Symmetry Breaking in Graphs

Michael O. Albertson [1]
Department of Mathematics
Smith College
Northampton MA 01063
albertson@smith.smith.edu

Karen L. Collins
Department of Mathematics
Wesleyan University
Middletown, CT 06459-0128
kcollins@wesleyan.edu

Submitted: September 1, 1995; Accepted: June 9, 1996.

Abstract

A labeling of the vertices of a graph G, $\phi : V(G) \rightarrow \{1, \ldots, r\}$, is said to be r-distinguishing provided no automorphism of the graph preserves all of the vertex labels. The distinguishing number of a graph G, denoted by $D(G)$, is the minimum r such that G has an r-distinguishing labeling. The distinguishing number of the complete graph on t vertices is t. In contrast, we prove (i) given any group Γ, there is a graph G such that $Aut(G) \cong \Gamma$ and $D(G) = 2$; (ii) $D(G) = O(log(|Aut(G)|))$; (iii) if $Aut(G)$ is abelian, then $D(G) \leq 2$; (iv) if $Aut(G)$ is dihedral, then $D(G) \leq 3$; and (v) If $Aut(G) \cong S_4$, then either $D(G) = 2$ or $D(G) = 4$. Mathematics Subject Classification 05C,20B,20F,68R

1 Introduction

A classic elementary problem with a surprise answer is Frank Rubin's key problem [15], which Stan Wagon recently circulated in the Macalester College problem column [13].

> Professor X, who is blind, keeps keys on a circular key ring. Suppose there are a variety of handle shapes available that can be distinguished by touch. Assume that all keys are symmetrical so that a rotation of the key ring about an axis in its plane is undetectable from an examination of a single key. How many shapes does Professor X need to use in order to keep n keys on the ring and still be able to select the proper key by feel?

[1] Research supported in part by NSA 93H-3051

The surprise is that if six or more keys are on the ring, there need only be 2 different handle shapes; but if there are three, four, or five keys on the ring, there must be 3 different handle shapes to distinguish them.

The answer to the key problem depends on the shape of the key ring. For instance, a linear key holder would require only two different shapes of keys. As long as the ends had differently shaped keys, the two ends could be distinguished, and one could count from an end to distinguish the other keys. Thinking about the possible shapes of the key holders, we are inspired to formulate the key problem as a problem in graph labeling.

A labeling of a graph G, $\phi : V(G) \to \{1, 2, \ldots, r\}$, is said to be *$r$-distinguishing* if no automorphism of G preserves all of the vertex labels. The point of the labels on the vertices is to destroy the symmetries of the graph, that is, to make the automorphism group of the labeled graph trivial. Formally, ϕ is r-distinguishing if for every non-trivial $\sigma \in Aut(G)$, there exists x in $V = V(G)$ such that $\phi(x) \neq \phi(x\sigma)$. We will often refer to a labeling as a coloring, but there is no assumption that adjacent vertices get different colors. Of course the goal is to minimize the number of colors used. Consequently we define the *distinguishing number of a graph G* by

$$D(G) = min\{r \mid G \text{ has a labeling that is } r\text{-distinguishing}\}.$$

The original key problem is to determine $D(C_n)$, where C_n is the cycle with n vertices. Clearly, $D(C_1) = 1$, and $D(C_2) = 2$. Let $n \geq 3$ and suppose the vertices of C_n are denoted $v_0, v_1, v_2, \ldots, v_{n-1}$ in order. We define two labelings, each of which makes the cycle look like a line with two differently shaped ends. Define labeling ϕ by $\phi(v_0) = 1, \phi(v_1) = 2$, and $\phi(v_i) = 3$ for $2 \leq i \leq n-1$. Then ϕ is 3-distinguishing. None of C_3, C_4, C_5 can be 2-distinguished. However, for $n \geq 6$, if ψ is defined by $\psi(v_0) = 1, \psi(v_1) = 2, \psi(v_2) = \psi(v_3) = 1$ and $\psi(v_i) = 2$ for $4 \leq i \leq n-1$, then ψ is 2-distinguishing. Hence the surprise.

We next illustrate how different graphs with the same automorphism group may have different distinguishing numbers. Let K_n be the complete graph on n vertices, and J_n be its complement. Let $K_{1,n}$ be J_n joined to a single vertex. Each of these graphs has S_n as its automorphism group. It is immediate that $D(K_n) = D(J_n) = D(K_{1,n}) = n$.

