GENERATING COUNTABLE SETS OF PERMUTATIONS

FRED GALVIN

ABSTRACT

Let E be an infinite set. In answer to a question of Wagon, I show that every countable subset of the symmetric group $\mathrm{Sym}(E)$ is contained in a 2-generator subgroup of $\mathrm{Sym}(E)$. In answer to a question of Macpherson and Neumann, I show that, if $\mathrm{Sym}(E)$ is generated by $A \cup B$ where $|B| \leqslant |E|$, then $\mathrm{Sym}(E)$ is generated by $A \cup \{\gamma\}$ for some permutation γ in $\mathrm{Sym}(E)$.

1. *Introduction*

This work was motivated by the following pair of well-known theorems.

THEOREM 1.1. *Every countable group is embeddable in a 2-generator group.*

This was first proved by Higman, Neumann and Neumann [**9**, Theorem IV] and (independently) Freudenthal [**9**, p. 254], using free products with amalgamations. A simpler proof using wreath products was given by Neumann and Neumann [**14**]; a short presentation of the Neumann–Neumann proof, avoiding explicit mention of wreath products, can be found in [**7**]. (I am indebted to Peter M. Neumann for pointing out that the main arguments of this paper are closely related to the methods of Neumann and Neumann [**14**].)

THEOREM 1.2. *Every countable set of selfmaps of an infinite set E is contained in the semigroup generated by two selfmaps of E.*

This was first proved by Sierpiński [**17**]; a simpler proof was given by Banach [**1**]. (See [**18**] for a survey of further developments related to Sierpiński's theorem.) In a 1979 letter, Stan Wagon asked whether one can substitute 'permutations' for 'selfmaps' in Sierpiński's theorem; he observed that the permutational analogue of Sierpiński's theorem would imply Theorem 1.1, just as Sierpiński's theorem itself implies the result of Evans [**5**, Theorem II] that every countable semigroup is embeddable in a 2-generator semigroup.

In this paper we answer Wagon's question in the affirmative. First, we show that every countable subset of $\mathrm{Sym}(E)$ is contained in a 2-generator subgroup (Theorem 3.3). Then, with a slightly more complicated construction (Theorem 3.5), we get the two generators to be of finite order, thereby showing that every countable subset of $\mathrm{Sym}(E)$ is contained in a 2-generator subsemigroup, as requested by Wagon. Of course, Theorem 3.3 already implies Theorem 1.1. B. H. Neumann [**13**, p. 542]

Received 1 September 1993.

1991 *Mathematics Subject Classification* 20B35.

This project was sponsored by the National Security Agency under Grant Number MDA904-92-H-3037.

generalized Theorem 1.1 by showing that every group G can be embedded in a group G^* such that every countable subset of G^* is contained in a 2-generator subgroup; in view of Theorem 3.3, we could simply take G^* to be a symmetric group.

Mal'cev **[12]** defined the *general rank* of a group G as the least number R in $\mathbb{N} \cup \{\infty\}$ such that every finite subset of G is contained in a subgroup generated by at most R elements. Thus, Theorem 3.3 implies that the infinite symmetric groups have general rank 2. If one merely wants to show that $\mathrm{Sym}(E)$ has finite general rank (a fact I have not been able to find stated in the literature), this can be done rather easily by showing that every countable subset of $\mathrm{Sym}(E)$ is contained in a 4-generator subgroup (Theorem 3.1).

Answering a question of B. H. Neumann [**13**, p. 541], Levin [**10**, Theorem 2.1] showed that every countable group is embeddable in a 2-generator group with generators of prescribed orders $p \geqslant 3$ and $q \geqslant 2$. My efforts to prove the analogous result for permutation groups have been only partially successful.

QUESTION 1.3. Let E be an infinite set. Is every countable subset of $\mathrm{Sym}(E)$ contained in a 2-generator subgroup with generators of prescribed orders $p \geqslant 3$ and $q \geqslant 2$?

I can prove this for countable subsets H such that

$$|\{x \in E : x\pi = x \text{ for all } \pi \in H\}| = |E|$$

(Theorem 4.1), which is enough to imply Levin's result; otherwise, I can do it only for even orders $q \geqslant 4$ (Theorem 4.3). The following weaker version of Question 1.3 seems especially appealing.

QUESTION 1.4. Let E be an infinite set. Is every countable subset of $\mathrm{Sym}(E)$ contained in a subgroup generated by three involutions?

Two involutions would not be enough, since, for example, the quaternion group is not embeddable in any group generated by two involutions; on the other hand, it follows from Theorem 3.3 (or 4.3) that four involutions suffice (or two involutions and a third permutation of any desired order $p \geqslant 3$), in view of the well-known fact (Lemma 2.2) that every permutation is the product of two involutions.

Let E be an infinite set. Macpherson and Neumann proved [**11**, Corollary 3.1] that, if $\mathrm{Sym}(E)$ is generated by $A \cup B$ where $|B| \leqslant |E|$, then $\mathrm{Sym}(E)$ is generated by $A \cup B_0$ for some finite subset B_0 of B; and they asked [**11**, Question 3.2] whether there is a subset A of $\mathrm{Sym}(E)$ such that $\mathrm{Sym}(E)$ can be generated by A together with two further elements, but cannot be generated by A together with a single element. This question is answered in the negative by Theorem 5.7. Combining Theorem 5.7 with the result of Macpherson and Neumann, we get the second result stated in the abstract (Theorem 5.8): if $\mathrm{Sym}(E)$ is generated by $A \cup B$, where $|B| \leqslant |E|$, then $\mathrm{Sym}(E)$ is generated by $A \cup \{\gamma\}$ for some permutation γ in $\mathrm{Sym}(E)$.

The following question is not really relevant to the concerns of this paper; I mention it here because it arose out of a discussion with Peter M. Neumann of possible strengthenings of Lemma 5.4.

QUESTION 1.5. Call a subgroup G of $\mathrm{Sym}(\omega_1)$ *almost disjoint* if no element of G other than the identity has uncountably many fixed points. Does the continuum hypothesis $2^{\aleph_0} = \aleph_1$ imply that $\mathrm{Sym}(\omega_1)$ has an almost disjoint subgroup of order $2^{\aleph_1}$?

It follows from a result of Baumgartner [**2**, Theorem 5.6] that the existence of such a subgroup is undecidable in ZFC (standard set theory including the axiom of choice but not the continuum hypothesis).

In §2 we introduce some standard notation and establish a few basic facts; experts on group theory can skip §2 except perhaps for Lemma 2.1. The lemmas are given in the easiest form that suffices for our purposes; for example, we show that every element of an infinite symmetric group is the product of two commutators (Lemma 2.5), having no need of the stronger result of Ore [**15**, Theorem 6] that every element is a commutator. Of the lemmas in §2, only Lemmas 2.1 and 2.2 will be used in §3 (and Lemma 2.2 only for the proof of Theorem 3.5). Sections 3, 4, and 5 are independent of one another, except that Theorem 4.6 will be needed in §5. The reader who is only interested in the results of §5 (the answer to the Macpherson–Neumann question) can start with Lemma 4.4, referring to §2 as needed.

The main results of this paper were stated in the abstracts [**6**, **8**].

