On the maximal size of a set of elements pairwise generating the symmetric groups of even degree

Martino Garonzi, University of Brasilia, Brasilia (DF, Brazil).

Joint work with

Francesco Fumagalli, University of Firenze, Firenze (Italy),
Attila Maróti, Rényi Institute of Mathematics, Budapest (Hungary).

Binghamton University
April 13^{th}, 2021

We dedicated this work to the memory of Carlo Casolo (1958-2020).

Let G be a group that can be generated by two elements but not by one element. For instance, all finite nonabelian simple groups have this property (this is a consequence of the CFSG).

The generating graph of G, introduced by M.W. Liebeck and A. Shalev in [8], is the simple graph whose vertices are the elements of G and there is an edge between two vertices x and y if and only if $\langle x, y \rangle = G$.

A graph is said to be complete if there are edges connecting any two of its vertices. The generating graph of a noncyclic 2-generated group G is never complete because of the identity element.

A clique of a graph is a complete subgraph. The clique number of G is the maximal size of a clique in the generating graph of G. It is denoted by $\omega(G)$ (although some authors denote it $\mu(G)$).

In other words, $\omega(G)$ is the maximal size of a subset S of G with the property that any two distinct elements of S generate G.

Let G be a group that can be generated by two elements but not by one element. For instance, all finite nonabelian simple groups have this property (this is a consequence of the CFSG).

The generating graph of G, introduced by M.W. Liebeck and A. Shalev in [8], is the simple graph whose vertices are the elements of G and there is an edge between two vertices x and y if and only if $\langle x, y \rangle = G$.

A graph is said to be complete if there are edges connecting any two of its vertices. The generating graph of a noncyclic 2-generated group G is never complete because of the identity element.

A clique of a graph is a complete subgraph. The clique number of G is the maximal size of a clique in the generating graph of G. It is denoted by $\omega(G)$ (although some authors denote it $\mu(G)$).

In other words, $\omega(G)$ is the maximal size of a subset S of G with the property that any two distinct elements of S generate G.

Let G be a group that can be generated by two elements but not by one element. For instance, all finite nonabelian simple groups have this property (this is a consequence of the CFSG).

The generating graph of G, introduced by M.W. Liebeck and A. Shalev in [8], is the simple graph whose vertices are the elements of G and there is an edge between two vertices x and y if and only if $\langle x, y \rangle = G$.

A graph is said to be complete if there are edges connecting any two of its vertices. The generating graph of a noncyclic 2-generated group G is never complete because of the identity element.

A clique of a graph is a complete subgraph. The clique number of G is the maximal size of a clique in the generating graph of G. It is denoted by $\omega(G)$ (although some authors denote it $\mu(G)$).

In other words, $\omega(G)$ is the maximal size of a subset S of G with the property that any two distinct elements of S generate G.

Let G be a group that can be generated by two elements but not by one element. For instance, all finite nonabelian simple groups have this property (this is a consequence of the CFSG).

The generating graph of G, introduced by M.W. Liebeck and A. Shalev in [8], is the simple graph whose vertices are the elements of G and there is an edge between two vertices x and y if and only if $\langle x, y \rangle = G$.

A graph is said to be complete if there are edges connecting any two of its vertices. The generating graph of a noncyclic 2-generated group G is never complete because of the identity element.

A clique of a graph is a complete subgraph. The clique number of G is the maximal size of a clique in the generating graph of G. It is denoted by $\omega(G)$ (although some authors denote it $\mu(G)$).

In other words, $\omega(G)$ is the maximal size of a subset S of G with the property that any two distinct elements of S generate G.

Let G be a group that can be generated by two elements but not by one element. For instance, all finite nonabelian simple groups have this property (this is a consequence of the CFSG).

The generating graph of G, introduced by M.W. Liebeck and A. Shalev in [8], is the simple graph whose vertices are the elements of G and there is an edge between two vertices x and y if and only if $\langle x, y \rangle = G$.

A graph is said to be complete if there are edges connecting any two of its vertices. The generating graph of a noncyclic 2-generated group G is never complete because of the identity element.

A clique of a graph is a complete subgraph. The clique number of G is the maximal size of a clique in the generating graph of G. It is denoted by $\omega(G)$ (although some authors denote it $\mu(G)$).

In other words, $\omega(G)$ is the maximal size of a subset S of G with the property that any two distinct elements of S generate G.

It is hard to draw generating graphs in a meaningful way, because either there are too many edges or the graph is too simple.

To understand the idea, here is the complement of the generating graph of the alternating group A_4 with the identity element removed from the set of vertices.

In this case, a maximal clique of the generating graph is obtained by choosing a representative in each connected component of the above graph.

Note (for later) that the subgroups generated by the connected components form a minimal covering of A_4.

It is hard to draw generating graphs in a meaningful way, because either there are too many edges or the graph is too simple.

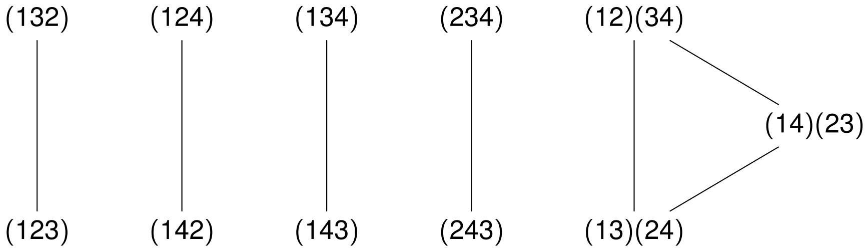
To understand the idea, here is the complement of the generating graph of the alternating group A_4 with the identity element removed from the set of vertices.

In this case, a maximal clique of the generating graph is obtained by choosing a representative in each connected component of the above graph.

Note (for later) that the subgroups generated by the connected components form a minimal covering of A_4.

It is hard to draw generating graphs in a meaningful way, because either there are too many edges or the graph is too simple.

To understand the idea, here is the complement of the generating graph of the alternating group A_4 with the identity element removed from the set of vertices.

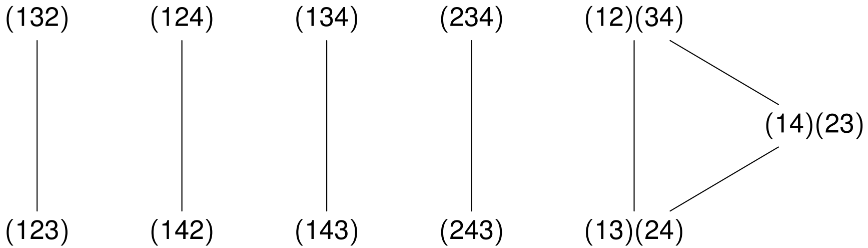


In this case, a maximal clique of the generating graph is obtained by choosing a representative in each connected component of the above graph.

Note (for later) that the subgroups generated by the connected components form a minimal covering of A_4.

It is hard to draw generating graphs in a meaningful way, because either there are too many edges or the graph is too simple.

To understand the idea, here is the complement of the generating graph of the alternating group A_4 with the identity element removed from the set of vertices.

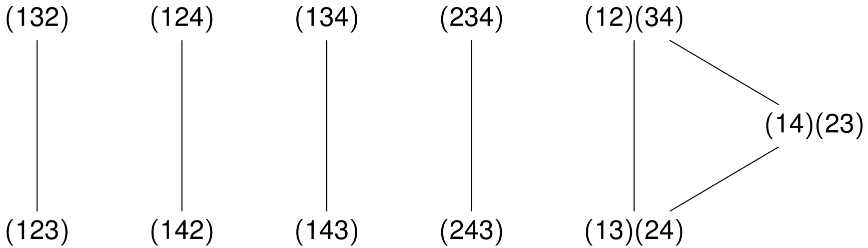


In this case, a maximal clique of the generating graph is obtained by choosing a representative in each connected component of the above graph.

Note (for later) that the subgroups generated by the connected components form a minimal covering of A_4.

It is hard to draw generating graphs in a meaningful way, because either there are too many edges or the graph is too simple.

To understand the idea, here is the complement of the generating graph of the alternating group A_4 with the identity element removed from the set of vertices.



In this case, a maximal clique of the generating graph is obtained by choosing a representative in each connected component of the above graph.

Note (for later) that the subgroups generated by the connected components form a minimal covering of A_4.

No group is the union of two proper subgroups.

A group G is a union of three proper subgroups A, B, C if and only if $G/N \cong C_2 \times C_2$ where $N := A \cap B \cap C \trianglelefteq G$. (Scorza, 1926.)

A covering of a non-cyclic group G is a family of proper subgroups of G whose union is G. In 1994, Cohn defined $\sigma(G)$ to be the smallest size of a covering of G. This is called the covering number of G.

If G is cyclic, we set $\sigma(G) = \infty$ for consistency of notation, with the convention that $m < \infty$ for every integer m.

We have a basic but very important inequality:

$$\omega(G) \leq \sigma(G).$$

This is because if $x, y \in G$ generate G then they cannot lie in the same proper subgroup of G.

It is a natural question to ask whether $\omega(G) = \sigma(G)$ for a given G.

No group is the union of two proper subgroups.

A group G is a union of three proper subgroups A, B, C if and only if $G/N \cong C_2 \times C_2$ where $N := A \cap B \cap C \trianglelefteq G$. (Scorza, 1926.)

A covering of a non-cyclic group G is a family of proper subgroups of G whose union is G. In 1994, Cohn defined $\sigma(G)$ to be the smallest size of a covering of G. This is called the covering number of G.

If G is cyclic, we set $\sigma(G) = \infty$ for consistency of notation, with the convention that $m < \infty$ for every integer m.

We have a basic but very important inequality:

$$\omega(G) \leq \sigma(G).$$

This is because if $x, y \in G$ generate G then they cannot lie in the same proper subgroup of G.

It is a natural question to ask whether $\omega(G) = \sigma(G)$ for a given G.

No group is the union of two proper subgroups.

A group G is a union of three proper subgroups A, B, C if and only if $G/N \cong C_2 \times C_2$ where $N := A \cap B \cap C \trianglelefteq G$. (Scorza, 1926.)

A covering of a non-cyclic group G is a family of proper subgroups of G whose union is G. In 1994, Cohn defined $\sigma(G)$ to be the smallest size of a covering of G. This is called the covering number of G.

If G is cyclic, we set $\sigma(G) = \infty$ for consistency of notation, with the convention that $m < \infty$ for every integer m.

We have a basic but very important inequality:

$$\omega(G) \leq \sigma(G).$$

This is because if $x, y \in G$ generate G then they cannot lie in the same proper subgroup of G.

It is a natural question to ask whether $\omega(G) = \sigma(G)$ for a given G.

No group is the union of two proper subgroups.

A group G is a union of three proper subgroups A, B, C if and only if $G/N \cong C_2 \times C_2$ where $N := A \cap B \cap C \trianglelefteq G$. (Scorza, 1926.)

A covering of a non-cyclic group G is a family of proper subgroups of G whose union is G. In 1994, Cohn defined $\sigma(G)$ to be the smallest size of a covering of G. This is called the covering number of G.

If G is cyclic, we set $\sigma(G) = \infty$ for consistency of notation, with the convention that $m < \infty$ for every integer m.

We have a basic but very important inequality:

$$\omega(G) \leq \sigma(G).$$

This is because if $x, y \in G$ generate G then they cannot lie in the same proper subgroup of G.

It is a natural question to ask whether $\omega(G) = \sigma(G)$ for a given G.

No group is the union of two proper subgroups.

A group G is a union of three proper subgroups A, B, C if and only if $G/N \cong C_2 \times C_2$ where $N := A \cap B \cap C \trianglelefteq G$. (Scorza, 1926.)

A covering of a non-cyclic group G is a family of proper subgroups of G whose union is G. In 1994, Cohn defined $\sigma(G)$ to be the smallest size of a covering of G. This is called the covering number of G.

If G is cyclic, we set $\sigma(G) = \infty$ for consistency of notation, with the convention that $m < \infty$ for every integer m.

We have a basic but very important inequality:

$$\omega(G) \leq \sigma(G).$$

This is because if $x, y \in G$ generate G then they cannot lie in the same proper subgroup of G.

It is a natural question to ask whether $\omega(G) = \sigma(G)$ for a given G.

No group is the union of two proper subgroups.

A group G is a union of three proper subgroups A, B, C if and only if $G/N \cong C_2 \times C_2$ where $N := A \cap B \cap C \trianglelefteq G$. (Scorza, 1926.)

