On the number of elements dominated by a subgroup

by John Ginsburg and Bill Sands[1]

ABSTRACT We obtain lower bounds for the number of elements dominated by a subgroup in a Cayley graph. Let G be a finite group and let U be a generating set for G such that $U = U^{-1}$ and $1 \in U$. Let H be an independent subgroup of G. Let r be a positive integer, and suppose that, in the Cayley graph (G, U), any two non-adjacent vertices have at most r common neighbours. Let $N[H]$ denote the set of elements of G which are dominated by the elements of H. We prove that

(i) $|N[H]| \geq \left\lceil \dfrac{|U|^2}{r(|H \cap U^2| - 1) + |U|} \right\rceil |H|$ and

(ii) $|N[H]| \geq |U||H| - \dfrac{|H|r}{2}(|H \cap U^2| - 1)$.

An interesting example illustrating these results is the graph on the symmetric group S_n, in which two permutations are adjacent if one can be obtained from the other by moving one element. For this graph we show that $r = 4$ and illustrate the inequalities.

1. Introduction

The ideas considered in this paper are motivated by earlier work on permutation graphs. For any positive integer n, let S_n denote the set of all permutations on $\{1, 2, ..., n\}$. Consider the adjacency relation $\sim$ defined on S_n as follows: for p and q in S_n, $p \sim q \leftrightarrow$ there is an integer i such that $p - i = q - i$.(here we are thinking of a permutation simply as an ordered list and $p - i$ denotes the permutation of length $n - 1$ obtained by deleting i from p.) We will refer to this graph as *the permutation graph* on $\{1, 2, ..., n\}$. The connection between this graph and coding theory is studied in [9], where it is shown that S_n has independence number $(n-1)!$ and chromatic number n. The clique number, local independence number and a chordal ring property of S_n are established in [6]. Another important parameter of S_n is its domination number - the smallest size of a dominating set. To our knowledge, this is not yet known for any values of n larger than 5. It is easy to see that the domination number of S_3 is 2; any element of S_3 and its reverse clearly dominate S_3. The domination number of S_4 is 4: for example, one verifies that the set of four permutations

[1]The work of the second author was supported by NSERC Discovery Grant #8306.

$D_4 = \{1234, 4321, 3412, 2143\}$ dominates S_4, and it is not hard to show that no set of three permutations can dominate S_4. One can form the set D_4 by starting with the permutation 1234 and then successively applying the following two operations to generate more permutations: (i) Interchange both the first and fourth and the second and third entries.
(ii) Interchange both the first and third and the second and fourth entries. These two operations produce 4 permutations, and sufficiently "move the entries around" to give a dominating set. Equivalently, we have formed a subgroup of the symmetric group S_4, generated by the set $\{(14)(23), (13)(24)\}$, where we are using ordinary cycle notation. Using this idea, and trying various reasonable looking generating sets, we have also been able to find a minimum dominating set for S_5. In this case, it turns out that the subgroup D_5 of S_5 generated by the two permutations (12)(45) and (24)(35) forms a dominating set of size 10. One further shows that no set having fewer than 10 elements can dominate S_5. With these results in hand, we moved on to $n = 6$, hoping to discover a general procedure to generate a subgroup D_n of S_n which can be shown to dominate S_n and have minimum size among dominating sets. This turned out to be no more than a pleasant delusion. With the help of the GAP program [5], we found that the smallest size of a subgroup of S_6 which dominates S_6 is 60. This does not, however, give the domination number of S_6: we have found a 48-element subset D of S_6 which dominates S_6. Such a set D was first found by starting with a particular subgroup H_6 of size 24, and then applying the greedy algorithm to dominate the set of elements of S_6 not dominated by H_6, which resulted in 24 more elements. A bit more attention produced a dominating set D which is the union of H_6 and a left coset of H_6. At this time, this is the smallest size of a dominating set for S_6 that we know of. Beyond this, finding useful constructions and good upper bounds for the domination number of S_n presents an interesting challenge which we hope to address in future work. It seems likely that the group structure of S_n will play a significant role in such investigations, unlike the purely combinatorial work in [9] and [6]. With the given adjacency relation, S_n is a Cayley graph (for readers unfamiliar with this notion, we include the definition below). In light of the types of dominating sets we have found so far for S_n, it is natural to consider subgroups and cosets in general Cayley graphs. This is exactly our focus in this paper. For a subgroup H of a Cayley graph G, we consider the following basic question: how many elements of G does H dominate? In the next section, we will obtain some useful estimates concerning this and other related questions. In the third section of the paper, we will see how these estimates look when applied to the permutation graph S_n above as well as other examples, and we will also have a bit more to say about

the domination number of S_n.

First we set down the basic concepts, notation, and terminology to be employed. For more background on these concepts and other basic notions of graph theory and group theory we refer the reader to [2] and [8].

Our set-theoretic notation is standard. In particular the cardinality of a set S is denoted by $|S|$.

For any real number x, the least integer which is $\geq x$ is denoted by $\lceil x \rceil$.

If $f(n)$ and $g(n)$ are real-valued functions of a positive integer n, as usual we write $f(n) = O(g(n))$ if there is a positive constant c, and a positive integer n_0 so that $f(n) \leq cg(n)$ for $n \geq n_0$. In this case, we say that $f(n)$ is *of order no larger than* $g(n)$. If both $f(n) = O(g(n))$ and $g(n) = O(f(n))$ we say that $f(n)$ and $g(n)$ have *the same order.*

In this paper the term *graph* refers to a finite, undirected graph with no loops or multiple edges. For a vertex v in a graph G, we let $d_G(v)$ denote the *degree* of v in G; that is, $d_G(v)$ is the number of vertices of G which are adjacent to v. The largest degree of any vertex of G is denoted by $\Delta(G)$, and the smallest degree of any vertex by $\delta(G)$. A set of vertices S in G is said to be *independent* if no two vertices of S are adjacent in G. $N_G[v]$ denotes the *closed neighbourhood of* v in G. Thus $N_G[v]$ consists of v together with all the vertices of G which are adjacent to v. Similarly, for any set of vertices S in G, we let $N_G[S]$ denote the closed neighbourhood of S in G: $N_G[S] = \bigcup_{v \in S} N_G[v]$. We say that the elements of $N_G[S]$ are *dominated* by the elements of S. A set of vertices S is said to be a *dominating set* for G if every vertex of G is either in S or is adjacent to a vertex of S. Equivalently, S is a dominating set if $N_G[S] = G$. The smallest cardinality of a dominating set for G is called *the domination number* for G and is denoted by $\gamma(G)$. Whenever the graph G is understood from the context, we will often drop the symbol G in the preceding notation and instead write $d(v), N[v], N[S]$ and γ. Two parameters of a graph G which will be central to our discussion are defined as follows:

$r_1(G) = \max\{\ |N[v] \cap N[w]| : v, w$ are vertices of G with $v \neq w\}$

$r_2(G) = \max\{\ |N[v] \cap N[w]|\ :\ v, w$ are non-adjacent vertices of G with $v \neq w\}$

These will be denoted by r_1 and r_2 when G is understood. Note that $r_1(G)$ is the largest number of common neighbours which any two distinct vertices of G have, and $r_2(G)$ is the largest number of common neighbours which any two distinct, non-adjacent vertices of G have.

All groups considered in this paper are assumed to be finite, and are written multiplicatively. For any group G we will let 1 denote the identity element of G. If S is a subset of a group G we will let $< S >$ denote *the subgroup of G which is generated by S*. If $< S >= G$ we say that S is a *generating set* for G.

For any subsets S and T of a group G, as usual we let $S^{-1} = \{x^{-1} : x \in S\}$ and $ST = \{xy : x \in S, y \in T\}$. We also let $S^2 = SS$ and for a one-element set $T = \{a\}$, we write Sa.

If H is a subgroup of a group G we write $H \leq G$. As usual, for any element g of G, the conjugate subgroup gHg^{-1} is denoted by H^g. If S is any subset of G, we will let $[S : H]$ denote the *left* index of S with respect to H. That is, $[S : H]$ is the number of distinct left cosets in the collection $\{xH : x \in S\}$.

Let G be a group, and let U be a generating set for G such that $U = U^{-1}$ and $1 \in U$. The *Cayley graph on G with respect to U* is the graph whose vertex set is G and having the adjacency relation $\sim$ defined as follows: for any elements x, y of G,

$$x \sim y \leftrightarrow \text{ there is an element } u \in U - \{1\} \text{ such that } y = ux.$$

The Cayley graph on G with respect to U is denoted by (G, U), or simply by G if the generating set U is understood.

