Independent generating sets and geometries for symmetric groups

Peter J. Cameron
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS
UK

Philippe Cara*
Department of Mathematics
Vrije Universiteit Brussel
Pleinlaan 2
B-1050 Brussel
Belgium

Abstract

Julius Whiston showed that the size of an independent generating set in the symmetric group S_n is at most $n-1$. We determine all sets meeting this bound. We also give some general remarks on the maximum size of an independent generating set of a group and its relationship to coset geometries for the group. In particular, we determine all coset geometries of maximum rank for the symmetric group S_n for $n > 6$.

*Postdoctoral fellow of the Fund for Scientific Research-Flanders (Belgium)

1 Independent generating sets

Let $S = (s_i : i \in I)$ be a family of elements of a group G. For $J \subseteq I$, let $G_J = \langle s_i : i \notin J \rangle$; we abbreviate $G_{\{i\}}$ to G_i. We say that S is *independent* if $s_i \notin G_i$ for all $i \in I$. It is *strongly independent* if, in addition, $G_J \cap G_K = G_{J \cup K}$ for all $J, K \subseteq I$.

A family of elements which generates G is independent if and only if it is a minimal generating set (that is, no proper subset generates G).

We let $\mu(G)$ denote the size of the largest independent generating set in G, and $\mu'(G)$ the size of the largest independent set. Clearly $\mu(G) \leq \mu'(G)$. Strict inequality can hold: Whiston [9] gives examples with $G = PSL(2,q)$.

We also define a relativised version. Let B be a subgroup of G. If $S = (s_i : i \in I)$ a family of elements of G, we say that S is *independent relative to* B if $s_i \notin \langle B, s_j : j \neq i \rangle$, and is an *independent generating set relative to* B if in addition $\langle B, S \rangle = G$. We denote by $\mu(G,B)$ and $\mu'(G,B)$ the largest size of an independent generating set and of an independent set relative to B.

We will also have to use another version. Let A be a group acting on the group G. Then $\mu'_A(G)$ is the largest size of a family of elements of G, none of which belongs to the subgroup generated by the A-images of the others; we call such a set *A-independent*. Also, $\mu_A(G)$ is the largest size of an A-independent generating set for G.

The first result is not in [8], but Whiston deploys the argument used to prove it in several places.

Theorem 1.1 *Let N be a normal subgroup of a group G. Then $\mu(G) \leq \mu(G/N) + \mu'(N)$. Moreover, if N is abelian, then $\mu(G) \leq \mu(G/N) + \mu'_G(N)$.*

Proof Let S be an independent generating set for G. Let $\overline{s}$ denote the image of s in G/N. Then $\overline{S}$ generates G/N, so there is a subset T of S such that $\overline{T}$ is an independent generating set for G/N. Thus, $|T| \leq \mu(G/N)$.

Now, for each $s \in S \setminus T$, there is a word $w(s)$ in the elements of T such that $\overline{s} = \overline{w(s)}$. Thus, $sw(s)^{-1} \in N$. We claim that these elements of N are independent. For suppose that

$$sw(s)^{-1} \in \langle uw(u)^{-1} : u \in S \setminus T \setminus \{s\} \rangle.$$

Since each $w(u)$ belongs to $\langle T \rangle$, we see that $s \in \langle u : u \in S \setminus \{s\} \rangle$, a contradiction.

So $|S \setminus T| \leq \mu'(N)$, from which we get

$$|S| \leq \mu(G/N) + \mu'(N).$$

Since this is true for any independent generating set for G, the first statement is proved.

Now suppose that N is abelian; then G acts on N by conjugation, with N in the kernel of the action. Now we claim that the elements $sw(s)^{-1} \in N$ are G-independent. For suppose that

$$sw(s)^{-1} \in \langle (uw(u)^{-1})^g : u \in S \setminus T \setminus \{s\}, g \in G \rangle.$$

Since each $w(u)$ belongs to $\langle T \rangle$, and the conjugating elements can be taken to belong to $\langle T \rangle$ also, we see that $s \in \langle u : u \in S \setminus \{s\} \rangle$, a contradiction. The proof concludes as before. ■

It follows that, if $\mu(G) = \mu'(G)$, then $\mu(G \times H) = \mu(G) + \mu(H)$ for any group H. (The upper bound comes from the theorem, and the lower bound from the fact that the union of independent generating sets in G and H is an independent generating set in $G \times H$.) We do not know whether the equation $\mu(G \times H) = \mu(G) + \mu(H)$ holds for any pair of groups.

