Minimal Permutation Representations of Nilpotent Groups

Ben Elias, Lior Silberman, and Ramin Takloo-Bighash

CONTENTS

A minimal permutation representation of a finite group G is a faithful G-set with the smallest possible size. We study the structure of such representations and show that for certain groups they may be obtained by a greedy construction. In these situations (except when central involutions intervene) all minimal permutation representations have the same set of orbit sizes. Using the same ideas, we also show that if the size $d(G)$ of a minimal faithful G-set is at least $c|G|$ for some $c > 0$, then $d(G) = |G|/m + O(1)$ for an integer m, with the implied constant depending on c.

1. INTRODUCTION

It is a classical theorem of Cayley's that a group G is isomorphic to a subgroup of a symmetric group. Accordingly, we let the *degree* $d(G)$ of the finite group G be the least integer d such that G can be embedded in S_d, the symmetric group on d letters. More precisely, the discussion in [Cayley 78] implicitly relies on the observation that the regular action of the group on itself gives an embedding of G into S_n, where $n = |G|$ is the order of G. It is then natural to ask to what extent the resulting bound $d(G) \leq n$ is sharp.

The problem of finding $d(G)$ was first studied by Johnson [Johnson 71]. Among other things, he classified those groups for which $d(G) = n$. Except for a family of 2-groups, these groups are precisely the cyclic p-groups. A structure theorem for groups with $d(G) \geq cn$, c any fixed positive constant, was obtained in [Babai et al. 93] (see Remark 4.2 below), while related results were obtained in [Berkovich 99].

Although easy to define, the degree is difficult to compute. It is more or less obvious that $d(G)$ can be computed by examining all subsets of the subgroup lattice of G. The main conceptual finding of this note is that in some cases a "greedy" algorithm is also available, that

2000 AMS Subject Classification: Primary 20B35, 20D15; Secondary 20D30, 20D60

Keywords: Permutation representations, nilpotent groups, lattices

is, an algorithm that proceeds by making locally optimal choices rather than directly searching for the global minimum. This is hardly of practical application (the subgroup lattice of a group may be exponentially larger than the group itself), but it has surprising consequences for the structure of a minimal permutation representation. We note that whenever a group G acts on a set X, the sizes of the orbits of the action determine a partition of $|X|$. Our main application is the following theorem.

Theorem 1.1. *Let G be a finite nilpotent group of odd order. For each prime p, let e_p be maximal such that the center of G contains a subgroup isomorphic to the elementary abelian group $\mathbb{F}_p^{e_p}$. Let X be a minimal faithful permutation representation of G. Then*

1. *The number of orbits for the G-action on X is $\sum_p e_p$.*
2. *The multiset of sizes of the orbits is a group isomorphism invariant.*

This is a special case of a more general result, Theorem 3.18. We remark that a restriction of the odd-order type is necessary, the simplest counterexample being the four-group $C_2 \times C_2$. Its regular representation is a minimal permutation representation, but it also has minimal representations with two orbits of size 2. Though not strictly necessary for the proofs of Theorems 1.1 and 3.18, we include Theorem 3.16. This theorem, which gives a method to find all *perfect* minimal faithful permutation representations (cf. Definition 3.12), forms the conceptual backbone of our work.

The main motivation of this work was to understand the distribution of $\Delta(G) \overset{\text{def}}{=} d(G)/|G|$ in the interval $[0, 1]$. For example, it was easy to show that every number of the form $\frac{1}{n}$, n a positive integer, is a limit point of $\Delta(G)$ as $|G|$ tends to infinity. Clearly, zero is also a limit point. We show here (Theorem 4.6) that these are the only limit points.

This paper is organized as follows. In Section 2 we recall basic definitions. Section 3 contains our main results. Section 4 contains our study of limit points of $\Delta(G)$ in the interval $[0, 1]$, plus some numerical results.

2. DEFINITIONS

We review some notation dealing with standard constructions of group actions. For further details and basic definitions see, e.g., [Cameron 99, Sections 1.1–1.4] or [Dixon and Mortimer 96, Sections 1.3–1.4]. For basic materials on the socle, see [Dixon and Mortimer 96, Section 4.3].

Let G be a finite group acting on a set X. We call this action a *minimal faithful permutation representation* if the action is faithful and the size of the set X is the smallest possible among all sets on which G acts in a faithful fashion. Under the action of G, the set X decomposes as a disjoint union of orbits. Choosing a point stabilizer subgroup in each orbit, it is clear that minimal faithful permutation representations correspond to collections[1] $\mathcal{H}$ of subgroups of G such that

1. the *core* of $\mathcal{H}$,
$$\mathrm{Core}_G(\mathcal{H}) \overset{\text{def}}{=} \bigcap_{H\in\mathcal{H}} \mathrm{Core}_G(H) = \bigcap_{H\in\mathcal{H}} \bigcap_{g\in G} H^g,$$
is trivial, and
2. $\sum_{H\in\mathcal{H}}[G : H]$ is minimal among all $\mathcal{H}$ satisfying (1).

We call such sets $\mathcal{H}$ "minimal faithful collections"; they are the subject of this paper. The first condition corresponds to faithfulness of the action, the second to the minimality of the degree. Clearly, if $\mathcal{H}$ is a minimal faithful collection, no two of its elements can be conjugate.

