The maximum distinguishing number of a group

Melody Chan
Princeton University
Princeton, New Jersey, USA
melody.chan@aya.yale.edu

Submitted: Sep 9, 2004; Accepted: Feb 10, 2006; Published: Aug 7, 2006
Mathematics Subject Classification: 05E15, 20B25, 20D60

Abstract

Let G be a group acting faithfully on a set X. The distinguishing number of the action of G on X, denoted $D_G(X)$, is the smallest number of colors such that there exists a coloring of X where no nontrivial group element induces a color-preserving permutation of X. In this paper, we show that if G is nilpotent of class c or supersolvable of length c then G always acts with distinguishing number at most $c+1$. We obtain that all metacyclic groups act with distinguishing number at most 3; these include all groups of squarefree order. We also prove that the distinguishing number of the action of the general linear group $GL_n(K)$ over a field K on the vector space K^n is 2 if K has at least $n+1$ elements.

1 Introduction

An action of a group G on a set X is said to be *faithful* if only the identity element of G fixes every element of X. Let G be a group acting faithfully on X. For $r \in \mathbb{N}$, an *r-coloring* of X is a function $c\colon X \to \{1, \ldots, r\}$. A permutation π of X *preserves* the coloring c if $c(\pi x) = c(x)$ for all $x \in X$. A coloring is said to be *distinguishing* if the only element in G that induces a color-preserving permutation of X is the identity element. The *distinguishing number* of the action of G on X, denoted $D_G(X)$, is the smallest r admitting a distinguishing r-coloring of X with respect to the action of G. If there does not exist a distinguishing r-coloring of X for any finite r, we say that $D_G(X) = \infty$.

The distinguishing number was first defined by Albertson and Collins in [2] as a property of graphs. More specifically, the distinguishing number of a graph M, denoted $D(M)$, is the smallest number of colors admitting a coloring of the vertices such that the only color-preserving automorphism of M is the identity; thus $D(M) = D_{\mathrm{Aut}(M)}(V(M))$. Note that distinguishing colorings of graphs need not be proper colorings in the graph theoretic sense: two adjacent vertices may or may not have the same color. Although Albertson and Collins initially defined the distinguishing number solely in terms of graphs, the approach they chose to take is nevertheless highly group theoretic. Given a group G, they define the *distinguishing set* of G, denoted $D(G)$, as

$$D(G) = \{D(\mathcal{G}) \mid \mathcal{G} \text{ is a graph with } \operatorname{Aut}(\mathcal{G}) \cong G\}.$$

Their results in [2] center around characterizing the distinguishing set of a group. For example, they show that $D(S_4) = \{2, 4\}$. They also prove the following result.

Theorem. *[2, Corollary 3.1, Theorem 6]*
(1) If G is Abelian then $\max\{D(G)\} \leq 2$.
(2) If G is dihedral then $\max\{D(G)\} \leq 3$.

In addition, the distinguishing number of several families of graphs, including trees, hypercubes, and generalized Petersen graphs, have been studied in [3], [5], [7], and [10].

In [12], Tymoczko generalizes the notion of the distinguishing number to group actions on sets and proves results about the distinguishing number of actions of the symmetric group S_n. She shows that the distinguishing number of group actions is indeed a more general question than the distinguishing number of graphs. For example, she exhibits a faithful S_4-action with distinguishing number 3, contrasting Albertson and Collins' result that $D(S_4) = \{2, 4\}$. This difference highlights the fact that not all faithful group actions are realized as actions of the automorphism group of a graph on its vertex set.

Following Tymoczko, it seems natural to expand the notion of the distinguishing set of a group to include all of its possible actions, not just those arising from graph automorphism groups. In this generalized context, we ask the following question: given a group G, what is the best upper bound we can give for $D_G(X)$? In Section 2, we give an upper bound for the maximum distinguishing number for a large class of groups including nilpotent and supersolvable groups.