Now let G_n denote the graph with $2n$ vertices obtained from K_n by attaching a single pendant vertex to each vertex in the clique. Clearly

$Aut(G_n) \cong S_n$. In an r-distinguishing labeling, each of the pairs consisting of a vertex of the clique and its pendant neighbor must have a different ordered pair of labels; there are r^2 possible ordered pairs of labels using r colors, hence $D(G_n) = \lceil \sqrt{n}\, \rceil$.

On the other hand, recall that the inflation of graph G, $Inf(G)$, is defined as follows: the vertices of $Inf(G)$ consist of ordered pairs of elements from G, the first being a vertex and the second an edge incident to that vertex. Two vertices in $Inf(G)$ are adjacent if they differ in exactly one component [3]. In the context of polyhedra, the inflation of a graph is also known as the truncation [4]. Label the vertices of K_n with $1, \ldots, n$. Then vertices of $Inf(K_n)$ can be labelled $\{i_j | 1 \leq i \leq n, 1 \leq j \leq n$, and $i \neq j\}$ in the obvious way. Assigning the color 1 to vertex i_j if $i < j$, and the color 2 otherwise shows that $D(Inf(K_n)) = 2$. It is easy to see that $Aut(Inf(K_n)) \cong S_n$, provided that $n \geq 4$.

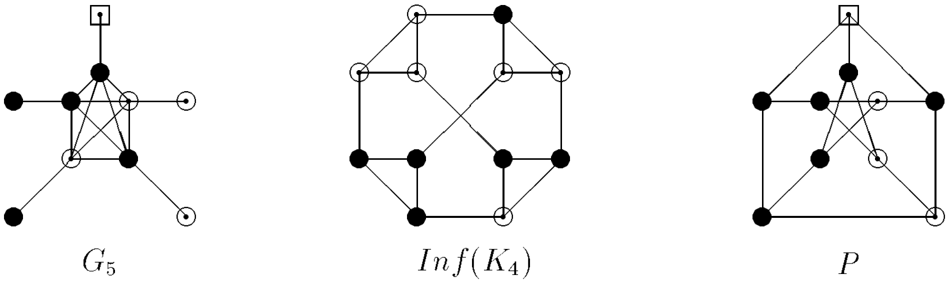

Figure 1 There are only 4 different pairs of 2 colors, hence $D(G_5) = 3$. $Inf(K_4)$ can be distinguished with 2 colors. The Petersen graph P can be distinguished with 3 colors, but not with 2.

As a final example, consider line graphs of complete graphs. Let $L(G)$ be the line graph of G. If $n \geq 5$, then $Aut(L(K_n)) \cong Aut(K_n) \cong S_n$ [10]. A case analysis proves that $D(L(K_5)) > 2$. The distinguishing number of a graph must be the same as the distinguishing number of its complement, and the complement of $L(K_5)$ is the Petersen graph. Thus our 3-distinguishing labeling of the Petersen graph shown in Figure 1 above shows that $D(L(K_5)) = 3$. In section 5 we sketch an argument due to Lovasz that for $n \geq 6, D(L(K_n)) = 2$.

There is a sense in which distinguishing vertices in a graph is reminiscent of Polya-Burnside enumeration. That context would provide a set, say $\mathcal{C}$, of labeled graphs closed under the action of a given group, say Γ. The Burnside lemma is a tool for computing the number of inequivalent labeled graphs in $\mathcal{C}$ where equivalence is given by some action from Γ. Our perspective is essentially dual. We take a particular labeled graph chosen so that it generates a large set of equivalents. If that set has cardinality $|\Gamma|$, then the labeling is distinguishing.

We now digress for a bit to consider the complexity of the distinguishing question. First we observe that $D(G) = 1$ if and only if G is a rigid graph, *i.e.,* one whose automorphism group is trivial. The complexity of deciding if a given graph has a non-trivial automorphism has not been settled [9, 11]. It is known to be Turing equivalent to Unique Graph Isomorphism, and is a candidate for a problem whose difficulty lies between being in P and being $NP - complete$. Hence determining if $D(G) = 1$ may be difficult. Let us fix the particular question to be: Given a graph G and an integer k, is $D(G) > k$? For $k = 1$, this question is in NP. To see this, it suffices to show that if $D(G) > 1$, there is a certificate that allows one to easily verify this fact. Here such a certificate could be a vertex bijection, since it is straightforward to check that a vertex bijection is a graph automorphism. In contrast, it seems plausible that this question is not in $co - NP$. For larger k, the question is not obviously in either NP or $co - NP$. To see this, suppose we are given a graph G with minimum degree at least 2 and an allegedly r-distinguishing labeling. If we attach a path of length i to each vertex in G that is labeled i, then the original vertices all have degree at least 3. The resulting graph is only polynomially larger than the original, and the original labeling is r-distinguishing if and only if the new graph is rigid.

