Normal Coverings of the Symmetric and Alternating Group

Daniela Bubboloni

Università degli Studi di Firenze
Dipartimento di Matematica per le Decisioni

To the memory of Silvia

Ischia , 12th April 2010

Definitions

Let G be a finite group.

i) A *covering* of G is a set of m proper subgroups of G, called *components*, whose union is G.

   $\sigma(G)$ is defined as the smallest integer m such that G has a covering with m components (Cohn, 1994).

   A covering with $\sigma(G)$ components is called a *minimal covering* which realizes $\sigma(G)$.

ii) A *normal covering* of G is a covering which is invariant under G-conjugation.

   A normal covering Σ is the set of the G-conjugacy classes of some non conjugated subgroups of G, say $H_1, \ldots, H_k$, called the *basic components* of the normal covering, such that

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

Definitions

Let G be a finite group.

i) A *covering* of G is a set of m proper subgroups of G, called *components*, whose union is G.
   $\sigma(G)$ is defined as the smallest integer m such that G has a covering with m components (Cohn, 1994).
   A covering with $\sigma(G)$ components is called a *minimal covering* which realizes $\sigma(G)$.

ii) A *normal covering* of G is a covering which is invariant under G-conjugation.
   A normal covering Σ is the set of the G-conjugacy classes of some non conjugated subgroups of G, say $H_1, \dots, H_k$, called the *basic components* of the normal covering, such that

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

Definitions

Let G be a finite group.

i) A *covering* of G is a set of m proper subgroups of G, called *components*, whose union is G.
$\sigma(G)$ is defined as the smallest integer m such that G has a covering with m components (Cohn, 1994).
A covering with $\sigma(G)$ components is called a *minimal covering* which realizes $\sigma(G)$.

ii) A *normal covering* of G is a covering which is invariant under G-conjugation.
A normal covering Σ is the set of the G-conjugacy classes of some non conjugated subgroups of G, say $H_1, \ldots, H_k$, called the *basic components* of the normal covering, such that

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

Definitions

Let G be a finite group.

i) A *covering* of G is a set of m proper subgroups of G, called *components*, whose union is G.
$\sigma(G)$ is defined as the smallest integer m such that G has a covering with m components (Cohn, 1994).
A covering with $\sigma(G)$ components is called a *minimal covering* which realizes $\sigma(G)$.

ii) A *normal covering* of G is a covering which is invariant under G-conjugation.
A normal covering Σ is the set of the G-conjugacy classes of some non conjugated subgroups of G, say $H_1, \ldots, H_k$, called the *basic components* of the normal covering, such that

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

Definitions

We say that $\delta = \{H_i < G \ : \ i = 1, \ldots, k\}$ is a *basic set* for the *k-normal covering* Σ.

We define $\gamma(G)$ as the smallest k such that G admits a k-normal covering.

A normal covering with $\gamma(G)$ basic components is called a *minimal normal covering* of G which realizes $\gamma(G)$.

Note:

a) Every non cyclic group admits a normal covering

b) When G is abelian $\sigma(G) = \gamma(G) \geq 3$

c) You can always replace a k-normal covering with a k-normal covering with maximal components

Definitions

We say that $\delta = \{H_i < G \ : \ i = 1, \ldots, k\}$ is a *basic set* for the *k-normal covering* Σ.
We define $\gamma(G)$ as the smallest k such that G admits a k-normal covering.
A normal covering with $\gamma(G)$ basic components is called a *minimal normal covering* of G which realizes $\gamma(G)$.

Note:

a) Every non cyclic group admits a normal covering
b) When G is abelian $\sigma(G) = \gamma(G) \geq 3$
c) You can always replace a k-normal covering with a k-normal covering with maximal components

Definitions

We say that $\delta = \{H_i < G \ : \ i = 1, \ldots, k\}$ is a *basic set* for the *k-normal covering* Σ.
We define $\gamma(G)$ as the smallest k such that G admits a k-normal covering.
A normal covering with $\gamma(G)$ basic components is called a *minimal normal covering* of G which realizes $\gamma(G)$.

Note:

a) Every non cyclic group admits a normal covering
b) When G is abelian $\sigma(G) = \gamma(G) \geq 3$
c) You can always replace a k-normal covering with a k-normal covering with maximal components

Introduction

I am going to present the results of a joined work with C. Praeger (2010) in which we investigate the natural numbers $\gamma(G)$, where $G = A_n,\ S_n$.

This number depends on the arithmetical complexity of n and can be expressed in terms of the Euler function ϕ.
We give the exact value when n decomposes in at most two odd primes, lower and upper bound as well as asymptotic estimate in the general case.

Introduction

I am going to present the results of a joined work with C. Praeger (2010) in which we investigate the natural numbers $\gamma(G)$, where $G = A_n,\ S_n$.

This number depends on the arithmetical complexity of n and can be expressed in terms of the Euler function ϕ.
We give the exact value when n decomposes in at most two odd primes, lower and upper bound as well as asymptotic estimate in the general case.