2. *Preliminaries*

If H is a subset of a group, then $\langle H\rangle$ is the subgroup generated by H; we shall abbreviate, for example, $\langle H\cup\{\alpha,\beta\}\rangle$ to $\langle H,\alpha,\beta\rangle$. The *commutator* of group elements α and β is $[\alpha,\beta]=\alpha^{-1}\beta^{-1}\alpha\beta$. The *symmetric group* $\mathrm{Sym}(E)$ is the group of all permutations of a set E; permutations are regarded as right operators, and are composed from left to right. The set of *fixed points* of a permutation π in $\mathrm{Sym}(E)$ is $\mathrm{fix}(\pi)=\{x\in E: x\pi=x\}$; the *support* of π is $\mathrm{supp}(\pi)=\{x\in E: x\pi\neq x\}$. If H is a subset of $\mathrm{Sym}(E)$, then $\mathrm{fix}(H)=\bigcap\{\mathrm{fix}(\pi):\pi\in H\}$, and $\mathrm{supp}(H)=\bigcup\{\mathrm{supp}(\pi):\pi\in H\}$. The *pointwise stabilizer* of a subset X of E is the group $S_X=\{\pi\in\mathrm{Sym}(E): X\subseteq\mathrm{fix}(\pi)\}$.

We shall make heavy use of the following lemma, which was proved by Dixon, Neumann and Thomas [**3**, Lemma, p. 580] for the case $|E|=\aleph_0$, and generalized by Macpherson and Neumann [**11**, Lemma 2.1] to arbitrary infinite sets.

LEMMA 2.1. *Let E be an infinite set. If $E=A\cup B\cup C$ where A, B, C are disjoint sets and $|A|=|B|=|C|$, then* $\mathrm{Sym}(E)=S_A S_B S_A\cup S_B S_A S_B$.

Proof. Let $\kappa=|E|$. Consider a permutation $\pi\in\mathrm{Sym}(E)$. It is easy to see that $\pi\in S_A S_B S_A$ if (and only if) $|(B\cup C)\backslash A\pi^{-1}|=\kappa$. In particular, $\pi\in S_A S_B S_A$ if $|C\backslash A\pi^{-1}|=\kappa$; similarly, $\pi\in S_B S_A S_B$ if $|C\backslash B\pi^{-1}|=\kappa$. At least one of these alternatives must hold, since $C=(C\backslash A\pi^{-1})\cup(C\backslash B\pi^{-1})$.

LEMMA 2.2 [**16**, Exercise 10.1.17, p. 259]. *Every permutation is the product of two involutions.*

Proof. It suffices to consider the case of a permutation consisting of a single (finite or infinite) cycle. Note, for example, that a 6-cycle is obtained by multiplying the involutions $(1,2)(3,4)(5,6)$ and $(2,3)(4,5)$. This example can easily be generalized to get cycles of any desired length.

LEMMA 2.3. *Let $2\leqslant q\leqslant\infty$ and let E be an infinite set. There is a positive integer k (depending only on q) such that every element of* $\mathrm{Sym}(E)$ *can be expressed as the product of k elements of order q.*

Proof. Leaving the (easier) case $q = \infty$ as an exercise for the reader, we assume that $q < \infty$. Choose a positive integer n that is divisible by 4 and large enough so that the finite symmetric group $\mathrm{Sym}(n)$ has an element of order q. Let π be a fixed-point-free involution in Sym(n); then π is an even permutation. Let G be the subgroup of $\mathrm{Sym}(n)$ generated by the elements of order q; then G is a nontrivial (meaning $|G| > 1$) normal subgroup of $\mathrm{Sym}(n)$. Since the only nontrivial normal subgroups of $\mathrm{Sym}(n)$ are $\mathrm{Sym}(n)$ itself, the alternating group $\mathrm{Alt}(n)$, and (if $n = 4$) the four-group, we must have $\pi \in G$; that is, π is the product of some number m of elements of order q. From this it clearly follows that every involution with infinite support can be expressed as the product of m permutations of order q. Now, it can easily be seen from the proof of Lemma 2.2 that every permutation of an infinite set E is the product of two involutions, each of which has infinite support; it follows that every element of $\mathrm{Sym}(E)$ is the product of $2m$ permutations of order q.

LEMMA 2.4. *Let E be an infinite set, and let $\phi \in \mathrm{Sym}(E)$. If $|\mathrm{fix}(\phi)| = |E|$, then ϕ is a commutator in* $\mathrm{Sym}(E)$.

Proof. Without loss of generality, we may assume that $E = \mathbb{Z} \times T$ where $|T| = |E|$, and that $\mathrm{supp}(\phi) \subseteq \{0\} \times T$. Define $\hat{\phi} \in \mathrm{Sym}(T)$ so that $(0,t)\phi = (0, t\hat{\phi})$ for $t \in T$. Define $\alpha, \beta \in \mathrm{Sym}(E)$ by setting $(m,t)\alpha = (m+1, t)$, $(m,t)\beta = (m, t\hat{\phi})$ for $m > 0$, and $(m,t)\beta = (m,t)$ for $m \leqslant 0$. Then $\phi = \alpha\beta\alpha^{-1}\beta^{-1} = [\alpha^{-1}, \beta^{-1}]$.

LEMMA 2.5. *If E is an infinite set, then every element of* $\mathrm{Sym}(E)$ *is the product of two commutators.*

Proof. Let $\kappa = |E|$. Consider a permutation $\pi \in \mathrm{Sym}(E)$. Choose $B \subset E$ so that $|B| = |E \backslash (B \cup B\pi)| = \kappa$. Let $D = E \backslash (B \cup B\pi)$, and choose $A \subset D$ so that $|A| = |D \backslash A| = \kappa$. Since $|E \backslash (A \cup B)| = |E \backslash (A \cup B\pi)| = \kappa$, we can define $\phi \in \mathrm{Sym}(E)$ so that $x\phi = x$ for $x \in A$ and $x\phi = x\pi$ for $x \in B$. Let $\psi = \phi^{-1}\pi$, so that $\pi = \phi\psi$. Since $A \subseteq \mathrm{fix}(\phi)$ and $B\pi \subseteq \mathrm{fix}(\psi)$, it follows by Lemma 2.4 that ϕ and ψ are commutators.

LEMMA 2.6. *Let $2 \leqslant q \leqslant \infty$ and let E be an infinite set. Then every element of* $\mathrm{Sym}(E)$ *can be expressed as a product of commutators of the form $[\phi_1 \phi_2 \ldots \phi_k, \psi_1 \psi_2 \ldots \psi_k]$ where the factors ϕ_i and ψ_i are permutations of order q.*

Proof. This follows immediately from Lemmas 2.5 and 2.3.

3. *Wagon's conjecture*

THEOREM 3.1. *Let E be an infinite set. Every countable subset of* $\mathrm{Sym}(E)$ *is contained in a* 4*-generator subgroup of* $\mathrm{Sym}(E)$.

Proof. We may assume that $E = \mathbb{Z} \times \mathbb{Z} \times T$, where $|T| = |E| = \kappa$. Let $E_0 = \{0\} \times \{0\} \times T$. Choose $A \subset E_0$ with $|A| = |E_0 \backslash A| = \kappa$; let $C = E_0 \backslash A$ and $B = E \backslash E_0$. Choose an involution $\varepsilon \in \mathrm{Sym}(E)$ so that $B\varepsilon = A$. Define $\alpha, \delta \in \mathrm{Sym}(E)$ by setting $(m,n,t)\alpha = (m+1, n, t)$, $(0,n,t)\delta = (0, n+1, t)$, and $(m,n,t)\delta = (m,n,t)$ for $m \neq 0$.