A covering of a non-cyclic group G is a family of proper subgroups of G whose union is G. In 1994, Cohn defined $\sigma(G)$ to be the smallest size of a covering of G. This is called the covering number of G.

If G is cyclic, we set $\sigma(G) = \infty$ for consistency of notation, with the convention that $m < \infty$ for every integer m.

We have a basic but very important inequality:

$$\omega(G) \leq \sigma(G).$$

This is because if $x, y \in G$ generate G then they cannot lie in the same proper subgroup of G.

It is a natural question to ask whether $\omega(G) = \sigma(G)$ for a given G.

The invariant $\sigma(G)$ has a reasonable history. One very basic fact is that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N)$$

because every covering of G/N can be lifted to a covering of G.

We will list some facts about $G = S_n$, the symmetric group.

1. $\sigma(S_3) = 4$, the Sylow subgroups form a minimal covering.
2. $\sigma(S_4) = 4$ because S_4 has S_3 as homomorphic image.
3. $\sigma(S_5) = 16$, Cohn (1994).
4. $\sigma(S_n) = 2^{n-1}$ for $9 \neq n \geq 7$ odd, Maróti (2005).
5. $\sigma(S_6) = 13$, Abdollahi, Ashraf and Shaker (2007).
6. $\sigma(S_8) = 64$, $\sigma(S_9) = 256 = 2^{9-1}$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, Kappe, Nikolova-Popova and Swartz (2016).
7. $\sigma(S_n)$ for $n \geq 18$ divisible by 6, Swartz (2016).
8. $\sigma(S_{14}) = 3096$, Oppenheim and Swartz (2019).

The invariant $\sigma(G)$ has a reasonable history. One very basic fact is that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N)$$

because every covering of G/N can be lifted to a covering of G.

We will list some facts about $G = S_n$, the symmetric group.

1. $\sigma(S_3) = 4$, the Sylow subgroups form a minimal covering.
2. $\sigma(S_4) = 4$ because S_4 has S_3 as homomorphic image.
3. $\sigma(S_5) = 16$, Cohn (1994).
4. $\sigma(S_n) = 2^{n-1}$ for $9 \neq n \geq 7$ odd, Maróti (2005).
5. $\sigma(S_6) = 13$, Abdollahi, Ashraf and Shaker (2007).
6. $\sigma(S_8) = 64$, $\sigma(S_9) = 256 = 2^{9-1}$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, Kappe, Nikolova-Popova and Swartz (2016).
7. $\sigma(S_n)$ for $n \geq 18$ divisible by 6, Swartz (2016).
8. $\sigma(S_{14}) = 3096$, Oppenheim and Swartz (2019).

The invariant $\sigma(G)$ has a reasonable history. One very basic fact is that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N)$$

because every covering of G/N can be lifted to a covering of G.

We will list some facts about $G = S_n$, the symmetric group.

1. $\sigma(S_3) = 4$, the Sylow subgroups form a minimal covering.
2. $\sigma(S_4) = 4$ because S_4 has S_3 as homomorphic image.
3. $\sigma(S_5) = 16$, Cohn (1994).
4. $\sigma(S_n) = 2^{n-1}$ for $9 \neq n \geq 7$ odd, Maróti (2005).
5. $\sigma(S_6) = 13$, Abdollahi, Ashraf and Shaker (2007).
6. $\sigma(S_8) = 64$, $\sigma(S_9) = 256 = 2^{9-1}$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, Kappe, Nikolova-Popova and Swartz (2016).
7. $\sigma(S_n)$ for $n \geq 18$ divisible by 6, Swartz (2016).
8. $\sigma(S_{14}) = 3096$, Oppenheim and Swartz (2019).

The invariant $\sigma(G)$ has a reasonable history. One very basic fact is that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N)$$

because every covering of G/N can be lifted to a covering of G.

We will list some facts about $G = S_n$, the symmetric group.

1. $\sigma(S_3) = 4$, the Sylow subgroups form a minimal covering.
2. $\sigma(S_4) = 4$ because S_4 has S_3 as homomorphic image.
3. $\sigma(S_5) = 16$, Cohn (1994).
4. $\sigma(S_n) = 2^{n-1}$ for $9 \neq n \geq 7$ odd, Maróti (2005).
5. $\sigma(S_6) = 13$, Abdollahi, Ashraf and Shaker (2007).
6. $\sigma(S_8) = 64$, $\sigma(S_9) = 256 = 2^{9-1}$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, Kappe, Nikolova-Popova and Swartz (2016).
7. $\sigma(S_n)$ for $n \geq 18$ divisible by 6, Swartz (2016).
8. $\sigma(S_{14}) = 3096$, Oppenheim and Swartz (2019).

The invariant $\sigma(G)$ has a reasonable history. One very basic fact is that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N)$$

because every covering of G/N can be lifted to a covering of G.

We will list some facts about $G = S_n$, the symmetric group.

1. $\sigma(S_3) = 4$, the Sylow subgroups form a minimal covering.
2. $\sigma(S_4) = 4$ because S_4 has S_3 as homomorphic image.
3. $\sigma(S_5) = 16$, Cohn (1994).
4. $\sigma(S_n) = 2^{n-1}$ for $9 \neq n \geq 7$ odd, Maróti (2005).
5. $\sigma(S_6) = 13$, Abdollahi, Ashraf and Shaker (2007).
6. $\sigma(S_8) = 64$, $\sigma(S_9) = 256 = 2^{9-1}$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, Kappe, Nikolova-Popova and Swartz (2016).
7. $\sigma(S_n)$ for $n \geq 18$ divisible by 6, Swartz (2016).
8. $\sigma(S_{14}) = 3096$, Oppenheim and Swartz (2019).

The invariant $\sigma(G)$ has a reasonable history. One very basic fact is that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N)$$

because every covering of G/N can be lifted to a covering of G.

We will list some facts about $G = S_n$, the symmetric group.

1. $\sigma(S_3) = 4$, the Sylow subgroups form a minimal covering.
2. $\sigma(S_4) = 4$ because S_4 has S_3 as homomorphic image.
3. $\sigma(S_5) = 16$, Cohn (1994).
4. $\sigma(S_n) = 2^{n-1}$ for $9 \neq n \geq 7$ odd, Maróti (2005).
5. $\sigma(S_6) = 13$, Abdollahi, Ashraf and Shaker (2007).
6. $\sigma(S_8) = 64$, $\sigma(S_9) = 256 = 2^{9-1}$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, Kappe, Nikolova-Popova and Swartz (2016).
7. $\sigma(S_n)$ for $n \geq 18$ divisible by 6, Swartz (2016).
8. $\sigma(S_{14}) = 3096$, Oppenheim and Swartz (2019).

The invariant $\sigma(G)$ has a reasonable history. One very basic fact is that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N)$$

because every covering of G/N can be lifted to a covering of G.

We will list some facts about $G = S_n$, the symmetric group.

1. $\sigma(S_3) = 4$, the Sylow subgroups form a minimal covering.
2. $\sigma(S_4) = 4$ because S_4 has S_3 as homomorphic image.
3. $\sigma(S_5) = 16$, Cohn (1994).
4. $\sigma(S_n) = 2^{n-1}$ for $9 \neq n \geq 7$ odd, Maróti (2005).
5. $\sigma(S_6) = 13$, Abdollahi, Ashraf and Shaker (2007).
6. $\sigma(S_8) = 64$, $\sigma(S_9) = 256 = 2^{9-1}$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, Kappe, Nikolova-Popova and Swartz (2016).
7. $\sigma(S_n)$ for $n \geq 18$ divisible by 6, Swartz (2016).
8. $\sigma(S_{14}) = 3096$, Oppenheim and Swartz (2019).

The invariant $\sigma(G)$ has a reasonable history. One very basic fact is that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N)$$

because every covering of G/N can be lifted to a covering of G.

We will list some facts about $G = S_n$, the symmetric group.

1. $\sigma(S_3) = 4$, the Sylow subgroups form a minimal covering.
2. $\sigma(S_4) = 4$ because S_4 has S_3 as homomorphic image.
3. $\sigma(S_5) = 16$, Cohn (1994).
4. $\sigma(S_n) = 2^{n-1}$ for $9 \neq n \geq 7$ odd, Maróti (2005).
5. $\sigma(S_6) = 13$, Abdollahi, Ashraf and Shaker (2007).
6. $\sigma(S_8) = 64$, $\sigma(S_9) = 256 = 2^{9-1}$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, Kappe, Nikolova-Popova and Swartz (2016).
7. $\sigma(S_n)$ for $n \geq 18$ divisible by 6, Swartz (2016).
8. $\sigma(S_{14}) = 3096$, Oppenheim and Swartz (2019).

The invariant $\sigma(G)$ has a reasonable history. One very basic fact is that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N)$$

because every covering of G/N can be lifted to a covering of G.

We will list some facts about $G = S_n$, the symmetric group.

1. $\sigma(S_3) = 4$, the Sylow subgroups form a minimal covering.
2. $\sigma(S_4) = 4$ because S_4 has S_3 as homomorphic image.
3. $\sigma(S_5) = 16$, Cohn (1994).
4. $\sigma(S_n) = 2^{n-1}$ for $9 \neq n \geq 7$ odd, Maróti (2005).
5. $\sigma(S_6) = 13$, Abdollahi, Ashraf and Shaker (2007).
6. $\sigma(S_8) = 64$, $\sigma(S_9) = 256 = 2^{9-1}$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, Kappe, Nikolova-Popova and Swartz (2016).
7. $\sigma(S_n)$ for $n \geq 18$ divisible by 6, Swartz (2016).
8. $\sigma(S_{14}) = 3096$, Oppenheim and Swartz (2019).

Consider $G = S_n$ with n odd.

The works of Maróti ($n \neq 9$), Kappe, Nikolova-Popova and Swartz ($n = 9$) show that a minimal covering of G is given by the following subgroups.

- The alternating group A_n.
- The intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq (n-1)/2$.

$$\sigma(S_n) = 1 + \sum_{i=1}^{(n-1)/2} \binom{n}{i} = 2^{n-1}.$$

In order to prove that $\sigma(G) = X$ one usually proves that

- Upper bound. $\sigma(G) \leq X$ by exhibiting a covering of size X.
- Lower bound. $\sigma(G) \geq X$ by finding a set Π of elements of G that require at least X proper subgroups to be covered.

In the case of S_n with n odd, the above set Π is given by the elements of S_n that are product of at most two disjoint cycles.

Consider $G = S_n$ with n odd.

The works of Maróti ($n \neq 9$), Kappe, Nikolova-Popova and Swartz ($n = 9$) show that a minimal covering of G is given by the following subgroups.

- The alternating group A_n.
- The intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq (n-1)/2$.

$$\sigma(S_n) = 1 + \sum_{i=1}^{(n-1)/2} \binom{n}{i} = 2^{n-1}.$$

In order to prove that $\sigma(G) = X$ one usually proves that

- Upper bound. $\sigma(G) \leq X$ by exhibiting a covering of size X.
- Lower bound. $\sigma(G) \geq X$ by finding a set Π of elements of G that require at least X proper subgroups to be covered.

In the case of S_n with n odd, the above set Π is given by the elements of S_n that are product of at most two disjoint cycles.

Consider $G = S_n$ with n odd.

The works of Maróti ($n \neq 9$), Kappe, Nikolova-Popova and Swartz ($n = 9$) show that a minimal covering of G is given by the following subgroups.

- The alternating group A_n.
- The intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq (n-1)/2$.

$$\sigma(S_n) = 1 + \sum_{i=1}^{(n-1)/2} \binom{n}{i} = 2^{n-1}.$$

In order to prove that $\sigma(G) = X$ one usually proves that

- Upper bound. $\sigma(G) \leq X$ by exhibiting a covering of size X.
- Lower bound. $\sigma(G) \geq X$ by finding a set Π of elements of G that require at least X proper subgroups to be covered.

In the case of S_n with n odd, the above set Π is given by the elements of S_n that are product of at most two disjoint cycles.

Consider $G = S_n$ with n odd.

The works of Maróti ($n \neq 9$), Kappe, Nikolova-Popova and Swartz ($n = 9$) show that a minimal covering of G is given by the following subgroups.

- The alternating group A_n.
- The intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq (n-1)/2$.

$$\sigma(S_n) = 1 + \sum_{i=1}^{(n-1)/2} \binom{n}{i} = 2^{n-1}.$$

In order to prove that $\sigma(G) = X$ one usually proves that

- Upper bound. $\sigma(G) \leq X$ by exhibiting a covering of size X.
- Lower bound. $\sigma(G) \geq X$ by finding a set Π of elements of G that require at least X proper subgroups to be covered.