Note that the core of a subgroup $H < G$ is precisely the largest normal subgroup of G contained in H.

We shall make use of the *socle*, $\mathrm{M}(G)$, of a finite group G, the subgroup generated by the set $\mathcal{M}(G)$ of all minimal normal subgroups of G. Specifically, the lattice $\mathcal{T}(G) = \{T \lhd G \mid T \subset \mathrm{M}(G)\}$ of normal subgroups of G contained in the socle will play a major role.

Every element $T \in \mathcal{T}$ can be written as a direct product of minimal normal subgroups [Suzuki 82, Theorem II.4.8]. Moreover, the number of factors in any such direct product is an invariant of the pair (G, T). We denote it by $\dim_G T$ and call it the *dimension* of T. In the language of order theory, the lattice $\mathcal{T}$ is *atomic*, with the minimal normal subgroups being the atoms. Since the lattice of normal subgroups of G is modular, both $\mathcal{T}$ and its dual are *matroids*. For readers unfamiliar with this theory, one should heuristically think of $\mathcal{T}$ as behaving in a similar fashion to the lattice of subspaces of a vector space.

When G is nilpotent, every normal subgroup intersects the center [Suzuki 86, Theorem IV.2.9]. The discussion above is then elementary. Since every subgroup of the center is normal, $\mathrm{M}(G) = \mathrm{M}(Z(G))$. Furthermore, the socle is a product of elementary abelian p-groups.

For a subgroup H of G we write $\mathrm{RC}_G(H)$ for the *relative core* of H, the subgroup $\mathrm{Core}_G(H) \cap \mathrm{M}(G)$. It is

[1] We shall use the term "collection" for such sets of subgroups.

then clear that

$$\mathrm{RC}_G(H) = \langle N \in \mathcal{M}(G) \mid N \subset H \rangle \, .$$

For a collection $\mathcal{H}$ of subgroups we similarly set

$$\mathrm{RC}_G(\mathcal{H}) \overset{\mathrm{def}}{=} \bigcap_{H \in \mathcal{H}} \mathrm{RC}_G(H) = \mathrm{Core}_G(\mathcal{H}) \cap \mathrm{M}(G).$$

It is clear that $\mathrm{Core}_G(\mathcal{H})$ is trivial if and only if $\mathrm{RC}_G(\mathcal{H})$ is trivial. This simple observation underlies our later analysis. We also occasionally write $\mathcal{H}_M$ for $\mathrm{RC}_G(\mathcal{H})$, and H_M for $\mathrm{RC}_G(H)$.

We extend the notion of dimension above to all subgroups of G by setting $\dim_G(H) = \dim_G(\mathrm{RC}_G(H))$. In particular, we write $\dim G$ for $\dim_G(G) = \dim_G(\mathrm{M}(G))$. We will also use the *codimension* $\mathrm{codim}_G(H) = \dim G - \dim_G(H)$.

3. DETERMINING $d(G)$

We discuss here the (algorithmic) problem of constructing a minimal permutation representation of G. As input, we give ourselves the subgroup lattice of G and, in addition, the order of each subgroup and whether it is normal in G. This analysis will shed light on the structure of the minimal permutation representations.

3.1 A Special Class of Groups

Definition 3.1. Let G be an arbitrary finite group, and let $\mathcal{T}$ be as above. We call G *socle friendly* if for all $H < G$, $T \in \mathcal{T}$, we have $\mathrm{RC}_G(H \cdot T) = \mathrm{RC}_G(H) \cdot T$.

Lemma 3.2. *If G is a nilpotent group, then G is socle friendly.*

Proof: Since the lattice $\mathcal{T}$ is relatively complemented, we may write $\mathcal{T} = (T \cap \mathrm{RC}_G(H)) \cdot S$ for some $T \in S$ disjoint from $\mathrm{RC}_G(H)$. We then have $H \cdot T = H \cdot S$ and $\mathrm{RC}_G(H) \cdot T = \mathrm{RC}_G(H) \cdot S$, so we may assume $H \cap T = \{1\}$. Clearly $\mathrm{RC}_G(H) \cdot T \subset \mathrm{RC}_G(H \cdot T)$.

Conversely, let $N < HT$ be a minimal normal subgroup of G. If $N < T$, there is nothing to prove, so we may assume $T \cap N = \{1\}$. Since H and T are disjoint, every $n \in N$ can be uniquely written in the form $n = h_n t_n$ for some $h_n \in H$ and $t_n \in T$. Note that the map $n \mapsto h_n$ is a group homomorphism (it is the restriction to N of the quotient map $H \cdot T/T \simeq H$), and since N and T are disjoint, it is an isomorphism onto its image N'.