Although a given group might be the automorphism group of graphs with different distinguishing numbers, there are some restrictions. An automorphism of a graph G can never take vertices in different vertex orbits to each other. Thus vertices in different orbits are always distinguished from each other. Recall that the orbit sizes must divide the order of the group. Thus it is no surprise that the automorphism group is inextricably entwined with the distinguishing number.

Let Γ be an abstract group. We will say that the graph G realizes Γ if $Aut(G) \cong \Gamma$. We define the *distinguishing set of a group* Γ by

$$D(\Gamma) = \{D(G) |\ G \text{ realizes } \Gamma\ \}$$

The purpose of this paper is to examine how properties of graphs and groups affect the parameters D. In section 2 we investigate arbitrary groups and show that $D(G) = O(log|Aut(G)|)$ and $2 \in D(\Gamma)$. In section 3 we develop some tools to distinguish orbits. One consequence is that if $Aut(G)$ is either abelian or hamiltonian (but not trivial), then $D(G) = 2$. We discuss dihedral groups in Section 4. If $Aut(G)$ is dihedral, then $D(G) \leq 3$. Furthermore if $n \neq 3, 4, 5, 6, 10$ and $Aut(G) \cong D_n$ ($D_n \cong Aut(C_n)$), then $D(G) = 2$. In section 5 we obtain the initially counterintuitive result that $D(S_4) = \{2, 4\}$. We make conjectures in Section 6.

2 Distinguishing arbitrary groups

Our first result says that given a fixed group, a graph that realizes that group cannot have an arbitrarily large distinguishing number.

Theorem 1 Suppose $H_k = \{e\} < H_{k-1} < \cdots < H_2 < H_1 = \Gamma$ is a longest chain of subgroups of Γ where H_{i+1} is a proper subgroup of H_i for $1 \leq i \leq k-1$. If G realizes Γ, then $D(G) \leq k$.

Proof Suppose ϕ is an r-distinguishing labeling of G, where $r = D(G)$. Let $G_1, G_2, \ldots, G_r$ be isomorphic copies of G. For $1 \leq i \leq r$ label G_i by $c_i : V(G_i) \to \{1, 2, 3, \ldots, i\}$ where

$$c_i(v) = \begin{cases} \phi(v) \text{ if } \phi(v) \leq i \\ 1 \text{ if } \phi(v) > i \end{cases}$$

Notice that if $c_i(v) \neq 1$, then $c_i(v) = \phi(v)$.

Now the automorphism group of G_i, $Aut(G_i)$, is the subgroup of $Aut(G)$, each element of which preserves the labeling c_i of the vertices of G_i. Clearly $Aut(G_{i+1})$ is a subgroup of $Aut(G_i)$. We claim $Aut(G_{i+1})$ is a proper subgroup of $Aut(G_i)$. By contradiction, suppose $Aut(G_{i+1}) = Aut(G_i)$. We show that there exists an automorphism that preserves ϕ, hence ϕ is not r-distinguishing. Let $\psi : V(G) \to \{1, 2, 3, \ldots, r\} - \{i+1\}$ by

$$\psi(v) = \begin{cases} 1 \text{ if } \phi(v) = i+1 \\ \phi(v) \text{ otherwise} \end{cases}$$

Then ψ uses only $r-1$ colors, and therefore cannot be distinguishing because $D(G) = r$. There must then exist a non-trivial automorphism g of G

such that $\psi(vg) = \psi(v)$ for all vertices v in G. If v is a vertex with $\phi(v) \neq i+1$, then $\psi(vg) = \psi(v) = \phi(v)$. If $\phi(vg) \neq i+1$, then $\phi(vg) = \psi(vg) = \phi(v)$. We need to prove that if $\phi(v) = i+1$ or $\phi(vg) = i+1$, then $\phi(vg) = \phi(v)$.