Theorem. *If G is nilpotent of class c or supersolvable of length c then G acts with distinguishing number at most $c + 1$.*

As a corollary, we obtain that all metacyclic groups act with distinguishing number at most 3 since they are supersolvable of length 2; these include all groups of squarefree order. Albertson and Collins' results for Abelian and dihedral groups are special cases of nilpotent groups of class 1 and metacyclic groups, respectively. In Section 3, we compute the distinguishing number for an important group action, that of the general linear group over a field K on a vector space over K. We show that the distinguishing number of this action is 2 if $|K| > n + 1$ where n denotes the dimension of the vector space.

Our definition of the distinguishing number of a group action differs from the one given in [12] in that we require the action to be faithful. This apparent restriction does not in actuality limit the question being considered, however, for given a nonfaithful action of G on X, we may consider instead the faithful action of the quotient group $G/Stab(X)$ on X, where $Stab(X)$ denotes the elements of G that fix each $x \in X$. Also, in contrast to both [2] and [12], we do not require our groups and sets to be finite, simply because there seems to be no reason to do so. We only note that if G is an infinite group acting faithfully on a set X, then X must be infinite as well.

2 The maximum distinguishing number of a group

Given a group G, let $\overline{D}(G) = \max\{D_G(X) \mid G \text{ acts faithfully on } X\}$ denote the largest distinguishing number that G admits, or $\overline{D}(G) = \infty$ if some $D_G(X) = \infty$. In [12], Tymoczko proves the bound $D_G(X) \leq k$ if $|G| \leq k!$, a result originally formulated by Albertson, Collins and Kleitman in terms of graphs. This result holds for any action of G on X, faithful or nonfaithful. In [2], Albertson and Collins show that if G is Abelian then $\overline{D}(G) \leq 2$ and if G is dihedral then $\overline{D}(G) \leq 3$. Their proof is formulated only in terms of graphs but also holds for group actions. In this section, we generalize these results to a class of groups that includes all nilpotent and supersolvable groups.

The following lemma gives some conditions under which we may characterize the maximum distinguishing number of a group. The idea to consider the intersection of a normal subgroup with the stabilizing subgroup of orbit representatives was inspired by Albertson and Collins' proof for dihedral groups in [2]. In what follows, we use $\langle x \rangle$ to denote the subgroup generated by a group element x. Also, we will denote group actions by exponentiation on the right. Thus, the image of an element $x \in X$ under the action of $g \in G$ is denoted x^g, and we have $(x^{g_1})^{g_2} = x^{(g_1 g_2)}$ for all $g_1, g_2 \in G$.

Lemma 2.1. *Suppose N is a normal subgroup of G with the property that if $n_1, n_2 \in N$ are conjugate elements in G, then $\langle n_1 \rangle = \langle n_2 \rangle$. Suppose further that any subgroup L of G/N has the property that $\overline{D}(L) \leq c$. Then $\overline{D}(G) \leq c + 1$.*

Proof. The case $G = 1$ is trivial. Suppose that a nontrivial group G acts faithfully on a set X. Choose a set U of representatives of the orbits of G on X (using the Axiom of Choice if there are infinitely many orbits), and let $H = \{g \in G \mid u^g = u \text{ for each } u \in U\}$ stabilize the set U pointwise. We claim that $H \cap N = 1$. Suppose that $n \in H \cap N$, so that n stabilizes each $u \in U$. Fix any $x \in X$ and let $u \in U$ be the representative of the orbit containing x. Let $g \in G$ satisfy $u = x^g$, and let H_x be the stabilizer subgroup of x. By assumption, n stabilizes u, so gng^{-1} stabilizes x. But the fact that $\langle n \rangle = \langle gng^{-1} \rangle$ implies that $n \in \langle gng^{-1} \rangle \leq H_x$. Therefore, n stabilizes each $x \in X$. Since G acts faithfully, $n = 1$ and so $H \cap N = 1$. Applying the Second Isomorphism Theorem, we conclude that $H \cong HN/N \leq G/N$.