Since N and T are central subgroups (here we use the nilpotency of G), it follows that N' is a central subgroup as well, and since N was a cyclic group of prime order, so is N'. It follows that N' is a minimal normal subgroup of G, contained in H. We conclude that $N \subset N'T \subset \mathrm{RC}_G(H) \cdot T$. □

Remark 3.3. Not every finite group is socle friendly. Here is the construction of an infinite family of examples simplifying the construction of [Saunders 07]. Let H be any finite group with two nonisomorphic one-dimensional representations V_1, V_2 over a finite field $\mathbb{F}$. We let $V = V_1 \oplus V_2$ and $G = H \rtimes V$. Then $\mathrm{M}(G) = V$ and $\mathcal{T} = \{0, V_1, V_2, V\}$. Let W be any one-dimensional $\mathbb{F}$-subspace not containing either of V_1, V_2. Then W is core-free, and consequently $\mathrm{RC}_G(W) \cdot V_1 = V_1$ and $\mathrm{RC}_G(W) \cdot V_2 = V_2$. But $W \cdot V_1 = W \cdot V_2 = V$, and as a result, $\mathrm{RC}_G(W \cdot V_1) = \mathrm{RC}_G(W \cdot V_2) = V$. This shows that G is not socle friendly.

3.2 Minimal Faithful Collections and Codimension-One Subgroups

Let G be a finite socle-friendly group. We are interested in constructing a minimal faithful collection of subgroups of G, and a natural way to do so is step by step, incrementally adding subgroups to our collection until it is faithful. Rather than keeping track of $\mathrm{Core}_G(\mathcal{H})$, we note that $\mathrm{RC}_G(\mathcal{H})$ carries sufficient information to decide whether $\mathrm{Core}_G(\mathcal{H})$ is trivial. Moreover, while the cores $\mathrm{Core}_G(\mathcal{H})$ decrease through the lattice of all normal subgroups of G, the relative cores $\mathrm{RC}_G(\mathcal{H})$ decrease through the lattice $\mathcal{T}(G)$, which is much easier to work with.

We now turn to the "minimality" property of a collection, which appears to push in the opposite direction from that of "faithfulness." The first favors selecting large subgroups, and having few of them. The second seems to suggest choosing small subgroups, or else many large ones will be needed. The multiplicative property of orders of subgroups actually implies that choosing many large subgroups is the right way. The analysis is very similar to that of [Johnson 71]. In both cases it is shown that the elements of a minimal faithful collection may be (and in some cases, must be) drawn from a particular class of subgroups, using the same trick. The reader should compare the following lemma with [Johnson 71, Lemma 1].

Lemma 3.4. (Replacement lemma.) *Let $H < G$ be of codimension at least 2. Then there exist subgroups H_1 and H_2 of G containing H such that $\mathrm{RC}_G(H_1) \cap \mathrm{RC}_G(H_2) = \mathrm{RC}_G(H)$ and $\frac{1}{|H_1|} + \frac{1}{|H_2|} \leq \frac{1}{|H|}$. Moreover, this inequality is strict unless G contains at least two central involutions.*

Proof: Since $\mathcal{T}$ is a matroid and $\mathrm{RC}_G(H)$ has codimension at least 2, there exist two minimal normal subgroups $N_1, N_2 \in \mathcal{M}(G)$ ("atoms of the lattice $\mathcal{T}(G)$") such that the lattice join $\mathrm{RC}_G(H)N_1N_2$ has dimension greater by 2 than that of $\mathrm{RC}_G(H)$. In other words, the lattice join is a direct product. The inclusions $\mathrm{RC}_G(H) < \mathrm{RC}_G(H)N_i$ are then proper, and we have $\mathrm{RC}_G(H) = \mathrm{RC}_G(H)N_1 \cap \mathrm{RC}_G(H)N_2$.

We thus set $H_i = H \cdot N_i$, $i = 1, 2$ (these are semidirect products, since the N_i are minimal normal subgroups). By Lemma 3.2, $\mathrm{RC}_G(H_i) = \mathrm{RC}_G(H)N_i$, and it follows that $\mathrm{RC}_G(H_1) \cap \mathrm{RC}_G(H_2) = \mathrm{RC}_G(H)$. Since H is a proper subgroup of both H_1 and H_2, its index in both subgroups is at least 2, and we have

$$\frac{1}{|H_1|} + \frac{1}{|H_2|} \leq \left(\frac{1}{2} + \frac{1}{2}\right)\frac{1}{|H|} = \frac{1}{|H|}.$$

Equality can happen only if both N_1 and N_2 are of order 2, in which case the nontrivial elements of N_i are both central involutions. □

Definition 3.5. Let $\mathcal{A} = \mathcal{A}(G)$ denote the set of subgroups of G of codimension 1.

The reader should compare the next theorem with [Johnson 71, Corollary 1].

Theorem 3.6. *There exist minimal faithful collections contained in $\mathcal{A}$, and these are the ones of maximal size. If G has at most one central involution, then every minimal faithful collection is contained in $\mathcal{A}$.*

Proof: Let $\mathcal{H}$ be a faithful collection, and let $H \in \mathcal{H}$. If H is of codimension 0 (i.e., $\mathrm{RC}_G(H) = \mathrm{M}(G)$), we have

$$\begin{aligned}\{1\} &= \mathrm{RC}_G(\mathcal{H}) \\ &= \mathrm{RC}\left(\mathcal{H} \setminus \{H\}\right) \cap \mathrm{RC}_G(H) = \mathrm{RC}\left(\mathcal{H} \setminus \{H\}\right).\end{aligned}$$