Since g preserves the labels $\{1, 2, 3, \ldots, i\}$, g preserves c_i and so $g \in Aut(G_i)$. We have assumed that $Aut(G_i) = Aut(G_{i+1})$, hence g preserves c_{i+1}. If $\phi(v) = i+1$, then $c_{i+1}(v) = i+1 = c_{i+1}(vg)$. Hence $\phi(vg) = i+1$, so $\phi(v) = \phi(vg)$. Conversely, if $\phi(vg) = i+1$, then $c_{i+1}(vg) = i+1 = c_{i+1}(v)$. Hence $\phi(v) = i+1 = c_{i+1}(v)$. Therefore, g preserves ϕ and ϕ cannot be distinguishing. This contradicts our assumption that ϕ is an r-distinguishing labeling.

We remark that this proves that the largest integer in $D(S_3)$ is 3, since the subgroups of S_3 have orders $1, 2, 3, 6$, and no order 2 subgroup can be contained in an order 3 subgroup. The complete graph on 3 vertices requires 3 colors to distinguish, and we show in the next theorem that 2 is in the distinguishing set of every group, so $D(S_3) = \{2, 3\}$.

Corollary 1.1 Let Γ have m elements. Then the largest integer in $D(\Gamma)$ is less than or equal to $1 + \lfloor log_2(m) \rfloor$.

Proof Let k be as defined in Theorem 1. Since $\frac{|H_{i+1}|}{|H_i|} \geq 2$, $|\Gamma| \geq 2^k$.

The standard construction of a graph that realizes a particular group is due to Frucht, see [7]. Recall that the construction begins with one vertex for each group element. Vertices corresponding to group elements u and v are joined by a directed colored edge labeled g precisely if $ug = v$. A graph is obtained by replacing the colored arcs by graph gadgets (typically paths with different length paths off each vertex). Given a group Γ, we denote the Frucht graph by $F(\Gamma)$ and note that $Aut(F(\Gamma)) \cong \Gamma$. Now if Σ is a subgroup of Γ, then we may obtain a labeled graph whose automorphism group is isomorphic to Σ by labeling $F(\Gamma)$ in the following way: If a vertex is one of the original vertices of the Cayley graph and is in Σ or if the vertex is in a gadget that replaced an arc labeled with an element of Σ, then that vertex is labeled 1. All other vertices are labeled 2. Any automorphism of the labeled graph must preserve the 1's and is thus an automorphism from $F(\Sigma)$. Consequently, we can realize any subgroup of a given group with a 2-colored Frucht graph.

Theorem 2 For any finite group Γ, $2 \in D(\Gamma)$.

Proof First we note that for any group Γ, there is a connected cubic graph G which realizes Γ, see [6]. Suppose G has n vertices. Attach a path with $\lceil log_2 n \rceil$ vertices to each vertex of G to obtain $\hat{G}$. There are $2^{\lceil log_2 n \rceil} \geq n$ possible colorings of the paths using 2 colors. Color each one differently. Then this labeling is 2-distinguishing for $\hat{G}$. Since we have attached the same sized path to every vertex, every automorphism of G is also an automorphism of $\hat{G}$. An automorphism of $\hat{G}$ must preserve the original vertices of G, since the original vertices have degree 4 in $\hat{G}$ and the new vertices have degree less than or equal to 2. This fixes the first vertex of each new path, and hence the rest of the new path.

3 Distinguishing via orbits

It is not necessary that a labeling distinguish every orbit separately in order to distinguish the entire graph. See Figure 2 below. Sometimes it is easy to distinguish each orbit separately. We say that an r-labeling distinguishes an orbit if every automorphism that acts non-trivially on the orbit maps at least one vertex to a vertex with a different label. Alternatively if $U \subseteq V(G)$ let $G[U]$ denote the induced subgraph of G on the vertex set U. Then if U is an orbit of G, a labeling distinguishes U if it distinguishes $G[U]$. Trivially an orbit of size 1 can be distinguished with 1 color.

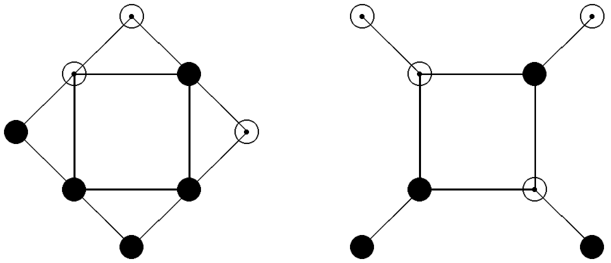

Figure 2 Two graphs which realize D_4. Each graph can be distinguished with 2 colors, even though no orbit is separately distinguished.

