Which S_m have a complement in S_n?

David Joyner

8-12-97

Abstract

We classify which symmetric groups S_m have a complement in S_n, $m < n$. Such questions are of interest to computer scientists who wish for efficient methods to store permutations.

This paper is essentially expository in the sense that it uses only well-known results.

Contents

1 Background 2
  1.1 Complements 2
  1.2 Stabilizers 5
2 A table 5
3 General results 7
4 Final remarks 13

This paper is inspired by a question of Herbert Kociemba [K], a computer scientist who has one of the best Rubik's cube solving programs known. Efficient methods of storing permutations in S_E and S_V (the groups of all permutations of the edges E and vertices V, respectively, of the Rubik's cube) are needed, hence leading naturally to the concept of the complement of S_m in S_n. Specifically, he asked if S_8 has a complement in S_{12} (this terminology is defined below). The answer is, as we shall see, "no". Nonetheless, it turns out to be possible to introduce a slightly more general notion of k complementary subgroups (defined below) for which the answer to the analogous question is "yes".

Notation: If X is any finite set then

- $|X|$ denotes the number of elements in X.
- S_X denotes the symmetric group on X.
- S_n denotes the symmetric group on $\{1, 2, ..., n\}$.
- A_n denotes its alternating subgroup of even permutations.
- C_n denotes the cyclic subgroup of S_n generated by the n-cycle $(1, 2, ..., n)$.
- M_{10} denotes "the Mathieu group of degree 10" and order $720 = 10!/7!$, which we define as the subgroup of S_{10} generated by $(2, 6, 10, 7)(3, 9, 4, 5)$ and $(1, 5)(3, 8)(4, 10)(7, 9)$.
- M_{11} denotes the Mathieu group of degree 11 and order $7920 = 11!/7!$ generated by $(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)$ and $(3, 7, 11, 8)(4, 10, 5, 6)$.
- M_{12} denotes the Mathieu group of degree 12 and order $95040 = 12!/7!$ generated by $(2, 3, 5, 9, 8, 10, 6, 11, 4, 7, 12)$ and $(1, 12)(2, 11)(3, 10)(4, 9)(5, 8)(6, 7)$.
- For any prime power q, $\mathbb{F}_q$ denotes the finite field with q elements.
- $AGL_n(\mathbb{F}_q)$ denotes the affine group of transformations on $\mathbb{F}_q^n$ of the form $\vec{v} \longmapsto A\vec{v} + \vec{a}$, where $A \in GL_n(\mathbb{F}_q)$ and $\vec{a} \in \mathbb{F}_q^n$.

For other undefined groups arising below, we refer to [DM].

1. Background

1.1. Complements

If G is a finite group and G_1, G_2 are subgroups then we say G_2 is the **complement** of G_1 when

- $G_1 \cap G_2 = \{1\}$, the identity of G, and
- $G = G_1 \cdot G_2 = \{g_1 g_2 \mid g_1 \in G_1,\ g_2 \in G_2\}$.

If G_1 and G_2 are complementary subgroups then we may write each $g \in G$ in the form $g = g_1 g_2$, for some unique $g_1 \in G_1$ and some unique $g_2 \in G_2$. We call g_1 and g_2 the **factors** of g. This implies the following result, whose (easy) proof is omitted.

Lemma 1.1. *Suppose G is a finite group and G_2 is the complement of G_1 in the sense above.*

- *There are well-defined projection maps $p_1 : G \to G_1$, $p_2 : G \to G_2$, defined by $p_1(g) = g_1$ and $p_2(g) = g_2$, where $g = g_1 g_2$ is the factorization of g.*
- *$G = G_2 \cdot G_1$ and we may write each $g \in G$ in the form $g = g_2 g_1$, for some unique $g_1 \in G_1$ and some unique $g_2 \in G_2$. In other words, G_1 is the complement of G_2 in the sense above.*