In particular, $\mathcal{H} \setminus \{H\}$ is also faithful. If H has codimension at least 2, let H_1, H_2 be the subgroups constructed in Lemma 3.4, and let $\mathcal{H}' = (\mathcal{H} \setminus \{H\}) \cup \{H_1, H_2\}$. By construction we have $\mathrm{RC}_G(\mathcal{H}') = \mathrm{RC}_G(\mathcal{H}) = \{1\}$, so that $\mathcal{H}'$ is faithful. In addition, Lemma 3.4 yields $\Delta(\mathcal{H}') \leq \Delta(\mathcal{H})$, with strict inequality if G has at most one central involution. In general, we note that $\mathcal{H}'$ has more elements than $\mathcal{H}$. In particular, a minimal faithful collection of maximal size must consist of codimension-one subgroups. □

Definition 3.7. Call a collection $\mathcal{H} \subset \mathcal{A}$ *independent* if its relative core is strictly contained in that of any proper subcollection, or in other words, if $\{\mathrm{RC}_G(H) \mid H \in \mathcal{H}\}$ is an independent set of atoms in the lattice dual to $\mathcal{T}$.

A minimal faithful collection $\mathcal{H} \subset \mathcal{A}$ is certainly independent; otherwise, it would have a faithful proper subcollection.

Proposition 3.8. *The set of independent collections of $\mathcal{A}$ forms a matroid, i.e., the following statements are true:*

1. *A subcollection of an independent collection is independent.*

2. *$\mathcal{H} \subset A$ is independent if and only if* $\mathrm{codim}_G \mathcal{H}_M = |\mathcal{H}|$.

3. *If $\mathcal{H}$, $\mathcal{H}'$ are independent collections with $|\mathcal{H}'| > |\mathcal{H}|$, then there exists $H' \in \mathcal{H}'$ such that $\mathcal{H} \cup \{H'\}$ is independent.*

Proof: This will follow via the replacement lemma from the general fact that $\mathcal{T}$ is a matroid.

1. Let $\mathcal{H} \subset \mathcal{A}$ be independent, and suppose $\mathcal{H}''$ is a proper subcollection of $\mathcal{H}' \subset \mathcal{H}$ such that $\mathcal{H}''_M = \mathcal{H}'_M$. Letting $\bar{\mathcal{H}} = \mathcal{H} \setminus \mathcal{H}'$, we have

$$\left(\bar{\mathcal{H}} \cup \mathcal{H}''\right)_M = \bar{\mathcal{H}}_M \cap \mathcal{H}''_M = \bar{\mathcal{H}}_M \cap \mathcal{H}'_M = \mathcal{H}_M,$$

contradicting the independence of $\mathcal{H}$.

2. Let $S, T \in \mathcal{T}(G)$ with $\mathrm{codim}_G T = 1$. Then ST equals either T or M, and we have $\dim_G S \cap T = \dim_G S$ or $\dim_G S - 1$, respectively, by the inclusion–exclusion formula for dimension. By induction on the size of any collection $\mathcal{H} = \left\{H^i\right\}_{i=1}^k \subset \mathcal{A}$, we see that $\mathrm{codim}_G \mathcal{H}_M \leq |\mathcal{H}|$, with equality if and only if the sequence of intersections $\bigcap_{i=1}^m \mathrm{RC}_G(H^i)$ is strictly decreasing with m, $1 \leq m \leq k$.

3. We have $\dim_G \mathcal{H}'_M < \dim_G \mathcal{H}_M$, and hence $\mathcal{H}'_M$ does not contain $\mathcal{H}_M$. It follows that we can find $H' \in \mathcal{H}'$ such that H'_M does not contain $\mathcal{H}_M$. Then $\dim_G(\mathcal{H}_M \cap H'_M) = \dim_G \mathcal{H}_M - 1$ (equality is impossible by the choice of H'). By part (2), we see that $\mathcal{H} \cup \{H'\}$ is independent. □

Corollary 3.9. *Let $\mathcal{H} \subset A$ be independent. Then the following are equivalent:*

1. *$|\mathcal{H}| = \dim G$;*

2. *$\mathcal{H}$ is faithful;*

3. *$\mathcal{H}$ is a maximal independent subset of $\mathcal{A}$. Here,* maximal *means maximal with respect to inclusion.*

Proof: The equivalence of (1) and (2) is contained in part (2) of Proposition 3.8. An independent collection with $\mathcal{H}_M = \{1\}$ is certainly maximal. An independent collection with $\mathcal{H}_M \neq \{1\}$ is not maximal, since in that case there exists some $T \in \mathcal{T}$ of codimension 1 that does not contain $\mathcal{H}_M$, and we can add it to $\mathcal{H}$ to form a larger independent collection. □

Corollary 3.10. *A subset $\mathcal{H} \subset \mathcal{A}$ is a minimal faithful collection if and only if it is independent and maximizes*

$$w(\mathcal{H}) = \sum_{H \in \mathcal{H}} \left(2 - \frac{1}{|H|}\right)$$

among the independent subsets.

Proof: We have already noted that a minimal faithful collection contained in $\mathcal{A}$ is independent and maximal (with respect to inclusion), and that a maximal (with respect to inclusion) independent set is a faithful collection. It is clear that a subset maximizing this weight function is maximal independent, since $2 - \frac{1}{|H|} > 0$ for all subgroups H. Finally, we note that a maximal independent set $\mathcal{H}$ satisfies $w(\mathcal{H}) = 2 \dim G - \Delta(\mathcal{H})$. □

Corollary 3.11. *There exist minimal faithful collections of size* $\dim G$*. If G has more than one central involution, there may also exist minimal faithful collections of smaller size.*

Proof: We have seen that there exist minimal faithful collections contained in $\mathcal{A}$, that these are independent sets, and that every independent set has $\dim G$ elements. □

Inspired by this corollary, we make the following definition.

