TRANSVERSALS AS GENERATING SETS IN FINITELY GENERATED GROUPS

JACK BUTTON, MAURICE CHIODO✉ **and MARIANO ZERON-MEDINA LARIS**

Abstract

We explore transversals of finite index subgroups of finitely generated groups. We show that when H is a subgroup of a rank-n group G and H has index at least n in G, we can construct a left transversal for H which contains a generating set of size n for G; this construction is algorithmic when G is finitely presented. We also show that, in the case where G has rank $n \leq 3$, there is a simultaneous left–right transversal for H which contains a generating set of size n for G. We finish by showing that if H is a subgroup of a rank-n group G with index less than $3 \cdot 2^{n-1}$, and H contains no primitive elements of G, then H is normal in G and $G/H \cong C_2^n$.

1. Introduction

Let H be a subgroup of G (written $H < G$). A *left* (respectively, *right*) *transversal* for H in G is a choice of exactly one representative from each left (respectively, right) coset of H. A *left–right* transversal for H is a set S which is simultaneously a left and a right transversal for H in G. The existence of a left or right transversal for subgroups of finitely generated groups is clear, and for general groups this condition is equivalent to the Axiom of Choice [1, Theorem 2.1]. However, it is not obvious that a left–right transversal always exists. We gave a short proof of this in [3] for the case where H is of finite index, as well as a brief historical discussion of this result.

Transversals are natural objects of study, especially when the index $[G : H]$ is finite. Moreover, finding generating sets for a group G is a well-known problem in the case where G is finitely generated. Therefore we ask: given a finitely generated group G and a finite index subgroup H of G, is there a (say) left transversal for H in G which also generates G? Jain asked Cameron this question under the added assumption

that G is a finite group and H is corefree in G, meaning that $\mathrm{core}_G(H) = \{e\}$ (where $\mathrm{core}_G(H) := \bigcap_{g \in G} g^{-1} H g$). Cameron showed in [4] that in this case a generating left transversal always exists (see also [5, Problem 100]). The proof is short but relies on a result of Whiston [13] on *minimal* generating sets (ones where no proper subset generates) of the symmetric group which uses the classification of finite simple groups.

A necessary condition for a subgroup $H < G$ to possess a generating left transversal is that $[G : H]$ must be at least $d(G)$ (the *rank* of G), defined to be the minimal number of generators for the finitely generated group G. In Theorem 3.7 we show that this condition is also sufficient, for G any finitely generated group and H any subgroup of finite index. We then try to strengthen this result by examining whether $[G : H] \geq d(G)$ implies that there exists a left–right transversal for H that generates G. We have not managed to establish this in general but we have shown in Theorem 3.11 that it is true if $d(G) \leq 3$.

Our main method of proof in Section 3 is a new technique which we call *shifting boxes*. It involves using the transitive action of a group G on the set of left (or right) cosets of a subgroup $H < G$ to systematically apply Nielsen transformations to a generating set of G, such that the resulting generators lie inside (or outside) particular desired cosets of H. We have found this technique to be very intuitive for developing proofs. Many of our results can be reduced to the case of subgroups of free groups (Proposition 3.13). An element of a rank-n group G is *primitive* if it lies in some generating set of size n for G. The location of primitive elements relative to cosets of subgroups is already an area of interest. Parzanchevski and Puder [11] show that if $w \in F_n$ is a nonprimitive element then there is a finite index subgroup $H < F_n$ such that the coset wH does not contain any primitive elements. Taking $w = e$ gives a finite index subgroup containing no primitive elements.

By applying the technique of shifting boxes developed in Section 3, we show in Theorem 4.4 that, if G is a rank-n group, then the only subgroup of G with index less than $3 \cdot 2^{n-1}$ that can contain *no* primitive elements is $[G,G]G^2$, and even then this only occurs when $G/([G,G]G^2) \cong C_2^n$. This gives an exponential lower bound on the index of subgroups which contain no primitive elements. We first announced many of the results of this paper in [2].

2. Coset intersection graphs

A useful tool for studying the way left and right cosets interact, and obtaining transversals, is the coset intersection graph. In this section we restate important results from our earlier work [3] on this concept. We denote the complete bipartite graph on (m, n) vertices by $\mathbf{K}_{m,n}$.

DEFINITION 2.1. Let $H, K < G$. We define the *coset intersection graph* $\Gamma_{H,K}^G$ as the graph with vertex set consisting of all left cosets of H ($\{l_i H\}_{i \in I}$) and all right cosets of K ($\{K r_j\}_{j \in J}$), where I, J are index sets. If a left coset of H and right coset of K correspond, they are still included twice. Edges (undirected) are included whenever any two of these cosets intersect, and an edge between aH and Kb (written $aH - Kb$) corresponds to the nonempty set $aH \cap Kb$.