Now, we know that $X \setminus U$ is nonempty because G is nontrivial, so consider the action of H on $X \setminus U$. This action is faithful since the action of G on X is faithful. Then $D_H(X \setminus U) \leq \overline{D}(H) \leq c$ since H is isomorphic to a subgroup of G/N. Then let $C\colon X \setminus U \to \{1, \ldots, c\}$ be a c-coloring of $X \setminus U$ that is distinguishing with respect to the action of H. Now define $C'\colon X \to \{1, \ldots, c+1\}$ as

$$C'(x) = \begin{cases} c+1 & \text{if } x \in U, \\ C(x) & \text{if } x \notin U. \end{cases}$$

We claim that C' is a distinguishing $(c+1)$-coloring of X with respect to the action of G. Suppose $g \in G$ preserves C'. Then g must fix each orbit representative $u \in U$, since they are the only elements of color $c + 1$ and lie in different orbits. Thus $g \in H$. Then consider the action of g on $X \setminus U$. Since the restriction of C' to $X \setminus U$ is a distinguishing coloring with respect to the action of H, and $g \in H$ preserves this coloring, we have $g = 1$. Therefore, C' is a distinguishing $c+1$-coloring with respect to the action of G. We conclude that an arbitrary action of G has distinguishing number at most $c+1$, and so $\overline{D}(G) \leq c+1$. $\square$

The next theorem is a consequence of Lemma 2.1. Following [8], we define a *normal series* for a group G to be a chain of subgroups $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_c = G$ with the additional condition that each $G_i \triangleleft G$.

Theorem 2.2. *Suppose a group G has a finite normal series*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_c = G$$

in which each quotient G_{i+1}/G_i is cyclic or is contained in $Z(G/G_i)$. Then $\overline{D}(G) \leq c+1$.

Proof. We proceed by induction on c. If $c = 0$, then $G = G_0 = 1$ and $\overline{D}(G) = 1$. Now let G have a normal series $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_c = G$ of length $c > 0$ with the required property. In order to apply Lemma 2.1, we wish to show that any two conjugate elements lying in G_1 generate the same subgroup, and in addition any subgroup of the quotient group G/G_1 acts with distinguishing number at most c.

Let n_1 and n_2 be conjugate elements in G_1. We have assumed that G_1 is either cyclic or contained in $Z(G)$. In the former case, note that since conjugation is a group automorphism, $[G_1 : \langle n_1 \rangle] = [G_1 : \langle n_2 \rangle]$. But G_1 is cyclic, so it has precisely one subgroup of this index. Therefore $\langle n_1 \rangle = \langle n_2 \rangle$. In the latter case, note that every element of $Z(G)$ has no conjugates other than itself, so $n_1 = n_2$ and $\langle n_1 \rangle = \langle n_2 \rangle$.

Next, it follows from the Third Isomorphism Theorem that

$$1 = G_1/G_1 \triangleleft G_2/G_1 \triangleleft \cdots \triangleleft G/G_1$$

is a normal series for G/G_1 of length $c-1$ in which each quotient group $(G_{i+1}/G_1)/(G_i/G_1)$ is cyclic or is contained in $Z((G/G_1)/(G_i/G_1))$. Now for any subgroup L of G/G_1, let $L_i = (G_{i+1}/G_1) \cap L$ for each i with $0 \leq i \leq c-1$. Then one can check that

$$1 = L_0 \triangleleft L_1 \triangleleft \cdots \triangleleft L_{c-1} = L$$

is a normal series of length $c-1$ for L with the property that each quotient group L_{i+1}/L_i is cyclic or is contained in $Z(L/L_i)$. Then $\overline{D}(L) \leq c$ by the inductive hypothesis. Thus, all the conditions of Lemma 2.1 are satisfied, so $\overline{D}(G) \leq c+1$. $\square$

As consequences of Theorem 2.2, we obtain upper bounds on the distinguishing number of nilpotent and supersolvable groups. We recall the definitions of these important classes of groups below; see [8] for a more detailed discussion of them.

A group G is said to be *nilpotent* if it possesses a finite normal series $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_c = G$ such that each quotient group G_{i+1}/G_i is contained in $Z(G/G_i)$. If the shortest such normal series has length c, then we say that G is *nilpotent of class c*.