Definition 3.12. A minimal faithful collection of size $\dim G$ is called *perfect.* Correspondingly, a minimal faithful permutation representation with $\dim G$ orbits under the G-action is called *perfect.*

Example 3.13. Let G be a p-group for a prime p, and let $Z = Z(G)$ be its center. It is well known (and follows from the class formula) that every normal subgroup of G intersects the center nontrivially. Since every subgroup of the center is normal, it follows that $\mathcal{M}(G) = \mathcal{M}(Z)$, and in particular $\dim G = \dim Z(G)$. This observation recovers [Johnson 71, Theorem 3]:

Theorem 3.14. *Let G be a p-group with center Z. Then there exists a minimal faithful collection for G of size* $\dim Z$*. If p is odd, this holds for all minimal faithful collections.*

3.3 Construction

In the remainder of this section we assume that G is a socle-friendly finite group. We have reduced the problem of finding a minimal faithful collection to maximizing an additive weight function on a matroid. This is a problem that is solvable by a greedy algorithm, and thus we may search for and construct perfect minimal faithful permutation representations. Before we present our method, we record a useful lemma.

Lemma 3.15. *Let $\mathcal{H} \subset \mathcal{A}$ be independent, and suppose $H' < G$ has the largest size possible such that H'_M does not contain $\mathcal{H}_M$. Then $H' \in \mathcal{A}$, $\mathcal{H} \cup \{H'\}$ is independent, and H' maximizes the function $w(H) = 2 - \frac{1}{|H|}$ among all $H \in \mathcal{A}$ such that $\mathcal{H} \cup \{H\}$ is independent.*

Proof: We can find $T \in \mathcal{T}$ of codimension 1 containing H'_M but not containing $\mathcal{H}_M$. Setting $H = H'T$, we have $H_M = H'_M T = T$, which does not contain $\mathcal{H}_M$. By the maximality of H' we have $H = H'$, implying $H'_M = T$, so that H' is of codimension 1 and $\mathcal{H} \cup \{H'\}$ is independent. Finally, H' was chosen to maximize $w(H)$ in an even larger family than needed. □

We now describe a method to find all perfect minimal faithful permutation representations. We assume that we are given the following data:

1. The subgroup lattice of G;
2. the sizes of every element of the subgroup lattice;
3. and that normal subgroups are marked as such.

Then for each $i \geq 0$ we recursively construct a sequence of triples $(\mathcal{H}_i, T_i, \Delta_i)$ with each $\mathcal{H}_i$ a collection of subgroups of G, T_i a subgroup of G, and Δ_i a nonnegative real number. In order to do this we proceed as follows. Let $\mathcal{H}_0 = \varnothing$, $T_0 = \mathrm{M}(G)$, $\Delta_0 = 0$. Now suppose $(\mathcal{H}_i, T_i, \Delta_i)$ is given, and $T_i \neq \{1\}$. First we find a subgroup H_{i+1} of G of maximal size not containing T_i. Then we set $\mathcal{H}_{i+1} = \mathcal{H}_i \cup \{H_{i+1}\}$, $T_{i+1} = T_i \cap \mathrm{Core}_G(H_{i+1})$, $\Delta_{i+1} = \Delta_i + \frac{1}{|H_{i+1}|}$. If $T_i = \{1\}$, we simply set $(\mathcal{H}_{i+1}, T_{i+1}, \Delta_{i+1}) = (\mathcal{H}_i, T_i, \Delta_i)$. The sequence $(\mathcal{H}_i, T_i, \Delta_i)$ is certainly not unique and depends on the choices of the subgroups H_i. Then we have the following theorem.

Theorem 3.16. *Let G be a socle-friendly finite group, and let $\dim G = \delta$. Then*

1. *For any choice of the subgroups H_i, $T_{\delta-1} \neq \{1\}$ whereas $T_\delta = \{1\}$. Furthermore, $\mathcal{H}_\delta$ is a minimal faithful collection of size δ, and $\Delta_\delta = \Delta(G)$.*

2. *Conversely, up to G-isomorphism any minimal faithful collection of size δ can be obtained this way.*

Proof: First we prove the first part. From Lemma 3.15 it is clear that for each i, the collection $\mathcal{H}_i$ is independent, and $T_i = (\mathcal{H}_i)_M$. Also, it is easy to see that for each i, $\dim T_{i+1} = \dim T_i - 1$ as long as $T_i \neq \{1\}$. These observations immediately give the first assertion of the theorem.