In the case of S_n with n odd, the above set Π is given by the elements of S_n that are product of at most two disjoint cycles.

Consider $G = S_n$ with n odd.

The works of Maróti ($n \neq 9$), Kappe, Nikolova-Popova and Swartz ($n = 9$) show that a minimal covering of G is given by the following subgroups.

- The alternating group A_n.
- The intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq (n-1)/2$.

$$\sigma(S_n) = 1 + \sum_{i=1}^{(n-1)/2} \binom{n}{i} = 2^{n-1}.$$

In order to prove that $\sigma(G) = X$ one usually proves that

- Upper bound. $\sigma(G) \leq X$ by exhibiting a covering of size X.
- Lower bound. $\sigma(G) \geq X$ by finding a set Π of elements of G that require at least X proper subgroups to be covered.

In the case of S_n with n odd, the above set Π is given by the elements of S_n that are product of at most two disjoint cycles.

Consider $G = S_n$ with n odd.

The works of Maróti ($n \neq 9$), Kappe, Nikolova-Popova and Swartz ($n = 9$) show that a minimal covering of G is given by the following subgroups.

- The alternating group A_n.
- The intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq (n-1)/2$.

$$\sigma(S_n) = 1 + \sum_{i=1}^{(n-1)/2} \binom{n}{i} = 2^{n-1}.$$

In order to prove that $\sigma(G) = X$ one usually proves that

- Upper bound. $\sigma(G) \leq X$ by exhibiting a covering of size X.
- Lower bound. $\sigma(G) \geq X$ by finding a set Π of elements of G that require at least X proper subgroups to be covered.

In the case of S_n with n odd, the above set Π is given by the elements of S_n that are product of at most two disjoint cycles.

Consider $G = S_n$ with n odd.

The works of Maróti ($n \neq 9$), Kappe, Nikolova-Popova and Swartz ($n = 9$) show that a minimal covering of G is given by the following subgroups.

- The alternating group A_n.
- The intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq (n-1)/2$.

$$\sigma(S_n) = 1 + \sum_{i=1}^{(n-1)/2} \binom{n}{i} = 2^{n-1}.$$

In order to prove that $\sigma(G) = X$ one usually proves that

- Upper bound. $\sigma(G) \leq X$ by exhibiting a covering of size X.
- Lower bound. $\sigma(G) \geq X$ by finding a set Π of elements of G that require at least X proper subgroups to be covered.

In the case of S_n with n odd, the above set Π is given by the elements of S_n that are product of at most two disjoint cycles.

Consider $G = S_n$ with n odd.

The works of Maróti ($n \neq 9$), Kappe, Nikolova-Popova and Swartz ($n = 9$) show that a minimal covering of G is given by the following subgroups.

- The alternating group A_n.
- The intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq (n-1)/2$.

$$\sigma(S_n) = 1 + \sum_{i=1}^{(n-1)/2} \binom{n}{i} = 2^{n-1}.$$

In order to prove that $\sigma(G) = X$ one usually proves that

- Upper bound. $\sigma(G) \leq X$ by exhibiting a covering of size X.
- Lower bound. $\sigma(G) \geq X$ by finding a set Π of elements of G that require at least X proper subgroups to be covered.

In the case of S_n with n odd, the above set Π is given by the elements of S_n that are product of at most two disjoint cycles.

Consider $G = S_n$ with n odd.

The works of Maróti ($n \neq 9$), Kappe, Nikolova-Popova and Swartz ($n = 9$) show that a minimal covering of G is given by the following subgroups.

- The alternating group A_n.
- The intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq (n-1)/2$.

$$\sigma(S_n) = 1 + \sum_{i=1}^{(n-1)/2} \binom{n}{i} = 2^{n-1}.$$

In order to prove that $\sigma(G) = X$ one usually proves that

- Upper bound. $\sigma(G) \leq X$ by exhibiting a covering of size X.
- Lower bound. $\sigma(G) \geq X$ by finding a set Π of elements of G that require at least X proper subgroups to be covered.

In the case of S_n with n odd, the above set Π is given by the elements of S_n that are product of at most two disjoint cycles.

Let us look closely at Swartz's result about S_n when n is divisible by 6, since this was one of our starting points.

We will leave $n = 18$ out since it is a bit different. If $n \geq 24$ is divisible by 6 then

$$\sigma(S_n) = 1 + \sum_{i=1}^{n/3-1} \binom{n}{i} + \frac{1}{2}\binom{n}{n/2}.$$

A minimal covering is given by

- the alternating group A_n,
- the intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq n/3 - 1$,
- the imprimitive maximal subgroups $S_{n/2} \wr S_2$ stabilizing partitions with two blocks of equal size.

Two years ago, in the beginning of 2019, Francesco Fumagalli and I tried to adapt Eric Swartz's argument to deal with all the even values of n, but we didn't succeed. Things progressed when we talked to Attila Maróti about this, in April of 2020.

Let us look closely at Swartz's result about S_n when n is divisible by 6, since this was one of our starting points.

We will leave $n = 18$ out since it is a bit different. If $n \geq 24$ is divisible by 6 then

$$\sigma(S_n) = 1 + \sum_{i=1}^{n/3-1} \binom{n}{i} + \frac{1}{2}\binom{n}{n/2}.$$

A minimal covering is given by

- the alternating group A_n,
- the intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq n/3 - 1$,
- the imprimitive maximal subgroups $S_{n/2} \wr S_2$ stabilizing partitions with two blocks of equal size.

Two years ago, in the beginning of 2019, Francesco Fumagalli and I tried to adapt Eric Swartz's argument to deal with all the even values of n, but we didn't succeed. Things progressed when we talked to Attila Maróti about this, in April of 2020.

Let us look closely at Swartz's result about S_n when n is divisible by 6, since this was one of our starting points.

We will leave $n = 18$ out since it is a bit different. If $n \geq 24$ is divisible by 6 then

$$\sigma(S_n) = 1 + \sum_{i=1}^{n/3-1} \binom{n}{i} + \frac{1}{2}\binom{n}{n/2}.$$

A minimal covering is given by

- the alternating group A_n,
- the intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq n/3 - 1$,
- the imprimitive maximal subgroups $S_{n/2} \wr S_2$ stabilizing partitions with two blocks of equal size.

Two years ago, in the beginning of 2019, Francesco Fumagalli and I tried to adapt Eric Swartz's argument to deal with all the even values of n, but we didn't succeed. Things progressed when we talked to Attila Maróti about this, in April of 2020.

Let us look closely at Swartz's result about S_n when n is divisible by 6, since this was one of our starting points.

We will leave $n = 18$ out since it is a bit different. If $n \geq 24$ is divisible by 6 then

$$\sigma(S_n) = 1 + \sum_{i=1}^{n/3-1} \binom{n}{i} + \frac{1}{2}\binom{n}{n/2}.$$

A minimal covering is given by

- the alternating group A_n,
- the intransitive maximal subgroups $S_i \times S_{n-i}$ stabilizing a set of size i for every i with $1 \leq i \leq n/3 - 1$,
- the imprimitive maximal subgroups $S_{n/2} \wr S_2$ stabilizing partitions with two blocks of equal size.

Two years ago, in the beginning of 2019, Francesco Fumagalli and I tried to adapt Eric Swartz's argument to deal with all the even values of n, but we didn't succeed. Things progressed when we talked to Attila Maróti about this, in April of 2020.

The result I am now presenting is the following.

Theorem (Fumagalli, G., Maróti)

If n is even and $n \geq 20$, $n \neq 22$, then $\omega(S_n) = \sigma(S_n)$ and

$$\omega(S_n) = \begin{cases} 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{n/3-1}\binom{n}{i} & \text{if } n \equiv 0 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-1)/3-2}\binom{n}{i} + \binom{n}{(n-1)/3} & \text{if } n \equiv 1 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-2)/3}\binom{n}{i} & \text{if } n \equiv 2 \mod 3. \end{cases}$$

It is quite surprising that we achieved the value of $\sigma(G)$ by calculating $\omega(G)$, which looks harder.

The result I am now presenting is the following.

THEOREM (FUMAGALLI, G., MARÓTI)

If n is even and $n \geq 20$, $n \neq 22$, *then* $\omega(S_n) = \sigma(S_n)$ *and*

$$\omega(S_n) = \begin{cases} 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{n/3-1}\binom{n}{i} & \text{if } n \equiv 0 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-1)/3-2}\binom{n}{i} + \binom{n}{(n-1)/3} & \text{if } n \equiv 1 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-2)/3}\binom{n}{i} & \text{if } n \equiv 2 \mod 3. \end{cases}$$

It is quite surprising that we achieved the value of $\sigma(G)$ by calculating $\omega(G)$, which looks harder.

The result I am now presenting is the following.

THEOREM (FUMAGALLI, G., MARÓTI)

If n is even and $n \geq 20$, $n \neq 22$, then $\omega(S_n) = \sigma(S_n)$ and

$$\omega(S_n) = \begin{cases} 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{n/3-1}\binom{n}{i} & \text{if } n \equiv 0 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-1)/3-2}\binom{n}{i} + \binom{n}{(n-1)/3} & \text{if } n \equiv 1 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-2)/3}\binom{n}{i} & \text{if } n \equiv 2 \mod 3. \end{cases}$$

It is quite surprising that we achieved the value of $\sigma(G)$ by calculating $\omega(G)$, which looks harder.

It is time to present our second starting point.

After Maróti's result about $\sigma(S_n)$ when n is odd and $n \neq 9$ (2005), Blackburn [2] (2006) proved that $\omega(G) = \sigma(G)$ when G is a symmetric group of large enough odd degree. Later, Stringer studied the small values of the degree. Combining their results, what they proved is

THEOREM (BLACKBURN, STRINGER, 2006)

If $n \geq 5$ is an odd integer and $n \neq 5, 9, 15$ then $\omega(S_n) = \sigma(S_n)$ (which equals 2^{n-1} by Maróti's result). Moreover $\omega(S_5) = 13$ and

$$235 \leq \omega(S_9) \leq 244 < 256 = \sigma(S_9).$$

Interestingly, this result gives us examples of groups for which $\omega \neq \sigma$, the symmetric groups S_5 and S_9.

The values of $\omega(S_9)$ and $\omega(S_{15})$ are not known. It is also not known whether $\omega(S_{15})$ equals $\sigma(S_{15})$ or not.

Surprisingly, the main tool to prove this theorem was probabilistic.

It is time to present our second starting point.

After Maróti's result about $\sigma(S_n)$ when n is odd and $n \neq 9$ (2005), Blackburn [2] (2006) proved that $\omega(G) = \sigma(G)$ when G is a symmetric group of large enough odd degree. Later, Stringer studied the small values of the degree. Combining their results, what they proved is

THEOREM (BLACKBURN, STRINGER, 2006)

If $n \geq 5$ is an odd integer and $n \neq 5, 9, 15$ then $\omega(S_n) = \sigma(S_n)$ (which equals 2^{n-1} by Maróti's result). Moreover $\omega(S_5) = 13$ and

$$235 \leq \omega(S_9) \leq 244 < 256 = \sigma(S_9).$$

Interestingly, this result gives us examples of groups for which $\omega \neq \sigma$, the symmetric groups S_5 and S_9.

The values of $\omega(S_9)$ and $\omega(S_{15})$ are not known. It is also not known whether $\omega(S_{15})$ equals $\sigma(S_{15})$ or not.

Surprisingly, the main tool to prove this theorem was probabilistic.

It is time to present our second starting point.

After Maróti's result about $\sigma(S_n)$ when n is odd and $n \neq 9$ (2005), Blackburn [2] (2006) proved that $\omega(G) = \sigma(G)$ when G is a symmetric group of large enough odd degree. Later, Stringer studied the small values of the degree. Combining their results, what they proved is

THEOREM (BLACKBURN, STRINGER, 2006)

If $n \geq 5$ is an odd integer and $n \neq 5, 9, 15$ then $\omega(S_n) = \sigma(S_n)$ (which equals 2^{n-1} by Maróti's result). Moreover $\omega(S_5) = 13$ and

$$235 \leq \omega(S_9) \leq 244 < 256 = \sigma(S_9).$$

Interestingly, this result gives us examples of groups for which $\omega \neq \sigma$, the symmetric groups S_5 and S_9.