As is well-known, for any finite group, the right multiplication map $\rho(x) : g \longmapsto gx^{-1}$, $g, x \in G$, yields a homomorphism $\rho : G \to S_G$, where S_G is the symmetric group on G. Though it shall not be needed, it is remarkable that a similar result holds for each of the complements:

Lemma 1.2. *Let $G = G_1 \cdot G_2$ be a finite group with G_2 a complement of G_1.*

(a) The right multiplication map $\rho(x) : g \longmapsto gx^{-1}$, $g, x \in G$, yields a homomorphism

$$\rho_2 : G \to S_{G_2},$$

where S_{G_2} is the symmetric group on G_2, $\rho_2(x)(g) = p_2(\rho(x)(g))$.

(b) The left multiplication map $\lambda(x) : g \longmapsto xg$, $g, x \in G$, yields a homomorphism

$$\lambda_1 : G \to S_{G_1},$$

$\lambda_1(x)(g) = p_1(\lambda(x)(g))$.

Remark 1. *The Lemma above was inspired by a remark of Kosiemba [K], in connection with an algorithm for his Rubik's cube solving program.*

proof: Write $g \in G$ in the form $g = g_1 g_2$, for some unique $g_1 \in G_1$ and some unique $g_2 \in G_2$. Fix $x \in G$ and let $g_1' \in G_1$ and $g_2' \in G_2$ denote the factors of gx: $gx = g_1' g_2'$.

Claim: g_2' depends on g_2 and x but not g_1. Indeed, if $g_2 x = g_1'' g_2''$, for some unique $g_1'' \in G_1$ and some unique $g_2'' \in G_2$ (which depend only on x, g_2 but not on g_1), then $gx = g_1(g_2 x) = (g_1 g_1'')g_2''$. By uniqueness, $g_2' = g_2''$ and so the claim follows.

Define $r_{x^{-1}} : G_2 \to G_2$ by $r_{x^{-1}}(g_2) = g_2'$. This is simply the restriction of the right translation map $\rho(x) : G \to G$ followed by projection onto the G_2 factor.

Claim: $r_{x^{-1}}$ is bijective. Surjectivity is obvious. For injectivity, if $g_2, h_2 \in G_2$ and $g_2 x = g_1' g_2'$, $h_2 x = g_1'' g_2'$ are factorizations with the same G_2 factor then plugging $g_2' = (g_1')^{-1} g_2 x$ into the second equation gives $h_2 x = (g_1''(g_1')^{-1}) g_2 x$, which implies $h_2 g_2^{-1} = g_1''(g_1')^{-1}$. This is impossible (by uniqueness) unless $h_2 = g_2$, which proves the claim.

Thus we have a map

$$\rho_2 : G \to S_{G_2}$$

defined by $\rho_2(x) = r_{x^{-1}}$.

Claim: ρ_2 is a homomorphism. Indeed, if we fix $x, y \in G$ and $g_1 \in G_1$, $g_2 \in G_2$ then we have

$$g_1''' r_{(xy)^{-1}}(g_2) = g_1' r_{x^{-1}}(g_2) y = g_1'' r_{y^{-1}}(r_{x^{-1}}(g_2)),$$

for some $g_1', g_1'', g_1''' \in G_1$. By uniqueness, we must have

$$r_{(xy)^{-1}} = r_{y^{-1}} \circ r_{x^{-1}},$$

which implies ρ_2 is a homomorphism.

This completes the proof of the first statement (for right multiplication) of the Lemma. The proof of the second statement (for left multiplication) is similar and hence omitted.