THEOREM 2.2. *Let $H, K < G$. Then the graph $\Gamma^G_{H,K}$ is a disjoint union of complete bipartite graphs. If $[G : H] = n$, $[G : K] = m$, then each connected component of $\Gamma^G_{H,K}$ is of the form $\mathbf{K}_{s_i, t_i}$ with $s_i/t_i = n/m$.*

COROLLARY 2.3. *Let $H, K < G$. Suppose that $[G : H] = n$ and $[G : K] = m$, where $m \geq n$. Then there exists a set $T \subseteq G$ which is a left transversal for H in G, and which can be extended to a right transversal for K in G. If $H = K$ in G, then T becomes a left–right transversal for H.*

Under the hypothesis of Theorem 2.2, we see that sets of s_i left cosets of H completely intersect sets of t_i right cosets of K, with s_i/t_i constant over i. With this in mind, another way of visualising $\Gamma^G_{H,K}$ is by the following simultaneous double-partitioning G: draw left cosets of H as columns, and right cosets of K as rows, partitioning G into irregular 'chessboards' denoted C_i, each with edge ratio $n : m$. Each chessboard C_i corresponds to the connected component $\mathbf{K}_{s_i, t_i}$ of $\Gamma^G_{H,K}$, and individual tiles in C_i correspond to the nonempty intersection of a left coset of H and a right coset of K (that is, edges in $\mathbf{K}_{s_i, t_i}$). Corollary 2.3 then follows by choosing one element from each tile on the leading diagonals of the C_i. An example of chessboards is given in [3].

The chessboard pictorial representation of partitioning G into left and right cosets is extremely useful in the analysis of transversals as generating sets in the next section. Note that the union of all the elements of G in a single chessboard gives a unique double coset KgH in G, and that a single chessboard is simply a double-partitioning of a double coset KgH into its respective left cosets of H and right cosets of K.

3. Transversals as generating sets

We have developed a technique which we call *shifting boxes* which, for the sake of brevity, we will describe here as a systematic way to apply Nielsen transformations to a generating set of a group G, such that the resulting generators lie inside (or outside) particular desired cosets of a subgroup $H < G$. We cannot 'shift' generators in/out of any coset we like, but we do have a substantial degree of control. For ease of notation, we will often refer to the coset eH as the *identity coset*. We begin with the following definitions.

DEFINITION 3.1. Let G be a group. Let $S := (g_1, \ldots, g_n)$ be a *generating n-tuple* of G (where $n \in \mathbb{N}$), that is, an element of the direct product G^n such that $\{g_1, \ldots, g_n\}$ generates G. A *standard Nielsen move* on S is the replacement of some entry g_i of S with one of $g_j g_i, g_j^{-1} g_i, g_i g_j$ or $g_i g_j^{-1}$, where we must have $i \neq j$. A *Nielsen move* is defined to be either a standard Nielsen move or an *extended Nielsen move*, where the latter consists of either replacing an entry g_i by its inverse, or transposing two entries g_i and g_j for $i \neq j$. Note that on applying any Nielsen move to S, the resulting n-tuple still generates G. Two generating n-tuples S_1, S_2 of G are said to be *Nielsen equivalent* if they differ by a finite number of Nielsen moves.

DEFINITION 3.2. Let $H < G$ be groups and S a generating n-tuple of G. We say that a left coset gH is *full* (with respect to S) if some entry of S lies in gH, otherwise we say that gH is *empty* (with respect to S). To save on notation, we usually suppress the term 'with respect to S' when there is no ambiguity.

We now give several techniques which we rely on heavily for our main results. Note that in this section we prove our results under very general conditions and all techniques are (for now) existential.

DEFINITION 3.3. Let $H < G$ be groups. An n-tuple S' with entries in G is said to be *left-cleaned* if all of its entries lie in distinct left cosets of H, apart from eH which may contain many entries of S'.

LEMMA 3.4. *Let $H < G$ be groups and S a generating n-tuple of G. Then there is a left-cleaned generating n-tuple S' of G, Nielsen equivalent to S.*

PROOF. We call the following process *left-cleaning* an n-tuple. Let $S = (g_1, \ldots, g_n)$. We can assume that there are g_i, g_j with $i \neq j$ both lying in the same nonidentity left coset of H, so that $g_i H = g_j H \neq eH$. Then $g_j^{-1} g_i \in H$ so we can apply the standard Nielsen move on S which replaces g_i with $g_j^{-1} g_i$ to obtain S_1. Then S_1 has fewer entries lying in this left coset of H and the same number in all other nonidentity left cosets. Iterating this procedure and then moving to other nonidentity left cosets, we eventually reach a left-cleaned n-tuple S'.   □

LEMMA 3.5. *Let $H < G$ be groups and S a generating n-tuple of G. If there exists at least one empty left coset of H, then there are entries s_j, s_k of S (possibly the same entry) and $\epsilon \in \{\pm 1\}$ such that $s_j^\epsilon s_k H$ is an empty left coset. That is, there is some full left coset of H which is taken to some empty left coset of H by left multiplication under some entry of S or its inverse.*

PROOF. Recall that G acts transitively on the set of left cosets by left multiplication. Assume that no entry of S or its inverse sends a full left coset to an empty left coset. Then, as the entries of S generate G, the collection of full left cosets is invariant under this action. Since there exists at least one empty left coset, this contradicts the transitive action of G.   □

LEMMA 3.6. *Let $H < G$ be groups and S a generating n-tuple of G. Suppose that at least one entry of S lies in H, and moreover that there exists an empty left coset of H with respect to S. Then there is a finite sequence of Nielsen moves on some entry s of S which is contained in H such that s is taken into an empty left coset of H.*

PROOF. By Lemma 3.5 there are (possibly identical) entries s_1, s_2 of S, and $\epsilon \in \{\pm 1\}$, with $s_j^\epsilon s_k H$ an empty left coset of H with respect to S. We consider all possible cases:

(1)   The case $s_j, s_k \in H$ never occurs, as then $s_j^\epsilon s_k H = H$ which is a full left coset by hypothesis.