2 Symmetric groups

The main result of [8] asserts that an independent subset of S_n has cardinality at most $n-1$, with equality if and only if it generates S_n. Thus, $\mu(S_n) = \mu'(S_n) = n-1$.

We are interested in the structure of independent subsets of S_n of maximum size. We prove the following theorem. Let T be a tree on n vertices, and let $S(T)$ be the set of $n-1$ transpositions in S_n corresponding to the edges of T.

Theorem 2.1 *Let S be an independent generating set for S_n of size $n-1$, where $n \geq 7$. Then there is a tree T on $\{1, \ldots, n\}$, such that one of the following holds:*

(a) $S = S(T)$;

(b) for some element $s \in S(T)$, we have

$$S = \{s\} \cup \{(st)^{\varepsilon(t)} : t \in S(T) \setminus \{s\}\},$$

where $\varepsilon(t) = \pm 1$.

Conversely, each of these sets is an independent generating set for S_n.

Note that in case (b), all the elements of S except the transposition s are either 3-cycles or double transpositions, and the support of each such element contains the support of s. The exponent $\varepsilon(t)$ is only necessary if st is a 3-cycle.

Proof We prove the converse first. It is well-known that any set of transpositions as in (a) generates S_n, from which it follows that a set of type (b) is also a generating set.

In case (a), removing an edge of the tree leaves a graph with two connected components, and so $\langle S \setminus \{s\}\rangle$ is intransitive for all $s \in S$. In case (b), removal of the generator $(st)^{\varepsilon(t)}$ gives the group generated by $S(T) \setminus \{t\}$; and if the generator s is removed, then all the others are even permutations and the group they generate is contained in the alternating group.

We now turn to the forward implication.

Let $S = (s_i : i \in I)$ be an independent generating set for $G = S_n$ of size $n-1$. From [8], we get the information that each subgroup G_i is one of the following:

(a) intransitive;

(b) transitive but imprimitive, with blocks of size 2;

(c) the alternating group A_n.

We now examine these cases in turn.

First we show that transitive but imprimitive subgroups cannot occur for $n \geq 7$. For such a subgroup is contained in $2^m : S_m$. We actually show that a transitive subgroup H of $2^m : S_m$ has $\mu(H) < 2m-2$ for $m \geq 4$.

Let H be a transitive subgroup of $2^m : S_m$ with $\mu(H) = 2m-2$, and let N be the kernel of the homomorphism to S_m. We have $\mu(H/N) \leq m-1$ and $\mu'_H(N) < m$ (since the action is nontrivial unless $|N| \leq 2$), while $\mu(H) = 2m-2$. So we must have $H/N = S_m$. Then it is easy to see that $\mu'_H(N) \leq 2$, and so $2m-2 = \mu(H) \leq m+1$, whence $m \leq 3$.

Now if $G_i = A_n$, then s_j is an even permutation for all $j \neq i$; so s_i must be an odd permutation. Hence G_j falls under case (a) (intransitive) for all $j \neq i$. We conclude that all or all but one of the subgroups G_i are intransitive. Choose the notation so that $G_2, \ldots, G_{n-1}$ are intransitive.

We construct a graph T, having an edge e_i for each generator s_i, as follows. Let $e_1 = \{x_1, y_1\}$, where x_1 is any point moved by s_1 and $y_1 = x_1 s_1$. For $i > 1$, the subgroup G_i is intransitive, and so s_i must map some point x_i to a point y_i in a different G_i-orbit; choose any such pair and let $e_i = \{x_i, y_i\}$.

We claim that T is a tree. For, if $j \neq i$, then e_j joins points in the same G_i-orbit; so no circuit contains e_i, as such a circuit would have to have at least two edges between different G_i-orbits. Thus, e_1 is the only edge which could be contained in a circuit. But no circuit contains a single edge! Since there are $n-1$ edges and n vertices, T is a tree, as claimed.