2. Lower bounds for the number of elements dominated by a subgroup

The following two elementary results contain several useful facts.

Theorem 2.1. Let (G, U) be a Cayley graph. Let $S \subseteq G$ and let H be a subgroup of G. Then

(i) $N[S] = US$.

(ii) $N[1] = U$.

(iii) $|N[S]| \leq |U||S|$.

(iv) $|N[H]| = [U : H]|H|$.

(v) H is independent $\leftrightarrow H \cap U = \{1\}$.

(vi) For each element x of H, there are exactly k elements of H distinct from x which have a common neighbour in G with x, where $k = |H \cap U^2| - 1$.

(vii) The elements of H have pairwise disjoint neighbourhoods in $G \leftrightarrow H \cap U^2 = \{1\}$.

Proof: The first three statements are obvious and (vii) follows directly from (vi). For statement (iv), note that $N[H] = UH = \bigcup_{u \in U} uH$, which is equal to a union of $[U : H]$ left cosets of H.

To prove (v), assume H is independent. If u is any element of $H \cap U - \{1\}$ then 1 and $u = u1$ are adjacent in G. Since H is independent, no such u exists. Conversely, suppose that $H \cap U = \{1\}$. Let x and y be any two distinct elements of H. If x and y are adjacent in G there is an element u in U for which $y = ux$. But this implies that $u = yx^{-1}$ is an element of $H \cap U - \{1\}$. Hence H is independent.

To prove (vi), let $k = |H \cap U^2| - 1$. Let x be any element of H. Let p be any element of $H \cap U^2 - \{1\}$. Let $y = px$. Then $y \in H$ and $y \neq x$. We have $p = uv$ for some elements u and v in U, and $p \in H$. Since $u^{-1}y = vx$, we see that x and y have a common neighbour in G, namely vx. In the other direction, suppose y is an element of H, distinct from x, for which x and y have a common neighbour. Then there are elements u and v in U such that $ux = vy$. This implies that the element $p = v^{-1}u$ belongs to H, since $v^{-1}u = yx^{-1}$. Thus $p \in H \cap U^2 - \{1\}$ and $y = px$. We have shown that the elements of $H - \{x\}$ which have a common neighbour in G with x are precisely the elements of the set $\{px : p \in H \cap U^2 - \{1\}\}$, which gives (vi). □

In the next theorem we use the parameters $r_1(G)$ and $r_2(G)$ defined in the introduction.

Theorem 2.2. Let (G, U) be a Cayley graph.
For each element $p \in U^2$, let $M(p) = \{(u, v) \in U \times U : uv = p\}$. Then

(i) $r_1(G) = \max\{|M(p)| : p \in U^2 - \{1\}\}$, and

(ii) $r_2(G) = \max\{|M(p)| : p \in U^2 - U\}$.

Proof: We prove the second statement. The first statement is done in a similar way. Let $k = r_2(G)$. Then, for any two non-adjacent vertices x and y of G, we have $|N[x] \cap N[y]| \leq k$. Now, let p be any element of the set $U^2 - U$. Since $p \notin U$, p is not adjacent to 1. So there are at most k elements in the set $N[1] \cap N[p]$. Let (u, v) be any element of $U \times U$ such that $uv = p$. Then $v = u^{-1}p$ and so $v \in N[1] \cap N[p]$. We have $(u, v) = (pv^{-1}, v)$. We see that $M(p) \subseteq \{(pv^{-1}, v) : v \in N[1] \cap N[p]\}$. In fact, we have $M(p) = \{(pv^{-1}, v) : v \in N[1] \cap N[p]\}$: let $v \in N[1] \cap N[p]$ and consider the pair (pv^{-1}, v). To show that this pair belongs to $M(p)$ we need to check that $pv^{-1} \in U$. Well, since $v \in N[p]$ there is an element $u \in U$ with $v = up$. Therefore $pv^{-1} = u^{-1} \in U$. It follows that $|M(p)| = |N[1] \cap N[p]| \leq k$. Let $k_1 = \max\{|M(p)| : p \in U^2 - U\}$. We have shown that $k_1 \leq k$. In the other direction, let x and y be any two non-adjacent vertices of G. We claim that $|N[x] \cap N[y]| \leq k_1$. If x and y have no common neighbour, this is trivial. Otherwise, let z be any common neighbour of x and y. Then there are elements u and v in U such that $z = ux = vy$. We have $y = v^{-1}ux$. Since y and x are not adjacent, we have $v^{-1}u \notin U$. Note that $v^{-1}u = yx^{-1}$. Let $p = yx^{-1}$. Then $p \in U^2 - U$. We now see that $(v^{-1}, u) \in M(p)$. Letting π_2 denote projection onto the second coordinate, we see that $z = ux$ for some $u \in \pi_2(M(p))$. We thus have $N[x] \cap N[y] \subseteq \pi_2(M(p))x$. Since $|\pi_2(M(p))| \leq |M(p)| \leq k_1$, it follows that $|N[x] \cap N[y]| \leq k_1$. This implies that $k \leq k_1$ as desired. □

We turn next to our first lower bound for the number of elements dominated by a subgroup H in a Cayley graph (G, U). Clearly any such estimate in general must account for the set $H \cap U^2$. A simple lower bound results by considering the function f from $U \times H$ to $UH = N[H]$ which sends (u, h) to uh. Letting $s = |H \cap U^2|$, we note that f is at most s to 1: Let (u_0, h_0) be any element of $U \times H$. If (u, h) is any element of $U \times H$ such that $uh = u_0h_0$ then we have $u_0^{-1}u = h_0h^{-1} \in H \cap U^2$. Letting $p = u_0^{-1}u$, we have $(u, h) = (u_0p, p^{-1}h_0)$. We see that the pre-images of u_0h_0 under f are contained in the set $\{(u_0p, p^{-1}h_0) : p \in H \cap U^2\}$. (Note that this inclusion may indeed be proper, since the element u_0p will in general not be in U). This latter set has cardinality s, and so f is at most s to 1. It follows that $|U||H| = |U \times H| \leq s|UH| = s|N[H]|$ and hence $|N[H]| \geq \dfrac{|U||H|}{s} = \dfrac{|U||H|}{|H \cap U^2|}$. Our first lower bound below will significantly improve this. Of course, since $|N[H]| = [U : H]|H|$, estimating $|N[H]|$ amounts to estimating the index $[U : H]$. Suppose we let $m = [U : H]$, and let $V \subseteq U$ be a complete system of distinct left representatives for U with respect to H with $|V| = m$. (In other words, the cosets vH, for $v \in V$, are distinct and give all of the left cosets uH for $u \in U$). We have $v^{-1}u \notin H$ for any two distinct elements u, v of V, and so $V^{-1}V - \{1\} \subseteq U^2 - (H \cap U^2)$. Conversely, if $V^{-1}V - \{1\} \subseteq U^2 - (H \cap U^2)$ then the cosets uH for $u \in V$ are all distinct, and so any direct way of estimating $[U : H]$ entails looking for large subsets V of U for which

$V^{-1}V - \{1\} \subseteq U^2 - (H \cap U^2)$.

We will make use of the following lemma.

Lemma 2.3. Let G be a group and let $U \subseteq G$. Let H be a subgroup of G and let $a = \frac{1}{|U|} \sum_{x \in U} |H \cap x^{-1}U|$. Then $[U : H] \geq \left\lceil \frac{|U|}{a} \right\rceil$.

Proof: Let $k = [U : H]$, and let $\{x_1, x_2, ..., x_k\}$ be a complete system of representatives for the left cosets xH for $x \in U$. Under the equivalence relation R which H induces on U, $xRy \leftrightarrow y^{-1}x \in H$, the equivalence class of any $x \in U$ is $U \cap xH$. Let $m_i = |U \cap x_i H|$ for $i \leq k$. Note that $|H \cap x_i^{-1}U| = |U \cap x_i H| = m_i$ for $i \leq k$. We have

$$\sum_{x \in U} |H \cap x^{-1}U| = \sum_{i=1}^{k} \sum_{x \in U \cap x_i H} |H \cap x^{-1}U| = \sum_{i=1}^{k} m_i^2 \geq \frac{\left(\sum_{i=1}^{k} m_i\right)^2}{k}$$

$= \frac{|U|^2}{k}$. We have made use of the Cauchy-Schwarz inequality here.

Dividing by $|U|$ we get $a \geq \frac{|U|}{k}$, which gives the lemma. □

Theorem 2.4. Let (G, U) be a Cayley graph, and let H be a subgroup of G. Then

(i) $|N[H]| \geq \left\lceil \frac{|U|^2}{r_1(|H \cap U^2| - 1) + |U|} \right\rceil |H|$.