(2)   In the case $s_j \notin H, s_k \in H$, the subcase $s_j^{+1} s_k H$ cannot occur, as then $s_j^{+1} s_k H = s_j^{+1} H$ which is clearly full. In the subcase $s_j^{-1} s_k H$, we replace s_k with $s_j^{-1} s_k$ lying in $s_j^{-1} s_k H$ which is empty.

(3)   In the case $s_j \in H, s_k \notin H$, we replace s_j with $s_j^\epsilon s_k$, as $s_j^\epsilon s_k H$ is empty.

(4)   In the case $s_j, s_k \notin H$, take some $s_i \in H$ and replace s_i with $s_j^\epsilon s_k s_i$, which lies in $s_j^\epsilon s_k s_i H = s_j^\epsilon s_k H$ which is empty. As s_i is a different entry than s_j and s_k, this is a composition of two Nielsen moves on the entry s_i (even if $s_j = s_k$).

We call this replacement process a *left-extraction* of an entry of S from H.   □

Using these techniques, we state the condition below for a finite index subgroup of a group to possess a left transversal which generates the whole group. For simplicity, when S is an n-tuple, we write $\tilde{S}$ for the set of entries of S.

THEOREM 3.7. *Let G be a finitely generated group and H a subgroup of finite index in G. Then the following are equivalent.*

(1) $[G : H] \geq d(G)$.

(2)   *There exists a left transversal T for H in G which contains a generating set X for G of size $|X| = d(G)$.*

PROOF. That $2 \Rightarrow 1$ is immediate.

We show $1 \Rightarrow 2$. Let $n = d(G)$, and let S be a generating n-tuple for G. Use Lemma 3.4 to produce an n-tuple S'' Nielsen equivalent to S which is left-cleaned. Now repeatedly apply Lemma 3.6 to begin left-extracting elements from inside H (thus Nielsen-transforming S''). As $n \leq [G : H]$, we can keep left-extracting until we reach S' which is Nielsen equivalent to our original S, and for which no two entries of S' lie in the same left coset of H. Now simply choose one element from each left coset of H which is empty with respect to S', and add these to $\tilde{S}'$ to form the set T. Then T is a left transversal for H and contains $\tilde{S}'$.   □

A slight variant of the above proof also shows the following result: when $[G : H] \leq d(G)$ then there is a generating set for G of size $d(G)$ which contains a set of left coset representatives for H.

Note that all preceding definitions and results in this section carry over to right transversals, which for the sake of brevity we do not restate explicitly.

For ease of writing, we will often refer to the overall process of cleaning and/or extracting elements (either left or right) as *shifting boxes*, and will usually just write 'this follows by shifting boxes' to mean that it follows by the process of cleaning and/or extracting elements. Our remarks in this section give sufficient conditions for cleaning and/or extracting to be algorithmic.

The most natural question to ask now is: when does a finite index subgroup have a left–right transversal which generates the whole group? This requires a deeper understanding of how cosets intersect, as discussed in Section 2. We urge the reader to consider the discussion of 'chessboards' given after Corollary 2.3, and to consult [3] for an example. These are vital in proving what follows.

Let $H < G$ be groups and S a generating n-tuple of G. Then by Lemma 3.4 we can first perform a left-cleaning of S to form S', followed by a right-cleaning of S' (which will remain left-cleaned) to obtain S''. It follows that S and S'' are Nielsen equivalent, and that S'' is both left-cleaned and right-cleaned.

LEMMA 3.8. *Let $H < G$ be of finite index in G and S a generating n-tuple of G. Then S is left–right-cleaned if and only if one can draw chessboards for H in G with distinct entries of S lying in distinct diagonal tiles of chessboards, except for the chessboard corresponding to the double coset $HeH = H$ which may contain several elements of S.*

PROOF. This is immediate from the fact that columns in chessboards correspond to left cosets of H, and rows correspond to right cosets. Thus, a column (respectively, row) in the chessboards contains multiple entries of S if and only if the corresponding left (respectively, right) coset of H contains multiple entries of S.   □

Note that we can obtain a left–right transversal for H by taking one element from each diagonal tile of each chessboard (Corollary 2.3). In fact, by left–right-cleaning and choosing an element from each unused diagonal we have the following lemma.

LEMMA 3.9. *Let $H < G$ be of finite index in G and S a generating n-tuple of G with at most one entry in H. If S is left–right-cleaned, then there is a set T containing all the entries of S which is a left–right transversal for H in G.*

PROOF. Given that columns in chessboards correspond to left cosets of H, and rows correspond to right cosets, no column or row in any chessboard contains more than one entry from S. Thus we can rearrange the positioning of the columns and rows in each chessboard so that the entries of S are all in tiles which lie on leading diagonals. Now simply choose one element from each lead-diagonal tile which does not contain an entry of S, and add these to the set S to form the set T. Then T contains precisely one element from each lead-diagonal tile of each chessboard, and no other elements. Thus T contains precisely one element in each left coset of H, and precisely one element in each right coset of H. So T is our desired left–right transversal which contains $\tilde{S}$.   □

Combining our shifting boxes technique with the properties of the coset intersection graph from Theorem 2.2, we are able to show the following theorem.