□

We end this discussion of complements with the following generalization:

Definition 1.3. *Let $G_1, G_2, ..., G_k$ denote subgroups of G. More generally, we say that these subgroups are* **complementary** *if*

- *for all $1 \leq i < j \leq k$, we have $G_i \cap G_j = \{1\}$, the identity of G,*
- *for all $1 \leq i < k$, we have $G_i \cap G_{i+1} \cdot ... \cdot G_k = \{1\}$, the identity of G,*
- *for all $1 \leq i < k$, $G_{i+1} \cdot ... \cdot G_k$ is a group, and*
- *$G = G_1 \cdot ... \cdot G_k = \{g_1 g_2 ... g_k \mid g_i \in G_i,\ 1 \leq i \leq k\}$.*

Remark 2. *Lemma 1.1 above has an "obvious" generalization to the case of k complementary subgroups. Lemma 1.2 (b) also has an analog. The statement and proof of these are left to the reader.*

We also point out that

$$|G| = |G_1| \cdot ... \cdot |G_k|.$$

One can use this to show that if $I \subset \{1, 2, ..., k\}$ is any subset and if we define the subset $G_I \subset G$ by

$$G_I = \prod_{i \in I} G_i = \{g_{i_1} \cdot ... \cdot g_{i_r} \mid \text{where } g_i \in G_i,\ i \in I = \{i_1, ..., i_r\}\},$$

then we have

$$G_I \cap G_{I^c} = \{1\},$$

where $I^c = \{1, 2, ..., k\} - I$.

1.2. Stabilizers

Let X denote a finite set. If G is a subgroup of S_X and $x \in X$ then we let G_x denote the **stabilizer** of x in G:

$$G_x = \{g \in G \mid g(x) = x\}.$$

Definition 1.4. *Let $k \geq 1$ be an integer and let*

$$X^{(k)} = \{\text{distinct } k\text{−tuples in } X\} = \{(x_1, x_2, ..., x_k) \mid x_i \neq x_j,\ 1 \leq i < j \leq k\}.$$

*We say G acts k-**transitively on** X if G acts transitively on $X^{(k)}$ via the "diagonal" action $g : (x_1, x_2, ..., x_k) \longmapsto (g(x_1), g(x_2), ..., g(x_k))$.*

*If G acts transitively on X and $G_x = 1$ for some (hence all) $x \in X$ then we say G acts **regularly** on X.*

Example 1.5. *If G is a subgroup of S_n and $x = (n - k + 1, ..., n) \in X^{(k)}$ then $G_x \cong S_{n-k}$.*

2. A table

We give a table which indicates, for small values of n, which S_m have a complement in S_n.

n	m	complement of S_m in S_n
4	2	A_4
4	3	C_4
5	2	A_5
5	3	$< (1,2,3,4,5),(2,3,5,4) > \cong AGL_1(\mathbb{F}_5)$ size 20
5	4	C_5
6	2	A_6
6	3	$< (2,3,4,5,6),(3,4,6,5) > \cong PGL_2(\mathbb{F}_5)$ size 120
6	5	C_6
7	2	A_7
7	5	$< (1,2,6,5,3,7),(1,4,3,2,5,6) > \cong AGL_1(\mathbb{F}_7)$ size 42
7	6	C_7
8	2	A_8
8	5	$< (1,5,8,6,7,4),(1,5,8,7)(2,3,4,6) > \cong PGL_2(\mathbb{F}_7)$ size 336
8	6	$AGL_1(\mathbb{F}_8)$ size 56
8	7	C_8
9	2	A_9
9	6	$PGL_2(\mathbb{F}_8)$ size 504
9	7	$AGL_1(\mathbb{F}_9)$ size 72
9	8	C_9
10	2	A_{10}
10	7	M_{10} size 720 ($PGL_2(\mathbb{F}_9)$ is another)
10	9	C_{10}

n	m	complement of S_m in S_n
11	2	A_{11}
11	7	M_{11} size 7920
11	9	$AGL_1(\mathbb{F}_{11})$ size 110
11	10	C_{11}
12	2	A_{12}
12	7	M_{12} size 95040
12	9	$PGL_2(\mathbb{F}_{11})$ $=< (1,2,3,4,5,6,7,8,9,10,11),(1,2,4,8,5,10,9,7,3,6),$ $(1,10)(2,5)(3,7)(4,8)(6,9)(11,12) >$ size 1320
12	11	C_{12}

3. General results

The following result may be found, for example, in [R], Theorem 9.9.

