Proof Delivery Form

Please return this form with your proof

LMS Acceptance No: BLMS 1830

Author(s): George M. Bergman

Typesetting Method: LaTeX

Journal and Article number: BLM 525

Volume and Issue Number: 38(2)

Number of colour figures: Nil

Number of pages (not including this page): 12

Author queries:

Typesetter queries:

Non-printed material:

Bull. London Math. Soc. 38 (2006) 1–12
doi:10.1112/S0024609305005254

GENERATING INFINITE SYMMETRIC GROUPS

GEORGE M. BERGMAN

Abstract

Let $S = \mathrm{Sym}(\Omega)$ be the group of all permutations of an infinite set Ω. Extending an argument of Macpherson and Neumann, it is shown that if U is a generating set for S as a group, then there exists a positive integer n such that every element of S may be written as a group word of length at most n in the elements of U. Likewise, if U is a generating set for S as a monoid, then there exists a positive integer n such that every element of S may be written as a monoid word of length at most n in the elements of U. Some related questions and recent results are noted, and a brief proof is given of a result of Ore's on commutators, which is used in the proof of the above result.

1. *Introduction, notation, and some lemmas on full moieties*

In [**14**, Theorem 1.1], Macpherson and Neumann show that if Ω is an infinite set, then the group $S = \mathrm{Sym}(\Omega)$ is not the union of a chain of $|\Omega|$ or fewer proper subgroups. We will repeat the beautiful proof of that result, with modifications that will allow us to obtain, along with it, the result stated in the abstract. The present section is devoted to obtaining strengthened versions of the lemmas used in that proof.

Following the notation of [**14**], for Ω an infinite set, $\mathrm{Sym}(\Omega)$, generally abbreviated to S, will denote the group of all permutations of Ω, and such permutations will be written to the right of their arguments. For subsets $\Sigma \subseteq \Omega$ and $U \subseteq S$, the symbol $U_{(\Sigma)}$ will denote the set of elements of U that stabilize Σ pointwise, and $U_{\{\Sigma\}}$ is the set $\{f \in U : \Sigma f = \Sigma\}$. (In [**14**] this notation is used only for U a subgroup.) A subset $\Sigma \subseteq \Omega$ will be called *full* with respect to $U \subseteq S$ if the set of permutations of Σ induced by members of $U_{\{\Sigma\}}$ is all of $\mathrm{Sym}(\Sigma)$. The cardinality of a set X will be written $|X|$, and a subset $\Sigma \subseteq \Omega$ will be called a *moiety* if $|\Sigma| = |\Omega| = |\Omega - \Sigma|$.

Suppose that Σ_1 and Σ_2 are moieties of Ω whose intersection is also a moiety, and whose union is all of Ω. Then [**14**, Lemma 2.3] says that if G is a subgroup of $S = \mathrm{Sym}(\Omega)$ such that Σ_1 and Σ_2 are both full with respect to G, then $G = S$. To strengthen this result, we will consider subsets $U, V \subseteq S$, closed under inverses, such that Σ_1 is full with respect to U and Σ_2 with respect to V. By the lemma cited, $\langle U \cup V\rangle = S$; our version of this result will bound the number of factors from U and V needed to obtain the general element of S.

Our proof will use the following fact, first proved by Ore [**18**]. Much stronger results have been proved since. In § 4 we will give a self-contained proof of a statement of intermediate strength.

Lemma 1 [**18**]; cf. § 4 below. *For Ω an infinite set, every element $f \in \mathrm{Sym}(\Omega)$ can be written as a commutator, $f = g^{-1}h^{-1}gh$ $(g, h \in \mathrm{Sym}(\Omega))$.* □

Received 26 July 2004; revised 23 March 2005.

2000 *Mathematics Subject Classification* 20B30 (primary), 20B07, 20E15 (secondary).

Here now is the result on full moieties.

Lemma 2 (cf. [**14**, Lemma 2.3]). *Suppose that Σ_1 and Σ_2 are moieties of Ω whose intersection is a moiety, and whose union is all of Ω; and suppose that U and V are subsets of $S = \mathrm{Sym}(\Omega)$, each closed under inverses, such that Σ_1 is full with respect to U and Σ_2 is full with respect to V. Then $S = (UV)^4V \cup (VU)^4U$.*

Proof. Note that

$$S_{(\Omega-(\Sigma_1\cap\Sigma_2))} \cong \mathrm{Sym}(\Sigma_1 \cap \Sigma_2).$$

By Lemma 1, any element f of the latter group may be written as a commutator $f = g^{-1}h^{-1}gh$. Since Σ_1 is full with respect to U, we can find an element of $U_{\{\Sigma_1\}}$ which behaves like g on $\Sigma_1 \cap \Sigma_2$ and as the identity on $\Sigma_1 - \Sigma_2$; likewise, we can find an element of $V_{\{\Sigma_2\}}$ which behaves like h on $\Sigma_1 \cap \Sigma_2$ and as the identity on $\Sigma_2 - \Sigma_1$. Clearly, the commutator of these elements behaves like f on $\Sigma_1 \cap \Sigma_2$, and as the identity on $\Omega - (\Sigma_1 \cap \Sigma_2)$. Hence

$$S_{(\Omega-(\Sigma_1\cap\Sigma_2))} \subseteq UVUV. \tag{1}$$

Now $|\Sigma_1 \cap \Sigma_2| = |\Omega| = |\Sigma_2 - \Sigma_1|$, where the first equality holds because $\Sigma_1 \cap \Sigma_2$ is a moiety, and the second because $\Sigma_1 = \Omega - (\Sigma_2 - \Sigma_1)$ is one. Hence $\mathrm{Sym}(\Sigma_2)$ contains an element interchanging the subsets $\Sigma_1 \cap \Sigma_2$ and $\Sigma_2 - \Sigma_1$; hence V has an element which behaves that way on Σ_2 (and in an unspecified manner on $\Sigma_1 - \Sigma_2$). Conjugating (1) by such an element, we obtain

$$S_{(\Sigma_1)} \subseteq VUVUVV. \tag{2}$$

Since the assumptions on Σ_1 and Σ_2 are symmetric, we also have the corresponding formula for $S_{(\Sigma_2)}$, with U and V interchanged.