THEOREM 3.10. *Let $H < G$ be of finite index in G and S a generating n-tuple of G with $n \leq [G : H]$. If $n \leq 3$ then there is a generating n-tuple S' Nielsen equivalent to S and a left–right transversal T for H in G with $\tilde{S'} \subseteq T$.*

PROOF. The case when $n = 1$ is trivial.

The case when $n = 2$ is done as follows. Left–right-clean S to form $S' = (a, b)$. Clearly we cannot have $a, b \in H$, or else $[G : H] < 2$. So at most one of a, b lies inside H. But then by Lemma 3.9 we can extend $\tilde{S'}$ to a (generating) set T which is a left–right transversal for H.

The case $n = 3$ is complicated and we consider several subcases. Left–right-clean S to form $S' = (a, b, c)$. Clearly we cannot have $a, b, c \in H$, or else $[G : H] < 3$. If at
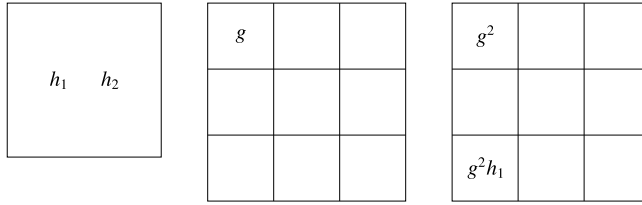
FIGURE 1. Part of Case 1 of the proof of Theorem 3.10.

most one of a, b, c lies inside H then we can apply Lemma 3.9 as before. So we are left with the case where two of a, b, c lie inside H (relabel them as $h_1, h_2 \in H$ and $g \notin H$).

Case 1. $g^2 \notin HgH \cup H$ (that is, g^2 lies in a different chessboard than g and h_1, h_2).

Make the Nielsen moves $h_1 \mapsto g^2 h_1$; clearly $g^2 h$ lies in the same left coset (and hence same chessboard) as g^2 (see Figure 1). So now $g, h_2, g^2 h_1$ lie in different chessboards, thus the triple $S'' := (g, h_2, g^2 h_1)$ is left–right cleaned. As only h_2 lies inside H, we can use Lemma 3.9 to extend $\tilde{S}''$ to a set T which is a left–right transversal for H. Since T contains $\tilde{S}''$, it generates G.

Case 2. $g^2 \in HgH$ (that is, g^2 lies in the same chessboard as g).

Clearly $g^2 H \neq gH$ and $Hg^2 \neq Hg$; otherwise we would have $g \in H$ which contradicts our initial hypothesis. So g^2 lies in a different left coset and different right coset than g (that is, in a different column and row than g in HgH). Consider $h_1 g^2$ and $h_2 g^2$ (which both lie in the same right coset as g^2, and hence in a different right coset than g). If $h_i g^2 H \neq gH$ for some $i \in \{1, 2\}$, then make the Nielsen moves $h_i \mapsto h_i g^2$. Then $h_i g^2$ lies in a different left and different right coset than g (but in the same chessboard) (see Figure 2). If on the other hand $h_1 g^2 H = h_2 g^2 H = gH$, then $h_2^{-1} h_1 g^2 H = g^2 H$ and so we make the Nielsen moves $h_1 \mapsto h_2^{-1} h_1 g^2$. Then $h_2^{-1} h_1 g^2$ lies in a different left and different right coset than g (but in the same chessboard) (see Figure 3). Either way, we now have a triple S'' which, after permutation of some rows and columns, has entries which lie along diagonal tiles of the chessboards. We conclude as in *Case 1*.

Case 3. $g^2 \in H$.

By the transitivity of the action of G on left (and right) cosets of H, there must be some h_i ($i \in \{1, 2\}$) and some $\epsilon \in \{\pm 1\}$ with $h_i^\epsilon gH \neq gH$, and similarly some h_j ($j \in \{1, 2\}$) and some $\delta \in \{\pm 1\}$ with $Hgh_j^\delta \neq Hg$. If $i \neq j$, then we make the Nielsen move $h_i \mapsto h_i^\epsilon g$ followed by the Nielsen move $g \mapsto gh_j^\delta$ (see Figure 4). If, on the other hand, $i = j$ (say, $i = j = 1$, without loss of generality), then consider the element $h_2 gh_1^\delta$. If $h_2 gh_1^\delta H \neq gH$, then $h_2 gh_1^\delta$ lies in a different left coset and different right coset than g, and so we make the Nielsen moves $h_2 \mapsto h_2 gh_1^\delta$ (see Figure 5). If, however, $h_2 gh_1^\delta H = gH$, then $h_2 gh_1^\delta$ lies in a different left coset and different right coset than $h_1^\epsilon g$, and so we make the Nielsen moves $h_2 \mapsto h_2 gh_1^\delta$ followed by $g \mapsto h_1^\epsilon g$ (see Figure 6). In all the subcases considered here, we end up with a triple S'' which, after permutation of some rows and columns, has entries which lie along diagonal tiles of the chessboards. We conclude as in *Case 1*.   □

FIGURE 2. Part of Case 2 of the proof of Theorem 3.10.