Next, we claim that, for $i \neq 1$, s_i is a transposition, a 3-cycle, or a double transposition; moreover, in the second and third case, its support contains e_1 (and e_1 is a cycle of s_i in the third case). The edge $e_i = \{x_i, y_i\}$ has its ends in different G_i-orbits. Let u and v be any points in the G_i-orbits of x_i and y_i respectively, and suppose that some power of s_i maps u to v. There is a path from x_i to u, and a path from y_i to v, in the tree T. Suppose that the union of these two paths contains some edge $e_j = \{x_j, y_j\}$ for $j \neq 1$. Then we can map x_j to y_j using only powers of s_i together with possibly generators other than s_j. But this contradicts the fact that x_j and y_j lie in different orbits of G_j. So in this case, we conclude that the set $\{x_i, y_i, u, v\}$ contains at most three points and supports a cycle of s_i; if it has three points then it contains e_1.

The same argument shows that the only possibility for two points u, v in the same G_i-orbit and in the same cycle of s_i is that they are the ends of the edge e_1. So the claim is proved.

Note that the edge e_1 is uniquely determined by s_i if s_i is not a transposition, since it must join two points in the same cycle and in the same G_i-orbit. This implies that s_1 is a transposition.

If all the subgroups G_i are intransitive, then any generator could be chosen to be s_1. So all the generators are transpositions, and we have case (a) of the theorem.

Suppose, on the other hand, that G_1 is the alternating group. Then the above argument shows that s_1 is a transposition, while all the other generators s_i are 3-cycles or double transpositions such that $s_1 s_i$ is a transposition. Thus case (b) of the theorem holds. ■

Corollary 2.2 *(a) The number of independent generating sets of type (a) in the Theorem is n^{n-2}.*

(b) The number of independent generating sets of type (b) in the Theorem is $n^{n-2}(n-1)$; if we don't distinguish between a 3-cycle and its inverse, then the number is $\binom{n}{2}(n-1)^{n-3}$.

Proof (a) The generating sets of type (a) are clearly bijective with the labelled trees on n vertices.

(b) Let S be a generating set of type (b). The tree associated with S is not uniquely determined. If $s = (a,b,c)$ is a 3-cycle in S, then one of the three transpositions with support contained in $\{a,b,c\}$, say (a,b), is in S, and we could choose either $\{a,c\}$ or $\{b,c\}$ as the edge associated with S. We can normalise by choosing $\{b,c\}$ in this case (that is, a vertex in the 2-cycle whose image under s is not in the 2-cycle). There is no ambiguity for double transpositions. So each such generating set is associated with a tree having one distinguished edge.

If we do not distinguish between 3-cycles and their inverses, then we cannot normalise as above, so there are several trees associated with the set. But all these trees become identical when the edge corresponding to the transposition is contracted. So the number of generating sets is equal to the number of choices for the transposition multiplied by the number of trees on $n-1$ vertices. ■

Corollary 2.3 *For $n \geq 7$, any independent generating set for S_n of size $n-1$ is strongly independent.*

Proof Let S be an independent generating set of size $n-1$. Suppose first that S consists of transpositions.

The group G_J is the direct product of the symmetric groups on the connected components of T_J, the forest obtained by deleting from T the edges corresponding to s_j for $j \in J$. We claim first that $G_J \cap G_K$ is the direct product of symmetric groups on the non-empty intersections of components of T_J and T_K. This just asserts that, if we have two partitions of a set, then a permutation preserves every part of both partitions if and only if it preserves all their intersections; this is clear.

So to finish, we have to show that a non-empty intersection of connected components of T_J and T_K is a connected component of $T_{J\cup K}$. Suppose that two points x,y lie in such an intersection. Then the (unique) path from x to y in T uses no edge labelled by an element of J, and uses no edge labelled by an element of K; so it is a path in $T_{J\cup K}$, as required.

Now suppose that case (b) of the Theorem occurs. For any $J \subseteq \{2,\ldots,n-1\}$, let T_J be the graph obtained from T by deleting the edges corresponding to elements of J. It is now easy to see that

(i) G_J is the direct product of the symmetric groups on the connected components of T_J;

(ii) $G_{J\cup\{1\}}$ is the subgroup of even permutations in G_J.