Theorem 3 Let Γ be the automorphism group of graph G. Let u be a vertex of G and $H_u = \{h \in \Gamma | uh = u\}$ be the stabilizer subgroup of u. Let O_u be the vertex orbit that contains u. If H_u is normal in Γ, then O_u can be distinguished with 2 colors.

Proof Color vertex u red and the rest of the vertices in O_u blue. Then if there exists an automorphism h in Γ which does not distinguish O_u, it must fix u and there must exist $x, y \in O_u$ such that $xh = y$, but $x \neq y$. Since h fixes u, $h \in H_u$. Since $x, y \in O_u$, there are group elements g_1, g_2 such that $x = ug_1$ and $y = ug_2$. Then $ug_1h = ug_2$. Since H_u is normal, there exists $h' \in H_u$ such that $g_1h = h'g_1$. Therefore, $uh'g_1 = ug_1$, since H_u is the stabilizer of u. This means $x = ug_1 = ug_2 = y$, hence h fixes every vertex in O_u.

Recall that a non-abelian group is called *hamiltonian* if every subgroup is normal [8].

Corollary 3.1 If non trivial Γ is abelian or hamiltonian, then $D(\Gamma) = \{2\}$.

Proof Every subgroup of Γ is normal. Hence every orbit can be distinguished with 2 colors.

A large orbit can force a graph to have a low distinguishing number.

Theorem 4 Let G be a graph with $Aut(G) = \Gamma$. If G has an orbit $O = \{u_1, u_2, u_3, \ldots, u_s\}$ that can be distinguished with k colors, and $\cap_{i=1}^{s} H_{u_i} = \{e\}$ where H_{u_i} is the stabilizer group of u_i, then G can be distinguished with k colors.

Proof Let O be labeled with a k-distinguishing labeling. Let $\sigma \in \Gamma$. Then σ acts non-trivially on O because the only element that fixes every member of O is the identity. Therefore, there exists a member of O, say u_i such that the color of u_i is different from the color of $u_i\sigma$.

If vertex u in G has stabilizer subgroup H_u, then the size of the orbit that contains u is $|Aut(G)|/|H_u|$.

Corollary 4.1 A graph G which has an orbit of size $|Aut(G)|$ can be distinguished with 2 colors.

Proof Let O be such an orbit. Then the stabilizer subgroup of every element of O has order 1, hence is trivial. Color one vertex red and the rest blue. Then every non-trivial automorphism of the graph must take the red vertex to a blue one.

Having many orbits can force a graph to be 2-distinguishable.

Theorem 5 Let G realize group Γ. Let $u_1, u_2, \ldots, u_t$ be vertices from different vertex orbits of G with $H_1, H_2, \ldots, H_t$ their respective stabilizing subgroups. If $H_1 \cap H_2 \cap \cdots \cap H_t = \{e\}$, then $D(G) = 2$.

Proof Color $u_1, u_2, \ldots, u_t$ red and the rest of the vertices blue. Let $g \in \Gamma$. Since the intersection of the stabilizers of $u_1, u_2, \ldots, u_t$ is just the identity, there is some some i such that g does not fix u_i. Thus $u_i g$ is colored blue, while u_i is colored red. Thus we have a 2-distinguishing labeling of G.

4 Dihedral groups

We use D_n $(n \geq 3)$ to denote the dihedral group of order $2n$. Such groups arise naturally in geometry as the symmetries of the regular n-gon and in graph theory as the automorphism groups of the cycles. The dihedral groups are the most elementary non-abelian groups, having a cyclic subgroup half the size of the original group. In this section we compute the distinguishing set of every dihedral group.

Let D_n be generated by σ, τ where $\sigma^n = e, \tau^2 = e$, and $\tau\sigma = \sigma^{n-1}\tau$. Every element $\tau\sigma^i$ for $0 \leq i \leq n-1$ is an involution of D_n. These are the only involutions of D_n unless n is even, in which case $\sigma^{\frac{n}{2}}$ is an involution and $\{e, \sigma^{\frac{n}{2}}\}$ is the center of D_n.

The non-trivial subgroups of D_n fall into one of three types: a subgroup of $< \sigma >$, the cyclic half of D_n, a subgroup isomorphic to D_m where $m|n$, and a subgroup with the identity and an order 2 element (which is not a power of σ). We describe these three types by their generators, and select coset representatives for the orbits of vertices with one of these subgroups as its stabilizer. Let $0 \leq i \leq n-1$ and $1 \leq j \leq n-1$. The three types of subgroups are

$$< \sigma^j >, < \sigma^j, \tau\sigma^i >, < \tau\sigma^i >$$

Then $< \sigma^j >$ is normal in D_n, so has no conjugates except itself. The intersection of its conjugates is also itself. If vertex v has stabilizer $< \sigma^j >$, then the orbit of v is $\{v, v\sigma, v\sigma^2, \ldots, v\sigma^{j-1}, v\tau, v\tau\sigma, v\tau\sigma^2, \ldots, v\tau\sigma^{j-1}\}$.