FIGURE 3. Part of Case 2 of the proof of Theorem 3.10.

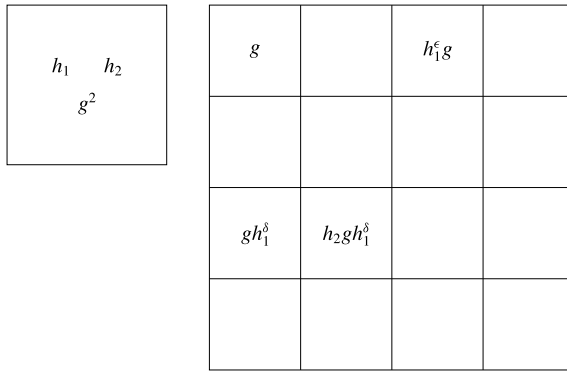FIGURE 4. Part of Case 3 of the proof of Theorem 3.10.

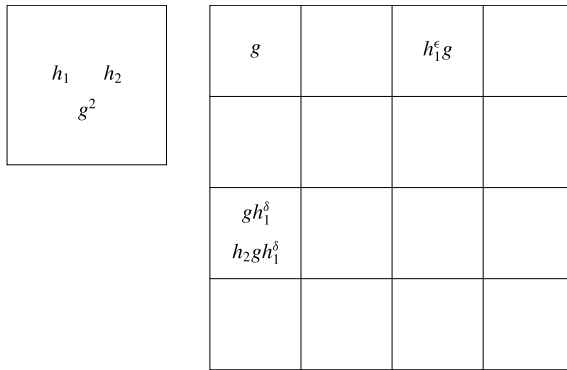FIGURE 5. Part of Case 3 of the proof of Theorem 3.10.

FIGURE 6. Part of Case 3 of the proof of Theorem 3.10.

We note that all previous results in this section are algorithmic, in that we have explicitly constructed the relevant transversals and generating sets.

THEOREM 3.11. *Let G be a group with $d(G) \leq 3$ and H a subgroup of finite index in G. Then the following are equivalent.*

(1)   *There exists a left–right transversal T for H in G with $\langle T \rangle = G$.*
(2) $[G : H] \geq d(G)$.

PROOF. That $1 \Rightarrow 2$ is immediate; that $2 \Rightarrow 1$ can be seen from Theorem 3.10.   □

This leads us to pose the following question:

QUESTION 3.12. Does Theorem 3.11 hold if we change the hypothesis '$d(G) \leq 3$' to '$d(G)$ finite'?

We have not yet been able to extend the proof of Theorem 3.10 to the case $n \geq 4$, as the scenarios to consider becomes very large in number and complex. However, we believe this should be possible with a more general technique of left–right-extraction.

We note that, in any extension of Theorem 3.11 to groups needing more than three generators, we need only consider free groups, as the following proposition shows.

PROPOSITION 3.13. *Theorem 3.11 holds for all finite rank groups (and not just groups of rank at most 3) if and only if it holds for all finite rank free groups.*

PROOF. Suppose Theorem 3.11 holds for all F_n. Let G be a group with $d(G) = n$, and $H < G$ have index $[G : H] = k \geq n$. Then there is a surjection $f : F_n \twoheadrightarrow G$, and it is a standard fact that the preimage $f^{-1}(H)$ also has index k in F_n. By hypothesis, there is a left–right transversal T of $f^{-1}(H)$ which generates F_n; it follows that $f(T)$ is a left–right transversal of H which generates G.   □

4. An application of shifting boxes: finding primitive elements

Recall that a primitive element of a finite rank free group F_n is one which lies in *some* generating set of size precisely n, which is equivalent to being an element of a free basis for F_n. If G is an arbitrary group of finite rank n, then we say that a *primitive element* in G is an element lying in *some* generating set of size n for G. This coincides with the definition of primitive elements in F_n.

An obvious question to ask is which subgroups of F_n (or more generally, rank-n groups) contain a primitive element (we can ask this for both finite and infinite index subgroups). We first consider the case of normal subgroups.

The following lemma is immediate by considering the image under the quotient map of a generating set of minimal size containing the relevant primitive element.

LEMMA 4.1. *Let G be a group of finite rank n and N a normal subgroup of G. If N contains some primitive element of G, then $d(G/N) < n$.*

The converse statement is not true, even in the special case that $G = F_n$, as was shown in [7, 9]. It is currently open in the case when N has finite index, and here we briefly mention the connection with product replacement graphs. More can be found in the survey [10] of Pak which contains a range of references.

Given a finitely generated group G and an integer $n \geq d(G)$, the product replacement graph $\Gamma_n(G)$ has vertices the generating n-tuples of G with edges between two vertices if one is the image of another under a standard Nielsen move. A big area of study here is the connectivity of $\Gamma_n(G)$. It can happen that $\Gamma_n(G)$ is disconnected when $n = d(G)$ (for instance, finite abelian groups), but no example is known of a finite group G and an integer $n > d(G)$ where $\Gamma_n(G)$ is disconnected. The relation with primitive elements is that if N is a normal subgroup of F_n containing no primitive element but $G = F_n/N$ has $d(G) < n$ then $\Gamma_n(G)$ is disconnected. Hence there are examples of infinite finitely generated groups G with $\Gamma_n(G)$ disconnected by [7, 9], but a normal subgroup N of finite index containing no primitive element and with $d(F_n/N) < n$ would give rise to a finite group G and integer $n > d(G)$ with $\Gamma_n(G)$ disconnected, the existence of which is currently unknown.