Let a countable set $H \subseteq \mathrm{Sym}(E)$ be given; we shall show that $H \subseteq \langle \alpha, \beta, \delta, \varepsilon \rangle$ for some $\beta \in \mathrm{Sym}(E)$. By Lemma 2.1, we may assume that $H \subseteq S_A \cup S_B$. Let

$H' = (H \cap S_B) \cup \varepsilon(H \cap S_A)\varepsilon$. Then H' is a countable subset of S_B; let $H' = \{\phi_i : i \in \mathbb{Z}\}$. Since $\operatorname{supp}(\phi_i) \subseteq E_0$, we can define $\hat{\phi}_i \in \operatorname{Sym}(T)$ so that $(0,0,t)\phi_i = (0,0,t\hat{\phi}_i)$ for $t \in T$, $i \in \mathbb{Z}$. Finally, define $\beta \in \operatorname{Sym}(E)$ by setting

$$(m,n,t)\beta = \begin{cases} (m,n,t\hat{\phi}_m) & \text{if } n \geqslant 0, \\ (m,n,t) & \text{if } n < 0. \end{cases}$$

Then $\phi_i = (\alpha^i\beta\alpha^{-i})\delta^{-1}(\alpha^i\beta^{-1}\alpha^{-i})\delta$ for each $i \in \mathbb{Z}$; thus we have $H' \subseteq \langle \alpha, \beta, \delta \rangle$ and $H \subseteq H' \cup \varepsilon H'\varepsilon \subseteq \langle \alpha, \beta, \delta, \varepsilon \rangle$.

COROLLARY 3.2. *A symmetric group is not the union of a countable chain of proper subgroups.*

This is the special case $\kappa = \aleph_0$ of the result of Macpherson and Neumann [**11**, Theorem 1.1] that, if $|E| \geqslant \kappa$, then $\operatorname{Sym}(E)$ is not the union of a chain of κ proper subgroups.

THEOREM 3.3. *Let E be an infinite set. Every countable subset of* $\operatorname{Sym}(E)$ *is contained in a 2-generator subgroup of* $\operatorname{Sym}(E)$.

Proof. We may assume that $E = \mathbb{Z} \times \mathbb{Z} \times T$ where $|T| = |E| = \kappa$. Define $\alpha \in \operatorname{Sym}(E)$ by setting $(m,n,t)\alpha = (m+1,n,t)$. Let $E_0 = \{1\} \times \{0\} \times T$. Choose $A \subset E_0$ with $|A| = |E_0 \backslash A| = \kappa$; let $C = E_0 \backslash A$ and $B = E \backslash E_0$. Choose an involution $\varepsilon \in S_C$ so that $B\varepsilon = A$.

Let a countable set $H \subseteq \operatorname{Sym}(E)$ be given; we shall construct a permutation $\gamma \in \operatorname{Sym}(E)$ so that $H \subseteq \langle \alpha, \gamma \rangle$. By Lemma 2.1, we may assume that $H \subseteq S_A \cup S_B$. Let $H' = (H \cap S_B) \cup \varepsilon(H \cap S_A)\varepsilon$. Then H' is a countable subset of S_B; let $H' = \{\phi_i : i = 3,5,7,\ldots\}$. Since $\operatorname{supp}(\phi_i) \subseteq E_0$, we can define $\hat{\phi}_i \in \operatorname{Sym}(T)$ so that $(1,0,t)\phi_i = (1,0,t\hat{\phi}_i)$ for $t \in T$ and $i = 3,5,7,\ldots$. Now define $\beta_0 \in S_{E_0}$ as follows:

$$(m,n,t)\beta_0 = \begin{cases} (m,n+1,t) & \text{if } m = 0; \\ (m,n,t\hat{\phi}_m) & \text{if } m \text{ is odd, } m \geqslant 3,\ n \geqslant 0; \\ (m,n,t) & \text{otherwise.} \end{cases}$$

Let $\gamma = \varepsilon\beta_0$. Note that $\gamma\pi\gamma^{-1} = \varepsilon\pi\varepsilon$ for all $\pi \in S_B$, whence $H \subseteq H' \cup \varepsilon H'\varepsilon = H' \cup \gamma H'\gamma^{-1}$. Thus, in order to show that $H \subseteq \langle \alpha, \gamma \rangle$, it will suffice to show that $H' \subseteq \langle \alpha, \gamma \rangle$.

Let $\beta = \gamma^2 = (\varepsilon\beta_0)^2$. Note that $x\beta = x\beta_0$ for all $x \in B$, and that $E_0\beta = E_0$. Now, for each $i = 3,5,7,\ldots$, we have $\alpha\phi_i\alpha^{-1} = (\alpha^i\beta\alpha^{-i})\beta^{-1}(\alpha^i\beta^{-1}\alpha^{-i})\beta$; hence $\phi_i \in \langle \alpha, \beta \rangle \subseteq \langle \alpha, \gamma \rangle$.

LEMMA 3.4. *Let E be an infinite set, and suppose that $E = A \cup B \cup C$ where A, B, C are disjoint sets and $|A| = |B| = |C|$. Then every countable subset of* $\operatorname{Sym}(E)$ *is contained in the subgroup generated by* 24 *involutions in $S_A \cup S_B$.*

Proof. By Theorem 3.1 (or 3.3), every countable subset of $\operatorname{Sym}(E)$ is contained in the subgroup generated by 4 permutations in $\operatorname{Sym}(E)$; by Lemmas 2.1 and 2.2, each of those permutations can be expressed as the product of 6 involutions in $S_A \cup S_B$.

THEOREM 3.5. *Let E be an infinite set. Every countable subset of* $\mathrm{Sym}(E)$ *is contained in a 2-generator subgroup of* $\mathrm{Sym}(E)$ *with one generator of order* 53 *and the other of order* 4.

Proof. We may assume that $E = \mathbb{Z}_{53} \times \mathbb{Z} \times T$ where $|T| = |E| = \kappa$. Define a permutation α of order 53 by setting $(m, n, t)\alpha = (m+1, n, t)$. Let $E_0 = \{0\} \times \{0\} \times T$. Choose $A \subset E_0$ with $|A| = |E_0 \backslash A| = \kappa$; let $C = E_0 \backslash A$ and $B = E \backslash E_0$. Choose an involution $\varepsilon \in S_C$ so that $B\varepsilon = A$.

Let a countable set $H \subseteq \mathrm{Sym}(E)$ be given; we shall construct a permutation γ of order 4 so that $H \subseteq \langle \alpha, \gamma \rangle$. By Lemma 3.4, we can assume that H is a set of 24 involutions in $S_A \cup S_B$. Then $H' = (H \cap S_B) \cup \varepsilon(H \backslash S_B)\varepsilon$ is a set of at most 24 involutions in S_B; let $H' = \{\phi_i : i \in I\}$, where $I = \{5, 7, 9, \ldots, 51\}$. Since $\mathrm{supp}(\phi_i) \subseteq E_0$, we can define involutions $\hat{\phi}_i \in \mathrm{Sym}(T)$ so that $(0, 0, t)\phi_i = (0, 0, t\hat{\phi}_i)$ for $t \in T$ and $i \in I$.

