w(C).$$

Then

$$\sum_i [G : H_i] - \sum_C w(C) = \sum_i \mathrm{slack}_w(H_i) + \mathrm{overlap}_w(\mathcal{H}).$$

In particular, if the cover has cost equal to $\sum_C w(C)$, then every subgroup used is w-tight and every positive-weight class is covered exactly once.

Proof.

This is the identity

$$\sum_i [G : H_i] = \sum_i w(H_i) + \sum_i ([G : H_i] - w(H_i)).$$

Subtracting $\sum_C w(C)$ gives the formula. Since every positive-weight class is covered at least once,

$$\mathrm{overlap}_w(\mathcal{H}) \geq 0.$$

If the total cost equals $\sum_C w(C)$, then both nonnegative terms on the right are zero. □

5 Imprimitive and primitive estimates

We use the following standard consequence of Maroti's bound on primitive permutation groups.

Lemma 5.1. For all sufficiently large n, if $H < S_n$ is primitive and does not contain A_n, then

$$[S_n : H] > 2^n.$$

If $H < A_n$ is primitive and proper, then

$$[A_n : H] > 2^{n-1}.$$

Proof.

By Maroti's bound,

$$|H| < 50n^{\sqrt{n}}.$$

Therefore

$$[S_n : H] > \frac{n!}{50n^{\sqrt{n}}}.$$

Stirling's formula gives

$$\log\left(\frac{n!}{50n^{\sqrt{n}}}\right) = n\log n - n - O(\sqrt{n}\log n),$$

which is larger than $n \log 2$ for all sufficiently large n. The alternating-group version differs only by a factor 2. □

Lemma 5.2. Let $H < S_n$ be transitive and imprimitive, and suppose that H contains an n-cycle. Then H is contained in a conjugate of

$$S_{n/b} \wr S_b$$

for some proper divisor $b \mid n$, $1 < b < n$. Conversely, every such wreath product contains an n-cycle.

Proof.

An imprimitive transitive subgroup preserves a system of b blocks of equal size n/b, with $1 < b < n$. Therefore it embeds in $S_{n/b} \wr S_b$. Conversely, label the points by pairs

$$(i, j) \in \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/(n/b)\mathbb{Z}.$$

The permutation

$$(i, j) \mapsto \begin{cases} (i+1, j), & i \neq b-1, \\ (0, j+1), & i = b-1, \end{cases}$$

lies in $S_{n/b} \wr S_b$ and is an n-cycle. $\square$

Lemma 5.3. Let n be composite and $q = P^-(n)$. Then

$$\max_{\substack{b \mid n \\ 1<b<n}} ((n/b)!)^b b! = ((n/q)!)^q q!.$$

Proof.
Put

$$D_b = ((n/b)!)^b b!.$$

Let

$$F(x) = x \log \Gamma(n/x + 1) + \log \Gamma(x + 1).$$

Then $F(b) = \log D_b$ for every divisor $b \mid n$.
Writing $y = n/x$, we have

$$F'(x) = \log \Gamma(y + 1) - y\psi(y + 1) + \psi(x + 1),$$

and

$$F''(x) = \frac{y^2}{x}\psi'(y + 1) + \psi'(x + 1) > 0.$$

Thus F is convex.
Every proper divisor b of n satisfies

$$q \leq b \leq n/q.$$

A convex function on this interval attains its maximum at an endpoint. Write $r = n/q$. Then

$$D_q = (r!)^q q!, \qquad D_r = (q!)^r r!,$$

so

$$\frac{D_q}{D_r} = \frac{(r!)^{q-1}}{(q!)^{r-1}}.$$

The function

$$t \mapsto (t!)^{1/(t-1)}$$

is increasing for $t \geq 2$, because

$$((t+1)!)^{1/t} \geq (t!)^{1/(t-1)}$$

is equivalent to

$$(t+1)^{t-1} \geq t!,$$

which is immediate. Hence $D_q \geq D_r$, and the maximum occurs at $b = q$. $\square$

Lemma 5.4. For all sufficiently large n, if $b \mid n$, $3 \leq b < n$, and $a = n/b$, then

$$[S_n : S_a \wr S_b] > 2^n.$$

The analogous alternating-group index is $> 2^{n-1}$.

Proof.

Let

$$I(n,b) = \frac{n!}{(a!)^b b!}, \qquad a = n/b.$$

We show uniformly that

$$\log I(n,b) > n \log 2$$

for n large.