The values of $\omega(S_9)$ and $\omega(S_{15})$ are not known. It is also not known whether $\omega(S_{15})$ equals $\sigma(S_{15})$ or not.

Surprisingly, the main tool to prove this theorem was probabilistic.

It is time to present our second starting point.

After Maróti's result about $\sigma(S_n)$ when n is odd and $n \neq 9$ (2005), Blackburn [2] (2006) proved that $\omega(G) = \sigma(G)$ when G is a symmetric group of large enough odd degree. Later, Stringer studied the small values of the degree. Combining their results, what they proved is

Theorem (Blackburn, Stringer, 2006)

If $n \geq 5$ is an odd integer and $n \neq 5, 9, 15$ then $\omega(S_n) = \sigma(S_n)$ (which equals 2^{n-1} by Maróti's result). Moreover $\omega(S_5) = 13$ and

$$235 \leq \omega(S_9) \leq 244 < 256 = \sigma(S_9).$$

Interestingly, this result gives us examples of groups for which $\omega \neq \sigma$, the symmetric groups S_5 and S_9.

The values of $\omega(S_9)$ and $\omega(S_{15})$ are not known. It is also not known whether $\omega(S_{15})$ equals $\sigma(S_{15})$ or not.

Surprisingly, the main tool to prove this theorem was probabilistic.

It is time to present our second starting point.

After Maróti's result about $\sigma(S_n)$ when n is odd and $n \neq 9$ (2005), Blackburn [2] (2006) proved that $\omega(G) = \sigma(G)$ when G is a symmetric group of large enough odd degree. Later, Stringer studied the small values of the degree. Combining their results, what they proved is

Theorem (Blackburn, Stringer, 2006)

If $n \geq 5$ is an odd integer and $n \neq 5, 9, 15$ then $\omega(S_n) = \sigma(S_n)$ (which equals 2^{n-1} by Maróti's result). Moreover $\omega(S_5) = 13$ and

$$235 \leq \omega(S_9) \leq 244 < 256 = \sigma(S_9).$$

Interestingly, this result gives us examples of groups for which $\omega \neq \sigma$, the symmetric groups S_5 and S_9.

The values of $\omega(S_9)$ and $\omega(S_{15})$ are not known. It is also not known whether $\omega(S_{15})$ equals $\sigma(S_{15})$ or not.

Surprisingly, the main tool to prove this theorem was probabilistic.

The proof of our result uses the same tool used by Blackburn and Stringer. Let us outline their argument for any group G.

- Consider a family $\mathscr{M}$ of maximal subgroups of G and $\Pi \subseteq G$.
- Suppose that the sets $C(M) := \Pi \cap M$, $M \in \mathscr{M}$, are non-empty and partition Π.
- Choose, uniformly and independently, an element g_M in each of the sets $C(M)$, $M \in \mathscr{M}$.
- Suppose that, whenever $M, K \in \mathscr{M}$ and $M \neq K$, the elements g_M, g_K generate G with high probability.
- Then, by a probabilistic argument based on the Lovász local lemma, the probability that the randomly chosen elements, one for each $C(M)$, generate G pairwise is positive.

This guarantees the existence of $g_M \in C(M)$ for every $M \in \mathscr{M}$ such that $\langle g_M, g_K \rangle = G$ for every $M, K \in \mathscr{M}$, $M \neq K$. This implies that $\{g_M : M \in \mathscr{M}\}$ is a clique of the generating graph of G, and its size is $|\mathscr{M}|$, so $|\mathscr{M}| \leq \omega(G)$.

If $\mathscr{M}$ happens to be a covering of G, then $|\mathscr{M}| \leq \omega(G) \leq \sigma(G) \leq |\mathscr{M}|$ therefore $\omega(G) = \sigma(G) = |\mathscr{M}|$.

The proof of our result uses the same tool used by Blackburn and Stringer. Let us outline their argument for any group G.

- Consider a family $\mathscr{M}$ of maximal subgroups of G and $\Pi \subseteq G$.
- Suppose that the sets $C(M) := \Pi \cap M$, $M \in \mathscr{M}$, are non-empty and partition Π.
- Choose, uniformly and independently, an element g_M in each of the sets $C(M)$, $M \in \mathscr{M}$.
- Suppose that, whenever $M, K \in \mathscr{M}$ and $M \neq K$, the elements g_M, g_K generate G with high probability.
- Then, by a probabilistic argument based on the Lovász local lemma, the probability that the randomly chosen elements, one for each $C(M)$, generate G pairwise is positive.

This guarantees the existence of $g_M \in C(M)$ for every $M \in \mathscr{M}$ such that $\langle g_M, g_K \rangle = G$ for every $M, K \in \mathscr{M}$, $M \neq K$. This implies that $\{g_M \ : \ M \in \mathscr{M}\}$ is a clique of the generating graph of G, and its size is $|\mathscr{M}|$, so $|\mathscr{M}| \leq \omega(G)$.

If $\mathscr{M}$ happens to be a covering of G, then $|\mathscr{M}| \leq \omega(G) \leq \sigma(G) \leq |\mathscr{M}|$ therefore $\omega(G) = \sigma(G) = |\mathscr{M}|$.

The proof of our result uses the same tool used by Blackburn and Stringer. Let us outline their argument for any group G.

- Consider a family $\mathscr{M}$ of maximal subgroups of G and $\Pi \subseteq G$.
- Suppose that the sets $C(M) := \Pi \cap M$, $M \in \mathscr{M}$, are non-empty and partition Π.
- Choose, uniformly and independently, an element g_M in each of the sets $C(M)$, $M \in \mathscr{M}$.
- Suppose that, whenever $M, K \in \mathscr{M}$ and $M \neq K$, the elements g_M, g_K generate G with high probability.
- Then, by a probabilistic argument based on the Lovász local lemma, the probability that the randomly chosen elements, one for each $C(M)$, generate G pairwise is positive.

This guarantees the existence of $g_M \in C(M)$ for every $M \in \mathscr{M}$ such that $\langle g_M, g_K \rangle = G$ for every $M, K \in \mathscr{M}$, $M \neq K$. This implies that $\{g_M : M \in \mathscr{M}\}$ is a clique of the generating graph of G, and its size is $|\mathscr{M}|$, so $|\mathscr{M}| \leq \omega(G)$.

If $\mathscr{M}$ happens to be a covering of G, then $|\mathscr{M}| \leq \omega(G) \leq \sigma(G) \leq |\mathscr{M}|$ therefore $\omega(G) = \sigma(G) = |\mathscr{M}|$.

The proof of our result uses the same tool used by Blackburn and Stringer. Let us outline their argument for any group G.

- Consider a family $\mathscr{M}$ of maximal subgroups of G and $\Pi \subseteq G$.
- Suppose that the sets $C(M) := \Pi \cap M$, $M \in \mathscr{M}$, are non-empty and partition Π.
- Choose, uniformly and independently, an element g_M in each of the sets $C(M)$, $M \in \mathscr{M}$.
- Suppose that, whenever $M, K \in \mathscr{M}$ and $M \neq K$, the elements g_M, g_K generate G with high probability.
- Then, by a probabilistic argument based on the Lovász local lemma, the probability that the randomly chosen elements, one for each $C(M)$, generate G pairwise is positive.

This guarantees the existence of $g_M \in C(M)$ for every $M \in \mathscr{M}$ such that $\langle g_M, g_K \rangle = G$ for every $M, K \in \mathscr{M}$, $M \neq K$. This implies that $\{g_M : M \in \mathscr{M}\}$ is a clique of the generating graph of G, and its size is $|\mathscr{M}|$, so $|\mathscr{M}| \leq \omega(G)$.

If $\mathscr{M}$ happens to be a covering of G, then $|\mathscr{M}| \leq \omega(G) \leq \sigma(G) \leq |\mathscr{M}|$ therefore $\omega(G) = \sigma(G) = |\mathscr{M}|$.

The proof of our result uses the same tool used by Blackburn and Stringer. Let us outline their argument for any group G.

- Consider a family $\mathscr{M}$ of maximal subgroups of G and $\Pi \subseteq G$.
- Suppose that the sets $C(M) := \Pi \cap M$, $M \in \mathscr{M}$, are non-empty and partition Π.
- Choose, uniformly and independently, an element g_M in each of the sets $C(M)$, $M \in \mathscr{M}$.
- Suppose that, whenever $M, K \in \mathscr{M}$ and $M \neq K$, the elements g_M, g_K generate G with high probability.
- Then, by a probabilistic argument based on the Lovász local lemma, the probability that the randomly chosen elements, one for each $C(M)$, generate G pairwise is positive.

This guarantees the existence of $g_M \in C(M)$ for every $M \in \mathscr{M}$ such that $\langle g_M, g_K \rangle = G$ for every $M, K \in \mathscr{M}$, $M \neq K$. This implies that $\{g_M : M \in \mathscr{M}\}$ is a clique of the generating graph of G, and its size is $|\mathscr{M}|$, so $|\mathscr{M}| \leq \omega(G)$.

If $\mathscr{M}$ happens to be a covering of G, then $|\mathscr{M}| \leq \omega(G) \leq \sigma(G) \leq |\mathscr{M}|$ therefore $\omega(G) = \sigma(G) = |\mathscr{M}|$.

The proof of our result uses the same tool used by Blackburn and Stringer. Let us outline their argument for any group G.

- Consider a family $\mathscr{M}$ of maximal subgroups of G and $\Pi \subseteq G$.
- Suppose that the sets $C(M) := \Pi \cap M$, $M \in \mathscr{M}$, are non-empty and partition Π.
- Choose, uniformly and independently, an element g_M in each of the sets $C(M)$, $M \in \mathscr{M}$.
- Suppose that, whenever $M, K \in \mathscr{M}$ and $M \neq K$, the elements g_M, g_K generate G with high probability.
- Then, by a probabilistic argument based on the Lovász local lemma, the probability that the randomly chosen elements, one for each $C(M)$, generate G pairwise is positive.

This guarantees the existence of $g_M \in C(M)$ for every $M \in \mathscr{M}$ such that $\langle g_M, g_K \rangle = G$ for every $M, K \in \mathscr{M}$, $M \neq K$. This implies that $\{g_M \ : \ M \in \mathscr{M}\}$ is a clique of the generating graph of G, and its size is $|\mathscr{M}|$, so $|\mathscr{M}| \leq \omega(G)$.

If $\mathscr{M}$ happens to be a covering of G, then $|\mathscr{M}| \leq \omega(G) \leq \sigma(G) \leq |\mathscr{M}|$ therefore $\omega(G) = \sigma(G) = |\mathscr{M}|$.

The proof of our result uses the same tool used by Blackburn and Stringer. Let us outline their argument for any group G.

- Consider a family $\mathscr{M}$ of maximal subgroups of G and $\Pi \subseteq G$.
- Suppose that the sets $C(M) := \Pi \cap M$, $M \in \mathscr{M}$, are non-empty and partition Π.
- Choose, uniformly and independently, an element g_M in each of the sets $C(M)$, $M \in \mathscr{M}$.
- Suppose that, whenever $M, K \in \mathscr{M}$ and $M \neq K$, the elements g_M, g_K generate G with high probability.
- Then, by a probabilistic argument based on the Lovász local lemma, the probability that the randomly chosen elements, one for each $C(M)$, generate G pairwise is positive.

This guarantees the existence of $g_M \in C(M)$ for every $M \in \mathscr{M}$ such that $\langle g_M, g_K \rangle = G$ for every $M, K \in \mathscr{M}$, $M \neq K$. This implies that $\{g_M : M \in \mathscr{M}\}$ is a clique of the generating graph of G, and its size is $|\mathscr{M}|$, so $|\mathscr{M}| \leq \omega(G)$.

If $\mathscr{M}$ happens to be a covering of G, then $|\mathscr{M}| \leq \omega(G) \leq \sigma(G) \leq |\mathscr{M}|$ therefore $\omega(G) = \sigma(G) = |\mathscr{M}|$.

The proof of our result uses the same tool used by Blackburn and Stringer. Let us outline their argument for any group G.

- Consider a family $\mathscr{M}$ of maximal subgroups of G and $\Pi \subseteq G$.
- Suppose that the sets $C(M) := \Pi \cap M$, $M \in \mathscr{M}$, are non-empty and partition Π.
- Choose, uniformly and independently, an element g_M in each of the sets $C(M)$, $M \in \mathscr{M}$.
- Suppose that, whenever $M, K \in \mathscr{M}$ and $M \neq K$, the elements g_M, g_K generate G with high probability.
- Then, by a probabilistic argument based on the Lovász local lemma, the probability that the randomly chosen elements, one for each $C(M)$, generate G pairwise is positive.