Our shifting boxes technique enables us to explore the location of primitive elements relative to cosets of finite index subgroups. We write $[n]$ for the set of integers $\{1, \ldots, n\}$, and $X \Delta Y$ for the symmetric difference.

LEMMA 4.2. *Let G be any group with $d(G) = n$, and H a subgroup of finite index in G with $[G : H] < 3 \cdot 2^{n-1}$. If H contains no primitive elements of G, then H contains the square of every primitive element of G.*

PROOF. Let $S = (g_1, \ldots, g_n)$ be any left-cleaned generating n-tuple for G. For any $\emptyset \neq M = \{i_1, \ldots, i_k\} \subseteq [n]$, ordered so that $i_1 < \cdots < i_k$, define the unique word $w_M := g_{i_k} g_{i_{k-1}} \cdots g_{i_1}$ and the disjoint sets of words $A := \{w_M \mid \emptyset \neq M \subseteq \{2, \ldots, n\}$ or $M = \{1\}\}$, $B := \{w_M g_1 \mid \emptyset \neq M \subseteq [n]\}$. Set $T := A \sqcup B$, so that $|T| = 3 \cdot 2^{n-1} - 1$. By construction, the only element in T which might not be primitive is g_1^2, and the rest are primitive by Nielsen transformations: for any $w_M g_1 \in B$ with $M \neq \{1\}$ we take some $1 \neq i \in M$ and perform the Nielsen transformation $g_i \mapsto w_M g_1$ (g_i appears precisely once in $w_M g_1$). A similar argument works for any $w_M \in A$.

We claim that, for any pair of distinct words $x, y \in T$, if $xH = yH$ then either H contains a primitive element or $g_1^2 \in H$ (possibly both). We consider all cases:

Case 1. $x, y \in A$, so $x = w_M$, $y = w_{M'}$, with $M \neq M'$. Then $w_M^{-1} w_{M'} \in H$ is primitive as there is some $i \in M \Delta M'$, so Nielsen-transform $g_i \mapsto w_M^{-1} w_{M'}$.

Case 2. Precisely one of x, y lie in A (say, $x \in A$), so $x = w_M$ and $y = w_{M'} g_1$. We consider all subcases:
(2A) $1 \notin M, M'$. In this case, $w_M^{-1} w_{M'} g_1 \in H$ is primitive (Nielsen-transform $g_1 \mapsto w_M^{-1} w_{M'} g_1$).
(2B) $1 \in M'$, $1 \notin M$, and $M' = M \cup \{1\}$. In this case, $w_M^{-1} w_{M'} g_1 = g_1^2 \in H$.
(2C) $1 \in M'$, $1 \notin M$, and there is some $1 < j \in M \Delta M'$. In this case, $w_M^{-1} w_{M'} g_1 \in H$ is primitive (Nielsen-transform $g_j \mapsto w_M^{-1} w_{M'} g_1$).
(2D) $M = \{1\}$. If $M' = \{1\}$ then $w_M^{-1} w_{M'} g_1 = g_1 \in H$ is primitive. Otherwise, there is some $1 \neq j \in M'$, in which case $w_M^{-1} w_{M'} g_1 \in H$ is primitive (Nielsen-transform $g_j \mapsto w_M^{-1} w_{M'} g_1$).

Case 3. $x, y \in B$. In this case, $x = w_M g_1$, $y = w_{M'} g_1$ ($M \neq M'$). If there is some $1 \neq i \in M \Delta M'$, then the element $g_1^{-1} w_M^{-1} w_{M'} g_1 \in H$ is primitive. Otherwise, $M' = M \cup \{1\}$ (or $M = M' \cup \{1\}$), in which case $g_1^{-1} w_M^{-1} w_{M'} g_1 = g_1^{-1} w_M^{-1} w_M g_1 g_1 = g_1 \in H$ (or $g_1^{-1} w_M^{-1} w_{M'} g_1 = g_1^{-1} g_1^{-1} w_{M'}^{-1} w_{M'} g_1 = g_1^{-1} \in H$) is primitive.

Suppose that H contains no primitive element. Since $|T| = 3 \cdot 2^{n-1} - 1 \geq [G : H]$, either two elements of T lie in the same coset (so by the claim above, $g_1^2 \in H$ as H contains no primitive element), or one element of T lies in H (which must be g_1^2, as all other elements of T are primitive). So $g_1^2 \in H$.