(ii) If H is independent then $|N[H]| \geq \left\lceil \frac{|U|^2}{r_2(|H \cap U^2| - 1) + |U|} \right\rceil |H|$.

Proof: The two statements have similar proofs. We will present the argument for the second one.

Assume that H is independent and consider the set of ordered pairs $C = \{(u, p) : p \in (H \cap U^2) - \{1\}\ , u \in U$ and there is an element $v \in U$ such that $uv = p\}$. Note that, since H is independent, by 2.1(v) above, $p \in (H \cap U^2) - \{1\} \to p \notin U$. For any $p \in (H \cap U^2) - \{1\}$, the number of elements u for which $(u, p) \in C$ is clearly $|M(p)|$, where $M(p)$ is defined in the statement of Theorem 2.2. It follows that, for every such element p, there are at most r_2 elements u such that $(u, p) \in C$. Therefore $|C| \leq r_2(|H \cap U^2| - 1)$.

On the other hand, let u be any element of U. For any element x in $(U \cap u^{-1}H) - \{u^{-1}\}$, let $p = ux$. Clearly $p \in (H \cap U^2) - \{1\}$ and $(u, p) \in C$. Conversely, if p is any element of $(H \cap U^2) - \{1\}$ for which $(u, p) \in C$, we have $p = ux$ for some $x \in U$. For such an element x we have $x = u^{-1}p$ and so $x \in U \cap u^{-1}H$. We also have $x \neq u^{-1}$, and so it follows that $p = ux$ for some $x \in (U \cap u^{-1}H) - \{u^{-1}\}$. Therefore the number of elements p for which $(u,p) \in C$ is $|(U \cap u^{-1}H) - \{u^{-1}\}| = |U \cap u^{-1}H| - 1$. Therefore we have

$$|C| = \sum_{u \in U} (|U \cap u^{-1}H| - 1) = \sum_{u \in U} |U \cap uH| \ - \ |U| \ .$$

It follows that $\sum_{u \in U} |U \cap uH| \ - \ |U| \ \leq \ r_2(|H \cap U^2| - 1)$, and therefore that

$$\frac{1}{|U|} \sum_{u \in U} |U \cap uH| \ \leq \ \frac{r_2(|H \cap U^2| - 1)}{|U|} \ + \ 1.$$

In other words, using the notation of Lemma 2.3, we have

$a \leq \dfrac{r_2(|H \cap U^2| - 1)}{|U|} \ + \ 1$, from which it follows that

$\dfrac{1}{a} \ \geq \ \dfrac{|U|}{r_2(|H \cap U^2| - 1) + |U|}$. Now Lemma 2.3 implies that

$$|N[H]| = [U : H]|H| \geq \left\lceil \frac{|U|}{a} \right\rceil \ |H| \geq \ \left\lceil \frac{|U|^2}{r_2(|H \cap U^2| - 1) + |U|} \right\rceil |H| \ . \ \square$$

A closer look at the proof of Theorem 2.4 gives the following corollary.

Corollary 2.5. Let (G, U) be a Cayley graph, and let H be a subgroup of G. Then

(i) $|N[H]| \ = \ \max_{V \subseteq U} \left\lceil \dfrac{|V|^2}{r_1(|H \cap V^{-1}V| - 1) + |V|} \right\rceil |H|$.

(ii) If H is independent then $|N[H]| \ = \ \max_{V \subseteq U} \left\lceil \dfrac{|V|^2}{r_2(|H \cap V^{-1}V| - 1) + |V|} \right\rceil |H|$.

Proof: We can replace U by any subset V of U in the proofs of (i) and (ii) of Theorem 2.4, taking care to replace U^2 by $V^{-1}V$ as appropriate (note that V is not assumed to satisfy $V^{-1} = V$ here). The only modification required is to change slightly the definition of the set C to become the set of pairs (u,p) for which $u \in V^{-1}, p \in H \cap V^{-1}V$ and for which there is a $v \in V$ with $uv = p$. There results corresponding lower bounds for $[V : H]$ and $|VH|$ which are identical to those in 2.4, with $|H \cap V^{-1}V|$ in place of $|H \cap U^2|$. Since $VH \subseteq UH$, it follows that the left-hand side is at least as big as the ght in each of the two statements in the corollary. On the other hand, if we ıoose V to be a complete set of distinct left representatives for U relative › H, we then have $H \cap V^{-1}V = \{1\}$. For this subset V of U, the right-and sides of (i) and (ii) are just equal to $|V||H| = [U : H]|H| = |N[H]|$. □

The corollary suggests a useful direction to take in certain kinds of com-›utational work. Suppose we are trying to estimate how many elements of ι Cayley graph (G, U) can be dominated by a subgroup of size m. We night begin with some particular subgroup H of this size. We can then try ;o identify a subset V of U(which is as large as possible) for which the elements of $V^{-1}V$ are easy to describe, and for which we can then try to find a conjugate subgroup $H' = gHg^{-1}$ which contains as few of these elements as possible. We can then use H' and V in the right-hand side of 2.5 to give a good lower bound. This approach will be illustrated for the permutation graph in the next section. A related idea, which we have also found to be useful for the permutation graph, is to try to construct a dominating set from a subgroup together with one of its cosets. Since, for any given element g of G, $N[gH] = UgH = \bigcup_{u \in U} ugH$, the elements of G dominated by gH which are not already dominated by H consist of the elements of the cosets ugH for $u \in U - UHg^{-1}$. That is, $N[gH] - N[H] = VgH$, where $V = U - UHg^{-1}$. Since $|VgH| = |(VgH)g^{-1}| = |V(gHg^{-1})| = |VH'|$, where $H' = gHg^{-1}$, we can estimate $|N[gH] - N[H]|$ using the above lower bound applied to the subgroup H' and the subset $V = U - UHg^{-1}$. (We remark that $|V| = |Vg| = |Ug - UH| = |N[g] - N[H]|$ is the number of elements of G which are dominated by g but which are not dominated by any of the elements of H.) This leads to the following corollary.

Corollary 2.6. Let (G, U) be a Cayley graph, and let H be a subgroup of G. Let $g \in G - H$, and let $V = U - UHg^{-1}$. Then

$$|N[H \cup gH]| \geq \left\lceil \frac{|U|^2}{r_1(|H \cap U^2| - 1) + |U|} \right\rceil |H| + \left\lceil \frac{|V|^2}{r_1(|(gHg^{-1}) \cap V^{-1}V| - 1) + |V|} \right\rceil |H|.$$

If both H and gHg^{-1} are independent the same results hold with r_2 in place of r_1.

The preceding lower bounds can also be used to give crude estimates for the domination number $\gamma(G)$. For any subset S of G, the set $S \cup (G - N[S])$ is a dominating set for G, and so $\gamma(G) \leq |S| + |G - N[S]|$. If we take S

to be a subgroup of G (or the union of a subgroup and one or more of its cosets) we can then use the above lower bounds to get an upper bound for $|G - N[S]|$ and hence for $\gamma(G)$. One might attempt to find a subgroup H (and coset gH) for which this will result in as small a dominating set as possible. In this regard, note that one can in general improve on the set $S \cup (G - N[S])$. Indeed, if D is any subset of G which dominates $G - N[S]$ then $S \cup D$ is a dominating set for G. Given a set S, one can then try to find a small subset D of G which dominates the set $T = G - N[S]$. One direct approach is the *greedy algorithm*: one inductively selects elements $x_1, x_2, ..., x_i, ...$ in G so that, of all the elements $x \in G$, the element x_i dominates the largest number of elements of $T - N[\{x_j : j < i\}]$. After the procedure is completed, the set $D = \{x_1, x_2, ...\}$ dominates all the elements of $G - N[S]$. This algorithm is applied in Theorem 2.2 of [1] where it is used to derive a basic estimate for the domination number of an arbitrary graph.

The idea of trying to construct small dominating sets in Cayley graphs (G, U) using subgroups and their cosets suggests the following type of greedy algorithm: starting with a subgroup H, inductively choose cosets $x_0 H = H$, $x_1 H$, $x_2 H, ...,$ $x_i H, ...$ so that, of all cosets xH, the coset $x_i H$ dominates the largest number of elements of the set $G - N\left[\bigcup_{j<i} x_j H\right]$. By starting with a "good" subgroup H, this type of procedure can indeed result in a small dominating set, as we have found with the permutation graphs discussed in the next section.

It is much easier to obtain another type of lower bound on $|N[H]|$, containing the same ingredients as the one in Theorem 2.4 above, by directly using the inclusion-exclusion principle, as in the following lemma.