If

$$3 \leq b \leq \frac{n}{(\log n)^2},$$

then Stirling's formula gives

$$\log I(n,b) = n \log b - b \log b + b + O(b \log a + \log b).$$

Since $b \leq n/(\log n)^2$, the error is $O(n/\log n)$, while $b \log b = o(n)$. Hence

$$\log I(n,b) \geq n \log 3 - o(n) > n \log 2$$

for large n.

If

$$b > \frac{n}{(\log n)^2},$$

then

$$a < (\log n)^2.$$

Writing $b = n/a$, we get

$$\log I(n,b) = n\left(1 - \frac{1}{a}\right)\log n + O(n \log\log n).$$

Since $a \geq 2$, this is at least

$$\frac{n}{2}\log n - O(n\log\log n) > n\log 2$$

for all sufficiently large n.

The alternating-group statement differs by at most a factor 2. □

6 Symmetric groups

Theorem 6.1. For all sufficiently large odd n,

$$\beta_{\text{faith}}(S_n) = 2^{n-1} + 1.$$

Moreover, the optimal cover is unique up to conjugacy and ordering: it consists of

$$A_n$$

and

$$S_k \times S_{n-k}, \qquad 1 \le k \le \frac{n-1}{2}.$$

Proof.

Let $n = 2m + 1$.

For the upper bound, take A_n and the intransitive subgroups

$$S_k \times S_{n-k}, \qquad 1 \le k \le m.$$

The cost is

$$2 + \sum_{k=1}^{m} \binom{n}{k} = 2^{n-1} + 1.$$

The subgroup A_n covers all even permutations. If g is odd, then g is not an n-cycle, because n-cycles are even when n is odd. Hence g has at least two cycles and preserves a nonempty proper union of cycle supports of size $k \le m$. Thus g lies in a conjugate of $S_k \times S_{n-k}$.

For the lower bound, assign weight 2 to the class of n-cycles and weight $\binom{n}{k}$ to the class of type $(k, n-k)$, for $1 \le k \le m$. All other classes have weight 0.

The subgroup A_n sees only the n-cycle class among the positive-weight classes, hence sees weight $2 = [S_n : A_n]$. An intransitive subgroup that sees $(k, n-k)$ has index at least $\binom{n}{k}$ by Lemma 3.1, and sees no other positive-weight two-cycle class. A transitive proper subgroup other than A_n has index greater than the total weight for n large, by Lemmas 5.1 and 5.4. Thus Proposition 4.1 gives the lower bound.

For uniqueness, use Proposition 4.2. Any optimal cover must use only tight subgroups. The tight subgroups for the above certificate are exactly A_n and the subgroups $S_k \times S_{n-k}$, $1 \le k \le m$. Each positive-weight class must be covered exactly once. Therefore every optimal cover consists precisely of these subgroups, up to conjugacy and ordering. □

Theorem 6.2. For $n \to \infty$ through even integers,

$$\beta_{\mathrm{faith}}(S_n) = \frac{1}{2}\binom{n}{n/2} + \Theta\left(\binom{n}{\lfloor n/3 \rfloor}\right).$$

Proof.

Let $n = 2m$. Since $n \geq 5$,

$$\beta_{\mathrm{faith}}(S_n) = \beta(S_n).$$

First, an n-cycle is odd. Therefore every normal cover of S_n must contain a subgroup whose conjugates meet the n-cycle class. The least index of a proper subgroup containing an n-cycle is

$$[S_n : S_m \wr S_2] = \frac{1}{2}\binom{n}{m}.$$

Indeed, this is the least imprimitive index by Lemmas 5.2 and 5.3, and primitive subgroups have larger index for large n by Lemma 5.1. Thus

$$\beta(S_n) \geq \frac{1}{2}\binom{n}{m}.$$

We now prove the lower bound for the second term. Choose a three-cycle type τ_n as follows.

If $n = 6r$, take

$$\tau_n = (2r-1, 2r, 2r+1).$$

If $n = 6r+2$, take

$$\tau_n = (2r, 2r+1, 2r+1).$$

If $n = 6r+4$, take

$$\tau_n = (2r+1, 2r+1, 2r+2).$$

Let

$$a_n = \min \tau_n.$$

Then

$$a_n = \lfloor n/3 \rfloor + O(1),$$

and

$$\binom{n}{a_n} \asymp \binom{n}{\lfloor n/3 \rfloor}.$$

The class τ_n consists of odd permutations, because it has exactly three cycles and n is even. It is not contained in any conjugate of

$$W = S_m \wr S_2.$$

Indeed, an element of W either preserves the two blocks, in which case some nonempty proper union of its cycle supports has size m, or interchanges the two blocks, in which case all of its cycles have even length. The chosen τ_n has at least one odd part and has no nonempty proper subset sum equal to m, for all sufficiently large n.