The subgroups conjugate to $< \sigma^j, \tau >$ are the subgroups

$$< \sigma^j, \tau\sigma >, < \sigma^j, \tau\sigma^2 >, \ldots, < \sigma, \tau\sigma^{j-1} >$$

whose intersection is $< \sigma^j >$. If vertex v has stabilizer $< \sigma^j, \tau\sigma^i >$, then the orbit of v is $\{v, v\sigma, v\sigma^2, \ldots, v\sigma^{j-1}\}$.

The subgroups conjugate to $< \tau >$ are generated by the involutions that have a τ:

$$< \tau\sigma >, < \tau\sigma^2 >, \ldots, < \tau\sigma^{n-1} >$$

whose intersection is just the identity. If vertex v has stabilizer $< \tau\sigma^i >$, then the orbit of v is $\{v, v\sigma, v\sigma^2, \ldots, v\sigma^{n-1}\}$.

Lemma 1 Let G realize D_n, and suppose that G has t orbits. Let $u_1, u_2, \ldots, u_t$ be vertices from the t different vertex orbits of G with $H_1, H_2, \ldots, H_t$ their respective stabilizing subgroups. Then $< \sigma > \cap H_1 \cap H_2 \cap \cdots \cap H_t = \{e\}$.

Proof We observe that the conjugacy class of σ^t in D_n is $\{\sigma^t, \sigma^{n-t}\}$, since $\sigma^l \sigma^t \sigma^{-l} = \sigma^t$ and $\tau\sigma^i\sigma^t\tau\sigma^i = \sigma^{n-t}$. Hence if σ^t is an element of any subgroup H, then σ^t is an element of any subgroup conjugate to H. Therefore, if $\sigma^t \in H_1 \cap H_2 \cap \cdots \cap H_t$, then σ^t is in every conjugate of each of these stabilizers, hence is in every stabilizer of every vertex of G. If σ^t fixes every vertex of G, since G realizes D_n, $\sigma^t = e$ and $t = n$.

Lemma 2 Let G realize D_n. Let u be a vertex in G whose stabilizer $H_u =< \sigma^j >$. Let O_u be the orbit of u. Then G can be distinguished with 2 colors.

Proof Let $u, u_2, \ldots, u_t$ be vertices from all the different vertex orbits of G with $H_u, H_2, \ldots, H_t$ their respective stabilizing subgroups. Then $H_u \cap H_2 \cap \cdots \cap H_t \subseteq H_u =< \sigma^j >$. By Lemma 1 the intersection must be the identity, in which case G is 2-distinguishable by Theorem 5.

Lemma 3 Let G realize D_n. Let u be a vertex in G whose stabilizer $H_u =< \sigma^j, \tau\sigma^i >$ or $< \tau\sigma^i >$. Let O_u be the orbit of u. If $|O_u| \geq 6$ then O_u can be distinguished with 2 colors.

Proof The orbit of u is $O_u = \{u, u\sigma, u\sigma^2, \ldots, u\sigma^{j-1}\}$, where we may assume that $j \geq 6$. Let $A = \{u, u\sigma^2, u\sigma^3\}$. Color the vertices in A red and the rest of O_u blue. Note that this corresponds with the labeling l' from the introduction. We claim that this is a 2-distinguishing coloring of O_u, *i.e.* that every automorphism that acts non-trivially on O_u does not fix A. The proof goes as follows: Suppose $g \in D_n$ fixes A, then $ug \in A$, hence $ug = u, u\sigma^2$ or $u\sigma^3$. The automorphisms that send u to u are H_u, the automorphisms that send u to $u\sigma^2$ are $H_u\sigma^2$ and the automorphisms that send u to $u\sigma^3$ are $H_u\sigma^3$. We check that each automorphism in $H_u, H_u\sigma^2, H_u\sigma^3$ either acts trivially on O_u or does not fix A. The subgroup of automorphisms that act trivially on O_u is the intersection of the stabilizer subgroups of each vertex, hence, if $H_u =< \sigma^j, \tau\sigma^i >$ this is $< \sigma^j >$ and if $H_u =< \tau\sigma^i >$, this is $\{e\}$.