Lemma 3.1. *Let $n > 2$ be an integer and let X denote a set with $n = |X|$. S_X acts n-transitively on X and A_n acts $(n-2)$-transitively on $\{1, 2, ..., n\}$.*

Lemma 3.2. *([DM], Corollary 1.4A) If G acts transitively on X then G acts regularly on X if and only if $|G| = |X|$.*

The following general result might be regarded as our main lemma. It's proof is omitted.

Lemma 3.3. *([DM], Exercise 1.4.1) If G acts transitively on X, $x \in X$, and H is any subgroup of G then*

$$G = G_x H = \{gh \mid g \in G_x, h \in H\}$$

if any only if H acts transitively on X.

The following result gives precise conditions which may be used to determine the answer to the question in the title to this paper.

Proposition 3.4. *S_m has a complement in S_n if and only if there is an subgroup H of S_n such that*

- *H acts $(n-m)$-transitively on $\{1, 2, ..., n\}$,*
- *$|H| = n(n-1)...(m+1) = n!/m!$.*

Remark 3. *The method of proof actually proves something more general: one may replace S_m in the statement of the above Proposition with any stabilizer of S_n acting on $\{1, 2, ..., n\}^{(n-m)}$.*

proof: Let $G = S_n$, which we regard as acting transitively on $X = \{1, 2, ..., n\}^{(n-m)}$. Identify S_m with the stabilizer G_x of $x = (m+1, ..., n) \in \{1, 2, ..., n\}^{(n-m)}$. The above lemma says that $G = G_x H$ for some H if and only if H acts transitively on X, i.e., acting $(n-m)$-transitively on $\{1, 2, ..., n\}$. H is a complement of G_x if and only if $H \cap G_x = 1$, which is equivalent to saying that H acts regularly on X. Since $|X| = n!/m!$, the result follows from Lemma 3.2. $\square$

Corollary 3.5. *In general, $S_2 =< (1, 2) >\subset S_n$ has a complement in S_n, namely A_n.*

Example 3.6. *If $n = 10$ and $m = 6$ then the Theorem says that S_6 has a complement in S_{10} if and only if there is a subgroup H of S_{10} of order 5040 which acts 4-transitively on $\{1, 2, ..., 10\}$. The only subgroups of S_{10} which act 4-transitively on $\{1, 2, ..., 10\}$ are S_{10} itself and A_{10}. This follows from the classification of all 4-transitive groups (see [DM], chapter 7, or [R], page 289). This implies S_6 has no complement in S_{10}. (However, S_{10} does have a subgroup of order 5040 but it is not even transitive on $\{1, 2, ..., 10\}$.)*

Similarly, S_5 has no complement in S_{10}.

Note that S_{10} has not one but two non-isomorphic subgroups, H_1 and H_2, of order $720 = 10!/7!$, each of which acts 3-transitively on $\{1, 2, ..., 10\}$ (see [DM], chapter 7). These groups satisfy $H_1 \cong M_{10}$ and $H_2 \cong PGL_2(\mathbb{F}_9)$. Thus S_7 has two non-isomorphic complements in S_{10}.

Lemma 3.7. *([DM], pages 242-243) Let $q = p^k$, p a prime and $k \geq 1$ an integer. There is a 2-transitive group $G \cong AGL_1(\mathbb{F}_q)$ acting on $X = \mathbb{F}_q$ of order $q(q-1)$. Consequently, S_{q-2} has a complement in S_q.*

Lemma 3.8. *([DM], pages 242-243) Let $q = p^k$, p a prime and $k \geq 1$ an integer. There is a 3-transitive group $G \cong PGL_2(\mathbb{F}_q)$ acting on $X = \mathbb{F}_q \cup \{\infty\}$ of order $(q+1)q(q-1)$. Consequently, S_{q-2} has a complement in S_{q+1}.*

The following Theorem is our main result.