Assign weight

$$I_n = \frac{1}{2}\binom{n}{m}$$

to the class of n-cycles, and weight

$$B_n = \binom{n}{a_n}$$

to the class τ_n.

We verify the dual inequalities. A subgroup contained in a conjugate of W sees the n-cycle class but not τ_n, so it sees weight at most $I_n = [S_n : W]$. A subgroup containing an n-cycle but not contained in a conjugate of W has index $> 2^n$ for large n, by Lemmas 5.1 and 5.4, while $I_n + B_n = o(2^n)$.

If an intransitive subgroup sees τ_n, then it has an orbit whose size is a nonempty proper subset sum of the three parts of τ_n. The smallest such size not exceeding $n/2$ is a_n. Hence its index is at least

$$\binom{n}{a_n} = B_n.$$

A transitive subgroup seeing τ_n but not lying in a conjugate of W again has index $> 2^n$ for large n, unless it is A_n; but A_n does not see τ_n, since τ_n is odd. Thus the dual certificate is valid, and

$$\beta(S_n) \geq \frac{1}{2}\binom{n}{m} + c\binom{n}{\lfloor n/3 \rfloor}$$

for some absolute $c > 0$.

For the upper bound, take $W = S_m \wr S_2$, take A_n, and take all intransitive subgroups

$$S_k \times S_{n-k}, \qquad 1 \leq k \leq n/3.$$

The subgroup W covers the n-cycles, and A_n covers all even permutations. Any odd permutation which is not an n-cycle has at least three cycles and therefore has a cycle of length at most $n/3$. Hence it is covered by one of the intransitive subgroups above.

The extra cost beyond W is

$$2 + \sum_{k \leq n/3} \binom{n}{k} = O\left(\binom{n}{\lfloor n/3 \rfloor}\right),$$

since the binomial coefficients are increasing up to $n/2$ and the sum up to $n/3$ is dominated by its final term. Therefore

$$\beta(S_n) \leq \frac{1}{2}\binom{n}{m} + C\binom{n}{\lfloor n/3 \rfloor}$$

for some absolute $C > 0$. $\square$

7 Alternating groups of even degree

Theorem 7.1. For all sufficiently large m,

$$\beta_{\text{faith}}(A_{2m}) = \sum_{\substack{1 \le k < m \\ k \text{ odd}}} \binom{2m}{k} + \frac{1}{2}\binom{2m}{m}.$$

Moreover, the optimal cover is unique up to conjugacy and ordering: it consists of

$$(S_m \wr S_2) \cap A_{2m}$$

and the subgroups

$$(S_k \times S_{2m-k}) \cap A_{2m}, \qquad 1 \le k < m,\ k \text{ odd}.$$

Proof.
Let $n = 2m$. Since A_n is simple for $n \ge 5$,

$$\beta_{\text{faith}}(A_n) = \beta(A_n).$$

For the upper bound, take

$$W = (S_m \wr S_2) \cap A_n$$

and

$$H_k = (S_k \times S_{n-k}) \cap A_n$$

for $k < m$ odd. The cost is

$$\frac{1}{2}\binom{n}{m} + \sum_{\substack{1 \le k < m \\ k \text{ odd}}} \binom{n}{k}.$$

If $g \in A_n$ has only even cycles, then alternatingly coloring each cycle puts g in a conjugate of W. If g has odd cycles, their number is even. If one odd cycle has length $k < m$, then g lies in a conjugate of H_k. The remaining case is two odd cycles both of length m, and this is covered by W.

For the lower bound, assign total weight $\binom{n}{k}$ to the two split A_n-classes of type $(k, n-k)$, for each odd $k < m$, and weight $\frac{1}{2}\binom{n}{m}$ to the class (m, m).

The dual inequalities follow as follows. Intransitive subgroups seeing $(k, n-k)$ have index at least $\binom{n}{k}$. Intransitive subgroups seeing (m, m) have index at least $\binom{n}{m}$, larger than the assigned weight. The subgroup W sees only (m, m), and sees exactly its index in weight. Other transitive imprimitive subgroups have at least three blocks and index $> 2^{n-1}$, and primitive subgroups are excluded by Lemma 5.1. Thus Proposition 4.1 gives equality.