Lemma 2.7. Let G be any graph. Let S be any set of vertices in G. Let $a = \delta(G) + 1$ and let $m = |S|$. Let b and c be non-negative integers. Suppose that, for each vertex $x \in S$, there are at most b elements of S distinct from x which have a common neighbour in G with x. And suppose that $|N[x] \cap N[y]| \leq c$ for any two distinct vertices x, y of S. Then

$$|N[S]| \geq m\left(a - \frac{bc}{2}\right).$$

Proof: We use the first two terms in the inclusion-exclusion principle to estimate $\left|\bigcup_{x\in S} N[x]\right|$. We have $\left|\bigcup_{x\in S} N[x]\right| \geq \sum_{x\in S} |N[x]| - \sum_{\{x,y\}\subseteq S} |N[x] \cap N[y]|$.

The second sum is over all two-element subsets of S. Our assumptions imply that there are at most $mb/2$ such subsets $\{x, y\}$ for which $|N[x] \cap N[y]| \neq 0$, and that $|N[x] \cap N[y]| \leq c$ for any such pair. So the second sum is at most $(mb/2)c$. The first sum is at least ma. The result follows. □

Theorem 2.8. Let (G, U) be a Cayley graph, and let H be a subgroup of G. Then

$$|N[H]| \geq |U||H| - \frac{|H|\, r_1}{2} (|H \cap U^2| - 1) .$$

If H is independent the same result holds with r_2 in place of r_1.

Proof: Referring to Theorem 2.1(vi) above, we see that Lemma 2.7 applies with $a = |U|, m = |H|, b = |H \cap U^2| - 1$, and $c = r_1(G)$. □

Just as we did in 2.6 above, we can extend the lower bound in 2.8 so that it applies to a subgroup together with one of its cosets.

Corollary 2.9. Let (G, U) be a Cayley graph, and let H be a subgroup of G. Let $g \in G - H$, and let $V = U - UHg^{-1}$. Then

$$|N[H \cup gH]| \geq (|U|+|V|)|H| - \frac{|H|\, r_1}{2} (|H \cap U^2|+|(gHg^{-1}) \cap V^{-1}V|-2) .$$

If H and gHg^{-1} are independent the same result holds with r_2 in place of r_1.

The lower bounds obtained in 2.4 and 2.8 above are in general non-comparable. For example, in the case when the integer $r_1(|H \cap U^2| - 1)$ is even, comparing the right-hand sides of these two estimates, we can see that

$$\left\lceil \frac{|U|^2}{r_1(|H \cap U^2| - 1) + |U|} \right\rceil |H| \leq |U||H| - \frac{|H|\, r_1}{2} (|H \cap U^2| - 1)$$

$$\longleftrightarrow r_1(|H \cap U^2| - 1)^2 \leq |U|(|H \cap U^2| - 1) .$$

If $|H \cap U^2| - 1 = 0$ then the neighbourhoods of the elements of H are pairwise disjoint and both estimates give $|U||H|$. If $|H \cap U^2| - 1 \neq 0$, then cancelling gives the equivalent statement $r_1(|H \cap U^2| - 1) \leq |U|$. This latter statement may or may not hold, depending on the particular subgroup H.

3. Illustrating the lower bounds

In order to illustrate the lower bounds in 2.4 and 2.8 above for a particular graph or class of graphs we of course need to first find the parameters r_1 and r_2 for those graphs. And to be able to compare these lower bounds to the actual number of elements dominated, the Cayley graphs and their subgroups which are used must either be simple enough or small enough to enable the exact computation of the number of elements dominated. We begin with two simple examples.

Examples

(i) Cyclic groups

Let $n \geq 5$ and let C_n be a cyclic group of order n, with generator x. Let $U = \{1, x, x^{-1}\}$. Note that $U^2 = \{1, x, x^{-1}, x^2, x^{-2}\}$. The Cayley graph (C_n, U) is an n-cycle. In this case, we have $r_1 = 2$ and $r_2 = 1$, and a subgroup H of C_n is independent if and only if H is a proper subgroup. Clearly a proper subgroup H can intersect U^2 in either 1 or 3 elements, with the latter being possible only if n is even. If $H \cap U^2 = \{1\}$, as we remarked above, both of our estimates coincide with $|N[H]| = |U||H|$. In the case when n is even and $|H \cap U^2| = 3, H$ is equal to $< x^2 >$ and $|H| = n/2$. In this case we have $N[H] = C_n$. Again both of our estimates coincide with $|N[H]|$: our first lower bound (2.4(ii) above with $r_2 = 1$) is $\lceil 9/5 \rceil |H| = 2|H| = |C_n| = |N[H]|$, and the second(2.8 with $r_2 = 1$) is $3|H| - (|H|/2)(2) = 2|H| = |N[H]|$. □

(ii) The permutation graph with respect to adjacent transpositions

Let $n \geq 3$, and let G_n be the symmetric group on $\{1, 2, ..., n\}$. The identity element of G_n will be denoted by ι. Note that we multiply permutations from left to right. Let U be the set of all adjacent transpositions of $\{1, 2, ..., n\}$ together with the identity. In the Cayley graph (G_n, U), two permutations are adjacent exactly when one can be obtained from the other by interchanging two adjacent elements. We have $|U| = n$. The set U^2 consists of U together with all 3-cycles of the form $(i, i+1, i+2)$ and their inverses, and all products of the form $(i, i+1)(j, j+1)$ for $1 \leq i < j-1 \leq n-2$. Thus $U^2 - \{\iota\}$ consists of $n-1$ 2-cycles, $2n-4$ 3-cycles, and $(n-2)(n-3)/2$ products of 2 disjoint 2-cycles. We have $|U^2| = (n+2)(n-1)/2$, and it is also easy to show that $r_1 = r_2 = 2$. For any subgroup H of the symmetric group, let $t_2(H)$ be the number of adjacent transpositions which belong to

H, let $t_3(H)$ denote the number of 3-cycles of the form $(i, i+1, i+2)$ which belong to H, and let $t_{2,2}(H)$ be the number of permutations of the form $(i, i+1)(j, j+1)$ for $1 \leq i < j-1 \leq n-2$ which belong to H. We note that H is independent if and only if H contains no adjacent transpositions, and that $|H \cap U^2| = 1 + t_2(H) + 2t_3(H) + t_{2,2}(H)$. In general the computation of $|N[H]|$ is non-trivial, and any assessment of our lower bounds is severely limited by our having no general way to describe all the possible subgroups H(and their elements) corresponding to the possible sizes of $|H \cap U^2|$. Our first lower bound for $|N[H]|$ is $\left\lceil \frac{n^2}{n + 2t_2(H) + 4t_3(H) + 2t_{2,2}(H)} \right\rceil |H|$, and our second is $n|H| - |H|(t_2(H) + 2t_3(H) + t_{2,2}(H))$.

Here are some sample calculations we have found with the help of GAP [5]. For $n = 4$, the subgroup $H =< (12)(34), (13), (24) >$ has cardinality 8 and dominates G_4. That is $N[H] = G_4$.(In fact this is the smallest size of a dominating subgroup for G_4.) We have $|H \cap U^2| = 2$. Our first lower bound is $\lceil \frac{4^2}{2(2-1)+4} \rceil |H| = 3|H| = 24 = |N[H]|$. The second lower bound also gives $|N[H]|$ exactly. For the 4-element subgroup $K =< (14), (23) >$, we have $|K \cap U^2| = 2$ and $|N[K]| = 12$. Our lower bounds are again exact: in the first case $\lceil \frac{4^2}{2(2-1)+4} \rceil |K| = 3|K| = 12 = |N[K]|$, and in the second $4|K| - |K|(2-1) = 3|K| = |N[K]|$. On the other hand, consider the subgroup $L =< (12), (34) >$, which is a conjugate of K. We have $|L \cap U^2| = 4$ and $|N[L]| = 8$. Our first lower bound is again equal to $|N[L]|$ in this case, but the second is $4|L| - |L|(4-1) = |L| = 4$. An example for $n = 5$ where both lower bounds fall short is the subgroup $M =< (24)(35), (23)(45), (234) >$. We have $|M| = 12, |M \cap U^2| = 6$, and $|N[M]| = 36$. Our first lower bound for $|N[M]|$ is $\lceil \frac{5^2}{2(6-1)+5} \rceil |M| = 2|M| = 24$. In this example, since $|M \cap U^2|$ is so large in relation to $|U|$, the second lower bound is pathetic: $5|M| - |M|(6-1) = 0$.