Now suppose that we are given $f \in S$, which we wish to write as a product of elements of U and V.

We shall see, roughly, that a product of one element from U and one element of V suffices to distribute the elements of Ω between Σ_1 and its complement exactly as f does. An application of an element of U will then put the elements that have been moved into Σ_1 in exactly the desired places, and a final application of (2) will administer the *coup de grâce*.

The details are as follows. Note first that the set $(\Sigma_1 \cap \Sigma_2)f^{-1}$ must contain either $|\Omega|$ elements of Σ_1 or $|\Omega|$ elements of Σ_2; without loss of generality, we assume the former. (This is the reason for the word 'roughly' in the preceding paragraph. In the contrary case, the roles stated there for Σ_1 and Σ_2, and likewise for U and V, will be reversed.) In particular, $\Sigma_1 f^{-1}$ contains $|\Omega|$ elements of Σ_1. Hence we can find a permutation $a \in U_{\{\Sigma_1\}}$ which maps all elements of Σ_1 which are not in $\Sigma_1 f^{-1}$ (if any) into $\Sigma_1 \cap \Sigma_2$, and which also maps into that set $|\Omega|$ elements of Σ_1 which *are* in $\Sigma_1 f^{-1}$. These conditions, and the fact that $a \in U_{\{\Sigma_1\}}$ takes $\Omega - \Sigma_1$ to itself, together imply that a maps all elements of $(\Omega - \Sigma_1)f^{-1}$ (both those in Σ_1 and those in $\Omega - \Sigma_1$) into Σ_2, and also takes $|\Omega|$ elements of $\Sigma_1 f^{-1}$ there. We can now choose $b \in V_{\{\Sigma_2\}}$ which maps into $\Omega - \Sigma_1$ the images under a of all elements of $(\Omega - \Sigma_1)f^{-1}$ and nothing else; that is, such that $(\Omega - \Sigma_1)f^{-1}ab = \Omega - \Sigma_1$. Taking complements, we have $\Sigma_1 f^{-1}ab = \Sigma_1$, so as Σ_1 is full with respect to U, we can find $c \in U_{\{\Sigma_1\}}$ which agrees on Σ_1 with the inverse of $f^{-1}ab$; that is, such that $f^{-1}abc \in S_{(\Sigma_1)}$. Now (2), applied to the inverse of the latter element, gives us

$(abc)^{-1}f \in VUVUVV$, so $f \in (UVU)(VUVUVV) = (UV)^4V$. As noted earlier, the roles of U and V may be the opposite of those that we have assumed, giving the alternative possibility that $f \in (VU)^4U$. □

The result from [**14**] that we have just strengthened is used there to show that if a subgroup $G \leqslant S$ has a full moiety, then there exists $x \in S$ such that $\langle G \cup \{x\}\rangle = S$. The version proved above yields the following, more precise, statement.

LEMMA 3 (cf. [**14**, Lemma 2.4]). *If a subset $U \subseteq S$ closed under inverses has a full moiety, then there exists $x \in S$ of order 2 such that $(Ux)^7U^2x \cup (xU)^7xU^2 = S$.*

Proof. Given a full moiety Σ_1 for U, choose any moiety $\Sigma_2 \subseteq \Omega$ such that $\Sigma_1 \cap \Sigma_2$ is a moiety and $\Sigma_1 \cup \Sigma_2 = \Omega$. Since $\Omega - \Sigma_1$ and $\Omega - \Sigma_2$ are disjoint and both have the cardinality of Ω, we can find an element x of order 2 which interchanges those two sets, and hence also interchanges their complements, Σ_1 and Σ_2. The fact that Σ_1 is a full moiety for U makes $\Sigma_2 = \Sigma_1 x$ a full moiety for $x^{-1}Ux = xUx$. Setting $xUx = V$, we may apply the preceding lemma. The expression $(UV)^4V$ becomes $(UxUx)^4xUx = (Ux)^8xUx = (Ux)^7UxxUx = (Ux)^7U^2x$, while the other term is the conjugate of this by x, namely $(xU)^7xU^2$. □

We conclude this section with a diagonal argument, using nothing but the definition of full moiety and basic set theory, which we extract virtually unchanged from the proof of [**14**, Theorem 1.1].