Now define an involution $\beta_0 \in S_{E_0}$ as follows:

$$(m, n, t)\beta_0 = \begin{cases} (m, n+(-1)^n, t) & \text{if } m = 2; \\ (m, n-(-1)^n, t) & \text{if } m = 3; \\ (m, n, t\hat{\phi}_m) & \text{if } m \in I,\ n \equiv 0 \pmod 4,\ n \geqslant 0; \\ (m, n, t) & \text{otherwise.} \end{cases}$$

Then $\gamma = \varepsilon\beta_0$ is a permutation of order 4. Note that $\gamma\pi\gamma^{-1} = \varepsilon\pi\varepsilon$ for all $\pi \in S_B$, whence $H \subseteq H' \cup \varepsilon H'\varepsilon = H' \cup \gamma H'\gamma^{-1}$. Thus, in order to show that $H \subseteq \langle \alpha, \gamma \rangle$, it will suffice to show that $H' \subseteq \langle \alpha, \gamma \rangle$.

Let $\beta = \gamma^2 = (\varepsilon\beta_0)^2$; note that β is an involution, $x\beta = x\beta_0$ for all $x \in B$, and $E_0\beta = E_0$. Let $\delta = (\beta\alpha\beta\alpha^{-1})^2$; note that $(2, n, t)\delta = (2, n+4(-1)^n, t)$, while $(m, n, t)\delta = (m, n, t)$ if $m \neq 2$. Now it is easy to see that

$$\phi_i = (\alpha^i\beta\alpha^{-i})(\alpha^2\delta^{-1}\alpha^{-2})(\alpha^i\beta\alpha^{-i})(\alpha^2\delta\alpha^{-2})$$

for each $i \in I$; hence $H' \subseteq \langle \alpha, \beta, \delta \rangle \subseteq \langle \alpha, \gamma \rangle$.

4. *Generators of prescribed order*

THEOREM 4.1. *Let $3 \leqslant p \leqslant \infty$ and $2 \leqslant q \leqslant \infty$, and let E be an infinite set. If H is a countable subset of* $\mathrm{Sym}(E)$ *with* $|\mathrm{fix}(H)| = |E|$, *then H is contained in a 2-generator subgroup of* $\mathrm{Sym}(E)$ *with one generator of order p and the other of order q.*

Proof. Leaving the case $q = \infty$ as an exercise for the reader, we assume that $q < \infty$.

We may assume that $E = \mathbb{Z}_p \times \mathbb{Z} \times T$ where $|T| = |E|$, and that $\mathrm{supp}(H) \subseteq E_0 = \{0\} \times \{0\} \times T$. By Lemma 2.6 we can choose $\phi_i \in \mathrm{Sym}(E)$ for $i \in \mathbb{N}$, so that each ϕ_i is a permutation of order q with $\mathrm{supp}(\phi_i) \subseteq E_0$, and every element of H can be expressed as a product of commutators of the form $[\phi_{i_1}\phi_{i_2}\ldots\phi_{i_k}, \phi_{j_1}\phi_{j_2}\ldots\phi_{j_k}]$. For each $i \in \mathbb{N}$ define a permutation $\hat{\phi}_i \in \mathrm{Sym}(T)$ of order q, so that $(0, 0, t)\phi_i = (0, 0, t\hat{\phi}_i)$ for $i \in T$.

Define a permutation $\alpha \in \mathrm{Sym}(E)$ of order p by setting $(m,n,t)\alpha = (m+1,n,t)$. Define $\beta \in \mathrm{Sym}(E)$ as follows:

$$(0,n,t)\beta = \begin{cases} (0,n,t\hat{\phi}_i) & \text{if } n = q^3 2^i \text{ with } i \in \mathbb{N}; \\ (0,n,t) & \text{if } n \notin \{q^3 2^i : i \in \mathbb{N}\}; \end{cases}$$

$$(1,n,t)\beta = \begin{cases} (1,n-1+q,t) & \text{if } n \equiv 0 \pmod q; \\ (1,n-1,t) & \text{otherwise}; \end{cases}$$

$$(2,n,t)\beta = \begin{cases} (2,n+1-q,t) & \text{if } n \equiv 0 \pmod q; \\ (2,n+1,t) & \text{otherwise}; \end{cases}$$

$$(m,n,t)\beta = (m,n,t) \quad \text{if } m \notin \{0,1,2\}.$$

Then β is a permutation of order q; thus it will suffice to show that

$$[\phi_{i_1} \cdots \phi_{i_k}, \phi_{j_1} \cdots \phi_{j_k}] \in \langle \alpha, \beta \rangle \text{ for all } i_1, \ldots, i_k, j_1, \ldots, j_k \in \mathbb{N}.$$

Let $\delta = (\beta\alpha\beta\alpha^{-1})^{q^2}$; then

$$(1,n,t)\delta = \begin{cases} (1,n+q^3,t) & \text{if } n \equiv 0 \pmod q; \\ (1,n-q^3,t) & \text{if } n \equiv 1 \pmod q; \\ (1,n,t) & \text{otherwise}; \end{cases}$$

$$(m,n,t)\delta = (m,n,t) \quad \text{if } m \neq 1.$$

Let $\psi_i = (\alpha\delta^{2^i}\alpha^{-1})\beta(\alpha\delta^{-2^i}\alpha^{-1})$ for each $i \in \mathbb{N}$. Then $(m,n,t)\psi_i = (m,n,t)\beta$ for $m \neq 0$, while

$$(0,n,t)\psi_i = \begin{cases} (0,n,t\hat{\phi}_j) & \text{if } n = q^3(2^j - 2^i) \text{ with } j \in \mathbb{N}; \\ (0,n,t) & \text{if } n \notin \{q^3(2^j - 2^i) : j \in \mathbb{N}\}; \end{cases}$$

in particular, $(0,0,t)\psi_i = (0,0,t\hat{\phi}_i) = (0,0,t)\phi_i$. For each $i \in \mathbb{N}$, let $N_i = \{q^3(2^j - 2^i) : j \in \mathbb{N} \setminus \{i\}\}$; then $N_i \subseteq \mathbb{Z} \setminus \{0\}$, and $N_i \cap N_j = \varnothing$ for $i \neq j$. Let $X_i = \{0\} \times N_i \times T$ and let $Y = \{1,2\} \times \mathbb{Z} \times T$.

Now E_0, Y, X_1, X_2, X_3, ... are disjoint sets, and for each $i \in \mathbb{N}$ we have $\mathrm{supp}(\phi_i) \subseteq E_0$, $\mathrm{supp}(\psi_i) \subseteq E_0 \cup Y \cup X_i$, $\psi_i | E_0 = \phi_i | E_0$, $\psi_i | Y = \beta | Y$, $E_0 \psi_i = E_0$, $Y\psi_i = Y$ and $X_i \psi_i = X_i$. It follows that

$$[\phi_{i_1} \cdots \phi_{i_k}, \phi_{j_1} \cdots \phi_{j_k}] = [\psi_{i_1} \cdots \psi_{i_k}, \psi_{j_1} \cdots \psi_{j_k}] \in \langle \alpha, \beta \rangle.$$

COROLLARY 4.2 [**10**, Theorem 2.1]. *If $3 \leqslant p \leqslant \infty$ and $2 \leqslant q \leqslant \infty$, then every countable group is embeddable in a 2-generator group with one generator of order p and the other of order q.*

THEOREM 4.3. *Let $3 \leqslant p \leqslant \infty$ and $2 \leqslant q \leqslant \infty$, and let E be an infinite set. Then every countable subset of* Sym(E) *is contained in a 2-generator subgroup of* Sym(E) *with one generator of order p and the other of order 2q.*

Proof. Leaving the case $q = \infty$ as an exercise for the reader, we assume that $q < \infty$.