Now the argument proceeds as before. ■

Corollary 2.4 *For $n \geq 7$, if $B \leq S_n$ and $\mu(S_n, B) = n-1$, then $B = 1$.*

Proof Let $S = (s_i : i \in I)$ be an independent generating set relative to B, of size $n-1$, and let $G_i = \langle s_j : j \neq i \rangle$ for $i \in I$. By Whiston's theorem (stated at the beginning of section 2), S is an independent generating set for S_n. From Theorem 2.1, G_i is a maximal subgroup of S_n except in the case where the removal of the edge e_i breaks the tree into two parts of equal size. If G_i is maximal, then $B \leq G_i$, since otherwise $\langle B, G_i \rangle = S_n$, contradicting independence. Taking j such that e_j is a pendant edge, we have $G_j = S_{n-1}$, so that B fixes a point. Thus, even in the case when G_i is not maximal, we have $B \leq G_i$. Then

$$B \leq \bigcap_{i=1}^{n-1} G_i = G_{\{1,\ldots,n-1\}} = \langle \emptyset \rangle = 1,$$

where the equality in the second place follows from Corollary 2.3. ■

Remark It is possible, with a combination of hand and computer calculation (the latter using GAP [6]), to determine the independent generating sets of size $n-1$ in S_n for $n \leq 6$ as well.

The theorem as stated holds for all $n \neq 4, 6$. For $n = 6$, as well as the sets given in the theorem, we have their images under the outer automorphism of S_6: these involve products of two or three transpositions and two 3-cycles. For $n = 4$, there is one type not appearing in the theorem, namely $\{(1,2),(1,3),(1,4)(2,3)\}$.

All are strongly independent except for the last example for $n = 4$.

We end this section with a question. Our main theorem depends on the theorem of Whiston, and hence on the Classification of Finite Simple Groups. Whiston uses the Classification to establish the following: if G is an almost simple proper subgroup of S_n (resp. A_n), then $\mu(G) \leq n-2$ (resp. $\mu(G) \leq n-3$). *Can this assertion be proved without using the Classification?*

3 Geometries

Let G be a group, and $(G_i : i \in I)$ a family of subgroups of G. for $J \subseteq I$, let $G_J = \bigcap_{j \in J} G_j$. Suppose that the following three conditions hold:

(G1) The subgroups G_J, for $J \subseteq I$, are all distinct.

(G2) If $J \subseteq I$ and $|J| < |I| - 1$, then $G_J = \langle G_{J \cup \{k\}} : k \in I \setminus J \rangle$.

(G3) If a family $(G_j x_j : j \in J)$ of right cosets have pairwise non-empty intersection, then there is an element of G lying in all these cosets.

The *coset geometry* $C(G,(G_i : i \in I))$ has type set I; the varieties of type i are the right cosets of G_i, and two varieties are incident if their intersection is non-empty. If conditions (G1)–(G3) hold, then this is a firm and residually connected geometry, and G acts flag-transitively on it by right multiplication. Conversely, any firm and residually connected geometry on which the group G acts flag-transitively arises as such a coset geometry.

The rank of the coset geometry is $|I|$. For $J \subseteq I$, the residue of the flag $(G_j : j \in J)$ is isomorphic to the coset geometry $(G_J,(G_{J\cup\{k\}} : k \in I \setminus J))$. The *Borel subgroup* of the geometry is the subgroup

$$B = G_I = \bigcap_{i\in I} G_i.$$

See [1] for more explanation of these terms.

Condition (G3) was re-phrased in terms of the subgroups G_i by Buekenhout and Hermand [4], following Tits [7], as follows:

For any $J \subseteq I$ with $|J| \geq 3$ and any $j \in J$, we have

$$G_j \left(\bigcap_{k\in J\setminus\{j\}} G_k \right) = \bigcap_{k\in J\setminus\{j\}} G_j G_k.$$

Moreover, if this holds for one $j \in J$, then it holds for all. We refer to this as condition (BH).