Theorem 3.9.

- *If $n > 2$ is not a prime power or a prime power plus 1 then the only $1 < m < n$ for which S_m has a complement in S_n are $m = 2$ and $m = n - 1$.*
- *If $n > 12$ is a prime power and not a prime power plus 1 then the only $1 < m < n$ for which S_m has a complement in S_n are $m = 2$, $m = n - 2$ and $m = n - 1$.*
- *If $n > 12$ is a prime power plus 1 but not a prime power then the only $1 < m < n$ for which S_m has a complement in S_n are $m = 2$, $m = n - 3$ and $m = n - 1$.*
- *If $n > 12$ is both a prime power plus 1 and a prime power then the only $1 < m < n$ for which S_m has a complement in S_n are $m = 2$, $m = n - 3$, $m = n - 2$ and $m = n - 1$.*
- *If $n \leq 12$ see the above table.*

Remark 4. *Roughly speaking, this theorem says that if you pick an integer $n > 2$ "at random" then, with "probability one" (in the sense of Dirichlet density), the only S_m's which have a complement in S_n are S_2 and S_{n-1}.*

proof: The proof below depends on the classification of 2-transitive groups of degree n (see [DM], §§7.6-7.7). The following groups are 2-transitive:

- Some "affine groups" and some of their subgroups are 2-transitive. These groups always act on a set of prime power degree.
- Projective special linear groups $PSL_d(\mathbb{F}_q)$ acts 2-transitively on projective $d-1$-space $\mathbb{P}^{d-1}(\mathbb{F}_q)$, a set of size $(q^d - 1)/(q - 1)$. In general (see [R], chapter 8, page 223),

$$|PSL_d(\mathbb{F}_q)| = \frac{(q^d - 1)(q^d - q)...(q^d - q^{d-1})}{gcd(d, q-1) \cdot (q-1)}.$$

In case $d = 2$, $PGL_2(\mathbb{F}_q)$ is sharply 3-transitive of degree $q+1$. If q is even then $PGL_2(\mathbb{F}_q) = PSL_2(\mathbb{F}_q)$. If q is odd then $PSL_2(\mathbb{F}_q)$ is a subgroup of index 2 in $PGL_2(\mathbb{F}_q)$.

- The symplectic groups $Sp_{2m}(\mathbb{F}_2)$, $m \geq 2$, act 2-transitively (in different ways) on a set of size $2^{m-1}(2^m+1)$ and a set of size $2^{m-1}(2^m-1)$ (see [DM], §7.7, page 245). We have

$$|Sp_{2m}(\mathbb{F}_2)| = 2^{m^2}(2^2-1)(2^4-1)...(2^{2m}-1)$$

  (see [R], chapter 8, page 245).

- Special projective unitary groups $PSU_3(\mathbb{F}_q)$. These groups are of order

$$|PSU_3(\mathbb{F}_q)| = \frac{1}{gcd(3, q+1)} q^3(q^2-1)(q^3+1)$$

  (see [R], chapter 8, page 245) and act 2-transitively on a set of size q^3+1 (see [DM], §7.7, page 249).

- Suzuki groups $Sz(q) = {}^2B_2(\mathbb{F}_q)$, where $q = 2^{2m+1}$. This group is order

$$|Sz(q)| = q^2(q-1)(q^2+1), \quad q > 2$$

  (see [DM], §7.7, page 250). If $q = 2$ then $Sz(2) \cong AGL_1(\mathbb{F}_5)$. This group acts 2-transitively on the q^2+1 points of a Steiner system of type $S(3, q+1, q^2+1)$.