We may assume that $E = \mathbb{Z}_p \times \mathbb{Z} \times T$ where $|T| = |E| = \kappa$. Define a permutation α of order p by setting $(m,n,t)\alpha = (m+1,n,t)$. Let $E_0 = \{0\}\times\{0\}\times T$. Choose $A \subset E_0$ with $|A| = |E_0\backslash A| = \kappa$; let $C = E_0\backslash A$ and $B = E\backslash E_0$. Choose an involution $\varepsilon \in S_C$ so that $B\varepsilon = A$.

Let a countable set $H \subseteq \mathrm{Sym}(E)$ be given; we shall construct a permutation γ of order $2q$ so that $H \subseteq \langle \alpha, \gamma\rangle$. By Lemma 2.1, we may assume that $H \subseteq S_A \cup S_B$; then $H' = (H \cap S_B) \cup \varepsilon(H \cap S_A)\varepsilon$ is a countable subset of S_B. By Lemma 2.6, we can choose elements $\phi_i \in S_B$ for $i \in \mathbb{N}$, so that each ϕ_i is a permutation of order q, and every element of H' can be expressed as a product of commutators of the form $[\phi_{i_1}\phi_{i_2}\dots\phi_{i_k}, \phi_{j_1}\phi_{j_2}\dots\phi_{j_k}]$. For each $i\in\mathbb{N}$ define a permutation $\hat{\phi}_i \in \mathrm{Sym}(T)$ of order q, so that $(0,0,t)\phi_i = (0,0,t\hat{\phi}_i)$ for $t \in T$.

Define a permutation $\beta_0 \in S_{E_0}$ of order q, as follows:

$$(0,n,t)\beta_0 = \begin{cases}(0,n,t\hat{\phi}_i) & \text{if } n = q^3(2^i-1) \text{ with } i\in\mathbb{N};\\ (0,n,t) & \text{if } n \notin \{q^3(2^i-1): i \in \mathbb{N}\};\end{cases}$$

$$(1,n,t)\beta_0 = \begin{cases}(1,n-1+q,t) & \text{if } n \equiv 0 \pmod q;\\ (1,n-1,t) & \text{otherwise};\end{cases}$$

$$(2,n,t)\beta_0 = \begin{cases}(2,n+1-q,t) & \text{if } n \equiv 0 \pmod q;\\ (2,n+1,t) & \text{otherwise};\end{cases}$$

$$(m,n,t)\beta_0 = (m,n,t) \quad \text{if } m \notin \{0,1,2\}.$$

Let $\gamma = \varepsilon\beta_0$ and let $\beta = \gamma^2$; then $\beta|B = \beta_0|B$, $\beta|E_0 = \varepsilon\beta_0\varepsilon|E_0$, $E_0\beta = E_0$, β is a permutation of order q, and γ is a permutation of order $2q$. Note that $\gamma\pi\gamma^{-1} = \varepsilon\pi\varepsilon$ for all $\pi \in S_B$, whence $H \subseteq H' \cup \varepsilon H'\varepsilon = H' \cup \gamma H'\gamma^{-1}$. Thus, in order to show that $H \subseteq \langle\alpha,\gamma\rangle$, it will suffice to show that $H' \subseteq \langle\alpha,\gamma\rangle$. In fact, we shall show that $H' \subseteq \langle\alpha,\beta\rangle$, by showing that $[\phi_{i_1}\dots\phi_{i_k}, \phi_{j_1}\dots\phi_{j_k}] \in \langle\alpha,\beta\rangle$ for all $i_1,\dots,i_k$, $j_1,\dots,j_k \in \mathbb{N}$.

Let $\delta = (\beta\alpha\beta\alpha^{-1})^{q^2}$; then

$$(1,n,t)\delta = \begin{cases}(1,n+q^3,t) & \text{if } n \equiv 0 \pmod q;\\ (1,n-q^3,t) & \text{if } n \equiv 1 \pmod q;\\ (1,n,t) & \text{otherwise};\end{cases}$$

$$(m,n,t)\delta = (m,n,t) \quad \text{if } m \neq 1.$$

Let $\psi_i = (\alpha\delta^{2^i-1}\alpha^{-1})\beta(\alpha\delta^{1-2^i}\alpha^{-1})$ for each $i \in \mathbb{N}$. Then $(m,n,t)\psi_i = (m,n,t)\beta$ for $m \neq 0$. If we define $\hat{\phi}_0 \in \mathrm{Sym}(T)$ so that $(0,0,t)\beta = (0,0,t\hat{\phi}_0)$ for $t \in T$, then

$$(0,n,t)\psi_i = \begin{cases}(0,n,t\hat{\phi}_j) & \text{if } n = q^3(2^j-2^i) \text{ with } j \in \mathbb{N}\cup\{0\};\\ (0,n,t) & \text{if } n \notin \{q^3(2^j-2^i): j \in \mathbb{N}\cup\{0\}\};\end{cases}$$

in particular, $(0,0,t)\psi_i = (0,0,t\hat{\phi}_i) = (0,0,t)\phi_i$. For each $i\in\mathbb{N}$, let $N_i = \{q^3(2^j-2^i): j \in \mathbb{N}\cup\{0\}, j \neq i\}$; then $N_i \subseteq \mathbb{Z}\backslash\{0\}$, and $N_i \cap N_j = \varnothing$ for $i \neq j$. Let $X_i = \{0\}\times N_i \times T$, and let $Y = \{1,2\}\times\mathbb{Z}\times T$.

Now $E_0, Y, X_1, X_2, X_3, \dots$ are disjoint sets, and for each $i \in \mathbb{N}$ we have

$$\mathrm{supp}(\phi_i) \subseteq E_0, \quad \mathrm{supp}(\psi_i) \subseteq E_0 \cup Y \cup X_i,$$

$$\psi_i|E_0 = \phi_i|E_0, \quad \psi_i|Y = \beta|Y, \quad E_0\psi_i = E_0, \quad Y\psi_i = Y, \quad X_i\psi_i = X_i.$$

It follows that $[\phi_{i_1}\dots\phi_{i_k}, \phi_{j_1}\dots\phi_{j_k}] = [\psi_{i_1}\dots\psi_{i_k}, \psi_{j_1}\dots\psi_{j_k}] \in \langle\alpha,\beta\rangle$.

LEMMA 4.4. *Let E be an infinite set with $|E| = \kappa$, and let $\alpha_1, \alpha_2 \in \mathrm{Sym}(E)$ be such that $|\{x \in E : x \neq x\alpha_1 \neq x\alpha_2 \neq x\}| = \kappa$. If $|\{x \in E : x\alpha^2 \neq x\}| < \kappa$ for each $\alpha \in \{\alpha_1, \alpha_2, \alpha_1\alpha_2\}$, then the set*

$$\{x \in E : x \neq x\alpha_1 \neq x\alpha_2 \neq x, x\alpha_1\alpha_2 = x\alpha_2\alpha_1, x\alpha_1^2 = x\alpha_2^2 = x, x\alpha_2\alpha_1^2 = x\alpha_2, x\alpha_1\alpha_2^2 = x\alpha_1\}$$

has cardinality κ.