Introduction

I am going to present the results of a joined work with C. Praeger (2010) in which we investigate the natural numbers $\gamma(G)$, where $G = A_n,\ S_n$.

This number depends on the arithmetical complexity of n and can be expressed in terms of the Euler function ϕ.
We give the exact value when n decomposes in at most two odd primes, lower and upper bound as well as asymptotic estimate in the general case.

Background

Theorem (D. B. (1998))

i) $\gamma(S_n) = 2$ *if and only if* $3 \leq n \leq 6$
ii) $\gamma(A_n) = 2$ *if and only if* $4 \leq n \leq 8$.

Here we deal with S_n for $n \geq 7$ and A_n for $n \geq 9$.

- A. Maróti (2005) explored the numbers $\sigma(S_n)$ and $\sigma(A_n)$.

Some of his ideas are useful also to compute $\gamma(S_n)$ and $\gamma(A_n)$, though our methods diverge.

Background

Theorem (D. B. (1998))

i) $\gamma(S_n) = 2$ *if and only if* $3 \leq n \leq 6$

ii) $\gamma(A_n) = 2$ *if and only if* $4 \leq n \leq 8$.

Here we deal with S_n for $n \geq 7$ and A_n for $n \geq 9$.

- A. Maróti (2005) explored the numbers $\sigma(S_n)$ and $\sigma(A_n)$.

Some of his ideas are useful also to compute $\gamma(S_n)$ and $\gamma(A_n)$, though our methods diverge.

Background

Theorem (D. B. (1998))

i) $\gamma(S_n) = 2$ *if and only if* $3 \leq n \leq 6$

ii) $\gamma(A_n) = 2$ *if and only if* $4 \leq n \leq 8$.

Here we deal with S_n for $n \geq 7$ and A_n for $n \geq 9$.

- A. Maróti (2005) explored the numbers $\sigma(S_n)$ and $\sigma(A_n)$.

Some of his ideas are useful also to compute $\gamma(S_n)$ and $\gamma(A_n)$, though our methods diverge.

Example: S_7

S_7 has no 2-normal coverings.
S_7 has the 3-normal covering Σ with basic maximal components

$$\delta = \{S_2 \times S_5, \quad S_3 \times S_4, \quad AGL_1(7) \cong C_7 \rtimes C_6\}.$$

Simply check that any type of permutation is inside one component $\implies \gamma(S_7) = 3.$

$|\Sigma| = 120 > \sigma(S_7) = 2^6 \implies \Sigma$ is not minimal.

A minimal covering Δ of S_7 is given by the four subgroups

$$S_2 \times S_5, \quad S_3 \times S_4, \quad S_6, \quad A_7$$

and all their conjugates in S_7.
Thus Δ is a 4-normal covering and $\sigma(S_7)$ is realizable through a normal covering.

Example: S_7

S_7 has no 2-normal coverings.
S_7 has the 3-normal covering Σ with basic maximal components

$$\delta = \{S_2 \times S_5, \quad S_3 \times S_4, \quad AGL_1(7) \cong C_7 \rtimes C_6\}.$$

Simply check that any type of permutation is inside one component $\implies \gamma(S_7) = 3.$

$|\Sigma| = 120 > \sigma(S_7) = 2^6 \implies \Sigma$ is not minimal.

A minimal covering Δ of S_7 is given by the four subgroups

$$S_2 \times S_5, \quad S_3 \times S_4, \quad S_6, \quad A_7$$

and all their conjugates in S_7.
Thus Δ is a 4-normal covering and $\sigma(S_7)$ is realizable through a normal covering.

Example: S_7

S_7 has no 2-normal coverings.
S_7 has the 3-normal covering Σ with basic maximal components

$$\delta = \{S_2 \times S_5, \quad S_3 \times S_4, \quad AGL_1(7) \cong C_7 \rtimes C_6\}.$$

Simply check that any type of permutation is inside one component $\implies$ $\gamma(S_7) = 3.$

$|\Sigma| = 120 > \sigma(S_7) = 2^6 \implies \Sigma$ is not minimal.

A minimal covering Δ of S_7 is given by the four subgroups

$$S_2 \times S_5, \quad S_3 \times S_4, \quad S_6, \quad A_7$$

and all their conjugates in S_7.
Thus Δ is a 4-normal covering and $\sigma(S_7)$ is realizable through a normal covering.

Example: S_7

S_7 has no 2-normal coverings.
S_7 has the 3-normal covering Σ with basic maximal components

$$\delta = \{S_2 \times S_5, \quad S_3 \times S_4, \quad AGL_1(7) \cong C_7 \rtimes C_6\}.$$

Simply check that any type of permutation is inside one component $\implies$ $\gamma(S_7) = 3.$

$|\Sigma| = 120 > \sigma(S_7) = 2^6 \implies \Sigma$ is not minimal.

A minimal covering Δ of S_7 is given by the four subgroups

$$S_2 \times S_5, \quad S_3 \times S_4, \quad S_6, \quad A_7$$

and all their conjugates in S_7.
Thus Δ is a 4-normal covering and $\sigma(S_7)$ is realizable through a normal covering.