This guarantees the existence of $g_M \in C(M)$ for every $M \in \mathscr{M}$ such that $\langle g_M, g_K \rangle = G$ for every $M, K \in \mathscr{M}$, $M \neq K$. This implies that $\{g_M \ : \ M \in \mathscr{M}\}$ is a clique of the generating graph of G, and its size is $|\mathscr{M}|$, so $|\mathscr{M}| \leq \omega(G)$.

If $\mathscr{M}$ happens to be a covering of G, then $|\mathscr{M}| \leq \omega(G) \leq \sigma(G) \leq |\mathscr{M}|$ therefore $\omega(G) = \sigma(G) = |\mathscr{M}|$.

It is time to present the main idea of the probabilistic argument we used. It could be informally phrased as follows: events with high probability have a chance of occurring simultaneously.

More formally, we have the following beautiful result, proved by Erdős and Lovász in 1975.

THEOREM (LOVÁSZ LOCAL LEMMA, ERDŐS AND LOVÁSZ, 1975)

Let $A_1, \ldots, A_n$ be events in an arbitrary probability space. Let (V, E) be a directed graph, where $V = \{1, \ldots, n\}$, and assume that

$$P(A_i \mid \bigcap_{j \in S} \overline{A_j}) = P(A_i) \quad \forall i \in V, \quad \forall S \subseteq \{j \in V \ : \ (i,j) \notin E\}.$$

(This is a mutual independence condition.) Let d be the maximum valency of a vertex of the graph (V, E).

$$\text{If} \quad P(A_i) \leq \frac{1}{e(d+1)} \quad \forall i \in V \quad \text{then} \quad P(\bigcap_{i \in V} \overline{A_i}) > 0.$$

It is time to present the main idea of the probabilistic argument we used. It could be informally phrased as follows: events with high probability have a chance of occurring simultaneously.

More formally, we have the following beautiful result, proved by Erdős and Lovász in 1975.

THEOREM (LOVÁSZ LOCAL LEMMA, ERDŐS AND LOVÁSZ, 1975)

Let $A_1, \ldots, A_n$ be events in an arbitrary probability space. Let (V, E) be a directed graph, where $V = \{1, \ldots, n\}$, and assume that

$$P(A_i \mid \bigcap_{j \in S} \overline{A_j}) = P(A_i) \quad \forall i \in V, \quad \forall S \subseteq \{j \in V \ : \ (i,j) \notin E\}.$$

(This is a mutual independence condition.) Let d be the maximum valency of a vertex of the graph (V, E).

$$\text{If} \quad P(A_i) \leq \frac{1}{e(d+1)} \quad \forall i \in V \quad \text{then} \quad P(\bigcap_{i \in V} \overline{A_i}) > 0.$$

It is time to present the main idea of the probabilistic argument we used. It could be informally phrased as follows: events with high probability have a chance of occurring simultaneously.

More formally, we have the following beautiful result, proved by Erdős and Lovász in 1975.

THEOREM (LOVÁSZ LOCAL LEMMA, ERDŐS AND LOVÁSZ, 1975)

Let $A_1, \ldots, A_n$ be events in an arbitrary probability space. Let (V, E) be a directed graph, where $V = \{1, \ldots, n\}$, and assume that

$$P(A_i \mid \bigcap_{j \in S} \overline{A_j}) = P(A_i) \quad \forall i \in V, \quad \forall S \subseteq \{j \in V \ : \ (i,j) \notin E\}.$$

(This is a mutual independence condition.) Let d be the maximum valency of a vertex of the graph (V, E).

$$\text{If} \quad P(A_i) \leq \frac{1}{e(d+1)} \quad \forall i \in V \quad \text{then} \quad P(\bigcap_{i \in V} \overline{A_i}) > 0.$$

As I mentioned, the idea of using the local lemma to compute $\omega(G)$ was introduced by Blackburn [2].

Let $G := S_n$ and assume that Π is a subset of G and $\mathscr{M}$ is a set of maximal subgroups of G which can be partitioned $\Pi = \bigcup_{i \in I} \Pi_i$, $\mathscr{M} = \bigcup_{i \in I} \mathscr{M}_i$ in such a way that

- (Covering condition.) $\bigcup_{M \in \mathscr{M}} M = G$.
- (Partition condition.) The sets

$$C(M) := M \cap \Pi, \qquad M \in \mathscr{M},$$

  are non-empty and pairwise disjoint. Moreover, $C(M) \subseteq \Pi_i$ if $M \in \mathscr{M}_i$, for every $i \in I$.

Choose, uniformly and independently, an element g_M in every $C(M)$. Let V be the set of 2-element subsets of $\mathscr{M}$ and set

$$E := \{(v, w) \in V \times V \ : \ v \cap w \neq \varnothing\}.$$

Then (V, E) is a simple regular graph with valency $d = 2(|\mathscr{M}| - 2)$.

As I mentioned, the idea of using the local lemma to compute $\omega(G)$ was introduced by Blackburn [2].

Let $G := S_n$ and assume that Π is a subset of G and $\mathscr{M}$ is a set of maximal subgroups of G which can be partitioned $\Pi = \bigcup_{i \in I} \Pi_i$, $\mathscr{M} = \bigcup_{i \in I} \mathscr{M}_i$ in such a way that

- (Covering condition.) $\bigcup_{M \in \mathscr{M}} M = G$.
- (Partition condition.) The sets

$$C(M) := M \cap \Pi, \qquad M \in \mathscr{M},$$

  are non-empty and pairwise disjoint. Moreover, $C(M) \subseteq \Pi_i$ if $M \in \mathscr{M}_i$, for every $i \in I$.

Choose, uniformly and independently, an element g_M in every $C(M)$. Let V be the set of 2-element subsets of $\mathscr{M}$ and set

$$E := \{(v, w) \in V \times V \ : \ v \cap w \neq \varnothing\}.$$

Then (V, E) is a simple regular graph with valency $d = 2(|\mathscr{M}| - 2)$.

As I mentioned, the idea of using the local lemma to compute $\omega(G)$ was introduced by Blackburn [2].

Let $G := S_n$ and assume that Π is a subset of G and $\mathscr{M}$ is a set of maximal subgroups of G which can be partitioned $\Pi = \bigcup_{i \in I} \Pi_i$, $\mathscr{M} = \bigcup_{i \in I} \mathscr{M}_i$ in such a way that

- (Covering condition.) $\bigcup_{M \in \mathscr{M}} M = G$.
- (Partition condition.) The sets

$$C(M) := M \cap \Pi, \qquad M \in \mathscr{M},$$

  are non-empty and pairwise disjoint. Moreover, $C(M) \subseteq \Pi_i$ if $M \in \mathscr{M}_i$, for every $i \in I$.

Choose, uniformly and independently, an element g_M in every $C(M)$. Let V be the set of 2-element subsets of $\mathscr{M}$ and set

$$E := \{(v, w) \in V \times V \ : \ v \cap w \neq \varnothing\}.$$

Then (V, E) is a simple regular graph with valency $d = 2(|\mathscr{M}| - 2)$.

As I mentioned, the idea of using the local lemma to compute $\omega(G)$ was introduced by Blackburn [2].

Let $G := S_n$ and assume that Π is a subset of G and $\mathscr{M}$ is a set of maximal subgroups of G which can be partitioned $\Pi = \bigcup_{i \in I} \Pi_i$, $\mathscr{M} = \bigcup_{i \in I} \mathscr{M}_i$ in such a way that

- (Covering condition.) $\bigcup_{M \in \mathscr{M}} M = G$.
- (Partition condition.) The sets

$$C(M) := M \cap \Pi, \qquad M \in \mathscr{M},$$

are non-empty and pairwise disjoint. Moreover, $C(M) \subseteq \Pi_i$ if $M \in \mathscr{M}_i$, for every $i \in I$.

Choose, uniformly and independently, an element g_M in every $C(M)$. Let V be the set of 2-element subsets of $\mathscr{M}$ and set

$$E := \{(v, w) \in V \times V \ : \ v \cap w \neq \varnothing\}.$$

Then (V, E) is a simple regular graph with valency $d = 2(|\mathscr{M}| - 2)$.

For every $v = \{M, K\} \in V$ let E_v be the event "$\langle g_M, g_K \rangle \neq G$".
The valency of every vertex is $d = 2(|\mathscr{M}| - 2)$. Using the local lemma, if we can prove that

$$P(E_v) \leq \frac{1}{e(d+1)} = \frac{1}{e(2|\mathscr{M}| - 3)},$$

then we can deduce that the event

$$\bigcap_{v \in V} \overline{E_v} = \text{“}\langle g_M, g_K \rangle = G \quad \forall M, K \in \mathscr{M}, \quad M \neq K\text{''}$$

has positive probability. Therefore there exists a choice of the elements g_M forming a clique of the generating graph of G, so that

$$|\mathscr{M}| \leq \omega(G).$$

Since $\bigcup_{M \in \mathscr{M}} M = G$, we have $\omega(G) \leq \sigma(G) \leq |\mathscr{M}|$, therefore

$$\omega(G) = \sigma(G) = |\mathscr{M}|.$$

For every $v = \{M, K\} \in V$ let E_v be the event "$\langle g_M, g_K \rangle \neq G$".
The valency of every vertex is $d = 2(|\mathscr{M}| - 2)$. Using the local lemma, if we can prove that

$$P(E_v) \leq \frac{1}{e(d+1)} = \frac{1}{e(2|\mathscr{M}| - 3)},$$

then we can deduce that the event

$$\bigcap_{v \in V} \overline{E_v} = \text{“}\langle g_M, g_K \rangle = G \quad \forall M, K \in \mathscr{M}, \quad M \neq K\text{''}$$

has positive probability. Therefore there exists a choice of the elements g_M forming a clique of the generating graph of G, so that

$$|\mathscr{M}| \leq \omega(G).$$

Since $\bigcup_{M \in \mathscr{M}} M = G$, we have $\omega(G) \leq \sigma(G) \leq |\mathscr{M}|$, therefore

$$\omega(G) = \sigma(G) = |\mathscr{M}|.$$

Recall that our main result is the following.

THEOREM (FUMAGALLI, G., MARÓTI)

If n is even and $n \geq 20$, $n \neq 22$, then $\omega(S_n) = \sigma(S_n)$ and

$$\omega(S_n) = \begin{cases} 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{n/3-1}\binom{n}{i} & \text{if } n \equiv 0 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-1)/3-2}\binom{n}{i} + \binom{n}{(n-1)/3} & \text{if } n \equiv 1 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-2)/3}\binom{n}{i} & \text{if } n \equiv 2 \mod 3. \end{cases}$$

We will give a sketch of the proof of this in the case of large degree $n \equiv 2 \mod 3$ with $n/2$ odd.

Recall that our main result is the following.

THEOREM (FUMAGALLI, G., MARÓTI)

If n is even and $n \geq 20$, $n \neq 22$, *then* $\omega(S_n) = \sigma(S_n)$ *and*

$$\omega(S_n) = \begin{cases} 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{n/3-1}\binom{n}{i} & \text{if } n \equiv 0 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-1)/3-2}\binom{n}{i} + \binom{n}{(n-1)/3} & \text{if } n \equiv 1 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-2)/3}\binom{n}{i} & \text{if } n \equiv 2 \mod 3. \end{cases}$$

We will give a sketch of the proof of this in the case of large degree $n \equiv 2 \mod 3$ with $n/2$ odd.

Recall that our main result is the following.

THEOREM (FUMAGALLI, G., MARÓTI)

If n is even and $n \geq 20$, $n \neq 22$, *then* $\omega(S_n) = \sigma(S_n)$ *and*

$$\omega(S_n) = \begin{cases} 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{n/3-1}\binom{n}{i} & \text{if } n \equiv 0 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-1)/3-2}\binom{n}{i} + \binom{n}{(n-1)/3} & \text{if } n \equiv 1 \mod 3, \\ 1 + \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{(n-2)/3}\binom{n}{i} & \text{if } n \equiv 2 \mod 3. \end{cases}$$

We will give a sketch of the proof of this in the case of large degree $n \equiv 2 \mod 3$ with $n/2$ odd.

Sketch of proof.

Assume $n \equiv 2 \mod 3$, with $n/2$ odd, and write $n = 3q + 2$, so that q is even. In this sketch, we will assume that n is as large as we need.