Corollary 2.3. *Let G be nilpotent of class c. Then $\overline{D}(G) \leq c+1$.*

In particular, since all Abelian groups are class-1 nilpotent, we have $\overline{D}(G) \leq 2$ for G Abelian, as shown in [2].

A group G is said to be *supersolvable* if it possesses a finite normal series $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_c = G$ such that each quotient group G_{i+1}/G_i is cyclic. In this case, we will say that G is *supersolvable of length c*. See [4] for a detailed discussion of supersolvable groups.

Corollary 2.4. *Let G be supersolvable of length c. Then $\overline{D}(G) \leq c+1$.*

A group G is called *metacyclic* if it has a normal subgroup $N \triangleleft G$ such that both N and G/N are cyclic. Such groups have been completely classified in [9], and include all groups of squarefree order.

Corollary 2.5. *Let G be a metacyclic group. Then $\overline{D}(G) \leq 3$.*

We obtain as a special case that if G is dihedral then $\overline{D}(G) \leq 3$, as shown in [2].

3 The action of $GL_n(K)$ on K^n

In this section, we consider the action of $GL_n(K)$, the group of $n \times n$ invertible matrices over a field K, on K^n, the n-dimensional vector space over K. We may regard the elements of K^n as column vectors and accordingly define a left action of $GL_n(K)$ on K^n as $A\colon v \mapsto Av$ for each $v \in K^n$, $A \in GL_n(K)$. This action is clearly faithful.

Our main result is that if K is sufficiently large, then 2 colors suffice to distinguish this action.

Theorem 3.1. *Let K be a field. If K is infinite or is finite of order greater than $n+1$, then $D_{GL_n(K)}(K^n) = 2$.*

Proof. We first observe that the multiplicative group $K^\times$ must contain a nonzero element α of order greater than n. For if K is infinite, then we may certainly choose such an α since there exist only finitely many solutions in K to the equations $x^l = 1$ for each $1 \leq l \leq n$. On the other hand, if K is finite, then we know that $K^\times$ is a cyclic group of order $|K|-1$. Let α generate the group $K^\times$, then the order of α is $|K|-1 > n$.

Now let $e_1, \ldots, e_n$ be the standard basis vectors in K^n, and let S be the set of vectors $\{\alpha^i e_j \mid 0 \leq i < j \leq n\}$. Each of these vectors is distinct since α has order greater than n, so the cardinality of S is $\frac{1}{2}n(n+1)$. Now color every vector in S blue and all remaining vectors red. We claim this is a distinguishing 2-coloring of K^n with respect to the action of $GL_n(K)$.

Suppose $A \in GL_n(K)$ preserves this coloring. It suffices to show that $Ae_k = e_k$ for each e_k. Since e_k is blue, the image of e_k must also be blue and so must have the form $\alpha^i e_j$ for $0 \leq i < j \leq n$. We wish to show that $i = 0$ and $j = k$. First, note that $Ae_k = \alpha^i e_j$ implies that $A^{-1}(\alpha^{i-1}e_j) = \alpha^{-1}A^{-1}(\alpha^i e_j) = \alpha^{-1}e_k$. Now, $\alpha^{-1}e_k$ is a red point, because if instead $\alpha^{-1}e_k = \alpha^c e_k$ for some $0 \leq c < k$, then α would have order at most $c+1$, but $c+1 \leq k \leq n$ and we assumed that the order of α was greater than n. So, $\alpha^{-1}e_k$ is red, and since A was assumed to be color preserving, $\alpha^{i-1}e_j$ is also red. This is only possible if $i = 0$. Thus $Ae_k = e_j$ and so A induces some permutation of the basis vectors $\{e_1, \dots, e_n\}$. Suppose for a contradiction that A permutes them nontrivially. Then there must exist $Ae_k = e_j$ with $k < j$. Then $\alpha^{j-1}e_k$ is red since $k \leq j-1$, but $\alpha^{j-1}e_j$ is blue, and $A(\alpha^{j-1}e_k) = \alpha^{j-1}e_j$, a contradiction. Therefore, A fixes each basis vector e_k and so $A = \mathbf{1}_n$ as desired. We have exhibited a distinguishing 2-coloring of K^n, so $D_{GL_n(K)}(K^n) \leq 2$. Now, it is possible that $D_{GL_n(K)}(K^n) = 1$ only if $GL_n(K)$ is the trivial group. This occurs only when $n = 1$ and $K = \mathbb{F}_2$, which was excluded by the assumption that $|K| > n+1$. Therefore, we have the equality $D_{GL_n(K)}(K^n) = 2$. □