We show by induction that for $k \leq \delta$, $\sum_{H \in \mathcal{H}_k} \frac{1}{|H|}$ is minimal among independent collections of size k. This is certainly the case for $k = 0$. Thus let $\mathcal{H}_{k-1}$ be given, and choose the subgroup H_k. Suppose there is an independent collection $\mathcal{H}' \subset \mathcal{A}$ of size k such that $\sum_{H' \in \mathcal{H}'} \frac{1}{|H'|} < \frac{1}{|H_k|} + \sum_{H \in \mathcal{H}_{k-1}} \frac{1}{|H|}$. We may then write $\mathcal{H}' = \mathcal{H}'' \cup \{H'_k\}$, where H'_k is a member of minimal size. By the inductive hypothesis, $\sum_{H \in \mathcal{H}_{k-1}} \frac{1}{|H|} \leq \sum_{H' \in \mathcal{H}''} \frac{1}{|H'|}$, and hence we must have $|H_k| < |H'_k|$. By the choice of H'_k, we actually have $|H_k| < |H'|$ for all $H' \in \mathcal{H}'$.

We now use the matroid property of the independent subcollections of $\mathcal{A}$ shown in Proposition 3.8(3): since $\mathcal{H}'$ is of size k, while $\mathcal{H}_{k-1}$ is of size $k-1$, there exists some $H' \in \mathcal{H}'$ such that $\mathcal{H}_{k-1} \cup \{H'\}$ is independent. In particular, this implies that $(\mathcal{H}_{k-1} \cup \{H'\})_M$ is strictly contained in $\mathcal{H}_M$, and since $|H'| > |H_k|$, we have a contradiction to the existence of $\mathcal{H}'$.

Now we prove the second part. Let $\mathcal{H} = \{H_i\}_{i=1}^{\delta}$ be a minimal faithful collection, ordered such that

$$|H_1| \geq |H_2| \geq \cdots \geq |H_\delta| \, .$$

Then we claim that for each k, H_k has maximal size among all subgroups H' of G such that $\left(\{H_i\}_{i=1}^{k-1} \cup \{H\}\right)_M$ is a proper subgroup of $\left(\{H_i\}_{i=1}^{k-1}\right)_M$. By induction, it suffices to check that if a subgroup $H' < G$ is independent of $\{H_i\}_{i=1}^{k-1}$, then there exists $l \geq k$ such that $\mathcal{H} \cup \{H'\} \setminus \{H_l\}$ is independent. For this we set $S_j = \cap_{i=1}^{j} \mathrm{RC}_G(H_i)$. It is then easy to see that we may take l to be the first j such that $\mathrm{RC}_G(H') \cap S_j = S_j$. The assertion of the theorem is now immediate. □

3.4 The Main Theorem

In this section we state and prove our main theorem. We start with a definition,

Definition 3.17. Let G be a finite group. Given a permutation representation X, we denote by $m(X)$ the multiset consisting of the sizes of the orbits of X under the G-action.

Theorem 3.18. *Let G be a socle-friendly finite group. Let X be a minimal faithful permutation representation of G. Then*

1. *The number of orbits of X under the action of G is at most $\dim G$;*

2. *G has perfect minimal faithful permutation representations; and if the center of G has at most one involution then every faithful permutation representation is perfect;*

3. *If X_1, X_2 are two perfect minimal faithful representations of G, then $m(X_1) = m(X_2)$.*

Proof: The first two parts of the theorem follow from Corollary 3.11. The third part easily follows from Theorem 3.16 and its proof. □

4. APPLICATIONS

4.1 Accumulation Points of $\Delta(G)$

Let $n, p \in \mathbb{N}$ with $p > n$ a prime. Then $\Delta(C_n \times C_p) = \frac{1}{n} + \frac{\Delta(C_n)}{p} = \frac{1}{n} + O(\frac{1}{p})$. In particular, $\lim_{p \to \infty} \Delta(C_n \times C_p) = \frac{1}{n}$. This means that for each positive integer n, the point $\frac{1}{n}$ is an accumulation point of the set $\{\Delta(G);\text{G finite group}\}$ in the interval $[0, 1]$. In Theorem 4.6 below, we show that these points are the only nonzero accumulation points. We begin with some preliminary lemmas.

Lemma 4.1. *Let $H < G$ be a subgroup. Then $d(H) \leq d(G)$ and $\Delta(G) \leq \Delta(H)$.*

Proof: The first claim is obvious. For the second, let $\mathcal{H}'$ be a faithful collection of subgroups of H and note that $\Delta(\mathcal{H})$ is independent of the ambient group. Then $K_G(H_i) \subset K_H(H_i)$ (larger intersection). In particular, $K_G(\mathcal{H}) = \{1\}$. Choosing $\mathcal{H}$ minimal for H, we deduce that $\Delta(G) \leq \Delta(\mathcal{H}) = \Delta(H)$. □

Remark 4.2. A cyclic p-group has relative degree 1. In particular, if $P < G$ is a cyclic p-group, then

$$\Delta(G) \geq \frac{d(P)}{|G|} = \frac{1}{[G:P]}.$$

Conversely, [Babai et al. 93] gives an explicit function $f\colon [0,1] \to \mathbb{R}$ such that if $\Delta(G) \geq \Delta$, then G has a cyclic p-subgroup of index at most $f(\Delta)$. In other words, as $|G|$ grows with $\Delta(G) \geq \Delta$, the degree of G is controlled (up to bounded multiplicative error) by the size of the largest cyclic p-subgroup of G. Specifically, Babai et al. show that when G does not possess a large cyclic group of prime-power order, it has a pair of reasonably large subgroups with trivial intersection.