A question

- The known examples of minimal coverings for A_n and S_n are normal:

Question

Is $\sigma(G)$, for $G = A_n,\ S_n$, always realizable through a normal covering?

The starting points

If $\pi \in S_n$ decomposes into the product of r disjoint cycles of lengths $l_1, \ldots, l_r,\ l_i \geq 1$ we say that π is of *type* $[l_1, \ldots, l_r]$.

- *$\delta = \{H_i < S_n \ : \ i = 1 \ldots k\}$ is a normal covering for S_n if and only if at least one permutation of any type in S_n belongs to some $H_i \in \delta$.*

  Dealing with A_n, recall that the if $\pi \in A_n$ then the S_n-conjugacy class π^{S_n} can splits into two A_n-conjugacy classes.

The starting points

If $\pi \in S_n$ decomposes into the product of r disjoint cycles of lengths $l_1, \ldots, l_r,\ l_i \geq 1$ we say that π is of *type* $[l_1, \ldots, l_r]$.

- $\delta = \{H_i < S_n \ :\ i = 1 \ldots k\}$ *is a normal covering for* S_n *if and only if at least one permutation of any type in* S_n *belongs to some* $H_i \in \delta$.

Dealing with A_n, recall that the if $\pi \in A_n$ then the S_n-conjugacy class π^{S_n} can splits into two A_n-conjugacy classes.

The starting points

If $\pi \in S_n$ decomposes into the product of r disjoint cycles of lengths $l_1, \ldots, l_r,\ l_i \geq 1$ we say that π is of *type* $[l_1, \ldots, l_r]$.

- *$\delta = \{H_i < S_n \ : \ i = 1 \ldots k\}$ is a normal covering for S_n if and only if at least one permutation of any type in S_n belongs to some $H_i \in \delta$.*

  Dealing with A_n, recall that the if $\pi \in A_n$ then the S_n-conjugacy class π^{S_n} can splits into two A_n-conjugacy classes.

- There is an useful link between the numbers $\gamma(S_n)$ and $\gamma(A_n)$:

Lemma

Any normal covering of S_n with maximal components all different from A_n defines, by intersection, a normal covering of A_n.

In particular if $\gamma(S_n)$ is realized by a normal covering with maximal components which does not involve A_n, then $\gamma(A_n) \leq \gamma(S_n)$.

- There is an useful link between the numbers $\gamma(S_n)$ and $\gamma(A_n)$:

Lemma

Any normal covering of S_n with maximal components all different from A_n defines, by intersection, a normal covering of A_n.

In particular if $\gamma(S_n)$ is realized by a normal covering with maximal components which does not involve A_n, then $\gamma(A_n) \leq \gamma(S_n)$.

Motivations

- *Group theory*
  Covering groups by subgroups is a classic topic in group theory
- *Number theory*
  Let $f \in \mathbf{Z}[x]$ be a polynomial with a root $mod\, p$, for all primes p and with no linear factors.
  Consider $G = Gal_{\mathbf{Q}}(f)$ acting on the set Ω of the roots of f.
  If f splits into k distinct irreducible factors, choosing a root ω_i for each of them, and taking their stabilizers G_{ω_i}, we get k basic components of a normal covering of G (D. Berend, Y. Bilou (1996)).
  In particular $k \geq \gamma(G)$.
  By a Van der Waerden's result, the most common event is $G = S_n,\ A_n$.
  An example is $f(x) = (x^2 + x + 1)(x^3 - 2)$ with $Gal_{\mathbf{Q}}(f) = S_3$.

Motivations

- *Group theory*
  Covering groups by subgroups is a classic topic in group theory
- *Number theory*
  Let $f \in \mathbf{Z}[x]$ be a polynomial with a root $mod\, p$, for all primes p and with no linear factors.
  Consider $G = Gal_{\mathbf{Q}}(f)$ acting on the set Ω of the roots of f.
  If f splits into k distinct irreducible factors, choosing a root ω_i for each of them, and taking their stabilizers G_{ω_i}, we get k basic components of a normal covering of G (D. Berend, Y. Bilou (1996)).
  In particular $k \geq \gamma(G)$.
  By a Van der Waerden's result, the most common event is $G = S_n,\ A_n$.
  An example is $f(x) = (x^2 + x + 1)(x^3 - 2)$ with $Gal_{\mathbf{Q}}(f) = S_3$.

Motivations

- *Group theory*
  Covering groups by subgroups is a classic topic in group theory
- *Number theory*
  Let $f \in \mathbf{Z}[x]$ be a polynomial with a root $mod\, p$, for all primes p and with no linear factors.
  Consider $G = Gal_{\mathbf{Q}}(f)$ acting on the set Ω of the roots of f.
  If f splits into k distinct irreducible factors, choosing a root ω_i for each of them, and taking their stabilizers G_{ω_i}, we get k basic components of a normal covering of G (D. Berend, Y. Bilou (1996)).
  In particular $k \geq \gamma(G)$.
  By a Van der Waerden's result, the most common event is $G = S_n,\ A_n$.
  An example is $f(x) = (x^2 + x + 1)(x^3 - 2)$ with $Gal_{\mathbf{Q}}(f) = S_3$.