The uniqueness statement follows from Proposition 4.2. The only tight subgroups are W and the H_k with $k < m$ odd. Every positive-weight class must be covered exactly once. □

The equivalent closed form follows from elementary binomial identities:

$$\beta_{\text{faith}}(A_{2m}) = \begin{cases} 2^{2m-2}, & m \text{ odd}, \\ 2^{2m-2} + \frac{1}{2}\binom{2m}{m}, & m \text{ even}. \end{cases}$$

8 Alternating groups of odd composite degree

Theorem 8.1. Let n be odd composite and let $q = P^-(n)$. Then

$$\beta_{\mathrm{faith}}(A_n) \sim \frac{n!}{((n/q)!)^q q!}.$$

Proof.
Let

$$C_n = \frac{n!}{((n/q)!)^q q!}.$$

Every normal cover of A_n must cover the n-cycles. Therefore at least one subgroup must contain an n-cycle. Such a subgroup is transitive. If it is imprimitive, Lemmas 5.2 and 5.3 show that its index is at least C_n.

If it is primitive, we use the stronger form of Maroti's estimate:

$$|H| < 50n^{\sqrt{n}}.$$

Hence

$$[A_n : H] > \frac{n!/2}{50n^{\sqrt{n}}}.$$

We compare this with C_n. It is enough to show

$$((n/q)!)^q q! > 100n^{\sqrt{n}}.$$

Since $q \leq \sqrt{n}$, we have $n/q \geq \sqrt{n}$. Therefore

$$\log\left(((n/q)!)^q q!\right) \geq q\left(\frac{n}{q}\log\frac{n}{q} - \frac{n}{q}\right) + O(q\log q) = n\log\frac{n}{q} - n + O(q\log q).$$

As $n/q \geq \sqrt{n}$,

$$n\log\frac{n}{q} \geq \frac{1}{2}n\log n.$$

Thus

$$\log\left(((n/q)!)^q q!\right) \geq \frac{1}{2}n\log n - O(n),$$

whereas

$$\log(100n^{\sqrt{n}}) = O(\sqrt{n}\log n).$$

For n large, the primitive index is therefore larger than C_n. Hence

$$\beta(A_n) \geq C_n.$$

For the upper bound, take

$$W_q = (S_{n/q} \wr S_q) \cap A_n.$$

This subgroup has index C_n and, by Lemma 3.3, meets both A_n-classes of n-cycles.

Every element of A_n which is not an n-cycle has at least three cycles, and therefore has a cycle of length $k \le n/3$. Adding all intransitive subgroups

$$(S_k \times S_{n-k}) \cap A_n, \qquad 1 \le k \le n/3,$$

covers all remaining elements. The total added cost is

$$\sum_{k \le n/3} \binom{n}{k} = 2^{H(1/3)n+o(n)}.$$

Since $q \ge 3$, C_n grows like at least 3^n up to subexponential factors, while $2^{H(1/3)n}$ has smaller exponential base. Thus the added cost is $o(C_n)$. □

9 Alternating groups of prime degree

Let

$$c_p = \min\{[A_p : H] : H < A_p,\ H \text{ contains a } p\text{-cycle}\}.$$

Lemma 9.1.

$$\log c_p = p \log p - p + O((\log p)^2).$$

Proof.

Let

$$M_p = \max\{|H| : H < A_p,\ H \text{ contains a } p\text{-cycle}\}.$$

The lower bound $M_p \ge p$ is immediate from the cyclic group generated by a p-cycle.

Conversely, any subgroup of A_p containing a p-cycle is transitive of prime degree, hence primitive. Jones's classification of primitive permutation groups containing a cycle implies that every proper primitive subgroup of S_p containing a p-cycle has order at most

$$p^{O(\log p)}.$$

Thus

$$M_p \le p^{O(\log p)}.$$

Since

$$c_p = \frac{|A_p|}{M_p},$$

Stirling's formula gives

$$\log c_p = \log(p!/2) - O((\log p)^2) = p \log p - p + O((\log p)^2).$$

□

Theorem 9.2. As $p \to \infty$ through primes,

$$\beta_{\text{faith}}(A_p) = (1 + o(1))c_p.$$

Moreover,

$$\log \beta_{\text{faith}}(A_p) = p \log p - p + O((\log p)^2).$$

Proof.

Every cover must cover the p-cycles, so

$$\beta(A_p) \geq c_p.$$

Choose $H_0 < A_p$ containing a p-cycle and satisfying

$$[A_p : H_0] = c_p.$$

By Lemma 3.4, H_0 meets both A_p-classes of p-cycles.