LEMMA 4. *Let Ω be an infinite set, let $S = \mathrm{Sym}(\Omega)$, and let $(U_i)_{i\in I}$ be any family of subsets of S such that $\bigcup_I U_i = S$ and $|I| \leqslant |\Omega|$. Then Ω contains a full moiety with respect to at least one of the U_i.*

Proof. Since $|\Omega|$ is infinite and $I \leqslant |\Omega|$, we can write Ω as a union of disjoint moieties Σ_i $(i \in I)$. If there are no full moieties with respect to U_i for any i, then in particular, for each i the set Σ_i is non-full with respect to U_i, so we can choose $f_i \in \mathrm{Sym}(\Sigma_i)$ which is not the restriction to Σ_i of a member of U_i. Now let $f \in \mathrm{Sym}(\Omega)$ be the permutation whose restriction to each Σ_i is f_i. Then f cannot belong to any of the U_i, contradicting the assumption that $\bigcup_I U_i = S$, and completing the proof. □

2. *Chains of subsets of* Sym(Ω)

Let us begin by recovering [**14**, Theorem 1.1]. Our statement will be the contrapositive of that in [**14**]. (I also include parenthetically the corresponding statement with chains of submonoids in place of chains of subgroups. As we will see, this follows trivially from the result on chains of subgroups, but it took me a long time to discover that trivial argument.)

THEOREM 5 [**14**, Theorem 1.1]. *If Ω is an infinite set and $(G_i)_{i\in I}$ a chain of subgroups (or more generally, submonoids) of $S = \mathrm{Sym}(\Omega)$, with $\bigcup_{i\in I} G_i = S$ and $|I| \leqslant |\Omega|$, then $G_i = S$ for some $i \in I$.*

Proof. Lemma 4 shows that Ω has a full moiety with respect to some G_i. Hence, if we assume that the G_i are subgroups, Lemma 3 shows that $S = \langle G_i \cup \{x\}\rangle$ for some $x \in S$. Since the G_j form a chain with union S, there is some $j \geqslant i$ with $x \in G_j$; hence $G_j \supseteq G_i \cup \{x\}$, and hence $G_j = S$.

If the G_i are merely submonoids, we apply the result of the preceding paragraph to $(G_i \cap G_i^{-1})_{i\in I}$, which is clearly a chain of sub*groups* with union S. □

Now for our new result.

Theorem 6. *Suppose that Ω is an infinite set, and U a generating set for* $\mathrm{Sym}(\Omega)$ *as a group. Then there exists a positive integer n such that every element of* $\mathrm{Sym}(\Omega)$ *is represented by a group word of length at most n in the elements of U. Likewise, if U is a generating set for* $\mathrm{Sym}(\Omega)$ *as a monoid, there exists a positive integer n such that every element of* $\mathrm{Sym}(\Omega)$ *is represented by a monoid word of length at most n in the elements of U.*

Proof. Here it suffices to prove the monoid case, since the group words in the elements of U are just the monoid words in the elements of $U \cup U^{-1}$.

So we assume that U generates S as a monoid. For $i = 1, 2, \ldots$, let $U_i = (U \cup \{1\})^i \cap (U^{-1} \cup \{1\})^i$. By assumption, the sets $(U \cup \{1\})^i$ have union S; hence so do their inverses, $(U^{-1} \cup \{1\})^i$, and hence so do the intersections U_i. Since $\aleph_0 \leqslant |\Omega|$, Lemma 4 says that Ω has a full moiety with respect to some U_i. By Lemma 3 there exists $x \in S$ such that $S = (U_i x)^7 U_i^2 x \cup (x U_i)^7 x U_i^2$, which we see is contained in $(U_i \cup \{x\})^{17}$. Taking a $j \geqslant i$ such that $x \in U_j$, we get

$$(U \cup \{1\})^{17j} = ((U \cup \{1\})^j)^{17} \supseteq (U_i \cup \{x\})^{17} = S. \qquad \square$$

One may ask whether, for a given set Ω, there is some single n as in Theorem 6 that works for every generating set U. To see that this is not so, let $\Omega = \mathbb{Q}/\mathbb{Z}$, and let us give this set the natural metric, of diameter $1/2$, under which the distance between two cosets of $\mathbb{Z}$ is the minimum of the distances between their members, as real numbers. (In other words, let us use the metric on $\Omega = \mathbb{Q}/\mathbb{Z}$ induced by the arc-length metric on $\mathbb{R}/\mathbb{Z}$.) Fixing an integer n, let U denote the set of permutations of Ω which move all elements by distances less than $1/(2n)$. Clearly, $U^n \neq \mathrm{Sym}(\Omega)$. However, I claim that U is a generating set for $\mathrm{Sym}(\Omega)$ as a group (and indeed, since it is closed under inverses, as a monoid).

Note first that if Σ is the image in Ω of any interval of length less than $1/(2n)$ in $\mathbb{Q}$, then U contains $S_{(\Omega-\Sigma)}$, the group of permutations that act arbitrarily on Σ and fix all elements outside it. Now we can cover Ω with a finite number of successive overlapping sets $\Sigma_1, \Sigma_2, \ldots, \Sigma_r$ of this sort, and then use Lemma 2 to conclude inductively that $\langle U\rangle \supseteq S_{(\Omega-(\Sigma_1\cup\ldots\cup\Sigma_i))}$ for $i = 1, \ldots, r$, and hence that $\langle U\rangle \supseteq S_{(\Omega-(\Sigma_1\cup\ldots\cup\Sigma_r))} = S_{(\varnothing)} = S$, as claimed.