Motivations

- *Group theory*
  Covering groups by subgroups is a classic topic in group theory
- *Number theory*
  Let $f \in \mathbf{Z}[x]$ be a polynomial with a root $mod\, p$, for all primes p and with no linear factors.
  Consider $G = Gal_{\mathbf{Q}}(f)$ acting on the set Ω of the roots of f.
  If f splits into k distinct irreducible factors, choosing a root ω_i for each of them, and taking their stabilizers G_{ω_i}, we get k basic components of a normal covering of G (D. Berend, Y. Bilou (1996)).
  In particular $k \geq \gamma(G)$.
  By a Van der Waerden's result, the most common event is $G = S_n,\ A_n$.
  An example is $f(x) = (x^2 + x + 1)(x^3 - 2)$ with $Gal_{\mathbf{Q}}(f) = S_3$.

An ongoing research

J. Sonn and his student D. Rebayev are working in constructing polynomials $f \in \mathbf{Z}[x]$ with

- roots $mod\, p$, for all primes p
- Galois group G the alternating or the symmetric group
- $\gamma(G)$ distinct irreducible factors

Using the knowledge of the minimal normal coverings and field theory techniques, they succeeded for S_n when $3 \leq n \leq 6$ and for A_n when $4 \leq n \leq 6$, which are all cases in which γ assumes value 2.

It is not clear, at the moment, how to deal with the general case: for such polynomials we have both an existence and an explicit construction problem, which is part of the inverse problem in Galois theory.

An ongoing research

J. Sonn and his student D. Rebayev are working in constructing polynomials $f \in \mathbf{Z}[x]$ with

- roots $mod\, p$, for all primes p
- Galois group G the alternating or the symmetric group
- $\gamma(G)$ distinct irreducible factors

Using the knowledge of the minimal normal coverings and field theory techniques, they succeeded for S_n when $3 \leq n \leq 6$ and for A_n when $4 \leq n \leq 6$, which are all cases in which γ assumes value 2.

It is not clear, at the moment, how to deal with the general case: for such polynomials we have both an existence and an explicit construction problem, which is part of the inverse problem in Galois theory.

An ongoing research

J. Sonn and his student D. Rebayev are working in constructing polynomials $f \in \mathbf{Z}[x]$ with

- roots $mod\, p$, for all primes p
- Galois group G the alternating or the symmetric group
- $\gamma(G)$ distinct irreducible factors

Using the knowledge of the minimal normal coverings and field theory techniques, they succeeded for S_n when $3 \leq n \leq 6$ and for A_n when $4 \leq n \leq 6$, which are all cases in which γ assumes value 2.

It is not clear, at the moment, how to deal with the general case: for such polynomials we have both an existence and an explicit construction problem, which is part of the inverse problem in Galois theory.

Methods

We get upper bounds for $\gamma(G),\ G = A_n,\ S_n$ constructing normal coverings, lower bounds finding some mandatory maximal components.

Examples

Let n be odd.

- *Permutations of type*

$$[k, n-k]$$

with $(k, n-k) = 1, \quad 2 \leq k < n/2$ belongs only to the maximal intransitive subgroup

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

Methods

We get upper bounds for $\gamma(G),\ G = A_n,\ S_n$ constructing normal coverings, lower bounds finding some mandatory maximal components.

Examples

Let n be odd.

- *Permutations of type*

  $$[k, n-k]$$

  with $(k, n-k) = 1, \quad 2 \leq k < n/2$ *belongs only to the maximal intransitive subgroup*

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

Methods

- *Permutations of type*

$$[p\alpha, p\beta],$$

where $p \mid n$ *is a prime,* $\alpha, \beta \in \mathbf{N}^*$ *are coprime and*

$$\alpha \leq \frac{2(\sqrt{n}-1)}{p},$$

belongs only to the maximal subgroups

$$S_p \wr S_{n/p}, \quad S_{n/p} \wr S_p$$

or to

$$S_{p\,\alpha} \times S_{p\,\beta}$$

Results: exact values and bounds

Theorem (A)

For any $p \neq 2,\ 3$ prime, the group S_p admits the minimal normal covering with basic set

$$\{AGL_1(p) \cong C_p \rtimes C_{p-1},\ S_k \times S_{(p-k)}\ :\ 2 \leq k \leq \frac{p-1}{2}\}.$$

In particular

$$\gamma(S_p) = \frac{p-1}{2}, \qquad \gamma(A_p) \leq \frac{p-1}{2}.$$

Moreover for any prime $p \neq 2$,

$$\gamma(A_{2p}) = \frac{p+1}{2}$$

Theorem (B)

For any p prime and $\alpha \geq 2$

$$\delta = \{S_p \wr S_{p^{\alpha-1}},\ S_k \times S_{(p^{\alpha}-k)}\ :\ 1 \leq k < \frac{p^{\alpha}}{2},\ p \nmid k\}$$

is a basic set for S_{p^α}*. In particular*

$$\gamma(S_{2^\alpha}) \leq \frac{\phi(2^\alpha)}{2} + 1 \quad \text{and for} \quad \alpha \geq 4, \quad \gamma(A_{2^\alpha}) = \frac{\phi(2^\alpha)}{2} + 1.$$