The coset geometry is *residually weakly primitive*, or RWPRI, if the following condition holds:

(G4) For any $J \subset I$, there exists $k \in I \setminus J$ such that $G_{J\cup\{k\}}$ is a maximal subgroup of G_J.

This means that the group G_J acts primitively on the varieties of at least one type in the residue of the standard flag of type J. (A geometry is called *weakly primitive* if its automorphism group acts primitively on the varieties of some type; the condition RWPRI asserts that this condition should hold "residually".)

Theorem 3.1 *The rank of a coset geometry for G with Borel subgroup B is at most $\mu'(G,B)$, while the rank of an* RWPRI *coset geometry is at most $\mu(G,B)$.*

Proof Choose elements s_i, for $i \in I$, so that s_i fixes the varieties G_j for $j \neq i$ but moves the variety G_i. In other words, $s_i \in G_{I\setminus\{i\}}$. Clearly the elements s_i are independent relative to B.

Suppose that (G4) holds. We claim that $G_J = \langle B, s_k : k \in I \setminus J\rangle$ for all $J \subseteq I$. The proof is by induction on $|I \setminus J|$, the conclusion being obvious if $J = I$. If $J \neq I$, choose k as in (G4). By the inductive hypothesis, $G_{J\cup\{k\}}$ is generated by B and s_l for $l \notin J \cup \{k\}$. Since $s_k \in G_J \setminus G_{J\cup\{k\}}$, and $G_{J\cup\{k\}}$ is a maximal subgroup of G_J, we see that the desired conclusion follows, and the inductive step is proved. In particular, we now see that $G = \langle B, s_i : i \in I\rangle$. ■

The proof shows more: if the coset geometry is RWPRI, then the elements $(s_i : i \in I)$ form a strongly independent generating set relative to B.

The converse is not true. If $(s_i : i \in I)$ is a strongly independent generating set for G relative to B, and we put $G_i = \langle B, s_j : j \neq i\rangle$, then conditions (G1) and (G2) hold, but (G3) and (G4) may fail. However, we show that they do hold in the case of independent generating sets of maximal size for symmetric groups.

Theorem 3.2 *For $n \geq 7$, there is a bijection between independent generating sets of size $n-1$ (up to conjugation and inversion of some generators) and* RWPRI *coset geometries of rank $n-1$ for the symmetric group S_n.*

Proof We have seen that any RWPRI coset geometry gives rise to an independent generating set S relative to B. By Corollary 2.4, if the rank is $n-1$, then $B = 1$, and S is of one of the types described in Theorem 2.1. In particular, the generators are determined up to choice of the maximal flag (that is, conjugacy) and inversion of some generators of order 3 (in case (b)).

Conversely, let $S = (s_i : i \in I)$ be an independent generating set for S_n, and define the subgroups G_i as usual. We have observed that S is strongly independent, so that (G1) and (G2) hold (with $B = 1$), and we must prove (G3) (that is, (BH)) and (G4). We do this for the two types separately.

Let T be a tree on n vertices, and $S(T)$ the set of transpositions corresponding to the edges of T.

To prove condition (BH) by induction, it suffices to show that

$$G_i(G_J \cap G_K) = G_iG_J \cap G_iG_K$$

for any two subsets J and K of I with $i \notin J \cup K$. Clearly the left-hand side is contained in the right-hand side; we have to prove the reverse inclusion.

Let A be one of the connected components of the forest obtained by deleting the edge e_i from T. Then G_i is the setwise stabiliser of A in the symmetric group. Now G_J is the direct product of symmetric groups on the connected components of T_J (obtained by deleting the edges e_j from T, for $j \in J$). Each such component, except the one containing e_i, is contained in A or its complement. So, if $g \in G_i G_J$, then $Ag \setminus X_J = A \setminus X_J$, where X_J is the connected component of T_J containing e_i. If also $g \in G_i G_K$, then we also have $Ag \setminus X_K = A \setminus X_K$. Hence $Ag \setminus (X_J \cap X_K) = A \setminus (X_J \cap X_K)$.