3. *Questions, examples, remarks, and related literature*

The statement of [**14**, Theorem 1.1] (equal to Theorem 5 above), unlike that of Theorem 6, depends on the cardinal $|\Omega|$. Let us, for the purposes of this section, weaken that statement to one that holds independently of this cardinal, by using the obvious lower bound $\aleph_0 \leqslant |\Omega|$. Then that theorem can be looked at as saying, for every infinite set Ω, that $\mathrm{Sym}(\Omega)$ belongs to the class of groups G satisfying the following condition.

$$\text{If } G \text{ is written as the union of a chain of subgroups } G_0 \leqslant G_1 \leqslant \ldots \text{ indexed by } \omega, \text{ then for some } n,\ G_n = G. \tag{3}$$

Theorem 6, similarly, says that $\mathrm{Sym}(\Omega)$ belongs to the class of groups G satisfying the next condition.

$$\text{If } G \text{ is generated as a group by a subset } U, \text{ then for some } n, \text{ every element of } G \text{ is represented by a group word of length at most } n \text{ in the elements of } U. \tag{4}$$

Clearly, (3) also holds for all finitely generated groups, and (4) for all finite groups. Thus, in a strange way, the groups $\mathrm{Sym}(\Omega)$ resemble finite groups.

Condition (3) on a non-finitely-generated group is commonly expressed by saying that G has *uncountable cofinality*, and is known to hold in many cases. Some works on cofinalities of groups are [**5**], [**9**], [**13**], [**19**], [**22**] and [**21**]; see also other papers cited in [**9**]. Whether or not G is finitely generated, (3) is equivalent to the condition that the fixed point set construction on G-sets commutes with direct limits over countable index sets [**1**, end of §2]. In fact, it was the wish to give in [**1**] an example of a non-finitely-generated group having this property that led me to read [**14**], eventually resulting in this note. The analog of condition (3) for modules has been studied under many different names; cf. [**11**, p. 895, top paragraph].

In response to a question posed in an earlier version of this note, Droste and Göbel [**9**] have obtained a general technique for showing that certain sorts of structures containing many isomorphic copies of themselves have automorphism groups satisfying (3) and (4); in particular, they find that (3) and (4) hold for the groups of all self-homeomorphisms of the Cantor set, of the rational numbers, and of the irrational numbers, and for the group of Borel automorphisms of the real numbers. Droste and Holland [**10**] obtain the same conclusions for the automorphism group of any doubly homogeneous totally ordered set, and Tolstykh [**23**, **24**] proves (4), and (insofar as it was not already known) (3), for the automorphism groups of infinite-dimensional vector spaces and various sorts of relatively free groups. In the final remark of [**23**] he suggests an approach to showing that the full automorphism groups of free objects in other well-behaved varieties of algebras have this property. Mesyan [**15**] obtains analogous results for endomorphism rings of infinite direct sums and products of a module, and Cornulier [**6**, Proposition 4.4] does the same for the Boolean ring of subsets of an infinite set; he also shows in [**6**, Theorem 3.1] that any ω_1-existentially closed group satisfies (3) and (4).

Let us note some general facts about conditions (3) and (4). It is not hard to see that both properties are preserved under taking homomorphic images, and that (3) is also preserved under group extensions and under passing to groups finitely generated over G. To get some similar results for (4), we will require the following lemma.

Lemma 7. *Let $H < G$ be groups and U a generating set for G. Suppose that for some $n \geqslant 0$, every right coset of H in G contains a group word of length at most n in the elements of U. Then the set of elements of H that can be written as words of length at most $2n+1$ in the elements of U generates H.*

Proof. Let V be a set of right coset representatives for H in G consisting of words of length at most n in U, with the coset H represented by the element 1, and let $r : G \to V$ be the retraction collapsing each coset to its representative. Let W denote the set of elements of H that can be written as words of length at most $2n+1$ in the elements of U.

For any $v \in V$ and $u \in U \cup U^{-1}$, note that $vu = (vu\, r(vu)^{-1}) r(vu)$. Since $r(vu)$ by definition lies in the same right coset as vu, the factor $vu\, r(vu)^{-1}$ lies in H, and since v and $r(vu)$, as members of V, each have length at most n in the elements of U, that factor has length at most $2n+1$, and so lies in W. Thus, $V(U \cup U^{-1}) \subseteq WV$. It follows that $\bigcup_i W^i V$ is closed under right multiplication by $U \cup U^{-1}$, and hence equals the whole group G. We now intersect the equation $\bigcup_i W^i V = G$ with H. This has the effect of discarding elements on the left-hand side having right factors from V other than 1, and so gives $\bigcup_i W^i = H$, completing the proof. □

We can now show that (4) is preserved under group extensions. Given a short exact sequence $1 \to H \to G \to E \to 1$ where H and E satisfy (4), and a generating set U for G, the fact that E satisfies (4) yields an n as in the hypothesis of Lemma 7. The conclusion of that lemma, combined with the fact that H satisfies (4), shows that all elements of H can be written as words of length at most m in the elements of U for some m. It follows that all elements of G can be written as words of length at most $n+m$. A similar application of that lemma shows that (4) is preserved under passing to overgroups in which G has finite index.

Clearly, a countable group satisfies (3) if and only if it is finitely generated, while an infinite group that is finitely generated can never satisfy (4). In particular, (4) is not preserved under passing to groups finitely generated over G. Neither property is preserved under passing to normal subgroups, since for Ω a countably infinite set, the subgroup of $\mathrm{Sym}(\Omega)$ consisting of permutations that move only finitely many elements is normal, but satisfies neither (3) nor (4).

In response to a question posed in an earlier version of this paper, Khelif has announced in [**12**] that (3), and also the conjunction of (3) and (4), are preserved under passing to subgroups of finite index, but that (4) alone is not.