Theorem 3.1 leaves open the case when the size of the field is relatively small. It is possible to show by case analysis that $D_{GL_2(\mathbb{F}_2)}(\mathbb{F}_2^2) = D_{GL_2(\mathbb{F}_3)}(\mathbb{F}_3^2) = 3$. However, we leave the case when $n > 2$ and $|K| \leq n+1$ as an open problem.

4 Discussion and open questions

The distinguishing number seems to be a very natural property of group actions, and efforts to relate the distinguishing number of a group action to group properties seem likely to be fruitful. Below, we give several possibilities for further investigation.

One interesting method of attack relies on the following simple fact.

Observation. Let G act faithfully on X. Fix a coloring c of X and let $H_c = \{g \in G \mid g \text{ preserves } c\}$. Then H_c is a subgroup of G.

The distinguishing number, then, is the smallest number of colors admitting a coloring c such that $H_c = 1$. Thus, it seems plausible that one could make direct use of information on the subgroup structure of G to characterize the distinguishing number. We present the theorem below as an example of employing this technique.

Theorem 4.1. *Let G be a finite group acting faithfully on a set X. Let p be the smallest prime dividing the order of G, and let M be the length of the largest orbit of the action of G on X. Then $D_G(X) \leq \lceil \frac{M}{p-1} \rceil$.*

Proof. With $\lceil \frac{M}{p-1} \rceil$ colors, we may color each orbit of X such that every color class within a given orbit has size at most $p-1$. Call this coloring c. Let $\sim$ be the equivalence relation given by $x_1 \sim x_2$ if and only if x_1 and x_2 are in the same orbit and have the same color. Let $P_1, P_2, \dots, P_k$ be the equivalence classes of this relation, and let $n_i = |P_i|$. Note that a color preserving permutation $h \in H_c$ can take a given element only to another element in its equivalence class. Thus $H_c \leq S_{n_1} \times S_{n_2} \times \cdots \times S_{n_k}$. Also, $H_c \leq G$. But since each $n_i < p$, the orders of $S_{n_1} \times S_{n_2} \times \cdots \times S_{n_k}$ and G are relatively prime. Since the order of H_c divides both orders, we have $H_c = 1$, and so c is distinguishing. □

In addition, we could use subgroup structure as a way to generalize the notion of the distinguishing number, as follows. Given a group G acting faithfully on a set X and H a subgroup of G, let $D_{G,H}(X)$ denote the smallest number of colors admitting a coloring of X such that the only elements of G that induce color-preserving permutations lie in H. Thus, when $H = 1$, we recover the original notion of the distinguishing number.

Question 1. *Characterize $D_{G,H}(X)$.*

In Section 2, we considered the maximum distinguishing number admitted by a given group. Intuitively, we would expect a large group to admit actions that require many colors to distinguish them. Thus, we ask whether the distinguishing number is ordered in a way that respects the partial ordering of groups defined by subgroup inclusion.

Question 2. *Let G and H be groups, H a subgroup of G. Does it follow that $\overline{D}(H) \leq \overline{D}(G)$?*

Note that if a given faithful action of H on X can be extended to a faithful action of G on X then $D_H(X) \leq D_G(X)$, because any coloring of X that is distinguishing with respect to the action of G is also distinguishing with respect to the action of H. However, since not every faithful action of H on X can necessarily be extended to a faithful action of G (for example if $|G| > |X|!$), the question cannot be answered immediately in the affirmative.