But $X_J \cap X_K$ is just the connected component of the tree $T_{J \cup K}$ containing the edge e_i. Since $G_J \cap G_K = G_{J \cup K}$ induces the symmetric group on this set, there is an element $h \in G_J \cap G_K$ such that h acts trivially outside $X_J \cap X_K$ and h maps $Ag \cap (X_J \cap X_K)$ to $A \cap (X_J \cap X_k)$. Thus gh^{-1} fixes A, and so $gh^{-1} = f \in G_i$, whence $g = fh \in G_i(G_J \cap G_K)$, as required.

To prove condition (G4) we note that, if $J \neq I$, then G_J acts as the symmetric group on each of its orbits. Take a pendant edge e_k in the forest T_J; then G_J acts on the cosets of $G_{J \cup \{k\}}$ as the symmetric group, whence $G_{J \cup \{k\}}$ is maximal in G_J, as required.

Now let $S^*(T)$ be a generating set of type (b) derived from the tree T, in which (without loss of generality) the generator s_1 is a transposition, while the others are 3-cycles or double transpositions.

We note that, if $1 \notin J$, then G_J is the same as it is for the generating set $S(T)$ (that is, the direct product of symmetric groups on the connected components of T_J); while, if $1 \in J$, then G_J consists of the even permutations in the direct product of symmetric groups on the connected components of $T_{J \setminus \{1\}}$.

It follows immediately that condition (BH) holds for any set J with $1 \notin J$. On the other hand, if $1 \in J$, then we can take $j = 1$ in (BH), so that G_1 is the alternating group. Since $G_{J \setminus \{1\}}$ contains an odd permutation, both sides of the equation are equal to the symmetric group, and equality holds.

For (G4), if $1 \notin J$, then we may take $k = 1$ and find that $G_{J \cup \{1\}}$ has index 2 (and is maximal) in G_J; if $1 \in J$, then G_J acts as the symmetric or alternating group on each of its orbits, and the same argument applies as we used in case (a). ■

Corollary 3.3 *For $n \geq 7$, any coset geometry of rank $n-1$ for S_n is* RWPRI.

Proof This follows immediately from Theorem 3.1, Corollary 2.4, Whiston's Theorem, and Theorem 3.2. ■

Remark The diagram for a geometry of type (a) arising from the generating set $S(T)$ is simply the line graph of the tree T. This was shown in [5] where these geometries are called *inductively minimal*. See also [3] and [2] for more details. For geometries of type (b), the node corresponding to the subgroup A_n is isolated in the diagram.

Remark Theorem 3.2 is true for all $n \neq 4$. As noted in the earlier remark, all independent generating sets for $n \neq 4$ are of the types found in the main theorem or the image of one of these under an outer automorphism. The geometry defined by the independent generating set $\{(1,2),(1,3),(1,4)(2,3)\}$ for S_4 is not RWPRI. Indeed, this set fails to be strongly independent.

References

[1] F. Buekenhout, Foundations of incidence geometry, pp. 63–105 in: *Handbook of Incidence Geometry* (ed. F. Buekenhout), North-Holland, Amsterdam, 1995.

[2] F. Buekenhout and Ph. Cara, Some Properties of Inductively minimal Geometries, *Bull. Belg. Math. Soc. Simon Stevin* **5** (1998), 213–219.

[3] F. Buekenhout, Ph. Cara and M. Dehon, Inductively minimal flag-transitive geometries, pp. 185–190 in: *Mostly finite geometries* (ed. N.L. Johnson), Marcel Dekker, New York , 1997.

[4] F. Buekenhout and M. Hermand, On flag-transitive geometries and groups, pp. 45–78 in: *Travaux de mathématiques*, Université Libre de Bruxelles, Vol I, 1991.

[5] Ph. Cara, S. Lehman and D.V. Pasechnik, On the number of inductively minimal geometries, *Theoret. Comp. Sci.* **263** (2001), 31–35.

[6] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.2; 2000, (`http://www.gap-system.org`).

[7] J. Tits, *Buildings of Spherical Type and Finite BN-Pairs*, Lecture Notes in Math. **382**, Springer–Verlag, Berlin, 1974.

[8] J. Whiston, Maximal independent generating sets of the symmetric group, *J. Algebra* **232** (2000), 255–268.

[9] J. Whiston, *The Independent Generating Sets of Maximal Size of Selected Groups*, Ph.D. thesis, University of Cambridge, 2001.