A question that, to my knowledge, is still unanswered is the following.

Question 8. Are there any countably infinite groups that satisfy (4)?

One can show that every non-finitely-generated abelian group can be mapped surjectively either onto a group Z_{p^∞}, or onto an infinite direct sum $Z_{p_1} \oplus Z_{p_2} \oplus \dots$ for (not necessarily distinct) prime numbers $p_1, p_2, \dots$. Neither of the latter sorts of groups satisfy (3) or (4), so no non-finitely-generated abelian group has either of these properties.

It is shown in [**13**] that the direct product of any family of copies of a nonabelian finite simple group satisfies (3). In [**6**, §4] this is strengthened to say that the direct product of any family of copies of a finite perfect group satisfies (3) and (4), while [**9**, Lemma 3.5] shows that the same is true of the direct product of any family of copies of $\mathrm{Sym}(\omega)$. These results suggest the general question of when (3) and (4) are inherited by products. They are both inherited by finite products, by our observations on group extensions. That they are not always inherited by infinite products is shown by any infinite direct product of nontrivial finite abelian groups: the factors, as finite groups, satisfy both conditions, but the product, a non-finitely-generated abelian group, satisfies neither. The same technique can be used to show the failure of these conditions for certain direct products of perfect groups, using the fact that an infinite product of perfect groups may be non-perfect. Khelif has announced the existence of a direct product of groups such that each factor satisfies (4) and the product is perfect but which still does not satisfy (4).

We saw in the proof of Theorem 5 that (3) implies the corresponding condition with 'subgroups' replaced by 'submonoids'. The same implication for the negations of these conditions is clear, and so the group and monoid versions of (3) are equivalent. For (4), the proof of Theorem 6 shows that the statement for generation as a monoid implies the statement for generation as a group. In this case, we can also get the converse *if* we assume (3). For suppose that the group G satisfies (3) and (4), and that U is a generating set for G as a monoid. As in the proof of Theorem 6, let $U_i = (U \cup \{1\})^i \cap (U^{-1} \cup \{1\})^i$ $(i \in \omega)$. These sets form a chain with union G; hence so do the subgroups $\langle U_i \rangle$, and hence by (3), some $\langle U_j \rangle$ is equal to G; so by (4), there is an n such that all elements of G are group words of length at most n in elements of U_j. By construction, U_j is closed under inverses, so these group words reduce to monoid words, so

$$G = (U_j)^n \subseteq ((U \cup \{1\})^j)^n = (U \cup \{1\})^{jn},$$

as claimed. However, the results announced in [**12**] on subgroups of finite index imply that there are groups satisfying (4) but not (3), leading to our next question.

Question 9. Among groups satisfying (4) but not (3), are there any which do not satisfy the analog of (4) obtained by replacing 'generated as a group' and 'group word' with 'generated as a monoid' and 'monoid word'? Are there any which *do* satisfy that condition?

We saw at the end of §2 that though $\mathrm{Sym}(\Omega)$ satisfies (4), there is no single n that works for all generating sets U. On the other hand, Shelah [**20**] constructs an uncountable group G in which every generating set U satisfies $U^{240} = G$.

We record two easy reformulations of the conjunction of (3) and (4).

Lemma 10. *For any group G, the following conditions are equivalent.*

(i) *G satisfies both* (3) *and* (4).

(ii) *If $U_0 \subseteq U_1 \subseteq \ldots \subseteq U_i \subseteq \ldots$ is a chain of subsets of G, indexed by the natural numbers and having union G, such that $U_i = (U_i)^{-1}$ for all i, and such that for all i, j there exists some k with $U_i U_j \subseteq U_k$, then some U_i is equal to G.*

(iii) *If L is a natural-number-valued function on G such that for all $g, h \in G$ one has $L(g^{-1}) = L(g)$ and $L(gh) \leqslant L(g) + L(h)$, then L is bounded above.* □

Functions L as in (iii) above are studied in geometric group theory. (Further conditions are generally assumed, in particular, that the number of $g \in G$ with $L(g) \leqslant n$ is finite and grows at most exponentially in n. Under this assumption, L is known to be approximable by the function giving the length of g with respect to some finite generating set of an overgroup of G; see [**17**]. Of course, such a finiteness condition cannot be satisfied when G is an uncountable group such as we are considering here.) In [**6**, §2], condition (iii) above is translated as saying that every isometric action of G on a metric space has bounded orbits, and it is deduced that isometric actions of G on certain sorts of metric spaces must in fact have fixed points.

A property of finite groups G that does *not* hold for the groups $\mathrm{Sym}(\Omega)$ is as follows.

$$\text{Every subset of } U \subseteq G \text{ which generates } G \text{ as a group generates } G \text{ as a monoid.} \tag{5}$$

To see the failure of (5) in $\mathrm{Sym}(\Omega)$ for countable Ω, we may take for U a submonoid M as in the next result.

LEMMA 11. *Let Ω be any countable totally ordered set without least or greatest element, and let M be the monoid $\{g \in \mathrm{Sym}(\Omega) : (\forall \alpha \in \Omega)\ \alpha g \geqslant \alpha\}$.*
Then $\mathrm{Sym}(\Omega) = MM^{-1}M$.