Let $\mathscr{M}$ be the set consisting of the alternating group A_n ($\mathscr{M}_0$), the maximal intransitive subgroups of type $S_i \times S_{n-i}$, with $i = 1, \ldots, q$ ($\mathscr{M}_i$, $i = 1, \ldots, q$), and the maximal imprimitive subgroups with two blocks, $S_{n/2} \wr S_2$ ($\mathscr{M}_{-1}$). Set

$$\Pi_{-1} = (n), \qquad \Pi_0 = (n/2 - 2, n/2 + 2), \qquad \Pi_1 = (1, n/2 - 2, n/2 + 1),$$

$$\Pi_2 = (2, n/2 - 4, n/2 + 2), \qquad \Pi_4 = (4, n/2 - 2, n/2 - 2).$$

For all i such that $3 \leq i \leq q - 2$, $i \neq 4$, set

$$\Pi_i = \begin{cases} (i,\ (n-i)/2 - 1,\ (n-i)/2 + 1) & \text{if } n - i \equiv 0 \pmod 4, \\ (i,\ (n-i)/2 - 2,\ (n-i)/2 + 2) & \text{if } n - i \equiv 2 \pmod 4, \\ (i, (n-i-1)/2, (n-i+1)/2) & \text{if } i \equiv 1 \pmod 2. \end{cases}$$

Finally, set $\Pi_{q-1} = (q-1, q+1, q+2)$, $\Pi_q = (q, q+1, q+1)$ and

$$\Pi := \Pi_{-1} \cup \Pi_1 \cup \Pi_2 \cup \ldots \cup \Pi_q.$$

Sketch of proof.

Assume $n \equiv 2 \mod 3$, with $n/2$ odd, and write $n = 3q+2$, so that q is even. In this sketch, we will assume that n is as large as we need.

Let $\mathscr{M}$ be the set consisting of the alternating group A_n ($\mathscr{M}_0$), the maximal intransitive subgroups of type $S_i \times S_{n-i}$, with $i = 1, \ldots, q$ ($\mathscr{M}_i$, $i = 1, \ldots, q$), and the maximal imprimitive subgroups with two blocks, $S_{n/2} \wr S_2$ ($\mathscr{M}_{-1}$). Set

$$\Pi_{-1} = (n), \qquad \Pi_0 = (n/2-2, n/2+2), \qquad \Pi_1 = (1, n/2-2, n/2+1),$$

$$\Pi_2 = (2, n/2-4, n/2+2), \qquad \Pi_4 = (4, n/2-2, n/2-2).$$

For all i such that $3 \leq i \leq q-2$, $i \neq 4$, set

$$\Pi_i = \begin{cases} (i,\ (n-i)/2-1,\ (n-i)/2+1) & \text{if } n-i \equiv 0 \pmod 4, \\ (i,\ (n-i)/2-2,\ (n-i)/2+2) & \text{if } n-i \equiv 2 \pmod 4, \\ (i, (n-i-1)/2, (n-i+1)/2) & \text{if } i \equiv 1 \pmod 2. \end{cases}$$

Finally, set $\Pi_{q-1} = (q-1, q+1, q+2)$, $\Pi_q = (q, q+1, q+1)$ and

$$\Pi := \Pi_{-1} \cup \Pi_1 \cup \Pi_2 \cup \ldots \cup \Pi_q.$$

Sketch of proof.

Assume $n \equiv 2 \mod 3$, with $n/2$ odd, and write $n = 3q + 2$, so that q is even. In this sketch, we will assume that n is as large as we need.

Let $\mathscr{M}$ be the set consisting of the alternating group A_n ($\mathscr{M}_0$), the maximal intransitive subgroups of type $S_i \times S_{n-i}$, with $i = 1, \ldots, q$ ($\mathscr{M}_i$, $i = 1, \ldots, q$), and the maximal imprimitive subgroups with two blocks, $S_{n/2} \wr S_2$ ($\mathscr{M}_{-1}$). Set

$$\Pi_{-1} = (n), \qquad \Pi_0 = (n/2 - 2, n/2 + 2), \qquad \Pi_1 = (1, n/2 - 2, n/2 + 1),$$

$$\Pi_2 = (2, n/2 - 4, n/2 + 2), \qquad \Pi_4 = (4, n/2 - 2, n/2 - 2).$$

For all i such that $3 \leq i \leq q - 2$, $i \neq 4$, set

$$\Pi_i = \begin{cases} (i,\ (n-i)/2 - 1,\ (n-i)/2 + 1) & \text{if } n - i \equiv 0 \pmod 4, \\ (i,\ (n-i)/2 - 2,\ (n-i)/2 + 2) & \text{if } n - i \equiv 2 \pmod 4, \\ (i, (n-i-1)/2, (n-i+1)/2) & \text{if } i \equiv 1 \pmod 2. \end{cases}$$

Finally, set $\Pi_{q-1} = (q - 1, q + 1, q + 2)$, $\Pi_q = (q, q + 1, q + 1)$ and

$$\Pi := \Pi_{-1} \cup \Pi_1 \cup \Pi_2 \cup \ldots \cup \Pi_q.$$

Sketch of proof.

Assume $n \equiv 2 \mod 3$, with $n/2$ odd, and write $n = 3q+2$, so that q is even. In this sketch, we will assume that n is as large as we need.

Let $\mathscr{M}$ be the set consisting of the alternating group A_n ($\mathscr{M}_0$), the maximal intransitive subgroups of type $S_i \times S_{n-i}$, with $i = 1, \ldots, q$ ($\mathscr{M}_i$, $i = 1, \ldots, q$), and the maximal imprimitive subgroups with two blocks, $S_{n/2} \wr S_2$ ($\mathscr{M}_{-1}$). Set

$$\Pi_{-1} = (n), \qquad \Pi_0 = (n/2-2, n/2+2), \qquad \Pi_1 = (1, n/2-2, n/2+1),$$

$$\Pi_2 = (2, n/2-4, n/2+2), \qquad \Pi_4 = (4, n/2-2, n/2-2).$$

For all i such that $3 \leq i \leq q-2$, $i \neq 4$, set

$$\Pi_i = \begin{cases} (i,\ (n-i)/2-1,\ (n-i)/2+1) & \text{if } n-i \equiv 0 \pmod 4, \\ (i,\ (n-i)/2-2,\ (n-i)/2+2) & \text{if } n-i \equiv 2 \pmod 4, \\ (i, (n-i-1)/2, (n-i+1)/2) & \text{if } i \equiv 1 \pmod 2. \end{cases}$$

Finally, set $\Pi_{q-1} = (q-1, q+1, q+2)$, $\Pi_q = (q, q+1, q+1)$ and

$$\Pi := \Pi_{-1} \cup \Pi_1 \cup \Pi_2 \cup \ldots \cup \Pi_q.$$

Sketch of proof.

Assume $n \equiv 2 \mod 3$, with $n/2$ odd, and write $n = 3q + 2$, so that q is even. In this sketch, we will assume that n is as large as we need.

Let $\mathscr{M}$ be the set consisting of the alternating group A_n ($\mathscr{M}_0$), the maximal intransitive subgroups of type $S_i \times S_{n-i}$, with $i = 1, \dots, q$ ($\mathscr{M}_i$, $i = 1, \dots, q$), and the maximal imprimitive subgroups with two blocks, $S_{n/2} \wr S_2$ ($\mathscr{M}_{-1}$). Set

$$\Pi_{-1} = (n), \qquad \Pi_0 = (n/2 - 2, n/2 + 2), \qquad \Pi_1 = (1, n/2 - 2, n/2 + 1),$$

$$\Pi_2 = (2, n/2 - 4, n/2 + 2), \qquad \Pi_4 = (4, n/2 - 2, n/2 - 2).$$

For all i such that $3 \leq i \leq q - 2$, $i \neq 4$, set

$$\Pi_i = \begin{cases} (i,\ (n-i)/2 - 1,\ (n-i)/2 + 1) & \text{if } n - i \equiv 0 \pmod 4, \\ (i,\ (n-i)/2 - 2,\ (n-i)/2 + 2) & \text{if } n - i \equiv 2 \pmod 4, \\ (i, (n-i-1)/2, (n-i+1)/2) & \text{if } i \equiv 1 \pmod 2. \end{cases}$$

Finally, set $\Pi_{q-1} = (q-1, q+1, q+2)$, $\Pi_q = (q, q+1, q+1)$ and

$$\Pi := \Pi_{-1} \cup \Pi_1 \cup \Pi_2 \cup \ldots \cup \Pi_q.$$

Sketch of proof.

Assume $n \equiv 2 \mod 3$, with $n/2$ odd, and write $n = 3q + 2$, so that q is even. In this sketch, we will assume that n is as large as we need.

Let $\mathscr{M}$ be the set consisting of the alternating group A_n ($\mathscr{M}_0$), the maximal intransitive subgroups of type $S_i \times S_{n-i}$, with $i = 1, \dots, q$ ($\mathscr{M}_i$, $i = 1, \dots, q$), and the maximal imprimitive subgroups with two blocks, $S_{n/2} \wr S_2$ ($\mathscr{M}_{-1}$). Set

$$\Pi_{-1} = (n), \qquad \Pi_0 = (n/2 - 2, n/2 + 2), \qquad \Pi_1 = (1, n/2 - 2, n/2 + 1),$$

$$\Pi_2 = (2, n/2 - 4, n/2 + 2), \qquad \Pi_4 = (4, n/2 - 2, n/2 - 2).$$

For all i such that $3 \leq i \leq q - 2$, $i \neq 4$, set

$$\Pi_i = \begin{cases} (i,\ (n-i)/2 - 1,\ (n-i)/2 + 1) & \text{if } n - i \equiv 0 \pmod 4, \\ (i,\ (n-i)/2 - 2,\ (n-i)/2 + 2) & \text{if } n - i \equiv 2 \pmod 4, \\ (i, (n-i-1)/2, (n-i+1)/2) & \text{if } i \equiv 1 \pmod 2. \end{cases}$$

Finally, set $\Pi_{q-1} = (q-1, q+1, q+2)$, $\Pi_q = (q, q+1, q+1)$ and

$$\Pi := \Pi_{-1} \cup \Pi_1 \cup \Pi_2 \cup \ldots \cup \Pi_q.$$

For every $M \in \mathscr{M}$ set $C(M) := \Pi \cap M$. For every maximal subgroup H of G outside $\mathscr{M}$, define

$$f_M(H) := \frac{|C(M) \cap H|}{|C(M)|}.$$

We can bound the probability of E_v, where $v = \{M, K\} \in V$, as follows, where H varies in the set of maximal subgroups of G.

$$P(E_v) \leq \sum_H f_M(H) \cdot f_K(H) = \sum_{H \in \mathscr{H}_1} f_M(H) \cdot f_K(H) + \sum_{H \in \mathscr{H}_2} f_M(H) \cdot f_K(H).$$

Here $\mathscr{H}_1$ is the set of intransitive maximal subgroups of G, $\mathscr{H}_2$ is the set of transitive maximal subgroups of G.

By the partition condition, if $H \in \mathscr{M}$ then one of $f_M(H)$ and $f_K(H)$ is zero, so we may assume that the sum is over the maximal subgroups H of G outside $\mathscr{M}$. We need to bound

$$\ell_j = \sum_{H \in \mathscr{H}_j} f_M(H) \cdot f_K(H), \qquad j \in \{1, 2\}.$$

We need to show that $\ell_1 + \ell_2 \leq \frac{1}{e(d+1)}$, which is roughly $(1/2)^n$.

For every $M \in \mathscr{M}$ set $C(M) := \Pi \cap M$. For every maximal subgroup H of G outside $\mathscr{M}$, define

$$f_M(H) := \frac{|C(M) \cap H|}{|C(M)|}.$$

We can bound the probability of E_v, where $v = \{M, K\} \in V$, as follows, where H varies in the set of maximal subgroups of G.

$$P(E_v) \leq \sum_H f_M(H) \cdot f_K(H) = \sum_{H \in \mathscr{H}_1} f_M(H) \cdot f_K(H) + \sum_{H \in \mathscr{H}_2} f_M(H) \cdot f_K(H).$$

Here $\mathscr{H}_1$ is the set of intransitive maximal subgroups of G, $\mathscr{H}_2$ is the set of transitive maximal subgroups of G.