If one wants to estimate, for a given integer m, how many elements of G_n can be dominated by a subgroup of size m, note that our lower bounds will be best when $t_2(H) + 2t_3(H) + t_{2,2}(H)$ is smallest. Therefore we want to find, of all subgroups H of G_n of size m, one for which the quantity $f(H) = t_2(H) + 2t_3(H) + t_{2,2}(H)$ is minimum. At present, owing to our lack of knowledge on these kinds of parameters for arbitrary subgroups of G_n, we have no general results to help with this question. In this graph, and even more so in our next example, explicit computation also seems to be a forbidding task for $n \geq 10$. The GAP program [5] provides generating sets for representatives of all of the conjugacy classes of the subgroups of the symmetric group. While the set of representatives may be sufficiently small to work with, the number of conjugates one must consider is prohibitive. Further work is required to determine, in terms of H, how large

$|N[H']|$ can be, or how small $f(H')$ can be, for any conjugate H' of H. The conjugacy class representatives do, however, enable some deductions. For example, suppose we are looking at a specific subgroup H of G_n, with $|H| = m$, say, and its conjugacy class. Now most of the elements of U^2 are products of 2 disjoint 2-cycles, $(n-2)(n-3)/2$ to be exact. Suppose we let W denote the set of such elements of U^2. If we can find a conjugate $H' = H^g$ of H which contains none of the elements of W, then it also follows that H' could contain at most two adjacent transpositions. And since $(i+1, i+2, i+3) \cdot (i, i+1, i+2) = (i, i+1)(i+2, i+3)$, H' could contain no more than half of the $2n-4$ three-cycles of $U^2 - \{\iota\}$. So we would have $|H' \cap U^2| - 1 \leq 2 + n - 2 = n$. Our first lower bound would then show that there is a subgroup H' of size m for which $|N[H']| \geq (n/3)m$. Can we tell whether such a conjugate can be found? A sufficient condition can be formulated as follows. First note that if p_1 and p_2 are both products of 2 disjoint 2-cycles, there are $8(n-4)!$ elements g of G_n for which $p_1^g = p_2$. So there are at most $8(n-4)!(n-2)(n-3)/2 = 4(n-2)!$ elements g for which p_1^g is equal to an element of W. Now let $c_{22}(H)$ be the number of elements of $|H|$ which are the disjoint product of two 2-cycles. It then follows that there are at most $4(n-2)!\ c_{22}(H)$ elements g of G_n for which H^g contains an element of W. So if $4(n-2)!\ c_{22}(H) < n!$ there is a conjugate of H which is disjoint from W. So we simply check whether $c_{22}(H) < n(n-1)/4$. If this holds, such a conjugate exists. In the same way, we can find a sufficient condition so that some conjugate of H intersects U^2 in only the identity element: namely, that $2(n-1)c_2(H) + 6c_3(H) + 4c_{22}(H) < n(n-1)$, where $c_2(H)$ and $c_3(H)$ denote the number of 2-cycles and 3-cycles respectively which belong to H. We thus have the following result.

Theorem 3.1. Let H be a subgroup of G_n with $|H| = m$. Let $c_2(H)$ and $c_3(H)$, respectively, denote the number of 2-cycles and 3-cycles which belong to H, and let $c_{22}(H)$ be the number of elements of $|H|$ which are the disjoint product of two 2-cycles.
(i) If $c_{22}(H) < n(n-1)/4$ then there is a subgroup H' of G_n with $|H'| = m$ for which $|N[H']| \geq (n/3)m$.
(ii) If $2(n-1)c_2(H) + 6c_3(H) + 4c_{22}(H) < n(n-1)$ then there is a subgroup H' of G_n with $|H'| = m$ for which $|N[H']| = nm$.

Computationally these kinds of conditions can provide at least some useful information, for somewhat larger values of n, by checking if such conditions hold for the subgroup conjugacy class representatives. This kind of approach can clearly be refined, and we hope to do so in future work.

We remark that little seems to be known in general about the domination number of G_n. A related question was considered in [3]: does there exist a subset C of G_n such that every element p of G_n can be *uniquely* represented as $p = ux$ for some element $u \in U$ and some element $x \in C$? Such a set C must have size $(n-1)!$. Elegant arguments using group representations are used in [3] to show that the answer is negative for a large class of values of n. The same type of question was investigated in a much earlier paper [11], also using group representations, with the set of all transpositions(together with ι) in place of the set U. Although our lower bounds are somewhat crude, they can provide some useful initial estimates for $\gamma(G_n)$, at least for small values of n. For example, in G_5, for any subgroup H, we can apply the greedy algorithm to obtain a dominating set D_H for $G_5 - N[H]$. The smallest value of $|H| + |D_H|$ that we find in this way, over all subgroups H of G_5, is 31, and so $\gamma(G_5) \le 31$. □

(iii) The permutation graph

Let $n \ge 3$, and let S_n be the symmetric group on $\{1, 2, ..., n\}$. As in example (ii) above, we denote the identity element of S_n by ι. Let U consist of ι together with all cycles of the form $(i, i+1, i+2, ..., j)$, where $1 \le i < j \le n$, and their inverses $(j, j-1, j-2, ..., i)$. These cycles will be referred to as *consecutive cycles.* We refer to the Cayley graph (S_n, U) as *the permutation graph.* (As usual, we will leave out the commas in using cycle notation whenever it will not lead to ambiguity.) We have $|U| = 1 + (n-1)^2$, and it can be shown that $|U^2| = \frac{1}{2}(n^4 - 6n^3 + 13n^2 - 10n + 6)$. The elements of U^2 are either cycles or products of two disjoint cycles. With some work, one can find explicit formulas, for $k = 2, 3, ..., n$, for the number $c_k(U^2)$ of cycles of length k which belong to U^2, and, for $2 \le k \le l \le n$, for the number $c_{k,l}(U^2)$ of elements of U^2 which are equal to the disjoint product of a k-cycle and an l-cycle. For example, all transpositions in S_n belong to U^2 and $c_2(U^2) = n(n-1)/2$, and, for $n \ge 4$, the number of n-cycles which belong to U^2 is $c_n(U^2) = n^2 - n - 6$. We will not need such formulas here.

In addition to giving a permutation by means of its disjoint cycle decomposition, we will also exhibit a permutation p as the ordered list $p(1), p(2), ..., p(n)$. If I is any subset of the set $\{1, 2, ..., n\}$, we will let $p - I$ denote the permutation of length $n - |I|$ obtained from p by deleting all of the elements of I from p and concatenating the remaining elements. If $I = \{i\}$, we write $p - i$ instead of $p - \{i\}$. For example, if p is $5, 1, 4, 2, 3$ then $p - 2$ is $5, 1, 4, 3$, and $p - \{1, 2\}$ is $5, 4, 3$.

Let $p \in S_n$ and let $u = (i, i+1, i+2, ..., j)$. Note that, as an ordered list, $q = up$ is the permutation obtained from p by moving the element $p(j)$ from its position in p into a new position immediately to the left of the element $p(i)$, and leaving all the other elements of p in their same relative order. If $p(j) = k$, we will say that q is obtained from p *by moving* k. To illustrate, in S_5, let $u = (234)$ and let $p = (15342)$. As a list, p is $5, 1, 4, 2, 3$, and so up is the list obtained by moving the fourth element of the list p immediately to the left of the second element of p, resulting in the list up given by $5, 2, 1, 4, 3$. This is equivalent to the equation $(234)(15342) = (153)$. We can therefore express the adjacency relation in the Cayley graph (S_n, U) as follows: for $p \neq q$ in S_n we have

$$p \sim q \text{ in } (S_n, U) \;\leftrightarrow\; p - k = q - k \quad \text{for some } k \leq n.$$

That is, $p \sim q$ in (S_n, U) if q can be obtained from p by changing the position of one element of p relative to the others. As we discussed in section 1 above, it is this form in which the adjacency relation has been employed in earlier work on this graph ([6], [9]).

Our first task is to determine the parameters r_1 and r_2 for S_n. Their values illustrate that, for some Cayley graphs, our lower bounds for *independent* subgroups of a given size will be much better than for arbitrary subgroups of the same size.

Lemma 3.2. Let $n \geq 3$. Then
(i) $r_1(S_n) = 2(n-1)$ and (ii) $r_2(S_n) = 4$.

Proof: (i) In part (ii) we will show that two independent vertices of S_n have at most 4 common neighbours, so for part (i) it is enough to show that two adjacent vertices of S_n can have at most $2(n-1)$ common neighbours, and that $2(n-1)$ is attained. Let p and q be adjacent in S_n. We consider two cases. First, if q results from p by interchanging the i'th and $i+1$'th elements of the list p, it is easy to see that p and q have exactly $2(n-1)$ common neighbours: any permutation obtained from p by moving either the i'th or $i+1$'th element of p, into any position, is a common neighbour of p and q, and these are the only common neighbours.