If $p \neq 2$*, then* δ *is minimal and*

$$\gamma(S_{p^\alpha}) = \frac{\phi(p^\alpha)}{2} + 1, \qquad \gamma(A_{p^\alpha}) \leq \frac{\phi(p^\alpha)}{2} + 1.$$

Theorem (C)

Let $n = pq$ with $p < q$ primes. Then:

$$\delta = \{S_p \wr S_q,\ S_k \times S_{(n-k)}\ :\ 1 \leq k < n/2,\ p,\ q \nmid k\}$$

and

$$\delta' = \{S_q \wr S_p,\ S_k \times S_{(n-k)}\ :\ 1 \leq k < n/2,\ p,\ q \nmid k\}$$

are basic sets for S_{pq}.

In particular $\gamma(A_{pq}) \leq \frac{\phi(pq)}{2} + 1$ *and, for any* $q \neq 2$,

$$\gamma(S_{2q}) \leq \frac{q+1}{2}.$$

If $p,\ q$ are odd then $\delta,\ \delta'$ are minimal and

$$\gamma(S_{pq}) = \frac{\phi(pq)}{2} + 1.$$

Example: $S_{10},\ A_{10}$

We know $\gamma(S_{10}),\ \gamma(A_{10}) \geq 3$.

By Theorem (C), $\gamma(S_{10}) \leq \dfrac{\phi(10)}{2} + 1 = 3 \implies \gamma(S_{10}) = 3$.

The normal covering of S_{10} with basic set

$$\delta = \{S_2 \wr S_5,\ S_3 \times S_7,\ S_9\}$$

has maximal components, all different from $A_{10} \implies$

$$\delta_{A_{10}} = \{[S_2 \wr S_5] \cap A_{10},\ [S_3 \times S_7] \cap A_{10},\ A_9\}$$

is a basic set for a normal covering of A_{10} and $\gamma(A_{10}) = 3$.

- We know that $\gamma(S_n) = \gamma(A_n)$ when $n \in \{4, 5, 6, 10\}$.

Question

What are all the solution of the equation $\gamma(S_n) = \gamma(A_n) \quad (*)$*?*

Example: $S_{10},\ A_{10}$

We know $\gamma(S_{10}),\ \gamma(A_{10}) \geq 3$.

By Theorem (C), $\gamma(S_{10}) \leq \dfrac{\phi(10)}{2} + 1 = 3 \implies \gamma(S_{10}) = 3.$

The normal covering of S_{10} with basic set

$$\delta = \{S_2 \wr S_5,\ S_3 \times S_7,\ S_9\}$$

has maximal components, all different from $A_{10} \implies$

$$\delta_{A_{10}} = \{[S_2 \wr S_5] \cap A_{10},\ [S_3 \times S_7] \cap A_{10},\ A_9\}$$

is a basic set for a normal covering of A_{10} and $\gamma(A_{10}) = 3.$

- We know that $\gamma(S_n) = \gamma(A_n)$ when $n \in \{4, 5, 6, 10\}$.

Question

What are all the solution of the equation $\gamma(S_n) = \gamma(A_n) \quad (*)$*?*

Example: $S_{10},\ A_{10}$

We know $\gamma(S_{10}),\ \gamma(A_{10}) \geq 3$.

By Theorem (C), $\gamma(S_{10}) \leq \dfrac{\phi(10)}{2} + 1 = 3 \implies \gamma(S_{10}) = 3$.

The normal covering of S_{10} with basic set

$$\delta = \{S_2 \wr S_5,\ S_3 \times S_7,\ S_9\}$$

has maximal components, all different from $A_{10} \implies$

$$\delta_{A_{10}} = \{[S_2 \wr S_5] \cap A_{10},\ [S_3 \times S_7] \cap A_{10},\ A_9\}$$

is a basic set for a normal covering of A_{10} and $\gamma(A_{10}) = 3$.

- We know that $\gamma(S_n) = \gamma(A_n)$ when $n \in \{4, 5, 6, 10\}$.

Question

What are all the solution of the equation $\gamma(S_n) = \gamma(A_n) \quad (*)$*?*

The case $n = 2q$

The case $n = 2q$, $q \geq 7$ prime, is an interesting open case to investigate. We know that

$$\gamma(S_{2q}) \leq \frac{q+1}{2} = \gamma(A_{2q}).$$

Thus either we find solution for $(*)$ or we discover some degrees for which the gamma function on the symmetric group is less then the gamma function on the alternating group, which is unexpected.

Question

Is always $\gamma(S_n) \geq \gamma(A_n)$?

The case $n = 2q$

The case $n = 2q$, $q \geq 7$ prime, is an interesting open case to investigate. We know that

$$\gamma(S_{2q}) \leq \frac{q+1}{2} = \gamma(A_{2q}).$$

Thus either we find solution for $(*)$ or we discover some degrees for which the gamma function on the symmetric group is less then the gamma function on the alternating group, which is unexpected.