If $H_u =< \sigma^j, \tau\sigma^i >$, then j divides n and the elements of H_u are

$$e, \sigma^j, \sigma^{2j}, \sigma^{3j}, \ldots, \sigma^{(\frac{n}{j}-1)j}, \tau\sigma^i, \tau\sigma^{i+j}, \tau\sigma^{i+2j}, \ldots, \tau\sigma^{i+(\frac{n}{j}-1)j}$$

Let $0 \leq d \leq \frac{n}{j} - 1$. The table below shows the outcomes when these automorphisms are applied to A.

$$\begin{array}{lcllcl}
A\sigma^{dj} & = & A & A\tau\sigma^{i+dj} & = & \{u, u\sigma^{n-2}, u\sigma^{n-3}\} \\
A\sigma^{dj}\sigma^2 & = & \{u\sigma^2, u\sigma^4, u\sigma^5\} & A\tau\sigma^{i+dj}\sigma^2 & = & \{u\sigma^2, u, u\sigma^{n-1}\} \\
A\sigma^{dj}\sigma^3 & = & \{u\sigma^3, u\sigma^5, u\sigma^6\} & A\tau\sigma^{i+dj}\sigma^3 & = & \{u\sigma^3, u\sigma, u\}
\end{array}$$

Since $n \geq 6$, only σ^{dj} preserve A, however, σ^{dj} acts trivially on O_u.

If $H_u =< \tau\sigma^i >$, then $H_u = \{e, \tau\sigma^i\}$. The table below shows the outcomes when $\tau\sigma^i, \tau\sigma^i\sigma^2, \tau\sigma^i\sigma^3$ are applied to A.

$$\begin{array}{lcl}
A\tau\sigma^i & = & \{u, u\sigma^{n-2}, u\sigma^{n-3}\} \\
A\tau\sigma^i\sigma^2 & = & \{u\sigma^2, u, u\sigma^{n-1}\} \\
A\tau\sigma^i\sigma^3 & = & \{u\sigma^3, u\sigma, u\}
\end{array}$$

Since $n \geq 6$, none of these preserve A.

Lemma 4 Let G realize D_n. Let u be a vertex in G whose stabilizer $H_u =< \sigma^j, \tau\sigma^i >$ or $< \tau\sigma^i >$. Let O_u be the orbit of u. If $|O_u| \geq 6$ then G can be distinguished with 2 colors.

Proof If $H_u =< \tau\sigma^i >$, then the intersection of the subgroups conjugate to H_u is just the identity. Thus we apply Lemma 3 to prove that O_u is 2-distinguishable and Theorem 4 to prove that G is 2-distinguishable.

Assume that $H_u =< \sigma^j, \tau\sigma^i >$. Then since O_u is 2-distinguishable, every automorphism that acts non-trivially on O_u takes a red vertex to a blue vertex. The automorphisms which act trivially on O_u are those in the intersection of the stabilizers of vertices in O_u. This intersection is the cyclic subgroup $\Lambda =< \sigma^j >$.

The action of Λ on G makes vertex orbits $U_1, U_2, \ldots, U_s$ (which are contained in the vertex orbits of G under D_n). The orbit O_u under Λ is broken into 1-orbits, since σ^j fixes O_u. For each orbit U_i which has order greater than 1, choose a vertex $v_i \in U_i$ and color v_i red and the rest of the vertices in U_i blue. Then we claim that every automorphism in Λ must take a red to a blue vertex, because every automorphism in Λ must move v_i for some i. Let $\sigma^{dj} \in \Lambda$, where $1 \leq d \leq (\frac{n}{j} - 1)$. If $v_i\sigma^{dj} = v_i$, then $U_i\sigma^{dj} = U_i$ since Λ is abelian. Thus if σ^{dj} fixes v_i for every $1 \leq i \leq s$, then σ^{dj} fixes U_i for every $1 \leq i \leq s$, hence σ^{dj} fixes all of G. This contradicts our assumption that G realizes D_n. Thus our coloring 2-distinguishes G.

Theorem 6 $D(D_n) = \{2\}$ unless $n = 3, 4, 5, 6, 10$, in which case, $D(D_n) = \{2, 3\}$.