Proof. Given $f \in \mathrm{Sym}(\Omega)$, I claim that we can find $g, h \in \mathrm{Sym}(\Omega)$ such that for all $\alpha \in \Omega$,

$$\alpha \leqslant \alpha g \geqslant \alpha h \leqslant \alpha f. \tag{6}$$

From this it will follow that $g,\ h^{-1}g,\ h^{-1}f \in M$, whence

$$f = g(h^{-1}g)^{-1}(h^{-1}f) \in MM^{-1}M,$$

as desired.

To find g and h satisfying (6), let an enumeration of the elements of Ω be chosen. (We will not introduce a notation for this enumeration, but simply speak of 'the first element with respect to our enumeration such that ...'. In particular, '$\leqslant$' will continue to denote the given ordering of Ω, not the ordering corresponding to our enumeration.) We shall now construct recursively for each $i \in \omega$ a 3-tuple $(\alpha_i, \beta_i, \gamma_i)$ of elements of Ω; these will eventually be the 3-tuples $(\alpha, \alpha g, \alpha h)$ $(\alpha \in \Omega)$.

To define $(\alpha_i, \beta_i, \gamma_i)$, let us, if i is divisible by 3, take for α_i the first element of Ω with respect to our enumeration which has not been chosen as α_j at any previous step (that is, for $0 \leqslant j < i$), let us then take for β_i any element of Ω which was not chosen as β_j at a previous step and which is $\geqslant \alpha_i$, and for γ_i any element not chosen as γ_j at a previous step which is both $\leqslant \beta_i$ and $\leqslant \alpha_i f$. On the other hand, if $i \equiv 1 \pmod 3$, we start by taking for β_i the first element of Ω with respect to our enumeration which was not chosen as β_j at any previous step, then take for α_i any element not previously chosen as an α_j which is $\leqslant \beta_i$, and for γ_i any element not previously chosen as a γ_j which is both $\leqslant \beta_i$ and $\leqslant \alpha_i f$. Finally, when $i \equiv 2 \pmod 3$, we take for γ_i the first element with respect to our enumeration that has not yet been used as a γ_j, for α_i any element not previously chosen as an α_j such that $\alpha_i f \geqslant \gamma_i$ (which is possible because there are infinitely many elements $\geqslant \gamma_i$), and for β_i any element not previously chosen in that role which is both $\geqslant \alpha_i$ and $\geqslant \gamma_i$.

Clearly, this construction uses each element of Ω once and only once in each position; hence the set of pairs (α_i, β_i) is the graph of a permutation $g \in \mathrm{Sym}(\Omega)$, and the set of pairs (α_i, γ_i) is the graph of a permutation $h \in \mathrm{Sym}(\Omega)$. The conditions that we imposed on our choices at each step ensure that (6) holds. □

(In the above lemma we can drop the countability assumption, if we replace the hypothesis of no least or greatest element by the assumption that each element of Ω has $|\Omega|$ elements above it and $|\Omega|$ elements below it. The assumption that the ordering is total can also be weakened to say that it is upward and downward directed.)

It would be interesting to know what sorts of groups satisfy (5), other than those whose elements all have finite order. One such group is the infinite dihedral group.

My first attempts to prove the statements about sub*monoids* of S in Theorems 5 and 6 revolved around trying to remove from Lemmas 2 and 3 the hypotheses on closure under inverses. Those hypotheses are required by our proof of Lemma 2, since inverses are needed to form commutators and conjugates. Though a different method eventually gave the monoid cases of those theorems, it would still be interesting to know the answer to the following question.

QUESTION 12. Are versions of Lemma 2 and/or 3 (possibly using longer products of x, U and V) true without the hypothesis that U and V are closed under inverses?

We shall note a weak result in this direction at the end of the next section.

We remark, finally, that it is easy to adapt the method of proof of Theorem 5 to give an apparently more general statement, in which the *chain* of subgroups G_i indexed by a set I of cardinality at most $|\Omega|$ is replaced by any *directed system* of subgroups G_i indexed by such a set, again having S as union. However, that result in fact follows easily from the theorem as stated. For, given such a directed system, let $\{G_i : i \in \kappa\}$ be a subset thereof whose union generates S, having least cardinality κ among such subsets, and indexed by that cardinal. Then $\{\langle \bigcup_{i<j} G_i \rangle : j < \kappa\}$ forms a chain of *proper* subgroups of S, which, unless κ is finite, will have union S. This would contradict Theorem 5; so κ is finite, and the finite family $\{G_i : i \in \kappa\}$ will be majorized by a member of the original directed system, which thus equals S.

Further results on the groups $\mathrm{Sym}(\Omega)$ are given in [**3**].

Note added July 2005. It is shown in [**2**, Section 6] that $S = \mathrm{Sym}(\Omega)$ has the property that its countable direct power S^ω is finitely generated over the diagonal image $\Delta(S) \subseteq S^\omega$, and that this property (for general finitary algebras in the sense of universal algebra, and for groups in particular) is strictly stronger than the conjunction of (3) and (4).

4. *Appendix: Writing every element of* Sym(Ω) *as a commutator*

In proving Lemma 2, we called on the result of [**18**] that every element of an infinite symmetric group is a commutator. Now a commutator is an element obtained by dividing an element by a conjugate, $(g^{-1}hg)^{-1}h$; moreover, it is clear that in a symmetric group, every element is conjugate to its inverse, so a commutator in a symmetric group can be described as a product of two elements in the same conjugacy class. Almost a decade after [**18**] appeared, it was shown that in an infinite symmetric group there in fact exist single conjugacy classes whose square is the whole group. In a series of papers by several authors, culminating in [**16**] (which describes this history), the conjugacy classes having this property were precisely characterized.