Question

Is always $\gamma(S_n) \geq \gamma(A_n)$?

The case $n = 2q$

The case $n = 2q$, $q \geq 7$ prime, is an interesting open case to investigate. We know that

$$\gamma(S_{2q}) \leq \frac{q+1}{2} = \gamma(A_{2q}).$$

Thus either we find solution for $(*)$ or we discover some degrees for which the gamma function on the symmetric group is less then the gamma function on the alternating group, which is unexpected.

Question

Is always $\gamma(S_n) \geq \gamma(A_n)$*?*

Example: A_9

For A_9, we have the 3-normal covering with basic set

$$\delta = \{P\Gamma L_2(8),\ P\Gamma L_2(8),\ [S_4 \times S_5] \cap A_9\},$$

where the two non conjugated copies of $P\Gamma L_2(8)$ in A_9 appear.
There are two conjugacy classes of 9-cycles and a representative of each of them belongs exactly to one of the two copies of $P\Gamma L_2(8)$.
So $\gamma(A_9) = 3$.

This example shows that in general we cannot avoid primitive components and in particular almost simple components.

Example: A_9

For A_9, we have the 3-normal covering with basic set

$$\delta = \{P\Gamma L_2(8),\ P\Gamma L_2(8),\ [S_4 \times S_5] \cap A_9\},$$

where the two non conjugated copies of $P\Gamma L_2(8)$ in A_9 appear.
There are two conjugacy classes of 9-cycles and a representative of each of them belongs exactly to one of the two copies of $P\Gamma L_2(8)$.
So $\gamma(A_9) = 3$.

This example shows that in general we cannot avoid primitive components and in particular almost simple components.

Example: A_9

For A_9, we have the 3-normal covering with basic set

$$\delta = \{P\Gamma L_2(8),\ P\Gamma L_2(8),\ [S_4 \times S_5] \cap A_9\},$$

where the two non conjugated copies of $P\Gamma L_2(8)$ in A_9 appear.
There are two conjugacy classes of 9-cycles and a representative of each of them belongs exactly to one of the two copies of $P\Gamma L_2(8)$.
So $\gamma(A_9) = 3$.

This example shows that in general we cannot avoid primitive components and in particular almost simple components.

Results: exact values and bounds

Theorem (D)

Let $n = p^{\alpha} q^{\beta}$ *with* $p < q$ *primes* $\alpha,\ \beta \geq 1$ *and* $(\alpha, \beta) \neq (1,1)$. *Then:*

$$\delta = \{S_p \wr S_{n/p},\ S_q \wr S_{n/q},\ S_k \times S_{(n-k)}\ :\ 1 \leq k < n/2,\ p,\ q \nmid k\}$$

is a basic set for S_n.
In particular

$$\gamma(S_n),\ \gamma(A_n) \leq \frac{\phi(n)}{2} + 2$$

Let $p,\ q$ *be* *odd*. *If* $\beta \geq 2$ *or if* $\beta = 1$ *and*

$$q \leq 2(p^{\alpha} - 1) + 2\sqrt{p^{\alpha}(p^{\alpha} - 2)}$$

then

$$\gamma(S_n) = \frac{\phi(n)}{2} + 2$$

Results: exact values and bounds

Theorem (D)

Let $n = p^\alpha q^\beta$ *with* $p < q$ *primes* $\alpha,\ \beta \geq 1$ *and* $(\alpha, \beta) \neq (1,1)$*. Then:*

$$\delta = \{S_p \wr S_{n/p},\ S_q \wr S_{n/q},\ S_k \times S_{(n-k)}\ :\ 1 \leq k < n/2,\ p,\ q \nmid k\}$$

is a basic set for S_n*.*
In particular

$$\gamma(S_n),\ \gamma(A_n) \leq \frac{\phi(n)}{2} + 2$$

Let $p,\ q$ *be odd. If* $\beta \geq 2$ *or if* $\beta = 1$ *and*

$$q \leq 2(p^\alpha - 1) + 2\sqrt{p^\alpha(p^\alpha - 2)}$$

then

$$\gamma(S_n) = \frac{\phi(n)}{2} + 2$$

- We are still working in understanding if the arithmetical assumption on q could be dropped.

Results: some general bounds

Proposition

i) *If* $n \in \mathbf{N}$ *is odd and not a prime, then*

$$\frac{\phi(n)}{2} + 1 \leq \gamma(S_n) \leq \lfloor \frac{n+1}{2} \rfloor$$

ii) *If* $n \geq 10$ *is even then* A_n *is normally covered through the basic set*

$$\delta = \{[S_{n/2} \wr S_2] \cap A_n,\ S_i \times S_{n-i}\ :\ 1 \leq i \leq n/2 - 1,\ i\ \textit{odd}\ \}.$$

Moreover

$$\frac{\phi(n)}{2} + 1 \leq \gamma(A_n) \leq \lfloor \frac{n+4}{4} \rfloor$$

- Note that the inequalities are sharp in the alternating case: use $n = 2^\alpha$ with $\alpha \geq 4$ for the upper bound and $n = 2p$ with p an odd prime for the lower bound.