Note that the above bound on $\Delta(G)$ is derived from a faithful collection of size 2. In Lemma 4.3 we show that when $\Delta(G) \geq \Delta$, there exists k depending only on Δ such that a minimal permutation representation of G has at most k orbits. The case of groups of prime exponent and nilpotency class two, studied in [Babai et al. 93, Theorem 3.6] as well as [Neumann 86], shows that we need $k > 2$ in general.

Lemma 4.3. *Let $k = \dim G$. Then $\Delta(G) \leq \frac{k}{2^{k-1}}$.*

Proof: Write the socle $M = \mathrm{M}(G)$ as the direct product of k minimal normal subgroups $\{S_i\}_{i=1}^{k}$. For $1 \leq i \leq k$ let $H_i = \prod_{j \neq i} S_j$. It is clear that $\{H_i\}$ is a faithful collection of size k and each of its elements has size at least 2^{k-1}. □

Lemma 4.4. *Let P be a cyclic p-subgroup of G. Then $\mathrm{RC}_G(P) < \mathrm{M}(P)$. If $|G|$ is large enough compared to $[G:P]$, then equality holds.*

Proof: Let $N < P$ be nontrivial and normal in G. Then $\mathrm{M}(P)$ is a characteristic subgroup of N. It follows that $\mathrm{RC}_G(P)$ is either trivial or equal to $\mathrm{M}(P)$. In any case, we have $\dim_G P \leq 1$.

Finally, the core of P has index at most $([G:P])!$ (it is the kernel of a homomorphism into $S_{[G:P]}$). If $|G| > ([G:P])!$, then $\mathrm{Core}_G(P)$ is a nontrivial normal subgroup of G contained in P, hence containing its unique subgroup of order p. In that case $\mathrm{M}(P)$ is normal in G, and thus $\mathrm{RC}_G(P) = \mathrm{M}(P)$. □

In fact, if G has a large cyclic p-subgroup, then a permutation representation with two orbits is almost optimal:

Corollary 4.5. *Let P be a cyclic p-subgroup of G, and let $l(G)$ be the order of the smallest point stabilizer in an orbit in a minimal permutation representation of G. Then*

$$\frac{1}{l(G)} \leq \Delta(G) \leq \frac{1}{l(G)} + \frac{1}{|P|}.$$

Proof: Let $\mathcal{H}$ be a minimal faithful collection for G, chosen so that it contains an element H_1 of smallest possible order (denoted above by $l(G)$). Clearly $\Delta(G) = \Delta(\mathcal{H}) \geq \frac{1}{l(G)}$. For the other assertion, we may as well assume $M(P) \in \mathcal{M}(G)$, for otherwise, $\mathrm{Core}_G(P) = \{1\}$ and the claim is clear. Then $\mathcal{H}$, being faithful, must contain an element H_2 disjoint from $M(P)$; hence $\{P, H_2\}$ is a faithful collection. □

Theorem 4.6. *Let G_n be a sequence of groups with orders increasing to infinity such that $\lim_{n\to\infty} \Delta(G_n) > 0$. Then this limit is of the form $1/l$ for some $l \in \mathbb{N}$.*

Proof: For n large enough we have $\Delta(G_n) > \Delta > 0$. The main result of [Babai et al. 93], already quoted above, is that G_n has a cyclic p_n-subgroup P_n of index at most $f(\Delta)$ for some $f\colon [0,1] \to \mathbb{N}$. It follows that

$$\left| \Delta(G_n) - \frac{1}{l(G_n)} \right| \leq \frac{f(\Delta)}{|G_n|}.$$

Here $l(G_n)$ is as in the statement of Corollary 4.5. As $|G_n| \to \infty$, we see that $\frac{1}{l(G_n)}$ tends to a positive limit. The sequence of integers $l(G_n)$ must then be eventually constant, equal to an integer l. Corollary 4.5, combined with the fact that the size of P_n goes to infinity, implies that $\lim_{n\to\infty} \Delta(G_n) = \frac{1}{l}$. □

Note that we have shown more, namely that if $\Delta(G) \geq \Delta > 0$, then any minimal permutation representation consists of one large orbit of size essentially $|G|\,\Delta(G)$, and several other orbits of size and number bounded in terms of Δ. Indeed, the number of orbits is bounded by Lemma 4.3. We have an obvious bound $l(G) \leq (\Delta(G) - f(\Delta)/|G|)^{-1}$.

Next, as soon as $|G|$ is large enough that $\frac{1}{l(G)+1} + \frac{f(\Delta)}{|G|} < \frac{1}{l(G)}$, the subgroups H_1, H_2 of Lemma 4.4 must have the same size. We conclude that if $\Delta(G) > \Delta$ and $|G|$ is large enough (depending on Δ), then G has both a cyclic p-subgroup P of index at most $f(\Delta)$ such that $M(P)$ is normal in G, and also a subgroup H of order $l(G)$ belonging to a minimal faithful collection and disjoint from $M(P)$. Then every other member of that minimal faithful collection may be replaced with P, keeping the collection faithful. Hence all other orbits in the representation must have size at most $f(\Delta)$.

4.2 Some Numerical Results

The thesis [Elias 05] contains an implementation of the procedure preceding Theorem 3.16 in the algebraic programming language MAGMA. Using the limited computing power of a personal computer, p-groups of order p^n for $n \leq 6$ and small p were examined. Any such group can be found in the MAGMA database. Let us summarize the findings.