Secondly, suppose q results from p by moving the i'th element of p by more than one position, say to the left, so that it occupies position j in q, where $i > j+1$. It is no loss of generality to assume that p is the identity $1, 2, 3, ..., n$ and so q is $1, 2, ..., j-1, i, j, j+1, ..., i-1, i+1, i+2, ..., n$. Any permutation obtained from p by moving i is a common neighbour of p and q. There are n such permutations (including p and q of course). If $i > j+2$ these are the only common neighbours: moving any element of p other than i will not result in a permutation which is adjacent to q. If $i = j+2$ there is one additional common neighbour: the permutation $1, 2, ..., j-1, j+1, j+2, j, j+3, ..., n$ which can be obtained from p by moving j and from q by moving $j+1$. So in this case there are $n+1$ common neighbours. Since $2(n-1) \geq n+1$, this proves (i).

(ii) If we reverse the first three entries in the identity permutation $1, 2, 3, ..., n$, leaving the others fixed, we get the permutation $3, 2, 1, 4, 5, ..., n$ which is not adjacent to ι. These two permutations have four common neighbours, namely the four permutations of the form $a, b, c, 4, 5, ..., n$ where a, b, c is any ordering of the numbers $1, 2, 3$ other than $1, 2, 3$ and $3, 2, 1$, and where the integers from 4 to n are in their usual order. To prove (ii), we must show that any two non-adjacent permutations in S_n have no more than 4 common neighbours in S_n. So, let p and q be elements of S_n which are not adjacent.

There is another way to characterize non-adjacency in S_n which will be useful here. We will use the following terminology. Let p, q be elements of S_n, and let i and j be integers in the set $\{1, 2, ..., n\}$. We say that $i < j$ in p if i occurs to the left of j in the list p, and we say that the pair $\{i, j\}$ is *opposite* in p and q if $i < j$ in one of the two permutations and $j < i$ in the other. Similarly, a triple of integers $\{i_1, i_2, i_3\}$ is said to be opposite in p and q if, for some permutation r_1, r_2, r_3 of $1, 2, 3$ we have $i_{r_1} < i_{r_2} < i_{r_3}$ in one of the two permutations and $i_{r_3} < i_{r_2} < i_{r_1}$ in the other. Lemma 4.1 in [6] establishes the following:

p is not adjacent to q if, and only if, one of the following two conditions holds: Either there are two disjoint pairs $\{i_1, j_1\}, \{i_2, j_2\}$, both of which are opposite in p and q, or there is a triple of elements $\{i_1, i_2, i_3\}$ which is opposite in p and q.

In applying these conditions we will say that the two pairs $\{i_1, j_1\}, \{i_2, j_2\}$, or the triple $\{i_1, i_2, i_3\}$, as the case may be, *witness* that p is not adjacent to q.

Again we can assume, without loss of generality, that p is the identity permutation $1, 2, 3, ..., n$. We first note that, if p and q have a common neighbour, then there are integers i and j such that $p - \{i, j\} = q - \{i, j\}$. Therefore we can assume that q is obtained from the list $1, 2, ..., n$ by choosing two integers i and j with $i < j$, and moving them relative to the other integers in $1, 2, 3, ..., n$ so that they occupy positions k and l respectively, leaving the other $n - 2$ integers in their usual relative order.

Our proof that $|N[p] \cap N[q]| \leq 4$ is carried out by considering several cases. Case 1 is when $k = i$. The case when $l = j$ is dual to case 1 by writing all lists backwards. Case 2 is when $k < i$ and Case 3 when $k > i$, in both of which we can assume that $l \neq j$. Special subcases of these, such as when $j = i + 1$, are also best treated separately. Since the arguments are similar in all of these cases, we will just give the details for a typical one. We give the proof for the case when the following conditions hold: $k < i$, $k < l$, and $i + 1 < j$. In this case we can display $q - j$ as $1, 2, ..., i, ..., i - 1, i + 1, ..., j - 1, j + 1, ..., n$. In this list i can be anywhere to the left of $i - 1$. In the list q, j is inserted into this latter list and can be anywhere to the right of i except (because q is not adjacent to p), not in its usual position immediately after $j - 1$. Now, let τ be a permutation which is adjacent to q in S_n. So τ can be obtained from q by moving one of the entries of q relative to the others. When can τ also be adjacent to the identity permutation p? Suppose the integer which is moved in obtaining τ from q is i. If i is moved into a position between $i-1$ and $i+1$ then τ is also adjacent to p. If j happens to be between $i-1$ and $i+1$ in q then there are two possibilities for placing i in this way, either immediately to the left or immediately to the right of j. If j is not between $i-1$ and $i+1$ in q, then there is only one. Suppose that τ is obtained from q by moving i into some position which is not between $i-1$ and $i+1$. Then one of the following four sets of two pairs will witness that τ is not adjacent to p : $\{i-1,i\},\{j-1,j\}$, or $\{i-1,i\},\{j,j+1\}$, or $\{i,i+1\},\{j-1,j\}$, or $\{i,i+1\},\{j,j+1\}$. So there are at most 2 common neighbours τ of p and q which can be obtained from q by moving i. On the other hand, if τ is obtained from q by moving j, then τ will also be adjacent to p if j is moved into position between $j-1$ and $j+1$. Since i is not between $j-1$ and $j+1$, there is only one such τ. If τ is obtained from q by moving j into any position other than between $j-1$ and $j+1$, then we can see that τ is not adjacent to p, as witnessed by either the two pairs $\{i-1,i\}$, $\{j-1,j\}$, or by the two pairs $\{i-1,i\},\{j,j+1\}$. So there is at most one common neighbour τ of p and q which can be obtained from q by moving j. Finally, if τ is obtained from q by moving some integer k which is different from both i and j, again, either $\{i-1,i\}$ and $\{j-1,j\}$ or $\{i-1,i\}$ and $\{j,j+1\}$ witness that τ is not adjacent to p. All together, p and q have at most three common neighbours τ.

The same kind of argument can be used in all the other cases. Given q not adjacent to p, we first identify either two pairs or a triple of integers which witnesses the non-adjacency, as described above. Any neighbour τ of q which is also adjacent to p must be obtainable from q by moving one of the four integers of the two pairs, or one of the three integers in the triple, as the case may be. By considering the possible acceptable positions into which these three or four integers can be moved, one shows that at most 4 common neighbours result. □

Using $r_2 = 4$, for any independent subgroup H of S_n our two lower bounds for $|N[H]|$ are, respectively:

$$\left\lceil \frac{n^4-4n^3+8n^2-8n+4}{n^2-2n-2+4|H\cap U^2|} \right\rceil |H| \quad \text{and} \quad \left[\, n^2-2n+4-2|H\cap U^2| \,\right] |H| \,.$$

We will get a lower bound of the same order as $n^2|H|$ in the second case when $|H\cap U^2| = O(n)$, but in the first case when $|H\cap U^2| = O(n^2)$, and so the first lower bound will be more useful in general.

Using the value $r_1 = 2(n-1)$ for arbitrary (not necessarily independent) subgroups H, our first lower bound for $|N[H]|$ is

$$\left\lceil \frac{n^4 - 4n^3 + 8n^2 - 8n + 4}{n^2 - 4n + 4 + (2n-2)|H \cap U^2|} \right\rceil |H|$$

This lower bound will be of the same order as $n^2|H|$ provided $|H \cap U^2| = O(n)$.

Here are some examples, for small values of n, comparing our first lower bound with the actual values. In S_4, the 4-element subgroup $H =< (1423) >$ is an independent dominating set: $|H \cap U| = 1$ and $|N[H]| = 24$. We have $|H \cap U^2| = 4$. Our lower bound for $|N[H]|$ is $\left\lceil \frac{(10)^2}{4(4-1)+10} \right\rceil (4) = 20$. This subgroup has a conjugate H^g, for $g = (243)$, which is also independent, also dominates S_4, but for which $|H^g \cap U^2| = 3$. Our lower bound for $|N[H^g]|$ is exact: $\left\lceil \frac{(10)^2}{4(3-1)+10} \right\rceil (4) = 24$. Another dominating subgroup of S_4 is the 8-element subgroup $K =< (12), (34), (13)(24) >$. We have $|N[K]| = 24$, $|K \cap U| = 3$ and $|K \cap U^2| = 7$. Our lower bound is again exact: $\left\lceil \frac{(10)^2}{6(7-1)+10} \right\rceil (8) = 24$.