- The lower bound for the symmetric case is sharp: use $n = p^\alpha$ with $\alpha \geq 2$.

  We don't know if there exists n such that $\gamma(S_n) = \lfloor \frac{n+1}{2} \rfloor$.

  The feeling is that $\gamma(S_n)$ is of type $\frac{\phi(n)}{2} + f(n)$ where the function $f(n)$ is small with respect to $\phi(n)$.

- What does it happen to $\gamma(S_n)$ in the even case and to $\gamma(A_n)$ in the odd case?

- Note that the inequalities are sharp in the alternating case: use $n = 2^{\alpha}$ with $\alpha \geq 4$ for the upper bound and $n = 2p$ with p an odd prime for the lower bound.

- The lower bound for the symmetric case is sharp: use $n = p^{\alpha}$ with $\alpha \geq 2$.
  We don't know if there exists n such that $\gamma(S_n) = \lfloor \frac{n+1}{2} \rfloor$.

  The feeling is that $\gamma(S_n)$ is of type $\frac{\phi(n)}{2} + f(n)$ where the function $f(n)$ is small with respect to $\phi(n)$.

- What does it happen to $\gamma(S_n)$ in the even case and to $\gamma(A_n)$ in the odd case?

- Note that the inequalities are sharp in the alternating case: use $n = 2^\alpha$ with $\alpha \geq 4$ for the upper bound and $n = 2p$ with p an odd prime for the lower bound.
- The lower bound for the symmetric case is sharp: use $n = p^\alpha$ with $\alpha \geq 2$.
  We don't know if there exists n such that $\gamma(S_n) = \lfloor \frac{n+1}{2} \rfloor$.

  The feeling is that $\gamma(S_n)$ is of type $\frac{\phi(n)}{2} + f(n)$ where the function $f(n)$ is small with respect to $\phi(n)$.
- What does it happen to $\gamma(S_n)$ in the even case and to $\gamma(A_n)$ in the odd case?

Results: some bounds

It is easy to get some upper bounds...

- When n is even, A_n contains all the permutations that decompose into two disjoint cycles $\Longrightarrow$

$$\delta = \{A_n,\ S_{n/2} \wr S_2,\ S_k \times S_{n-k}\ :\ 1 \le k \le \lfloor \frac{n}{3} \rfloor\}$$

is a basic set for $S_n \Longrightarrow\ \gamma(S_n) \le 2 + \lfloor \frac{n}{3} \rfloor$

- When n is odd, A_n does not contain permutations that decompose into two disjoint cycles; thus we get a basic set for A_n taking a subgroup containing a n-cycle and the

$$[S_k \times S_{n-k}] \cap A_n$$

with $1 \le k \le \lfloor \frac{n}{3} \rfloor \Longrightarrow\ \gamma(A_n) \le 1 + \lfloor \frac{n}{3} \rfloor$.

Results: some bounds

It is easy to get some upper bounds...

- When n is even, A_n contains all the permutations that decompose into two disjoint cycles $\Longrightarrow$

$$\delta = \{A_n,\ S_{n/2} \wr S_2,\ S_k \times S_{n-k}\ :\ 1 \leq k \leq \lfloor \frac{n}{3} \rfloor\}$$

  is a basic set for $S_n \Longrightarrow\ \gamma(S_n) \leq 2 + \lfloor \frac{n}{3} \rfloor$

- When n is odd, A_n does not contain permutations that decompose into two disjoint cycles; thus we get a basic set for A_n taking a subgroup containing a n-cycle and the

$$[S_k \times S_{n-k}] \cap A_n$$

  with $1 \leq k \leq \lfloor \frac{n}{3} \rfloor \Longrightarrow\ \gamma(A_n) \leq 1 + \lfloor \frac{n}{3} \rfloor$.

Results: lower bounds for the symmetric group of even degree

Less easy to get some lower bounds...

Theorem

i) *If $n \geq 10$ is even and not divisible by 3, then*

$$\gamma(S_n) \geq \left|\left\{i \in \left(\frac{n}{4}, \frac{n-2}{3}\right] \cap \mathbf{N}^* \ : \ (i,n)=1\right\}\right| + 1 \sim \frac{\phi(n)}{12}.$$

ii) *If $n \geq 12$ is even and divisible by 3, then*

$$\gamma(S_n) \geq \left|\left\{i \in \left(\frac{n}{15}, \frac{n}{9}\right) \cap \mathbf{N}^* \ : \ (i,n)=1\right\}\right| + 1 \sim \frac{2\phi(n)}{45}.$$

Results: lower bounds for the symmetric group of even degree

Less easy to get some lower bounds...