We also ask whether the bounds obtained in Section 2 for nilpotent and supersolvable groups are tight.

Question 3. *For which $k > 2$ does there exist a group G that is nilpotent group of class k (or a supersolvable group of length k) acting faithfully on a set X such that $D_G(X) = k+1$?*

In Section 3, we showed that $D_{GL_n(K)}(K^n) = 2$ if $|K| > n+1$ and $D_{GL_n(K)}(K^n) = 3$ if $|K| \in \{2, 3\}$ and $n = 2$. As mentioned, we leave the remaining cases as an open question.

Question 4. *Compute $D_{GL_n(K)}(K^n)$ for $n > 2$ and $|K| \leq n + 1$.*

The generalization of the distinguishing number to infinite groups acting on infinite sets is new, and it might be interesting to investigate conditions on the finiteness or infiniteness of the distinguishing number. This leads to many questions, including the following.

Question 5. *Suppose G is a group that always acts with finite distinguishing number. Does it follow that $\overline{D}(G) < \infty$, that is, that the set $\{D_G(X)\}$ has a maximum element?*

Another approach would simply be to define the distinguishing number of an action to be the cardinality of the smallest set of colors admitting a distinguishing coloring. This would eliminate the formal distinction between the finite and infinite cases.

Finally, throughout this paper, we have considered the distinguishing numbers that a fixed group admits in its actions on various sets. We could instead fix a set $[n]$ and consider the distinguishing numbers it admits under the actions of various groups.

Question 6. *For each n, characterize the set*

$$T_n = \{D_G([n]) \mid G \textit{ is a transitive subgroup of } S_n\}.$$

One may show that $T_n = \{2, \ldots, n\}$ for $n = 2, 3, 4, 5$, and 6. We ask whether T_n has this form for larger n. Note that we require our group G to be transitive, for otherwise each distinguishing number k between 1 and n could be achieved by taking a subgroup of S_n that fixes each $k+1, k+2, \ldots, n$ and whose action on $1, \ldots, k$ is isomorphic to the action of S_k.

5 Acknowledgments

This research was conducted at the University of Minnesota Duluth Research Experience for Undergraduates, while the author was a student at Yale University. The author would like to express her thanks to Melanie Wood for numerous ideas and suggestions on drafts of this paper, to Philip Matchett and Daniel Isaksen for several very helpful conversations, and to Joseph Gallian for his support. This research was funded by the National Science Foundation (DMS-0137611) and the National Security Agency (H-98230-04-1-0050).

References

[1] M. Albertson and K. Collins, An introduction to symmetry breaking in graphs, Graph Theory Notes N.Y. 30 (1996) 6-7.

[2] M. Albertson and K. Collins, Symmetry breaking in graphs, Electronic Journal of Combinatorics 3 (1996) R18.

[3] B. Bogstad and L. Cowen, The distinguishing number of the hypercube, Discrete Mathematics 283 (2004) 29-35.

[4] H. G. Bray et al., Between Nilpotent and Solvable, Polygonal Publishing House, NJ, 1982.

[5] M. Chan, The distinguishing number of the augmented cube and hypercube powers, preprint.

[6] M. Chan, The distinguishing number of the direct product and wreath product action, Journal of Algebraic Combinatorics, to appear.

[7] C.C.T. Cheng, Three problems in graph labeling, Ph.D. Thesis, Department of Mathematical Sciences, Johns Hopkins University, 1999.

[8] M. Hall, The Theory of Groups, Macmillan, New York, 1959.

[9] C. E. Hempel, Metacyclic groups, Communications in Algebra 28, 3865-3897, 2000.

[10] K. Potanka, Groups, graphs and symmetry breaking, Masters Thesis, Department of Mathematics, Virginia Polytechnic Institute, 1998.

[11] A. Russell and R. Sundaram, A note on the asymptotics and computational complexity of graph distinguishability, Electronic Journal of Combinatorics 5 (1998) R23.

[12] J. Tymoczko, Distinguishing numbers for graphs and groups, Electronic Journal of Combinatorics 11 (1) (2004) R63.