By the partition condition, if $H \in \mathscr{M}$ then one of $f_M(H)$ and $f_K(H)$ is zero, so we may assume that the sum is over the maximal subgroups H of G outside $\mathscr{M}$. We need to bound

$$\ell_j = \sum_{H \in \mathscr{H}_j} f_M(H) \cdot f_K(H), \qquad j \in \{1, 2\}.$$

We need to show that $\ell_1 + \ell_2 \leq \frac{1}{e(d+1)}$, which is roughly $(1/2)^n$.

For every $M \in \mathscr{M}$ set $C(M) := \Pi \cap M$. For every maximal subgroup H of G outside $\mathscr{M}$, define

$$f_M(H) := \frac{|C(M) \cap H|}{|C(M)|}.$$

We can bound the probability of E_v, where $v = \{M, K\} \in V$, as follows, where H varies in the set of maximal subgroups of G.

$$P(E_v) \leq \sum_H f_M(H) \cdot f_K(H) = \sum_{H \in \mathscr{H}_1} f_M(H) \cdot f_K(H) + \sum_{H \in \mathscr{H}_2} f_M(H) \cdot f_K(H).$$

Here $\mathscr{H}_1$ is the set of intransitive maximal subgroups of G, $\mathscr{H}_2$ is the set of transitive maximal subgroups of G.

By the partition condition, if $H \in \mathscr{M}$ then one of $f_M(H)$ and $f_K(H)$ is zero, so we may assume that the sum is over the maximal subgroups H of G outside $\mathscr{M}$. We need to bound

$$\ell_j = \sum_{H \in \mathscr{H}_j} f_M(H) \cdot f_K(H), \qquad j \in \{1, 2\}.$$

We need to show that $\ell_1 + \ell_2 \leq \frac{1}{e(d+1)}$, which is roughly $(1/2)^n$.

It is possible to show that, for every $M \in \mathscr{M}$,

$$|C(M)| \geq \frac{4}{n^3} 2^{2n/3} \left(\frac{n}{3e}\right)^n .$$

From now on, let H be a maximal subgroup of G outside $\mathscr{M}$.

Assume first that H is intransitive. Using the fact that $H \notin \mathscr{M}$, it is possible to show that

$$f_M(H) \leq \frac{6n}{2^{2n/3}}.$$

Let M, K be two distinct members of $\mathscr{M}$. Since at most two members of $\mathscr{H}_1 - \mathscr{M}$ intersect both $C(M)$ and $C(K)$, we obtain that

$$\ell_1 = \sum_{H \in \mathscr{H}_1} f_M(H) \cdot f_K(H) \leq 2 \cdot \left(\frac{6n}{2^{2n/3}}\right)^2 = 72n^2 \cdot (1/2)^{4n/3}.$$

This is good for us since $(1/2)^{4/3} < 1/2$.

It is possible to show that, for every $M \in \mathscr{M}$,

$$|C(M)| \geq \frac{4}{n^3} 2^{2n/3} \left(\frac{n}{3e}\right)^n .$$

From now on, let H be a maximal subgroup of G outside $\mathscr{M}$.

Assume first that H is intransitive. Using the fact that $H \notin \mathscr{M}$, it is possible to show that

$$f_M(H) \leq \frac{6n}{2^{2n/3}}.$$

Let M, K be two distinct members of $\mathscr{M}$. Since at most two members of $\mathscr{H}_1 - \mathscr{M}$ intersect both $C(M)$ and $C(K)$, we obtain that

$$\ell_1 = \sum_{H \in \mathscr{H}_1} f_M(H) \cdot f_K(H) \leq 2 \cdot \left(\frac{6n}{2^{2n/3}}\right)^2 = 72n^2 \cdot (1/2)^{4n/3}.$$

This is good for us since $(1/2)^{4/3} < 1/2$.

It is possible to show that, for every $M \in \mathscr{M}$,

$$|C(M)| \geq \frac{4}{n^3} 2^{2n/3} \left(\frac{n}{3e}\right)^n.$$

From now on, let H be a maximal subgroup of G outside $\mathscr{M}$.

Assume first that H is intransitive. Using the fact that $H \notin \mathscr{M}$, it is possible to show that

$$f_M(H) \leq \frac{6n}{2^{2n/3}}.$$

Let M, K be two distinct members of $\mathscr{M}$. Since at most two members of $\mathscr{H}_1 - \mathscr{M}$ intersect both $C(M)$ and $C(K)$, we obtain that

$$\ell_1 = \sum_{H \in \mathscr{H}_1} f_M(H) \cdot f_K(H) \leq 2 \cdot \left(\frac{6n}{2^{2n/3}}\right)^2 = 72n^2 \cdot (1/2)^{4n/3}.$$

This is good for us since $(1/2)^{4/3} < 1/2$.

Assume now that H is transitive. If H is primitive then $|H| \leq 4^n$ (Praeger, Saxl 1980, not depending on CFSG), and if H is imprimitive then, since n is large and not divisible by 3, the largest value of $|H|$ is given by the case $H \cong S_{n/5} \wr S_5$. It follows that

$$|H| \leq (n/5)!^5 \cdot 5! \leq 120n^3(n/5e)^n.$$

Therefore

$$f_M(H) = \frac{|C(M) \cap H|}{|C(M)|} \leq \frac{|H|}{|C(M)|} \leq \frac{120n^3(n/5e)^n}{\frac{4}{n^3}2^{2n/3}\left(\frac{n}{3e}\right)^n} = 30n^6 \cdot \left(\frac{3}{5 \cdot 2^{2/3}}\right)^n.$$

Note that $\qquad f_M(H) \leq 30n^6 \cdot a^n, \qquad a = 3/(5 \cdot 2^{2/3}) < 1/2.$

For technical reasons (that depend on CFSG !!) the term $f_M(H)$ is the main contribution in the bound for ℓ_2 in the sense that

$$\ell_2 = \sum_{H \in \mathscr{H}_2} f_M(H) \cdot f_K(H) \leq n^{O(1)} \cdot \max_{H \in \mathscr{H}_2} f_M(H) \leq n^{O(1)} a^n.$$

This is less than $(1/2)^n$ when n is large.
This finishes the sketch of the proof.

Assume now that H is transitive. If H is primitive then $|H| \leq 4^n$ (Praeger, Saxl 1980, not depending on CFSG), and if H is imprimitive then, since n is large and not divisible by 3, the largest value of $|H|$ is given by the case $H \cong S_{n/5} \wr S_5$. It follows that

$$|H| \leq (n/5)!^5 \cdot 5! \leq 120n^3(n/5e)^n.$$

Therefore

$$f_M(H) = \frac{|C(M) \cap H|}{|C(M)|} \leq \frac{|H|}{|C(M)|} \leq \frac{120n^3(n/5e)^n}{\frac{4}{n^3}2^{2n/3}\left(\frac{n}{3e}\right)^n} = 30n^6 \cdot \left(\frac{3}{5 \cdot 2^{2/3}}\right)^n.$$

Note that $f_M(H) \leq 30n^6 \cdot a^n, \quad a = 3/(5 \cdot 2^{2/3}) < 1/2.$

For technical reasons (that depend on CFSG !!) the term $f_M(H)$ is the main contribution in the bound for ℓ_2 in the sense that

$$\ell_2 = \sum_{H \in \mathscr{H}_2} f_M(H) \cdot f_K(H) \leq n^{O(1)} \cdot \max_{H \in \mathscr{H}_2} f_M(H) \leq n^{O(1)} a^n.$$

This is less than $(1/2)^n$ when n is large.
This finishes the sketch of the proof.

Assume now that H is transitive. If H is primitive then $|H| \leq 4^n$ (Praeger, Saxl 1980, not depending on CFSG), and if H is imprimitive then, since n is large and not divisible by 3, the largest value of $|H|$ is given by the case $H \cong S_{n/5} \wr S_5$. It follows that

$$|H| \leq (n/5)!^5 \cdot 5! \leq 120n^3(n/5e)^n.$$

Therefore

$$f_M(H) = \frac{|C(M) \cap H|}{|C(M)|} \leq \frac{|H|}{|C(M)|} \leq \frac{120n^3(n/5e)^n}{\frac{4}{n^3}2^{2n/3}\left(\frac{n}{3e}\right)^n} = 30n^6 \cdot \left(\frac{3}{5 \cdot 2^{2/3}}\right)^n.$$

Note that $\quad f_M(H) \leq 30n^6 \cdot a^n, \qquad a = 3/(5 \cdot 2^{2/3}) < 1/2.$

For technical reasons (that depend on CFSG !!) the term $f_M(H)$ is the main contribution in the bound for ℓ_2 in the sense that

$$\ell_2 = \sum_{H \in \mathscr{H}_2} f_M(H) \cdot f_K(H) \leq n^{O(1)} \cdot \max_{H \in \mathscr{H}_2} f_M(H) \leq n^{O(1)} a^n.$$

This is less than $(1/2)^n$ when n is large.

This finishes the sketch of the proof.

Assume now that H is transitive. If H is primitive then $|H| \leq 4^n$ (Praeger, Saxl 1980, not depending on CFSG), and if H is imprimitive then, since n is large and not divisible by 3, the largest value of $|H|$ is given by the case $H \cong S_{n/5} \wr S_5$. It follows that

$$|H| \leq (n/5)!^5 \cdot 5! \leq 120n^3(n/5e)^n.$$

Therefore

$$f_M(H) = \frac{|C(M) \cap H|}{|C(M)|} \leq \frac{|H|}{|C(M)|} \leq \frac{120n^3(n/5e)^n}{\frac{4}{n^3} 2^{2n/3} \left(\frac{n}{3e}\right)^n} = 30n^6 \cdot \left(\frac{3}{5 \cdot 2^{2/3}}\right)^n.$$

Note that $f_M(H) \leq 30n^6 \cdot a^n, \qquad a = 3/(5 \cdot 2^{2/3}) < 1/2.$

For technical reasons (that depend on CFSG !!) the term $f_M(H)$ is the main contribution in the bound for ℓ_2 in the sense that

$$\ell_2 = \sum_{H \in \mathscr{H}_2} f_M(H) \cdot f_K(H) \leq n^{O(1)} \cdot \max_{H \in \mathscr{H}_2} f_M(H) \leq n^{O(1)} a^n.$$

This is less than $(1/2)^n$ when n is large.
This finishes the sketch of the proof.

Let us go back to bounding the probability.

Given a family $\mathscr{H}_j$ of maximal subgroups of $G = S_n$ outside $\mathscr{M}$ and a vertex $v = \{M, K\}$ of the graph, let E_v^j be the event that "$g_M, g_K \in H$ for some $H \in \mathscr{H}_j$". A technical computation shows that

$$P(E_v^j) \leq c_{v,j} \cdot \min_{\{L_1,L_2\}=\{M,K\}} \left(\max_{\substack{S \in \mathscr{H}_j \\ H \in [S]}} (m_{L_1}([S]) \cdot f_{L_2}(H)) \right).$$

- $[S]$ denotes the G-conjugacy class of a subgroup S of G.
- $m_L([S]) = \max_{g \in C(L)} |\{S^x \ : \ x \in G, \ g \in S^x\}|$.
- $c_{v,j}$ denotes the number of conjugacy classes of subgroups in $\mathscr{H}_j$ such that there exists H in such a class such that $H \cap C(M) \neq \varnothing$ and $H \cap C(K) \neq \varnothing$.

It is elementary to see that $m_L([S]) \leq n^3$.

However, there is no elementary way (i.e. without CFSG) to effectively bound $c_{v,j}$ when $\mathscr{H}_j$ is the family of primitive maximal subgroups. Using CFSG, a deep theorem of Liebeck and Shalev [7] (1996) implies that $c_{v,j} \leq n$ for large enough n in this case.

Let us go back to bounding the probability.

Given a family $\mathscr{H}_j$ of maximal subgroups of $G = S_n$ outside $\mathscr{M}$ and a vertex $v = \{M, K\}$ of the graph, let E_v^j be the event that "$g_M, g_K \in H$ for some $H \in \mathscr{H}_j$". A technical computation shows that

$$P(E_v^j) \leq c_{v,j} \cdot \min_{\{L_1, L_2\} = \{M, K\}} \left(\max_{\substack{S \in \mathscr{H}_j \\ H \in [S]}} (m_{L_1}([S]) \cdot f_{L_2}(H)) \right).$$

- $[S]$ denotes the G-conjugacy class of a subgroup S of G.
- $m_L([S]) = \max_{g \in C(L)} |\{S^x \ : \ x \in G, g \in S^x\}|$.
- $c_{v,j}$ denotes the number of conjugacy classes of subgroups in $\mathscr{H}_j$ such that there exists H in such a class such that $H \cap C(M) \neq \varnothing$ and $H \cap C(K) \neq \varnothing$.