There is only one group G of order p, and for this group, $\Delta(G) = 1$. There are two groups of order p^2, namely $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$. Here $\Delta(\mathbb{Z}_p \times \mathbb{Z}_p) = \frac{2}{p}$ and $\Delta(\mathbb{Z}_{p^2}) = 1$. Consequently, $\sum_{|G|=p^2} \Delta(G) = 1 + \frac{2}{p}$. There are five groups of order p^3: one cyclic with $\Delta = 1$; one elementary abelian with $\Delta = \frac{3}{p^2}$; one abelian with a generator of order p^2, having $\Delta = \frac{1}{p} + \frac{1}{p^2}$; and two nonabelian groups both having $\Delta = \frac{1}{p}$. Observe that $\sum_{|G|=p^3} \Delta(G) = 1 + \frac{3}{p} + \frac{4}{p^2}$. For groups of order p^4 and p^5 we state the following conjecture.

Conjecture 4.7. *For $p > 3$,*

$$\sum_{|G|=p^4} \Delta(G) = 1 + \frac{5}{p} + \frac{11}{p^2} + \frac{9}{p^3},$$

$$\sum_{|G|=p^5} \Delta(G) = 1 + \frac{7}{p} + \frac{34 + 2\gcd(p-1,3) + \gcd(p-1,4)}{p^2} + \frac{54}{p^3} + \frac{24}{p^4}.$$

For any prime $p \geq 3$, there are exactly fifteen groups of order p^4, and these can be enumerated and described. So the proof of the first part of the conjecture should be straightforward. We have computationally verified the conjecture for groups of order p^4 for every prime p in the range $3 < p < 50$ and several larger values of p (≈ 1000). We considered the groups of order p^5 for $p \leq 19$. Note that the number of groups of order p^5 is $61+2p+2\gcd(p-1,3) + \gcd(p-1,4)$. For groups of order p^6, we did not have enough data points to be able to guess a formula.

ACKNOWLEDGMENTS

We thank John Conway, Evan Haas, William Kantor, Andre Kornell, Avinoam Mann, and James Wilson for useful conversations.

In an earlier draft of this paper we claimed that every finite group is socle friendly (Definition 3.1). We wish to thank Neil Saunders for pointing out this inaccuracy and constructing a counterexample [Saunders 07]; see also Remark 3.3, where a simplification of Saunders's example is presented.

We also thank two anonymous referees for their careful reading of the manuscript and their many suggestions, which led to considerable improvement in the style and presentation of the paper.

The second author's research was supported in part by a Porter Ogden Jacobus Fellowship at Princeton University, a Clay Mathematics Foundation Liftoff Fellowship, and the National Science Foundation under agreement No. DMS-0111298. The third author's research was partially funded by Young Investigator Grant No. 215-6406 from the NSA and by the National Science Foundation grant No. DMS-0701753.

REFERENCES

[Babai et al. 93] László Babai, Albert J. Goodman, and László Pyber. "On Faithful Permutation Representations of Small Degree." *Comm. Algebra* 21:5 (1993), 1587–1602.

[Berkovich 99] Yakov Berkovich. "The Degree and Index of a Finite Group." *J. Algebra* 214:2 (1999), 740–761.

[Cameron 99] Peter J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts 45. Cambridge, UK: Cambridge University Press, 1999.

[Cayley 78] Arthur Cayley. "Desiderata and Suggestions: No. 1: The Theory of Groups." *Amer. J. Math.* 1:1 (1878), 50–52.

[Dixon and Mortimer 96] John D. Dixon and Brian Mortimer, *Permutation Groups*, Graduate Texts in Mathematics 163. New York: Springer, 1996.

[Elias 05] Benjamin Elias. "Minimally Faithful Group Actions and p-Groups." Senior thesis, Princeton University 2005.

[Johnson 71] D. L. Johnson, "Minimal Permutation Representations of Finite Groups." *Amer. J. Math.* 93 (1971), 857–866.

[Neumann 86] Peter M. Neumann. "Some Algorithms for Computing with Finite Permutation Groups." In *Proceedings of Groups—St. Andrews 1985 (Cambridge)*, London Math. Soc. Lecture Note Ser. 121, pp. 59–92. Cambridge, UK: Cambridge Univ. Press, 1986.

[Saunders 07] Neil Saunders. Private communication, September 1, 2007.

[Suzuki 82] Michio Suzuki. *Group Theory I*, Grundlehren der Mathematischen Wissenschaften 247. Berlin: Springer, 1982.

[Suzuki 86] Michio Suzuki. *Group theory II*, Grundlehren der Mathematischen Wissenschaften 248. New York: Springer, 1986.

Ben Elias, Columbia University Department of Mathematics, New York, NY 10027 (belias@math.columbia.edu)

Lior Silberman, Department of Mathematics, University of British Columbia, Vancouver,BC, V6T 1Z4, Canada
(lior@math.ubc.ca)

Ramin Takloo-Bighash, Department of Math, Stat, and Comp Sci, University of Illinois at Chicago, Chicago, IL 60607
(rtakloo@math.uic.edu)

Received March 6, 2008; accepted in revised form August 4, 2009.