Theorem

i) *If* $n \geq 10$ *is even and not divisible by* 3*, then*

$$\gamma(S_n) \geq |\{i \in \left(\frac{n}{4}, \frac{n-2}{3}\right] \cap \mathbf{N}^* \;:\; (i,n) = 1\}| + 1 \sim \frac{\phi(n)}{12}.$$

ii) *If* $n \geq 12$ *is even and divisible by* 3*, then*

$$\gamma(S_n) \geq |\{i \in \left(\frac{n}{15}, \frac{n}{9}\right) \cap \mathbf{N}^* \;:\; (i,n) = 1\}| + 1 \sim \frac{2\phi(n)}{45}.$$

Results: a lower bound for the alternating group of odd degree

Theorem

Let n be odd. If $n \geq 47$, then

$$\gamma(A_n) \geq \left|\left\{i \in \left(\frac{\sqrt{n}-1}{2}, \sqrt{n}-1\right) \cap \mathbf{N}^* \ : \ (i,n)=1\right\}\right| +$$

$$+\left|\left\{i \in \left(\frac{n}{4}, \frac{n}{3}\right) \cap \mathbf{N}^* \ : \ (i,n)=1\right\}\right| + 1 \sim \frac{\phi(n)}{12}.$$

Number theory

The asymptotic estimates are due to this number theory result:

Lemma

Let $n \in \mathbf{N}^*$ *and let* $0 < x < y < n$ *with* $x, y \in \mathbf{R}$*.*
For any interval I *with extremes* x *and* y*, define*

$$\phi(I; n) = |\{i \in \mathbf{N}^* \ : \ i \in I, \ (i, n) = 1\}|.$$

If $y - x \sim c\, n^{\beta}$ *for some* $\beta \in (0, 1], \ c > 0$ *then*

$$\phi(I; n) \sim \frac{\phi(n)}{n}(y - x)$$

Final comments on $\gamma(S_n),\ \gamma(A_n)$

We consider $\gamma(S_n),\ \gamma(A_n)$ as functions $\mathbf{N} \longrightarrow \mathbf{N}$:

- $\lim_{n\to+\infty} \gamma(S_n) = \lim_{n\to+\infty} \gamma(A_n) = +\infty$ since $\lim_{n\to+\infty} \phi(n) = +\infty$

We can give a look to the information we collected through our theorems on the γ values, when $n \leq 20$.

Final comments on $\gamma(S_n),\ \gamma(A_n)$

We consider $\gamma(S_n),\ \gamma(A_n)$ as functions $\mathbf{N} \longrightarrow \mathbf{N}$:

- $\lim_{n\to+\infty} \gamma(S_n) = \lim_{n\to+\infty} \gamma(A_n) = +\infty$ since $\lim_{n\to+\infty} \phi(n) = +\infty$

We can give a look to the information we collected through our theorems on the γ values, when $n \leq 20$.

Final comments on $\gamma(S_n),\ \gamma(A_n)$

We consider $\gamma(S_n),\ \gamma(A_n)$ as functions $\mathbf{N} \longrightarrow \mathbf{N}$:

- $\lim_{n\to+\infty} \gamma(S_n) = \lim_{n\to+\infty} \gamma(A_n) = +\infty$ since $\lim_{n\to+\infty} \phi(n) = +\infty$

We can give a look to the information we collected through our theorems on the γ values, when $n \leq 20$.

Some values

n	$\gamma(S_n)$	$\gamma(A_n)$
3	2	/
4	2	2
5	2	2
6	2	2
7	3	2
8	3	2
9	4	3
10	3	3
11	5	4
12	3, 4	3, 4
13	6	≤ 6
14	3, 4	4
15	5	≤ 5
16	≤ 5	5
17	8	≤ 8
18	≤ 9	4, 5
19	9	≤ 9
20	≤ 10	5, 6

Final comments on $\gamma(S_n),\ \gamma(A_n)$

- $\gamma(S_n)$ is not increasing :

$$\gamma(S_9) = \frac{\phi(9)}{2} + 1 = 4 > \gamma(S_{10}) = 3$$

- $\gamma(S_n)$ "jumps":

$$\gamma(S_{10}) = 3, \quad \gamma(S_{11}) = \frac{11-1}{2} = 5$$

- A question: Are $\gamma(S_n),\ \gamma(A_n)$ surjective?

Final comments on $\gamma(S_n),\ \gamma(A_n)$

- $\gamma(S_n)$ is not increasing :

$$\gamma(S_9) = \frac{\phi(9)}{2} + 1 = 4 > \gamma(S_{10}) = 3$$

- $\gamma(S_n)$ "jumps":

$$\gamma(S_{10}) = 3, \quad \gamma(S_{11}) = \frac{11-1}{2} = 5$$

- A question: Are $\gamma(S_n),\ \gamma(A_n)$ surjective?

Final comments on $\gamma(S_n),\ \gamma(A_n)$

- $\gamma(S_n)$ is not increasing :

$$\gamma(S_9) = \frac{\phi(9)}{2} + 1 = 4 > \gamma(S_{10}) = 3$$

- $\gamma(S_n)$ "jumps":

$$\gamma(S_{10}) = 3, \quad \gamma(S_{11}) = \frac{11-1}{2} = 5$$

- A question: Are $\gamma(S_n),\ \gamma(A_n)$ surjective?