It is elementary to see that $m_L([S]) \leq n^3$.

However, there is no elementary way (i.e. without CFSG) to effectively bound $c_{v,j}$ when $\mathscr{H}_j$ is the family of primitive maximal subgroups. Using CFSG, a deep theorem of Liebeck and Shalev [7] (1996) implies that $c_{v,j} \leq n$ for large enough n in this case.

Let us go back to bounding the probability.

Given a family $\mathscr{H}_j$ of maximal subgroups of $G = S_n$ outside $\mathscr{M}$ and a vertex $v = \{M, K\}$ of the graph, let E_v^j be the event that "$g_M, g_K \in H$ for some $H \in \mathscr{H}_j$". A technical computation shows that

$$P(E_v^j) \leq c_{v,j} \cdot \min_{\{L_1,L_2\}=\{M,K\}} \left(\max_{\substack{S \in \mathscr{H}_j \\ H \in [S]}} (m_{L_1}([S]) \cdot f_{L_2}(H)) \right).$$

- $[S]$ denotes the G-conjugacy class of a subgroup S of G.
- $m_L([S]) = \max_{g \in C(L)} |\{S^x \ : \ x \in G, \ g \in S^x\}|$.
- $c_{v,j}$ denotes the number of conjugacy classes of subgroups in $\mathscr{H}_j$ such that there exists H in such a class such that $H \cap C(M) \neq \varnothing$ and $H \cap C(K) \neq \varnothing$.

It is elementary to see that $m_L([S]) \leq n^3$.

However, there is no elementary way (i.e. without CFSG) to effectively bound $c_{v,j}$ when $\mathscr{H}_j$ is the family of primitive maximal subgroups. Using CFSG, a deep theorem of Liebeck and Shalev [7] (1996) implies that $c_{v,j} \leq n$ for large enough n in this case.

Let us go back to bounding the probability.

Given a family $\mathscr{H}_j$ of maximal subgroups of $G = S_n$ outside $\mathscr{M}$ and a vertex $v = \{M, K\}$ of the graph, let E_v^j be the event that "$g_M, g_K \in H$ for some $H \in \mathscr{H}_j$". A technical computation shows that

$$P(E_v^j) \leq c_{v,j} \cdot \min_{\{L_1,L_2\}=\{M,K\}} \left(\max_{\substack{S\in\mathscr{H}_j \\ H\in[S]}} (m_{L_1}([S]) \cdot f_{L_2}(H)) \right).$$

- $[S]$ denotes the G-conjugacy class of a subgroup S of G.
- $m_L([S]) = \max_{g\in C(L)} |\{S^x \ : \ x \in G, \ g \in S^x\}|$.
- $c_{v,j}$ denotes the number of conjugacy classes of subgroups in $\mathscr{H}_j$ such that there exists H in such a class such that $H \cap C(M) \neq \varnothing$ and $H \cap C(K) \neq \varnothing$.

It is elementary to see that $m_L([S]) \leq n^3$.

However, there is no elementary way (i.e. without CFSG) to effectively bound $c_{v,j}$ when $\mathscr{H}_j$ is the family of primitive maximal subgroups. Using CFSG, a deep theorem of Liebeck and Shalev [7] (1996) implies that $c_{v,j} \leq n$ for large enough n in this case.

Let us go back to bounding the probability.

Given a family $\mathscr{H}_j$ of maximal subgroups of $G = S_n$ outside $\mathscr{M}$ and a vertex $v = \{M, K\}$ of the graph, let E_v^j be the event that "$g_M, g_K \in H$ for some $H \in \mathscr{H}_j$". A technical computation shows that

$$P(E_v^j) \leq c_{v,j} \cdot \min_{\{L_1, L_2\} = \{M, K\}} \left(\max_{\substack{S \in \mathscr{H}_j \\ H \in [S]}} (m_{L_1}([S]) \cdot f_{L_2}(H)) \right).$$

- $[S]$ denotes the G-conjugacy class of a subgroup S of G.
- $m_L([S]) = \max_{g \in C(L)} |\{S^x \ : \ x \in G, \ g \in S^x\}|$.
- $c_{v,j}$ denotes the number of conjugacy classes of subgroups in $\mathscr{H}_j$ such that there exists H in such a class such that $H \cap C(M) \neq \varnothing$ and $H \cap C(K) \neq \varnothing$.

It is elementary to see that $m_L([S]) \leq n^3$.

However, there is no elementary way (i.e. without CFSG) to effectively bound $c_{v,j}$ when $\mathscr{H}_j$ is the family of primitive maximal subgroups. Using CFSG, a deep theorem of Liebeck and Shalev [7] (1996) implies that $c_{v,j} \leq n$ for large enough n in this case.

In other words, the technical reasons above (the ones depending on CFSG) depend on us being able to bound the number of conjugacy classes of primitive maximal subgroups of $G = S_n$.

To obtain a proof not depending of CFSG (for n large) we would need to prove, without using CFSG, that the number of conjugacy classes of maximal primitive subgroups of $G = S_n$ (n large) is at most

$$(n/8e)^n.$$

This seems to be out of reach.

Even classifying primitive groups of degree n containing n-cycles requires the classification.

THEOREM (TURÁN 1941)

A simple graph on m vertices which does not contain a clique of size $r+1$ has at most $(1-1/r)m^2/2$ vertices.

Using this, together with a result of Virchow about generating pairs in the alternating and symmetric groups, we can prove without using CFSG that $\omega(S_n) > n/5$ for large n.

In other words, the technical reasons above (the ones depending on CFSG) depend on us being able to bound the number of conjugacy classes of primitive maximal subgroups of $G = S_n$.

To obtain a proof not depending of CFSG (for n large) we would need to prove, without using CFSG, that the number of conjugacy classes of maximal primitive subgroups of $G = S_n$ (n large) is at most

$$(n/8e)^n.$$

This seems to be out of reach.

Even classifying primitive groups of degree n containing n-cycles requires the classification.

THEOREM (TURÁN 1941)

A simple graph on m vertices which does not contain a clique of size $r+1$ has at most $(1-1/r)m^2/2$ vertices.

Using this, together with a result of Virchow about generating pairs in the alternating and symmetric groups, we can prove without using CFSG that $\omega(S_n) > n/5$ for large n.

In other words, the technical reasons above (the ones depending on CFSG) depend on us being able to bound the number of conjugacy classes of primitive maximal subgroups of $G = S_n$.

To obtain a proof not depending of CFSG (for n large) we would need to prove, without using CFSG, that the number of conjugacy classes of maximal primitive subgroups of $G = S_n$ (n large) is at most

$$(n/8e)^n.$$

This seems to be out of reach.

Even classifying primitive groups of degree n containing n-cycles requires the classification.

THEOREM (TURÁN 1941)

A simple graph on m vertices which does not contain a clique of size $r+1$ has at most $(1-1/r)m^2/2$ vertices.

Using this, together with a result of Virchow about generating pairs in the alternating and symmetric groups, we can prove without using CFSG that $\omega(S_n) > n/5$ for large n.

In other words, the technical reasons above (the ones depending on CFSG) depend on us being able to bound the number of conjugacy classes of primitive maximal subgroups of $G = S_n$.

To obtain a proof not depending of CFSG (for n large) we would need to prove, without using CFSG, that the number of conjugacy classes of maximal primitive subgroups of $G = S_n$ (n large) is at most

$$(n/8e)^n.$$

This seems to be out of reach.

Even classifying primitive groups of degree n containing n-cycles requires the classification.

THEOREM (TURÁN 1941)

A simple graph on m vertices which does not contain a clique of size $r+1$ has at most $(1-1/r)m^2/2$ vertices.

Using this, together with a result of Virchow about generating pairs in the alternating and symmetric groups, we can prove without using CFSG that $\omega(S_n) > n/5$ for large n.

There are certain hidden technicalities in the above sketch.

The main one is that when H is an imprimitive maximal subgroups with 3 or 4 blocks, i.e. of type $S_{n/3} \wr S_3$ or $S_{n/4} \wr S_4$, the bound

$$f_M(H) = \frac{|C(M) \cap H|}{|C(M)|} \leq \frac{|H|}{|C(M)|}$$

is not good enough. We need to work out the exact value of $|C(M) \cap H|$ in these cases.

When looking at small values of n ($20 \leq n < 166$, $n \neq 22$), the above bound is not good enough either. We have a general lemma computing the exact value of $f_M(H)$ in case H is not primitive.

There are certain hidden technicalities in the above sketch.

The main one is that when H is an imprimitive maximal subgroups with 3 or 4 blocks, i.e. of type $S_{n/3} \wr S_3$ or $S_{n/4} \wr S_4$, the bound

$$f_M(H) = \frac{|C(M) \cap H|}{|C(M)|} \leq \frac{|H|}{|C(M)|}$$

is not good enough. We need to work out the exact value of $|C(M) \cap H|$ in these cases.

When looking at small values of n ($20 \leq n < 166$, $n \neq 22$), the above bound is not good enough either. We have a general lemma computing the exact value of $f_M(H)$ in case H is not primitive.

There are certain hidden technicalities in the above sketch.

The main one is that when H is an imprimitive maximal subgroups with 3 or 4 blocks, i.e. of type $S_{n/3} \wr S_3$ or $S_{n/4} \wr S_4$, the bound

$$f_M(H) = \frac{|C(M) \cap H|}{|C(M)|} \leq \frac{|H|}{|C(M)|}$$

is not good enough. We need to work out the exact value of $|C(M) \cap H|$ in these cases.

When looking at small values of n ($20 \leq n < 166$, $n \neq 22$), the above bound is not good enough either. We have a general lemma computing the exact value of $f_M(H)$ in case H is not primitive.

This settles the problem of calculating $\omega(S_n)$ and $\sigma(S_n)$ for every positive integer n, with the following exceptions.

$$\sigma(S_{16}),\ \sigma(S_{22}),$$
$$\omega(S_6),\ \omega(S_8),\ \omega(S_9),\ \omega(S_{10}),\ \omega(S_{12}),$$
$$\omega(S_{14}),\ \omega(S_{15}),\ \omega(S_{16}),\ \omega(S_{18}),\ \omega(S_{22}).$$

In other words, our theorem reduces the set of unknown values of $\omega(S_n)$ and $\sigma(S_n)$ to the above list.

[1] N. Alon, J. H. Spencer.
The probabilistic method. Fourth edition.
Wiley Series in Discrete Mathematics and Optimization. John Wiley and Sons, Inc., Hoboken, NJ, 2016.

[2] S. R. Blackburn.
Sets of permutations that generate the symmetric group pairwise.
J. Combin. Theory Ser. A 113 (2006), no. 7, 1572–1581.

[3] J. R. Britnell, A. Evseev, R. M. Guralnick, P. E. Holmes, A. Maróti.
Sets of elements that pairwise generate a linear group.
J. Combin. Theory Ser. A 115 (2008), no. 3, 442–465.

[4] J. H. E. Cohn,
On *n*-sum groups.
Math. Scand., 75(1) (1994), 44–58.

[5] P. Erdős, L. Lovász.
Problems and results on 3-chromatic hypergraphs and some related questions,
A. Hajnal, R. Rado, V. Sós (Eds.), Colloquium Math. Society Janos Bolyai, vol. 11, North-Holland, Amsterdam, 1973, pp. 609–627.

[6] F. Fumagalli, M. Garonzi, A. Maróti.
The maximal number of elements pairwise generating the symmetric group of even degree.
Preprint. ArXiv link: https://arxiv.org/abs/2011.14426

[7] M.W. Liebeck, A. Shalev,
Maximal subgroups of symmetric groups,
J. Combin. Theory Ser. A 75 (1996) 341–352.

[8] M.W. Liebeck, A. Shalev.
Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky.
J. Algebra 184 (1996), no. 1, 31–57.

[9] A. Lucchini, A. Maróti,
On the clique number of the generating graph of a finite group.
Proc. Amer. Math. Soc. 137 (2009), no. 10, 3207–3217.

[10] A. Maróti.
Covering the symmetric groups with proper subgroups.
J. Combin. Theory Ser. A, 110(1):97–111, 2005.

[11] L. Stringer.
Pairwise generating sets for the symmetric and alternating groups. PhD thesis.
Royal Holloway, University of London, 2008.

[12] E. Swartz.
On the covering number of symmetric groups having degree divisible by six.
Discrete Math. 339(11):2593–2604, 2016.