Proof. Let

$$X = \{x \in E : x \neq x\alpha_1 \neq x\alpha_2 \neq x, x(\alpha_1\alpha_2)^2 = x\alpha_1^2 = x\alpha_2^2 = x, x\alpha_2\alpha_1^2 = x\alpha_2, x\alpha_1\alpha_2^2 = x\alpha_1\}.$$

Clearly $|X| = \kappa$; we have to show that $x\alpha_1\alpha_2 = x\alpha_2\alpha_1$ for all $x \in X$. In fact,

$$x \in X \Rightarrow x(\alpha_1\alpha_2)^2 = x\alpha_2^2 \Rightarrow x\alpha_1\alpha_2\alpha_1 = x\alpha_2 = x\alpha_2\alpha_1^2 \Rightarrow x\alpha_1\alpha_2 = x\alpha_2\alpha_1.$$

LEMMA 4.5. *Let E be an infinite set with $|E| = \kappa$, and let α_1, $\alpha_2 \in \mathrm{Sym}(E)$ be such that $|\{x \in E : x \neq x\alpha_1 \neq x\alpha_2 \neq x\}| = \kappa$. Then we can choose permutations $\alpha, \theta \in \langle \alpha_1, \alpha_2 \rangle$ and distinct points $x_i^\xi \in E$ for $\xi \in \kappa$, $i \in \{0, 1, 2, 3\}$, so that, setting*

$$D = E \backslash \{x_i^\xi : \xi \in \kappa,\ i \in \{0, 1, 2, 3\}\},$$

one of the following four cases holds for all $\xi \in \kappa$:

$$\begin{array}{rllll}
\text{(I)} & x_0^\xi\alpha = x_1^\xi, & x_1^\xi\alpha = x_2^\xi, & x_2^\xi\alpha = x_0^\xi, & x_3^\xi\alpha \varepsilon D; \\
\text{(II)} & x_0^\xi\alpha = x_1^\xi, & x_1^\xi\alpha = x_2^\xi, & x_2^\xi\alpha = x_3^\xi, & x_3^\xi\alpha = x_0^\xi; \\
\text{(III)} & x_0^\xi\alpha = x_1^\xi, & x_1^\xi\alpha = x_2^\xi, & x_2^\xi\alpha \in D, & x_3^\xi\alpha = x_0^\xi; \\
\text{(IV)} & x_0^\xi\alpha = x_3^\xi, & x_1^\xi\alpha = x_2^\xi, & x_2^\xi\alpha = x_1^\xi, & x_3^\xi\alpha = x_0^\xi, \\
 & x_0^\xi\theta = x_1^\xi, & x_1^\xi\theta = x_0^\xi, & x_2^\xi\theta = x_3^\xi, & x_3^\xi\theta = x_2^\xi.
\end{array}$$

Proof. If possible, we choose $\alpha \in \langle \alpha_1, \alpha_2 \rangle$ so that $|\{x \in E : x\alpha^2 \neq x\}| = \kappa$; then we get case (I) (if α has κ 3-cycles) or (II) (if α has κ 4-cycles) or (III) (if α has κ cycles of length at least 5, or else $\kappa = \aleph_0$ and α has an infinite cycle). On the other hand, suppose that $|\{x \in E : x\alpha^2 \neq x\}| < \kappa$ for each $\alpha \in \langle \alpha_1, \alpha_2 \rangle$; then we can set $\alpha = \alpha_1$ and $\theta = \alpha_2$, and use Lemma 4.4 to get case (IV).

THEOREM 4.6. *Let $2 \leqslant q < \infty$, and let E be an infinite set. Suppose that α_1, $\alpha_2 \in \mathrm{Sym}(E)$ are such that $|\{x \in E : x \neq x\alpha_1 \neq x\alpha_2 \neq x\}| = |E|$. Then, for every countable subset H of $\mathrm{Sym}(E)$, there is a permutation $\gamma \in \mathrm{Sym}(E)$, of order $2q$, such that $H \subseteq \langle \alpha_1, \alpha_2, \gamma \rangle$.*

Proof. Let $\kappa = |E|$. By Lemma 4.5, we may assume that $\{0, 1, 2, 3\} \times \mathbb{Z} \times T \subseteq E$, $|T| = \kappa$, $D = E \backslash (\{0, 1, 2, 3\} \times \mathbb{Z} \times T)$, and that there are permutations $\alpha, \theta \in \langle \alpha_1, \alpha_2 \rangle$ such that one of the following four cases holds for all $n \in \mathbb{Z}$, $t \in T$:

$$\begin{array}{rl}
\text{(I)} & (0,n,t)\alpha = (1,n,t), (1,n,t)\alpha = (2,n,t), (2,n,t)\alpha = (0,n,t), (3,n,t)\alpha \in D; \\
\text{(II)} & (0,n,t)\alpha = (1,n,t), (1,n,t)\alpha = (2,n,t), (2,n,t)\alpha = (3,n,t), (3,n,t)\alpha = (0,n,t); \\
\text{(III)} & (0,n,t)\alpha = (1,n,t), (1,n,t)\alpha = (2,n,t), (2,n,t)\alpha \in D, (3,n,t)\alpha = (0,n,t); \\
\text{(IV)} & (0,n,t)\alpha = (3,n,t), (1,n,t)\alpha = (2,n,t), (2,n,t)\alpha = (1,n,t), (3,n,t)\alpha = (0,n,t), \\
 & (0,n,t)\theta = (1,n,t), (1,n,t)\theta = (0,n,t), (2,n,t)\theta = (3,n,t), (3,n,t)\theta = (2,n,t);
\end{array}$$

moreover, in cases (I) to (III) we can take $\theta = \alpha$, so that $(0,n,t)\theta = (1,n,t)$ in all cases. Note that $D\alpha \subseteq D \cup (\{3\} \times \mathbb{Z} \times T)$. Let $E_0 = \{0\} \times \{0\} \times T$. Choose $A \subset E_0$ with $|A| = |E_0 \backslash A| = \kappa$; let $C = E_0 \backslash A$ and $B = E \backslash E_0$. Choose an involution $\varepsilon \in S_C$ so that $B\varepsilon = A$.

By Lemma 2.1, we may assume that $H \subseteq S_A \cup S_B$; then

$$H' = (H \cap S_B) \cup \varepsilon(H \cap S_A)\varepsilon$$

is a countable subset of S_B. By Lemma 2.6, we can choose elements $\phi_i \in S_B$ for $i \in \mathbb{N}$, so that each ϕ_i is a permutation of order q, and every element of H' can be expressed as product of commutators of the form $[\phi_{i_1}\phi_{i_2}\dots\phi_{i_k}, \phi_{j_1}\phi_{j_2}\dots\phi_{j_k}]$. For each $i \in \mathbb{N}$ define a permutation $\hat{\phi}_i \in \mathrm{Sym}(T)$ of order q, so that $(0,0,t)\phi_i = (0,0,t\hat{\phi}_i)$ for $i \in T$.