In S_5, consider the 6-element subgroup $H =< (345), (45) >$. One finds that $|H \cap U| = 5$ and $|H \cap U^2| = 6$, and that $|N[H]| = 54 = 9|H|$. Using $r_1 = 2(5-1) = 8$, our lower bound is $|N[H]| \geq 36 = 6|H|$. Calculating the value $|H^g \cap U^2|$ for all conjugates of H in S_5(with the help of GAP), we find that the minimum value is 4 and occurs for $g = (124)(35)$. For this value of g, the subgroup H^g happens to be independent, and we find that $|N[H^g]| = 66 = 11|H^g|$. Our lower bound for $|N[H^g]|$ is $\left\lceil \frac{(17)^2}{4(4-1)+17} \right\rceil (6) = 60 = 10|H^g|$. Another interesting example in S_5 is the 8-element subgroup $K =< (23), (45), (24)(35) >$. We have $|N[K]| = 64 = 8|K|$, $|K \cap U| = 3$ and $|K \cap U^2| = 7$, and our lower bound is $5|H| = 40$. If we calculate the value $|K^g \cap U^2|$ for all conjugates of K in S_5, we find that the minimum value is 3 and occurs for $g = (12)$. For this value of g, we have $|N[K^g]| = 88 = 11|K^g|$, $|K^g \cap U| = 2$ and our lower bound for $|N[K^g]|$ is $9|H| = 72$. One further finds that the value $|N[K^g]| = 88$ is in fact the maximum of $|N[H]|$ over all 8-element subgroups of S_5.

For $n = 6$, GAP gives three different conjugacy classes for subgroups of S_6 of size 36. A representative of the first of these is $H =< (23), (123), (56), (456) >$, for which we find that $|H \cap U| = 9$ and $|H \cap U^2| = 27$, and that $|N[H]| = 216 = 6|H|$. Using $r_1 = 2(6-1) = 10$, our lower bound for $|N[H]|$ is just $108 = 3|H|$. Among all the conjugates

H^g of H, there is one which is independent, for $g = (1245)(36)$. For this conjugate we have $|H^g \cap U| = 1$, $|H^g \cap U^2| = 16$, and $|N[H]| = 360 = 10|H|$, and using $r_2 = 1$, our lower bound for $|N[H^g]|$ is $288 = 8|H|$. The largest number of elements of S_6 dominated by any of the conjugates of H turns out to be 396, realized with $g = (124635)$.

The other two conjugacy classes can be examined similarly. For the second, we take the representative $H =< (123), (456), (23)(56), (14)(2536) >$. We find that $|H \cap U| = 5$ and $|H \cap U^2| = 13$, and that $|N[H]| = 432 = 12|H|$, and our lower bound for $|N[H]|$ is very weak: $180 = 5|H|$. Again, by examining all of the conjugates H^g of H in S_6, we find one which is independent, for $g = (125364)$. For this conjugate we have $|H^g \cap U| = 1$ and $|H^g \cap U^2| = 10$, and $|N[H]| = 540 = 15|H|$, and our lower bound for $|N[H^g]|$ is $396 = 11|H|$. By further computing $|N[H^g]|$ for all of the conjugates of H in S_6, and for all the subgroups in the third conjugacy class, we find that the largest number of elements of S_6 dominated by a subgroup of size 36 is $612 = (17)(36)$, which is realized by $H =< (123), (456), (23)(56), (14)(2536) >$ and $g = (124635)$. This subgroup $K = H^g$ is independent and $|K \cap U^2| = 8$. Our lower bound gives $|N[K]| \geq 468 = (13)(36)$. The only way our lower bound could possibly give a larger value for a subgroup K of size 36 is if we were to use a subgroup K for which $|K \cap U| = 1$ and $|K \cap U^2| = 7$, but no such subgroup exists in S_6. □

Our numerical examples indicate that independence is greatly to be desired to obtain good lower bounds. We can find a sufficient condition for a conjugate of H to be independent in S_n using the same method as we did for G_n in (ii). We note that, for $k = 3, 4, ..., n$, the set U contains $2(n-k+1)$ cycles of length k, and U contains $n-1$ cycles of length 2. Let H be a subgroup of S_n, and, for $k = 2, 3, ..., n$, let $c_k(H)$ be the number of cycles of length k which belong to H. If p_1 and p_2 are k-cycles, there are $k(n-k)!$ elements g of S_n for which $p_1^g = p_2$. So, if $k > 2$, there are at most $2(n-k+1)k(n-k)! = 2k(n-k+1)!$ elements g for which p_1^g is equal to an element of U and there are at most $(n-1)2(n-2)! = 2(n-1)!$ such g for $k = 2$. It follows that there are at most $2c_2(H)(n-1)! + \sum_{k=3}^{n} 2kc_k(H)(n-k+1)!$ elements g for which H^g contains an element of $U - \{\iota\}$. For any other g, the conjugate H^g will be independent. So we get the following sufficient condition.

Theorem 3.3 Let H be a subgroup of S_n, and for $k \geq 2$, let $c_k(H)$ be the number of cycles of length k which belong to H.

If $2c_2(H)(n-1)! + \sum_{k=3}^{n} 2kc_k(H)(n-k+1)! < n!$ then there is a conjugate of H which is independent in S_n.

The condition in 3.3 can be useful for estimating how many elements of S_n can be dominated by a subgroup of a given cardinality. If the condition holds for a given subgroup of size m, we can then find an independent subgroup of size m for which we can then use our lower bound. While this condition is easy to check for any given subgroup, it is not a necessary condition for a subgroup to have an independent conjugate. For example, in S_5, the subgroup $H = <(345), (45)>$ has an independent conjugate, whereas the condition fails for H. Moreover, we do not as yet know for which m there is a subgroup H of S_n of size m for which the condition holds. This in itself appears to be a challenging question.

In a similar way, one can formulate conditions implying that some conjugate of H has a prescribed small intersection with U^2, utilizing the number $c_k(U^2)$ of cycles of length k which belong to U^2, and, for $2 \leq k \leq l \leq n$, the number $c_{k,l}(U^2)$ of elements of U^2 which are equal to the disjoint product of a k-cycle and an l-cycle (as mentioned at the beginning of example (iii), these comprise all of the elements of U^2). We will not pursue such conditions here.

In general, the most we can expect from our lower bound is an estimate for $|N[H]|$ having order $n^2|H|$. One way to try to find a subgroup H which gives an estimate of this order is to first identify a subset V of U, with $|V|$ of order n^2, for which we can formulate a simple condition for a subgroup H to satisfy the condition that $|H \cap V^{-1}V| = O(n)$. A subgroup H satisfying such a condition would then give an estimate of order $n^2|H|$, since

$$|N[H]| = |UH| \geq |VH| \geq \left\lceil \frac{|V|^2}{r_1(|H \cap V^{-1}V| - 1) + |V|} \right\rceil |H| \, .$$

One promising possibility is the set V consisting of all "increasing" cycles in U of length $> n/2$, that is, all cycles of the form $(i, i+1, ..., j)$, where $1 \leq i < j \leq n$ and $j - i > (n/2) - 1$. We have $|V| = n(n+2)/8$ if n is even and $|V| = (n+1)(n+3)/8$ if n is odd. For any distinct elements x and y of V, the product $x^{-1}y$ is a cycle of a particular form. To describe this form, let us use the following notation. If A and B are disjoint ordered subsets of $\{1, 2, ..., n\}$, then (A, B) will denote the cycle of length $|A|+|B|$ obtained by listing all the elements of A, in their given order, before all of the elements of B, which are listed in their given order. We allow the possibility that one of A or B is empty, with the obvious meaning for (A, ϕ) and (ϕ, B).

For example, in S_7, let $A = \{3, 2\}$, and let $B = \{5, 6, 7\}$. Then (A, B) is the 5-cycle (32567). Let us say that a cycle in S_n is *special* if it can be written in the form (A, B) where A is either empty or is a consecutive increasing or consecutive decreasing subset of the set $\{1, 2, ..., \lceil n/2 \rceil\}$ and B is either empty or is a consecutive increasing or consecutive decreasing subset of the set $\{\lceil n/2 \rceil + 1, \lceil n/2 \rceil + 2, ..., n\}$. It is easy to see that $x^{-1}y$ is a special cycle for any distinct elements x and y of V.(We remark that $V^{-1}V$ does not contain all special cycles, but we do not need the exact number of elements belonging to $V^{-1}V$ here.) This leads to the following condition.

Theorem 3.4. Let H be a subgroup of S_n and let $s(H)$ be the number of special cycles which belong to H. If $s(H) = O(n)$ then $|N[H]|$ is of order $n^2|H|$.