Now take *any* primitive element $x \in G$, which is part of some generating set $\{x, y_2, \ldots, y_n\}$ for G (which must be left-cleaned, otherwise H would contain a primitive element). Using the exact same argument above, with $g_1 := x$, $g_i := y_i$ for all $2 \leq i \leq n$, we see that if H contains no primitive element then $x^2 \in H$. So H contains the square of *every* primitive element. □

LEMMA 4.3. *Let G be any group with $d(G) = n$, and H a subgroup of finite index in G with $[G : H] < 3 \cdot 2^{n-1}$. If H contains no primitive elements of G, then H is normal in G and $G/H \cong C_2^m$ for some $m \leq n$.*

PROOF. Suppose H contains no primitive element. Then, by Lemma 4.2, H contains the square of every primitive element. Set $T := \{g^2 \mid g \text{ is primitive in } G\}$. Then T is a normal subset of G, since the conjugate of a primitive element is again a primitive element (conjugation is an automorphism). Thus $\langle T \rangle \triangleleft G$, the (normal) subgroup generated by all the squares of primitive elements of G. So by hypothesis, $\langle T \rangle < H$. Now take any generating set $\{t_1, \ldots, t_n\}$ for G. Then $t_i^{-1} t_j$ is a primitive element, for any pair i, j with $i \neq j$. Thus $t_i^2, t_j^2, (t_i^{-1} t_j)^2$ lie in $\langle T \rangle$, and hence so will $t_i^2 (t_i^{-1} t_j)^2 t_j^{-2} = [t_i, t_j]$. So $G/\langle T \rangle$ is abelian as $\langle T \rangle$ is normal and contains the commutator of every pair in the generating set $\{t_1, \ldots, t_n\}$ for G. So $\langle T \rangle$, and hence H, contain the commutator subgroup $[G, G]$. Thus H is normal in G and G/H is generated by the images of $\{t_1, \ldots, t_n\}$, all of which have order 2 in this quotient. So $G/H \cong C_2^m$ for some $m \leq n$. □

We now give the following complete characterisation of finite index subgroups of a group of rank n which contain primitive elements, up to index $3 \cdot 2^{n-1} - 1$.

THEOREM 4.4. *Let G be any group with $d(G) = n$ and let H be a subgroup of finite index in G with $[G : H] < 3 \cdot 2^{n-1}$. Then H contains no primitive elements of G if and only if H is normal in G and the quotient G/H is isomorphic to C_2^n, whereupon every coset distinct from H contains a primitive element of G.*

PROOF. First, if H is normal and contains an element g of a generating n-tuple for G, then the image of this n-tuple gives rise to a generating $(n - 1)$-tuple of G/H, just as in Lemma 4.1, but $d(C_2^n) = n$.

Now suppose that H does not contain a primitive element of G and let $q : G \twoheadrightarrow G/H$ be the quotient homomorphism, where we know that H is normal in G and $G/H \cong C_2^m$ for some $m \leq n$ by Lemma 4.3. Given a generating n-tuple $(g_1, \ldots, g_n)$ for G, let F_n be the free group on $x_1, \ldots, x_n$ and set $\theta : F_n \twoheadrightarrow G$ to be the homomorphism extending the map $x_i \mapsto g_i$. Note that if we have $k \leq n$ and integers $1 \leq i_1 < i_2 < \cdots < i_k \leq n$, then $x_{i_1} x_{i_2} \cdots x_{i_k}$ is primitive in F_n and $\theta(x_{i_1} x_{i_2} \cdots x_{i_k}) = g_{i_1} g_{i_2} \cdots g_{i_k}$ is primitive in G.

Assume that $m < n$ and consider the map $q \circ \theta : F_n \to C_2^m$, which factors through C_2^n via the abelianisation map $\mathrm{ab} : F_n \twoheadrightarrow C_2^n$ and the map $\psi : C_2^n \twoheadrightarrow C_2^m$. That is, the following diagram commutes, and all maps are surjections:

$$
\begin{array}{ccc}
F_n & \xrightarrow{\ \mathrm{ab}\ } & C_2^n \\
{\scriptstyle \theta}\big\downarrow & & \big\downarrow{\scriptstyle \psi} \\
G & \xrightarrow[\ q\ ]{} & C_2^m
\end{array}
$$

As ψ is now a linear map from an n-dimensional vector space over $\mathbb{F}_2$ to an m-dimensional space, we have a nontrivial element $(v_1, \ldots, v_n)$ of C_2^n in the kernel of ψ. Now we can assume that each v_i takes the value 0 or 1, so we form the

primitive element $x = x_1^{v_1} x_2^{v_2} \cdots x_n^{v_n}$ of F_n which maps to the identity under $\psi \circ \mathrm{ab}$. Thus $g_1^{v_1} g_2^{v_2} \cdots g_n^{v_n} = \theta(x)$ is a primitive element of G which maps to the identity under q and so it is in H; a contradiction. Similarly, if $n = m$, then for any $(w_1, \ldots, w_n) \in \mathbb{F}_2^n \setminus \{0\}$ the coset of H in G corresponding to this point contains the primitive element $g_1^{w_1} g_2^{w_2} \cdots g_n^{w_n}$ of G.   □

Thus if G is a group with $d(G) = n$ we have two possibilities: either C_2^n is not a quotient of G in which case all subgroups of G having index less than $3 \cdot 2^{n-1}$ contain primitive elements, or G surjects to C_2^n in which case there is a single subgroup of index less than $3 \cdot 2^{n-1}$ which fails to contain a primitive element. The uniqueness in the second case comes about because a homomorphism from a rank-n group G to an abelian group of exponent 2 must factor through $G/[G,G]G^2$. As $G/([G,G]G^2) \cong C_2^m$ for $m \le n$, we see that when $n = m$ any exceptional subgroup must be equal to $[G,G]G^2$.