Define a permutation $\beta_0 \in S_{E_0}$, of order q, as follows:

$$(0,n,t)\beta_0 = \begin{cases} (0,n,t\hat{\phi}_i) & \text{if } n = q^3(2^i-1) \text{ with } i \in \mathbb{N}; \\ (0,n,t) & \text{if } n \notin \{q^3(2^i-1) : i \in \mathbb{N}\}; \end{cases}$$

$$(1,n,t)\beta_0 = \begin{cases} (1,n-1+q,t) & \text{if } n \equiv 0 \pmod{q}; \\ (1,n-1,t) & \text{otherwise}; \end{cases}$$

$$(2,n,t)\beta_0 = \begin{cases} (2,n+1-q,t) & \text{if } n \equiv 0 \pmod{q}; \\ (2,n+1,t) & \text{otherwise}; \end{cases}$$

$$(3,n,t)\beta_0 = (3,n,t);$$

$$x\beta_0 = x \quad \text{if } x \in D.$$

Let $\gamma = \varepsilon\beta_0$ and let $\beta = \gamma^2$; then $\beta|B = \beta_0|B$, $\beta|E_0 = \varepsilon\beta_0\varepsilon|E_0$, $E_0\beta = E_0$, β is a permutation of order q, and γ is a permutation of order $2q$. Note that $\gamma\pi\gamma^{-1} = \varepsilon\pi\varepsilon$ for all $\pi \in S_B$, whence $H \subseteq H' \cup \varepsilon H'\varepsilon = H' \cup \gamma H'\gamma^{-1}$. Thus, in order to show that $H \subseteq \langle \alpha_1, \alpha_2, \gamma \rangle$, it will suffice to show that $H' \subseteq \langle \alpha_1, \alpha_2, \gamma \rangle$. In fact, we will show that $H' \subseteq \langle \alpha, \theta, \beta \rangle$, by showing that $[\phi_{i_1}\dots\phi_{i_k}, \phi_{j_1}\dots\phi_{j_k}] \in \langle \alpha, \theta, \beta \rangle$ for all $i_1, \dots, i_k, j_1, \dots, j_k \in \mathbb{N}$.

Let $\delta = (\beta\alpha\beta\alpha^{-1})^{q^2}$; then

$$(1,n,t)\delta = \begin{cases} (1,n+q^3,t) & \text{if } n \equiv 0 \pmod{q}; \\ (1,n-q^3,t) & \text{if } n \equiv 1 \pmod{q}; \\ (1,n,t) & \text{otherwise}; \end{cases}$$

$$(0,n,t)\delta = (0,n,t);$$

$$(3,n,t)\delta = (3,n,t);$$

$$x\delta = x \quad \text{if } x \varepsilon D;$$

and in cases (I) to (III) we have

$$(2,n,t)\delta = (2,n,t);$$

however, in case (IV) we have

$$(2,n,t)\delta = \begin{cases} (2,n-q^3,t) & \text{if n} \equiv 0 \pmod{q}; \\ (2,n+q^3,t) & \text{if } n \equiv -1 \pmod{q}; \\ (2,n,t) & \text{otherwise.} \end{cases}$$

Let $\psi_i = (\theta\delta^{2^i-1}\theta^{-1})\beta(\theta\delta^{1-2^i}\theta^{-1})$ for each $i \in \mathbb{N}$. Then $x\psi_i = x\beta$ for $x \in E\backslash(\{0\}\times\mathbb{Z}\times T)$. If we define $\hat{\phi}_0 \in \mathrm{Sym}(T)$ so that $(0,0,t)\beta = (0,0,t\hat{\phi}_0)$ for $t \in T$, then

$$(0,n,t)\,\psi_i = \begin{cases}(0,n,t\hat{\phi}_j) & \text{if } n = q^3(2^j-2^i) \text{ with } j \in \mathbb{N}\cup\{0\};\\ (0,n,t) & \text{if } n \notin \{q^3(2^j-2^i): j \in \mathbb{N}\cup\{0\}\};\end{cases}$$

in particular $(0,0,t)\,\psi_i = (0,0,t\hat{\phi}_i) = (0,0,t)\,\phi_i$. For each $i \in \mathbb{N}$, let $N_i = \{q^3(2^j-2^i): j \in \mathbb{N}\cup\{0\},\ j \neq i\}$; then $N_i \subseteq \mathbb{Z}\backslash\{0\}$, and $N_i \cap N_j = \varnothing$ for $i \neq j$. Let $X_i = \{0\}\times N_i \times T$, and let $Y = \{1,2\}\times\mathbb{Z}\times T$.

Now E_0, Y, $X_1, X_2, X_3, \ldots$ are disjoint sets, and for each $i \in \mathbb{N}$ we have

$$\mathrm{supp}(\phi_i) \subseteq E_0, \quad \mathrm{supp}(\psi_i) \subseteq E_0 \cup Y \cup X_i,$$
$$\psi_i|E_0 = \phi_i|E_0, \quad \psi_i|Y = \beta|Y, \quad E_0\psi_i = E_0, \quad Y\psi_i = Y \quad \text{and} \quad X_i\psi_i = X_i.$$

It follows that $[\phi_{i_1}\cdots\phi_{i_k}, \phi_{j_1}\cdots\phi_{j_k}] = [\psi_{i_1}\cdots\psi_{i_k}, \psi_{j_1}\cdots\psi_{j_k}] \in \langle\alpha,\theta,\beta\rangle$.

5. *Large subgroups of symmetric groups*

We use the notation $[X]^\kappa$ for $\{Y \subseteq X : |Y| = \kappa\}$, where X is a set and κ is a cardinal number.

LEMMA 5.1. *Let E be an infinite set with $|E| = \kappa$, let $A \subseteq \mathrm{Sym}(E)$, and suppose that there do not exist $\alpha_1, \alpha_2 \in A$ such that $|\{x \in E : x \neq x\alpha_1 \neq x\alpha_2 \neq x\}| = \kappa$. Given a set $X \in [E]^\kappa$ and a permutation $\gamma \in \mathrm{Sym}(E)$, we can find a set $Y \in [X]^\kappa$ and a permutation $\delta \in \mathrm{Sym}(E)$ such that, for each $\alpha \in A$, we have $|\{x \in Y : x\gamma\alpha \notin \{x\gamma, x\delta\}\}| < \kappa$.*

Proof. If possible, choose $\alpha_1 \in A$ so that $|\{x \in X : x\gamma\alpha_1 \neq x\gamma\}| = \kappa$, and let $Y = \{x \in X : x\gamma\alpha_1 \neq x\gamma\}$ and $\delta = \gamma\alpha_1$. If no such α_1 exists, let $Y = X$ and $\delta = \gamma$.

LEMMA 5.2. *Let E be an infinite set with $|E| = \kappa$, let $A \subseteq \mathrm{Sym}(E)$, and suppose that there do not exist $\alpha_1, \alpha_2 \in A$ such that $|\{x \in E : x \neq x\alpha_1 \neq x\alpha_2 \neq x\}| = \kappa$. Given a set $X \in [E]^\kappa$ and n permutations $\beta_1, \ldots, \beta_n \in \mathrm{Sym}(E)$, we can find a set $Y \in [X]^\kappa$ and 2^{n+1} permutations $\delta_1, \ldots, \delta_{2^{n+1}} \in \mathrm{Sym}(E)$ such that, for each $\pi \in A\beta_1 A\beta_2 \cdots A\beta_n A$, we have $|\{x \in Y : x\pi \notin \{x\delta_1, \ldots, x\delta_{2^{n+1}}\}\}| < \kappa$.*

Proof. By induction on n, using Lemma 5.1.

The next lemma follows from a theorem of Engelking and Karłowicz [**4**, Theorem 3]; we give a direct proof for the convenience of the reader.