The condition in 3.4 of course leads to more questions. For what orders of subgroups of S_n does there exist a subgroup H with $s(H) = O(n)$? Can we always find one of order $(n-2)!$? We hope to take up such questions in future work.

4. Concluding remarks

How many elements of the permutation graph S_n can be dominated by a subgroup of size m?

What is the smallest size of a subgroup of S_n which dominates S_n ?

The results in section 2 and example 3(iii) above unfortunately do not lead to definitive answers to either of these questions. For those results to provide good general estimates, what is further required is an understanding of the values of functionals of the form $\sum_k a_k c_k(H)$ on the subgroups H of S_n. For the second question, let s_n be the smallest size of a subgroup of S_n which dominates S_n. Direct computational methods are possible for small values of n, and it can be determined that $s_4 = 4, s_5 = 10$, and $s_6 = 60$. Since S_{n-1} dominates S_n, we have $s_n \leq (n-1)!$. And if $N[H] = S_n$, it obviously follows that $n! \leq |H|(1 + (n-1)^2)$, and so $|H|$ must have order at least $(n-2)!$. Beyond this scant information, we are not aware of any other general estimates or constructions. A compelling question here is whether $s_n = O((n-2)!)$. A similar open question concerns $\gamma(S_n)$, the domination number of S_n. We note that, when applied to S_n, the basic upper bound for domination number in arbitrary graphs, Theorem 2.2 of [1], implies that $\gamma(S_n) = O((n-2)! \log n)$. As we mentioned in the introduction, we have found that $\gamma(S_4) = 4$ and $\gamma(S_5) = 10$. In both cases, there is a minimum dominating set which is a subgroup. For $n = 5$, after having found a dominating subgroup of size 10, we showed that $\gamma(S_5) \geq 10$

by solving a corresponding integer program. We are grateful to James Currie for his considerable help in this and subsequent computational work. As for $n = 6$, we have $\gamma(S_6) \leq 48$. We can exhibit a subgroup $H =< (15)(23), (23)(46), (134)(265), (13)(25) >$ of S_6 having 24 elements, and a coset aH, (with $a = (12)$), for which $H \cup aH$ dominates S_6. We have been unable to determine whether 48 is minimum. One other computational result is worth mentioning: $\gamma(S_7) \leq 240$. A construction in [7] utilizes the subgroup $K =< (1234567), (12)(36) >$. Here we have $|K| = 168$, and K dominates 4872 elements of S_7. Applying the greedy algorithm, 72 additional elements of S_7 are found which dominate $S_7 - N[K]$. In all cases of which we are aware, S_n has a dominating set of cardinality $2(n-2)!$ and it seems reasonable to conjecture that $\gamma(S_n) \leq 2(n-2)!$ for $n \geq 4$. An interesting related question is whether n divides $\gamma(S_n)$ for $n \geq 4$.

There is a simple connection between covering designs and dominating sets in S_n which gives further reason to conjecture that $\gamma(S_n) = O((n-2)!)$. Let n and k be positive integers with $k < n$. Recall that a collection of subsets $\mathcal{C}$ of the set $\{1, 2, ..., n\}$ is called an $(n, k+1, k)$ *covering* if $|C| = k+1$ for all $C \in \mathcal{C}$ and if every k-element subset of $\{1, 2, ..., n\}$ is contained in a set belonging to $\mathcal{C}$. Let $z_{n,k}$ be the minimum cardinality of an $(n, k+1, k)$ covering. We will also use the following notation, where we are again thinking of a permutation just as an ordered list. Suppose A is a subset of $\{1, 2, ..., n\}$. If p is a permutation of the elements of A and q is a permutation of the elements of $\{1, 2, ..., n\} - A$, we will let $p \star q$ denote the permutation of $\{1, 2, ..., n\}$ obtained by concatenating the two lists.

Theorem 4.1
(i) Let n and k be positive integers with $k < n$. Then
$\gamma(S_n) \leq z_{n,k}\ k!\ (n-k-1)!$
(ii) If $z_{n,\lceil n/2 \rceil} = O\left(\frac{1}{n}\binom{n}{\lceil n/2 \rceil}\right)$ then $\gamma(S_n) = O((n-2)!)$

Proof: (i) Let $\mathcal{C}$ be an $(n, k+1, k)$ covering of the set $\{1, 2, ..., n\}$ such that $|\mathcal{C}| = z_{n,k}$. For each C in $\mathcal{C}$, consider the set S_C consisting of all permutations of C, which is isomorphic to S_{k+1}. By Theorem 3.1 of [9], the graph S_{k+1} has an independent set of cardinality $k!$. This implies that there is a subset I_C of S_C, with $|I_C| = k!$ having the property that every k-permutation of elements of C is a subsequence of exactly one permutation belonging to I_C. Let $C' = \{1, 2, ..., n\} - C$ and let $S_{C'}$ be the set of all permutations of C'. For each $C \in \mathcal{C}$, let $T_C = \{p \star q : p \in I_C \text{ and } q \in S_{C'}\}$. Finally let $T = \bigcup_{C \in \mathcal{C}} T_C$. Clearly $|T| = z_{n,k}\ k!\ (n-k-1)!$. To prove (i) we show that T is a dominating set in S_n: Let r be any element of S_n. Let A be the set of elements of $\{1, 2, ..., n\}$ which occur as the first k elements in the list r, and let $r|k$ denote the restriction of r to these elements(so $r|k$

is the list $r(1), r(2), ..., r(k))$. There is a set $C \in \mathcal{C}$ with $A \subset C$, and there is an element p of I_C such that $r|k$ is a subsequence of p. Let i be the element of $C - A$, and let q be the restriction of the list r to the elements of $\{1, 2, ..., n\} - C$. Clearly r can be obtained from $p \star q$ by moving the element i, and so r is adjacent to $p \star q$ in S_n. Since $p \star q \in T$, we have shown that T is a dominating set in S_n.

(ii) For simplicity, suppose n is even, say $n = 2m$. If c is a positive constant and $z_{2m,m} \leq c \frac{1}{2m} \binom{2m}{m}$, then, with $k = m$, part (i) implies that $\gamma(S_n) \leq c\frac{(2m-1)!}{m} \leq 2c(n-2)!$ □

Rödl's celebrated theorem in [10] implies that, for a fixed k, $z_{n,k}$ is asymptotic to $\frac{1}{k+1}\binom{n}{k}$ as $n \to \infty$. (We refer the reader to [4] for a discussion of coverings and related topics.) This, as well as known sizes for various covering designs(as in [12], for example) lends plausibility to the conjecture that $\gamma(S_n) = O((n-2)!)$.

Acknowledgements. The second author would like to thank the Department of Mathematics and Statistics of the University of Winnipeg for their hospitality during the time this research was undertaken.

References

1. N.Alon and J.Spencer, The Probabilistic Method, J.Wiley, 1991.

2. G.Chartrand and L.Lesniak, Graphs and Digraphs, third edition, Chapman and Hall, London, 1996.

3. P.Edelman and D.White, Codes, transforms and the spectrum of the symmetric group, Pacific Journ. Math. Vol. 143, No. 1,(1990), 47-67.

4. P.Erdos and J.Spencer, Probabilisitic Methods in Combinatorics, Academic Press, 1974.

5. GAP, The GAP Group, GAP – Groups, Algorithms and Programming, Version 4.2 ; Aachen, St. Andrews, 1999.

6. J.Ginsburg, A coloring problem on chordal rings, Ars Combinatoria 45(1997), 109-127.

7. J.Ginsburg and S.Gosselin, Dominating sets in S_n for small values of n, Technical report, University of Winnipeg, 2001.

8. I.N.Herstein, Topics in Algebra, 2nd edition, J.Wiley and Sons, 1975.

9. V.I.Levenshtein, On perfect codes in deletion and insertion metric, Discrete Math. Appl. Vol.2, No.3(1992), 241-258.

10. V.Rödl, On a packing and covering problem, European Journal of Combinatorics 5(1985), 69-78.

11. O.Rothaus and J.G.Thompson, A combinatorial problem in the symmetric group, Pacific Journ. Math. Vol. 18, No. 1(1966), 175-178.

12. N.Soltankhah, Directed quadruple designs, in Combinatorics Advances(1995), C.J.Colbourn and E.S.Mahmoodian editors,Kluwer Academic Publishers, The Netherlands.

Department of Mathematics and Statistics, University of Winnipeg, Winnipeg, Manitoba, Canada(j.ginsburg@uwinnipeg.ca)

Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada(sands@math.ucalgary.ca)