We shall give a self-contained proof of this property for one such conjugacy class in Lemma 14 below, and then use the fact that $\mathrm{Sym}(\Omega)$ is the square of a conjugacy class to obtain a result related to Question 12.

Definition 13. For Ω an infinite set, we shall call an element $f \in \mathrm{Sym}(\Omega)$ *replete* if it has $|\Omega|$ orbits of each positive cardinality $\leqslant \aleph_0$ (including 1). For a subset $\Sigma \subseteq \Omega$ of cardinality $|\Omega|$, we shall say that f is replete on Σ if $\Sigma f = \Sigma$ and the restriction of f to Σ is a replete permutation of Σ.

Note that a permutation of Ω that is replete on a subset $\Sigma \subseteq \Omega$ of cardinality $|\Omega|$ is necessarily replete on Ω.

The replete permutations of Ω clearly form a conjugacy class, so it will suffice to prove the next lemma.

Lemma 14. *Every permutation f of an infinite set Ω is the product of two replete permutations.*

Proof. Given f, let us choose a moiety Σ_0 of Ω such that f moves only finitely many elements from Σ_0 to $\Omega - \Sigma_0$ or from $\Omega - \Sigma_0$ to Σ_0. That there exists such a Σ_0 is immediate if Ω is uncountable, for we can break Ω into two families of $|\Omega|$ orbits each, and take for Σ_0 the union of one of these families. If Ω is countable, then we can use the same method if f has infinitely many orbits, and can also obtain the same conclusion in an obvious way if f has more than one infinite orbit. If it has exactly one infinite orbit, $\alpha_0\langle f\rangle$, and finitely many finite orbits, then we can take $\Sigma_0 = \{\alpha_0 f^n : n \leqslant 0\}$; clearly, f moves exactly one element out of Σ_0, and none into it.

After choosing Σ_0, let us split $\Omega - \Sigma_0$ into two disjoint moieties Σ_1 and Σ_2, so that Σ_1 contains the finitely many elements of $(\Sigma_0 f \cup \Sigma_0 f^{-1}) - \Sigma_0$. I claim that if g_0 is any permutation of Σ_0, and g_2 is any permutation of Σ_2, then there exists a permutation h of Ω such that fh agrees on Σ_0 with g_0, while h agrees on Σ_2 with g_2. Indeed, this pair of conditions specifies the values of h on the two disjoint sets $\Sigma_0 f$ and Σ_2 in a one-to-one fashion, and both the set on which it leaves h unspecified and the set of elements that it does not specify as values for h are of cardinality $|\Omega|$. Hence the former set can be mapped bijectively to the latter, and the resulting bijection will serve to complete the definition of h. (We have used Σ_1 as a 'Hilbert's hotel' in the case $\Sigma_0 f \neq \Sigma_0$.)

Now if we take for g_0 and g_2 replete permutations of Σ_0 and Σ_2 respectively, then h will be replete on Σ_2, and hence replete, while fh will be replete on Σ_0, and hence replete. Thus $f = (fh)h^{-1}$ is a product of two replete permutations, as we wished to show. □

(In [**8**, Theorem 3.1(a)] the same result is proved for a different conjugacy class, that of permutations with $|\Omega|$ infinite orbits and no finite orbits, also by an unexpectedly simple argument. However, it takes some work to isolate that argument from the lengthier proofs of other results that are being carried out there simultaneously. A different sort of generalization of Ore's result is obtained in [**7**] and papers cited there, which characterize the group words w which are 'universal' in infinite permutation groups, in the sense established for the word $x^{-1}y^{-1}xy$ by Ore's result.)

We shall now show that the proofs of Lemmas 2 and 3 can be adapted to the situation where U and V are not assumed closed under inverses if we allow ourselves to use, along with multiplication, the right conjugation operation

$$g^h = h^{-1}gh. \tag{7}$$

LEMMA 15 (cf. Lemma 3). *Let Ω be an infinite set, and $U \subseteq S = \mathrm{Sym}(\Omega)$ a subset with respect to which some moiety of Ω is full. Then there exist $x, y \in S$, with x of order 2, such that*

$$S = (Ux)^3(y^U)^2x \cup x(Ux)^3(y^U)^2. \tag{8}$$

Sketch of proof. Let Σ_1 be a full moiety for U, let Σ_2 be a moiety such that $\Sigma_1 \cap \Sigma_2$ is a moiety and $\Sigma_1 \cup \Sigma_2 = \Omega$, let $x \in S$ be an involution such that $\Sigma_1 x = \Sigma_2$, and let $y \in S_{(\Sigma_2)}$ be an element such that the group $S_{(\Sigma_2)} \cong \mathrm{Sym}(\Omega - \Sigma_2)$ is the square of the conjugacy class of y in that group. Such a y exists by Lemma 14 above, or by the results in the papers cited. Combining this property of y with the fact that Σ_1, and hence its subset $\Omega - \Sigma_2$, is full with respect to U, we conclude that $S_{(\Sigma_2)} \subseteq (y^U)^2$; hence, conjugating by x,

$$S_{(\Sigma_1)} \subseteq x(y^U)^2x. \tag{9}$$

Now let $V = xUx$.Since Σ_1 is a full moiety under U, Σ_2 will be a full moiety under V. Using the technique of proof of Lemma 2, with (9) in place of (2), we get (8). □

Acknowledgements. I am grateful to Peter Biryukov, Manfred Droste, Dugald Macpherson, Gadi Moran, Peter Neumann and Marc Rieffel for helpful information on the relevant literature.