LEMMA 5.3. *Let T be a set with $|T| = \kappa \geqslant \aleph_0$. Then there is a family F of functions $f: T \to \mathbb{Z}$ such that $|F| = 2^\kappa$ and, whenever $f_1, \ldots, f_n$ are finitely many distinct elements of F, we have $|\{t \in T : f_1(t), f_2(t), \ldots, f_n(t) \text{ are all distinct}\}| = \kappa$.*

Proof. We may assume that T is the set of all finite sequences in κ. For each subset I of κ define $f_I: T \to \mathbb{Z}$ by setting $f_I(\xi_0, \ldots, \xi_{m-1}) = \sum\{2^i : 0 \leqslant i < m, \xi_i \in I\}$, and let $F = \{f_I : I \subseteq \kappa\}$.

LEMMA 5.4. *Let E be an infinite set with $|E| = \kappa$. Then there is a set $C \subseteq \mathrm{Sym}(E)$ such that $|C| = 2^\kappa$ and, for each finite subset D of C, we have $|\{x \in E : |xD| = |D|\}| = \kappa$.*

Proof. We may assume that $E = T \times \mathbb{Z}$ where $|T| = \kappa$. Choose a family F of functions $f: T \to \mathbb{Z}$ as in Lemma 5.3. For each $f \in F$ define $\pi_f \in \mathrm{Sym}(E)$ by setting $(t, n)\pi_f = (t, n+f(t))$, and let $C = \{\pi_f : f \in F\}$.

LEMMA 5.5. *Let E be an infinite set with $|E| = \kappa$, let A be a subgroup of* $\mathrm{Sym}(E)$, *and suppose that there do not exist $\alpha_1, \alpha_2 \in A$ such that $|\{x \in E : x \neq x\alpha_1 \neq x\alpha_2 \neq x\}| = \kappa$. If $B \subseteq \mathrm{Sym}(E)$ and $|B| < 2^\kappa$, then $\langle A, B\rangle \neq \mathrm{Sym}(E)$.*

Proof. We may assume that $B^{-1} = B$; then

$$\langle A, B\rangle = \bigcup\{A\beta_1 A\beta_2 \cdots A\beta_n A : n < \omega; \beta_1, \ldots, \beta_n \in B\}.$$

Choose a set $C \subseteq \mathrm{Sym}(E)$ as in Lemma 5.4. It is easy to show using Lemma 5.2 that $|C \cap (A\beta_1 A\beta_2 \cdots A\beta_n A)| \leqslant 2^{n+1}$ for each finite sequence $\beta_1, \ldots, \beta_n$ in B; hence $|C \cap \langle A, B\rangle| \leqslant |B| + \aleph_0 < |C|$.

LEMMA 5.6. *Let E be an infinite set with $|E| = \kappa$, and let A be a subgroup of* $\mathrm{Sym}(E)$. *If* $\mathrm{Sym}(E) = \langle A, B\rangle$ *for some set $B \subseteq \mathrm{Sym}(E)$ with $|B| < 2^\kappa$, then there exist $\alpha_1, \alpha_2 \in A$ such that $|\{x \in E : x \neq x\alpha_1 \neq x\alpha_2 \neq x\}| = \kappa$.*

Proof. This is just a restatement of Lemma 5.5.

THEOREM 5.7. *Let $2 \leqslant q < \infty$ and let E be an infinite set with $|E| = \kappa$. Suppose that* $\mathrm{Sym}(E) = \langle A, B\rangle$ *and $|B| < 2^\kappa$. Then, for every countable subset H of* $\mathrm{Sym}(E)$, *there is a permutation $\gamma \in \mathrm{Sym}(E)$ of order $2q$, such that $\langle A, H\rangle \subseteq \langle A, \gamma\rangle$.*

Proof. This follows immediately from Lemma 5.6 and Theorem 4.6.

THEOREM 5.8. *Let $2 \leqslant q < \infty$ and let E be an infinite set. Suppose that* $\mathrm{Sym}(E) = \langle A, B\rangle$ *where $|B| \leqslant |E|$. Then there is a permutation $\gamma \in \mathrm{Sym}(E)$ of order $2q$, such that* $\mathrm{Sym}(E) = \langle A, \gamma\rangle$.

Proof. By a result of Macpherson and Neumann [**11**, Corollary 3.1], there is a finite set $H \subseteq B$ such that $\mathrm{Sym}(E) = \langle A, H\rangle$. (In the case of a countable set E, we could get this from our Corollary 3.2.) By Theorem 5.7, there is a permutation γ of order $2q$ such that $\langle A, H\rangle \subseteq \langle A, \gamma\rangle$.

The case $|B| = 2$ of Theorem 5.8 answers Question 3.2 of Macpherson and Neumann [**11**] in the negative.

Acknowledgements. I am grateful to Peter M. Neumann for his comments on a preliminary draft of this paper.

Note added in March, 1994. The answer to Question 1.5 above is yes; the proof will appear elsewhere.

References

1. STEFAN BANACH, 'Sur un théorème de M. Sierpiński', *Fund. Math.* 25 (1935) 5–6.
2. JAMES E. BAUMGARTNER, 'Almost-disjoint sets, the dense set problem and the partition calculus', *Ann. Math. Logic* 9 (1976) 401–439.
3. JOHN D. DIXON, PETER M. NEUMANN and SIMON THOMAS, 'Subgroups of small index in infinite symmetric groups', *Bull. London Math. Soc.* 18 (1986) 560–586.

4. R. Engelking and M. Karłowicz, 'Some theorems of set theory and their topological consequences', *Fund. Math.* 57 (1965) 275–285.
5. Trevor Evans, 'Embedding theorems for multiplicative systems and projective geometries', *Proc. Amer. Math. Soc.* 3 (1952) 614–620.
6. Fred Galvin, 'Generating countable sets of permutations', *Abstracts Amer. Math. Soc.* 13 (1992) 509.
7. Fred Galvin, 'Embedding countable groups in 2-generator groups', *Amer. Math. Monthly* 100 (1993) 578–580.
8. Fred Galvin, 'On a question of Macpherson and Neumann', *Abstracts Amer. Math. Soc.* 14 (1993) 266.
9. Graham Higman, B. H. Neumann and Hanna Neumann, 'Embedding theorems for groups', *J. London Math. Soc.* 24 (1949) 247–254.
10. F. Levin, 'Factor groups of the modular group', *J. London Math. Soc.* 43 (1968) 195–203.
11. H. D. Macpherson and Peter M. Neumann, 'Subgroups of infinite symmetric groups', *J. London Math. Soc.* (2) 42 (1990) 64–84.
12. A. I. Mal'cev, 'On groups of finite rank', *Mat. Sb.* 22 (64) (1948) 351–352 (in Russian).
13. B. H. Neumann, 'An essay on free products of groups with amalgamations, *Philos. Trans. Roy. Soc. London Ser.* A 246 (1954) 503–554.
14. B. H. Neumann and Hanna Neumann, 'Embedding theorems for groups', *J. London Math. Soc.* 34 (1959) 465–479.
15. Oystein Ore, 'Some remarks on commutators', *Proc. Amer. Math. Soc.* 2 (1951) 307–314.
16. W. R. Scott, *Group theory* (Prentice-Hall, Englewood Cliffs, New Jersey, 1964).
17. W. Sierpiński, 'Sur les suites infinies de fonctions définies dans les ensembles quelconques', *Fund. Math.* 24 (1935) 209–212.
18. 'Composition of functions' (solution of Problem 6244, proposed by John Myhill), *Amer. Math. Monthly* 87 (1980) 676–678.

Department of Mathematics
University of Kansas
Lawrence
Kansas 66045-2142
USA