- Ree groups $R(q) = {}^2G_2(\mathbb{F}_q)$, where $q = 3^{2m+1}$. This group is order

$$|R(q)| = q^3(q-1)(q^3+1).$$

  (see [DM], §7.7, page 251). This group acts 2-transitively on the q^3+1 points of a Steiner system of type $S(2, q+1, q^3+1)$.

- The Mathieu groups (see [R], chapter 9):
  - M_{10} is 3-transitive of degree 10, $|M_{10}| = 720$.
  - M_{11} is 4-transitive of degree 11, $|M_{11}| = 7920$. Also, M_{11} has a 3-transitive action of degree 12. (See [DM], §7.7, page 252.)

- M_{12} is 5-transitive of degree 12, $|M_{12}| = 95040$.
- M_{22} is 3-transitive of degree 22, $|M_{22}| = 443520$.
- M_{23} is 4-transitive of degree 23, $|M_{23}| = 10200960$.
- M_{24} is 5-transitive of degree 24, $|M_{24}| = 244823040$.

- $PSL_2(\mathbb{F}_{11})$ has a 2-transitive action of degree 11 (recall $|PSL_2(\mathbb{F}_{11})| = 120 \cdot 110/20 = 660$). (See [DM], §7.7, page 252.)
- A_7 has a 2-transitive action of degree 15 (see [DM], §7.7, page 252).
- Higman-Sims group HS of order 44352000 has a 2-transitive action on a set of size 176 (see [DM], §7.7, pages 252-253).
- The Conway group Co_3 of order 495766656000 has a 2-transitive action of degree 276 (see [DM], §7.7, page 253).

There are no other 2-transitive groups.

To see if S_m has a complement in S_n not already listed (i.e., to try to find a counterexample to the statement of the Theorem above), we must find an $(n-m)$-transitive group of degree n and order $n!/m!$. Because of Lemmas 3.7 and 3.8, we may assume $m \in \{2,3,4,5\}$, $n > 12$, $(n,m) \neq (\text{a prime power}, n-2)$, and $(n,m) \neq (\text{a prime power plus } 1, n-3)$.

The argument shall be case-by-case:

Case 1: The projective special linear groups $PSL_d(\mathbb{F}_q)$. We may assume $d > 2$ since otherwise n will be a prime power plus 1. In this case $n = (q^d-1)/(q-1)$ and $m = n-2$. In order for $H = PSL_d(\mathbb{F}_q)$ to be a complement of S_{n-2} we must have

$$|H| = |PSL_d(\mathbb{F}_q)| = \frac{(q^d-1)(q^d-q)...(q^d-q^{d-1})}{gcd(d,q-1)\cdot(q-1)} = n(n-1),$$

by Proposition 3.4. In other words, q must satisfy

$$\frac{(q^d-q)...(q^d-q^{d-1})}{gcd(d,q-1)} = n-1 = (q^d-q)/(q-1),$$

which is impossible if $d > 2$.

Case 2: The symplectic groups $Sp_{2m}(\mathbb{F}_2)$, $m \geq 2$. In this case $n = 2^{r-1}(2^r+1)$ or $n = 2^{r-1}(2^r-1)$ and $m = n-2$. In order for $H = Sp_{2r}(\mathbb{F}_2)$ to be a complement of S_{n-2} we must have

$$|H| = |Sp_{2r}(\mathbb{F}_2)| = 2^{r^2}(2^2-1)(2^4-1)...(2^{2r}-1) = n(n-1).$$

In other words, r must satisfy either

$$2^{r^2}(2^2-1)(2^4-1)...(2^{2r}-1) = 2^{r-1}(2^r+1)(2^{r-1}(2^r+1)-1)$$

or

$$2^{r^2}(2^2-1)(2^4-1)...(2^{2r}-1) = 2^{r-1}(2^r-1)(2^{r-1}(2^r-1)-1).$$

Both of these equalities are impossible since for $r > 1$ the left-hand side is always larger than the right-hand side.