Every element of A_p which is not a p-cycle has at least three cycles, hence has a cycle of length $k \leq p/3$. Adding all intransitive subgroups

$$(S_k \times S_{p-k}) \cap A_p, \qquad 1 \leq k \leq p/3,$$

covers all remaining elements, at cost

$$2^{H(1/3)p+o(p)}.$$

By Lemma 9.1 this is $o(c_p)$. Therefore

$$\beta(A_p) = (1 + o(1))c_p.$$

The logarithmic asymptotic follows from Lemma 9.1. □

10 The exact second term for even symmetric groups

Theorem 6.2 determines the order of the second term in

$$\beta_{\text{faith}}(S_{2m}) - \frac{1}{2}\binom{2m}{m}.$$

It is natural to ask for the exact coefficient. This becomes a finite additive-combinatorial covering problem on cycle types.

Let n be even and let

$$W = S_{n/2} \wr S_2.$$

An odd cycle type of S_n, other than the n-cycle type, is already covered by W if either all cycle lengths are even, or some nonempty subset of its cycle lengths has sum $n/2$. The residual classes are those odd cycle types with no subset sum $n/2$ and with at least one odd cycle length.

Define $\mathcal{R}_n$ to be the set of such residual cycle types. Let

$$\rho(n) = \min_{\mathcal{T} \subseteq \{1,\ldots,n/2\}} \sum_{k \in \mathcal{T}} \binom{n}{k},$$

where the minimum is taken over all $\mathcal{T}$ such that every $\lambda \in \mathcal{R}_n$ has a nonempty proper subset of parts whose sum lies in $\mathcal{T}$.

Then the upper-bound construction in Theorem 6.2 shows

$$\beta_{\text{faith}}(S_n) \leq \frac{1}{2}\binom{n}{n/2} + 2 + \rho(n).$$

The lower-bound problem is to construct matching dual certificates for this residual weighted hitting problem. Determining $\rho(n)$ and proving equality would give the exact second term. Theorem 6.2 shows that

$$\rho(n) = \Theta\left(\binom{n}{\lfloor n/3 \rfloor}\right),$$

but the exact coefficient remains open.

11 Arithmetic interpretation

Let L/K be a finite Galois extension of global fields with group G. Finite etale K-schemes split by L are equivalent to finite G-sets. Under this equivalence, the degree of the finite etale scheme is the cardinality of the G-set, and exact monodromy G corresponds to faithfulness of the action.

If Z/K corresponds to Ω, then

$$Z(K) \neq \varnothing$$

if and only if

$$\Omega^G \neq \varnothing.$$

For almost all good primes $\mathfrak{p}$,

$$Z(k_\mathfrak{p}) \neq \varnothing$$

if and only if

$$\Omega^{\text{Frob}_\mathfrak{p}} \neq \varnothing.$$

By Chebotarev, this condition for almost all good primes is equivalent to

$$\Omega^g \neq \varnothing \qquad \text{for every } g \in G.$$

Thus $\beta_{\text{faith}}(G)$ is the minimum degree of a finite etale K-scheme split by L, with exact monodromy G, with no K-point, but with points over $k_\mathfrak{p}$ for almost all good primes. In the polynomial formulation, it is the group-theoretic lower bound for the minimum total degree of an intersective product with Galois group G, not merely for the minimum number of irreducible factors.

This interpretation concerns almost all good primes. Requiring local points over every completion K_v, or roots modulo every prime, imposes additional conditions at ramified primes and is a separate local problem.

References

[BS] D. Bubboloni and J. Sonn, *Intersective S_n polynomials with few irreducible factors*, arXiv:1507.08593.

[BPS] D. Bubboloni, C. E. Praeger, and P. Spiga, *Normal coverings and pairwise generation of finite alternating and symmetric groups*, Journal of Algebra 390 (2013), 199-215.

[EM] S. Eberhard and C. Mellon, *Normal covering numbers for S_n and A_n and additive combinatorics*, arXiv:2410.06999.

[GL] M. Garonzi and A. Lucchini, *Covers and normal covers of finite groups*, Journal of Algebra 422 (2015), 148-165.

[J] G. A. Jones, *Primitive permutation groups containing a cycle*, Bulletin of the Australian Mathematical Society 89 (2014), 159-165.

[K] J. Konig, *Intersective polynomials with non-solvable Galois groups*, Journal of Algebra 502 (2018), 79-94.

[M] A. Maroti, *On the orders of primitive groups*, Journal of Algebra 258 (2002), 631-640.

[PS] C. E. Praeger and J. Saxl, *On the orders of primitive permutation groups*, Bulletin of the London Mathematical Society 12 (1980), 303-307.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, ChatGPT, by OpenAI, was used to assist with mathematical drafting, formalization, review, and editing. This work is shared as a preliminary AI-assisted mathematical note. The mathematical content may have been only partially reviewed and may contain errors; it should not be treated as peer-reviewed or as a fully verified manuscript.