Note that the inequality $[G : H] < 3 \cdot 2^{n-1}$ in Theorem 4.4 is somewhat necessary: here is an example of what occurs when the inequality does not hold.

EXAMPLE 4.5. Take the (free) subgroup $H := [F_n, F_n]F_n^2 < F_n$ of index 2^n with no primitive elements of F_n. Then H itself has several normal subgroups of index 2, none of which contain primitive elements of F_n. In F_n, these subgroups have index $2 \cdot 2^n > 3 \cdot 2^{n-1}$, so this is not a counterexample to Theorem 4.4.

We remark that the number of subgroups of F_n with index less than 2^n is vast, being bounded below by $((2^n)!)^{n-1}$ (see [8, Corollary 2.1.2]).

It would be interesting to find a closed-form expression for $M(n)$, which we define to be the smallest number i such that F_n has a subgroup other than $[F_n, F_n]F_n^2$ of index i which contains no primitive elements. By Theorem 4.4, and the example immediately proceeding it, we have $3 \cdot 2^{n-1} \le M(n) \le 2 \cdot 2^n$. In particular, consider any quotient map $f : F_2 \twoheadrightarrow S_3$; the kernel N of this map has index $6 = 3 \cdot 2^{2-1}$, and N contains no primitive elements of F_2 by Lemma 4.1. So $M(2) = 6$. Moreover, it is straightforward to see that $M(1) = 3$. We do not know $M(n)$ for any other values of n.

Our analysis of finite index subgroups of F_n containing no primitive elements was motivated by the following result of Parzanchevski and Puder in [11].

THEOREM 4.6 [11, Corollary 1.5]. *The set P of primitive elements in F_n is closed in the profinite topology.*

COROLLARY 4.7. *Given F_n and $w \in F_n$, a nonprimitive element, there is a finite index subgroup $H < F_n$ such that the coset wH does not contain any primitive elements. Taking $w = e$ gives a finite index subgroup with no primitive elements.*

We finish by remarking that a recent result of Clifford and Goldstein [6] proves that there is an algorithm to determine which finitely generated subgroups of F_n contain primitive elements, although they say that they do not expect it to be implemented in practice. One of our overall aims is to give a characterisation of such subgroups that leads to computationally efficient recognition. A classical result of Whitehead [14] gives an algorithm for determining whether an element of F_n is primitive; Roig *et al.* [12] refine this to a polynomial time algorithm.

Acknowledgements

References

[1] A. Blass, 'Injectivity, projectivity, and the axiom of choice', *Trans. Amer. Math. Soc.* **255** (1979), 31–59.

[2] J. Button, M. Chiodo and M. Zeron-Medina Laris, 'Coset intersection graphs, and transversals as generating sets for finitely generated groups', in: *Extended Abstracts Fall 2012, Trends in Mathematics: Automorphisms of Free Groups*, 1 (eds. J. González-Meneses *et al.*) (Springer, New York, 2014), 29–34.

[3] J. Button, M. Chiodo and M. Zeron-Medina Laris, 'Coset intersection graphs for groups', *Amer. Math. Monthly* **121**(10) (2014), 922–926.

[4] P. Cameron, 'Generating a group by a transversal', Preprint available at
http://www.maths.qmul.ac.uk/ pjc/preprints/transgenic.pdf.

[5] P. Cameron, 'Problem 100 from a problem set', available at
http://www.maths.qmul.ac.uk/~pjc/oldprob.html.

[6] A. Clifford and R. Goldstein, 'Subgroups of free groups and primitive elements', *J. Group Theory* **13** (2010), 601–611.

[7] M. J. Evans, 'Primitive elements in free groups', *Proc. Amer. Math. Soc.* **106** (1989), 313–316.

[8] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics, 212 (Birkhaüser, Basel, 2003).

[9] G. A. Noskov, 'Primitive elements in a free group', *Mat. Zametki* **30** (1981), 497–500.

[10] I. Pak, 'What do we know about the product replacement algorithm?', in: *Groups and Computation, III*, Ohio State Univ. Math. Res. Inst. Publ. 8 (de Gruyter, Berlin, 2001), 301–347.

[11] O. Parzanchevski and D. Puder, 'Measure preserving words are primitive', *J. Amer. Math. Soc.* **28** (2015), 63–97.

[12] A. Roig, E. Ventura and P. Weil, 'On the complexity of the Whitehead minimization problem', *Internat. J. Algebra Comput.* **17**(8) (2007), 1611–1634.

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

[14] J. H. C. Whitehead, 'On equivalent sets of elements in a free group', *Ann. of Math.* (2) **37**(4) (1936), 782–800.

JACK BUTTON, Selwyn College, Cambridge, Grange Road,
Cambridge CB3 9DQ, UK
e-mail: J.O.Button@dpmms.cam.ac.uk

MAURICE CHIODO, Mathematics Department, University of Neuchâtel,
Rue Emile-Argand 11, CH-2000 Neuchâtel, Switzerland
e-mail: maurice.chiodo@unine.ch

MARIANO ZERON-MEDINA LARIS, 31 Mariner's Way,
Cambridge CB4 1BN, UK
e-mail: marianozeron@gmail.com