Case 3: The special projective unitary groups $PSU_3(\mathbb{F}_q)$ In this case $n = q^3+1$ and $m = n-2$. In order for $H = PSU_3(\mathbb{F}_q)$ to be a complement of S_{n-2} we must have

$$|H| = |PSU_3(\mathbb{F}_q)| = \frac{1}{gcd(3, q+1)} q^3(q^2-1)(q^3+1) = n(n-1) = (q^3+1)q^3.$$

This is impossible unless $gcd(3, q+1) = q^2-1$, i.e., unless $q = 2$. But if $q = 2$ then the degree is $n = 9$ and we have already covered this case in the table above.

Case 4: The Suzuki groups $Sz(q) = {}^2B_2(\mathbb{F}_q)$, where $q = 2^{2m+1}$. In this case $n = q^2+1$ and $m = n-2$. In order for $H = Sz(q)$ to be a complement of S_{n-2} we must have

$$|H| = |Sz(q)| = q^2(q-1)(q^2+1) = n(n-1) = (q^2+1)q^2.$$

This is impossible.

Case 5: The Ree groups $R(q) = {}^2G_2(\mathbb{F}_q)$, where $q = 3^{2m+1}$. In this case $n = q^3+1$ and $m = n-2$. In order for $H = R(q)$ to be a complement of S_{n-2} we must have

$$|H| = |R(q)| = q^3(q-1)(q^3+1) = n(n-1) = (q^3+1)q^3.$$

This is impossible.

Case 6: The Mathieu groups. Since we are assuming $n > 12$, we need only consider

- M_{22} is 3-transitive of degree 22, $|M_{22}| = 443520$.
- M_{23} is 4-transitive of degree 23, $|M_{23}| = 10200960$.
- M_{24} is 5-transitive of degree 24, $|M_{24}| = 244823040$.

None of these satisfy $|H| = n!/m!$, for $m = n-3, n-4, n-5$, respectively.

Case 7: A_7 has a 2-transitive action of degree 15. In this case, $n = 15$ and $m = n-2$. But $|A_7| = 2520 \neq 15 \cdot 14 = 210$, so A_7 is not a complement of S_{13} in S_{15}.

Case 8: The Higman-Sims group HS. In this case $n = 176$ and $m = n-2$. But $|HS| = 44352000 \neq 176 \cdot 175 = 30800$, so HS is not a complement of S_{174} in S_{176}.

Case 9: The Conway group Co_3. In this case, $n = 276$ and $m = n-2$. But $|Co_3| = 495766656000 \neq 276 \cdot 275 = 75900$, so Co_3 is not a complement of S_{274} in S_{276}.

This exhausts the 2-transitive groups, so the proof is complete.

□

4. Final remarks

From the table in §2, we see that S_8 does not have a complement in S_{12}. However, $PGL_2(\mathbb{F}_{11}), C_9, S_8$ are complementary in S_{12} (in the sense of Definition 1.3),

$$S_{12} = PGL_2(\mathbb{F}_{11}) \cdot C_9 \cdot S_8.$$

This yields one method of storing permutations in S_{12} using those of S_8.

More generally, given any m and any n with $m < n$, Theorem 3.9 and the table in §2 may be used to find the smallest k such G_1, G_2, ..., $G_k = S_m$ are complements (in the sense of Definition 1.3) in S_n.

Acknowledgements: I'd like to thank Herbert Kociemba for several interesting and inspiring communications. This paper used GAP [GAP] to verify some of the results stated in the table in §2.

References

[DM] John Dixon, Brian Mortimer, Permutation groups, Springer-Verlag, 1996

[GAP] Martin Schönert et al, GAP manual, Lehrstuhl D für Mathematik, RWTH Aachen

[K] H. Kociemba, private communications, Summer 1997

[R] Joseph Rotman, An introduction to the theory of groups, 4th edition, Springer-Verlag, 1995