References

1. G. M. BERGMAN, 'Direct limits and fixed point sets', *J. Algebra*, to appear; preprint, June 2003, 28 pp., http://math.berkeley.edu/~gbergman/papers/dirlimfix.{tex,dvi,ps}, arXiv:math.CT/0306127.

2. G. M. BERGMAN, 'Two statements about infinite products that are not quite true', preprint, July 2005, 16 pp., http://math.berkeley.edu/~gbergman/papers/P_vs_cP.{tex,dvi,ps,pdf}.

3. G. M. BERGMAN and S. SHELAH, 'Closed subgroups of the infinite symmetric group', *Algebra Universalis*, issue in honor of Walter Taylor, to appear; preprint, http://math.berkeley.edu/~gbergman/papers/Sym_Omega:2.{tex,dvi,ps}, or publication 823 at http://shelah.logic.at, arXiv:math.GR/0401305.

4. S. BIGELOW, 'Supplements of bounded permutation groups', *J. Symbolic Logic* 63 (1998) 89–102; MR 99b:20007.

5. P. BIRYUKOV, 'Automorphism groups of homogeneous Boolean spaces', preprint, 14 pp., http://mmedia2.kemsu.ru/people/person.xsql.en?aid=122.

6. Y. DE CORNULIER, 'Strongly bounded groups and infinite powers of finite groups', *Comm. Algebra*, to appear; preprint, 8 pp., http://www.eleves.ens.fr/home/decornul/FHpasT3.pdf, arXiv/math.GR/0411466.

7. R. DOUGHERTY and J. MYCIELSKI, 'Representations of infinite permutations by words. II', *Proc. Amer. Math. Soc.* 127 (1999) 2233–2243; MR 99j :20002.

8. M. DROSTE, 'Classes of universal words for the infinite symmetric groups', *Algebra Universalis* 20 (1985) 205–216; MR 87d:20049.

9. M. DROSTE and R. GÖBEL, 'Uncountable cofinalities of permutation groups', *J. London Math. Soc.* (2) 71 (2005) 335–344; MR 2122432.

10. M. DROSTE and W. C. HOLLAND, 'Generating automorphism groups of chains', *Forum Math.* 17 (2005) 699–710.

11. R. EL BASHIR, T. KEPKA and P. NĚMEC, 'Modules commuting (via Hom) with some colimits', *Czechoslovak Math. J.* 53 (128) (2003) 891–905; MR 2004i:16002.

12. A. KHELIF, 'A propos de la propriété de Bergman', announcement, Université Paris 7, June 2005, 4 pp. (superseding an earlier 1-page announcement: 'On the Bergman property').

13. S. Koppelberg and J. Tits, 'Une propriété des produits directs infinis de groupes finis isomorphes', *C. R. Acad. Sci. Paris Sér. A* 279 (1974) 583–585; MR 51#13058.

14. H. D. Macpherson and P. M. Neumann, 'Subgroups of infinite symmetric groups', *J. London Math. Soc.* (2) 42 (1990) 64–84; MR 92d:20006. (Note: It is pointed out in [**4**] that Theorem 1.2 of this paper requires additional set-theoretic hypotheses for some κ.)

15. Z. Mesyan, 'Generating endomorphism rings of infinite direct sums and products of modules', *J. Algebra* 283 (2005) 364–366; MR 2005g:16057.

16. G. Moran, 'Conjugacy classes whose square is an infinite symmetric group', *Trans. Amer. Math. Soc.* 316 (1989) 493–522; MR 91a:20005.

17. A. Yu. Ol'shanskii, 'Distortion functions for subgroups', *Geometric group theory down under* (Canberra, 1996) (de Gruyter, Berlin, 1999) 281–291; MR 2000j:20077.

18. O. Ore, 'Some remarks on commutators', *Proc. Amer. Math. Soc.* 2 (1951) 307–314; MR 12,671e.

19. G. Sabbagh, 'Sur les groupes que ne sont pas réunion d'une suite croissante de sous-groupes propres', *C. R. Acad. Sci. Paris Sér. A–B* 280 (1975) A763–A766; MR 51#3270.

20. S. Shelah, 'On a problem of Kurosh, Jónsson groups, and applications', *Word problems, II*, Conf. on Decision Problems in Algebra, Oxford, 1976, Stud. Logic Found. Math. 95 (North-Holland, Amsterdam/New York, 1980) 373–394; MR 81j:20047.

21. S. Thomas, 'Cofinalities of infinite permutation groups', *Advances in algebra and model theory* (Essen, 1994; Dresden, 1995), Algebra Logic Appl. 9 (Gordon and Breach, Amsterdam, 1997) 101–120; MR 2000a:20005.

22. S. Thomas, 'The cofinalities of the infinite-dimensional classical groups', *J. Algebra* 179 (1996) 704–719; MR 96k:20005.

23. V. Tolstykh, 'Infinite-dimensional general linear groups are groups of universally finite width', preprint, March 2004, 6 pp., arXiv:math.GR/0403223.

24. V. Tolstykh, 'On Bergman's property for the automorphism groups of relatively free groups', preprint, June 2004, 14 pp., arXiv:math.GR/0406586.

George M. Bergman
Department of Mathematics
University of California
Berkeley, CA 94720-3840
USA

gbergman@math.berkeley.edu