Proof Let G be a graph that realizes D_n. By Lemmas 2, 3, 4, if G has an orbit of size at least 6, then G is 2-distinguishable. Let p be a prime divisor of n, and suppose that p^α is the largest power of p that divides n. Then the action of the cyclic subgroup $\Lambda =< \sigma^{\frac{n}{p^\alpha}} >$ makes vertex orbits in G of size $1, p, p^2, \ldots,$ or p^α. Let u be a vertex in G, and let d be the smallest positive integer such that $u\sigma^{d\frac{n}{p^\alpha}} = u$. Then d is the size of the Λ-orbit that contains u. Therefore, d divides p^α. We claim that there must be an orbit O under Λ of size p^α. If not, then for each $u \in G$, $u\sigma^{d\frac{n}{p^\alpha}} = u$ for some $d = p^\beta$ and $\beta < \alpha$. Since $d\frac{n}{p^\alpha} = p^\beta \frac{n}{p^\alpha} = \frac{n}{p^{\alpha-\beta}}$, and $\alpha - \beta \geq 1$, then $u\sigma^{\frac{n}{p}} = u$. Hence $\sigma^{\frac{n}{p}}$ fixes all of G, which contradicts our assumption that G realizes D_n. Thus O stays the same size or becomes larger under the action of D_n. Therefore, if n has a divisor which is a prime power p^α greater than 6, then $D(D_n) = \{2\}$.

We may therefore assume that n has no prime divisor greater than 5, that n has at most one factor of 5, one factor of 3, and two factors of 2. Thus the only remaining cases are $n = 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$. We prove first that if $n \geq 12$, then $D(D_n) = \{2\}$.

We may assume that every orbit of G has size less than or equal to 5. By Lemma 2, we may assume that the stabilizer of every vertex is one of the second two types: either $< \sigma^j, \tau\sigma^i >$ of order $\frac{2n}{j}$ or $< \tau\sigma^i >$ of order 2. However, an order 2 stabilizer corresponds to an order n orbit, which is greater than 5 if $n \geq 12$. Let u be a vertex in an orbit O of size d (where $d = 1, 2, 3, 4$ or 5 and d divides n) with stabilizer H_u, of size $\frac{2n}{d}$. Then $H_u =< \sigma^d, \tau\sigma^i >$ for some $0 \leq i \leq d-1$. Thus $< \sigma^d >$ fixes O. Let u' be a vertex in an orbit O' of size d' with stabilizer $H_{u'} =< \sigma^{d'}, \tau\sigma^{i'} >$. Let $l = lcm(d, d')$. Then $< \sigma^{d'} >$ fixes O' and $< \sigma^l >$ fixes both O and O'. In order for G to realize D_n, G must have orbits with sizes whose least common multiple is n.

Hence if $n = 12$, there are orbits of size $3, 4$; if $n = 15$, there are orbits of size $3, 5$; if $n = 20$, then $4, 5$; if $n = 30$, then $2, 3, 5$; if $n = 60$, then $3, 4, 5$. Since 15 is odd and 30 has only one prime factor of 2, there is no 2-orbit if $n = 15$, and no 4-orbit if $n = 30$. If $n = 12, 20, 60$, then there must be a 4-orbit, but then there is no 2-orbit, because we can choose a stabilizer from the 2-orbit, $< \sigma^2, \tau >$, and a stabilizer from the 4-orbit, $< \sigma^4, \tau\sigma >$, whose intersection is $< \sigma^4 >$. By Lemma 1, the intersection of stabilizer subgroups from all the orbits is then just the identity, and hence by Theorem 5 G can be 2-distinguished. Similarly, G cannot have two orbits of the same size. Except for 1-orbits, then, the orbit sizes for each n must be exactly as listed in the first sentence of this paragraph.

Hence if $n \geq 12$, the orbits of G have sizes which are all pairwise relatively prime. The bipartite graphs formed by the vertices of two orbits and the edges between the orbits are then either complete or empty. By Lemma 5 below, D_n is the product of the automorphism group of each orbit, considered as a subgraph of G. Since each orbit must form a vertex transitive graph, the orbits of size 3 are K_3 or its complement; the orbits of size 4 are K_4, its complement, C_4 or its complement; and the orbits of size 5 are K_5 or its complement, C_5, or its complement. In each case, the product of the sizes of the appropriate groups is larger than the size of D_n for the corresponding value of n. Thus if $n \geq 12$, $D(D_n) = \{2\}$.

Next we show that if $n = 3, 4, 5, 6, 10$, then $D(D_n) = \{2, 3\}$. As observed above, $D(S_3) = \{2, 3\}$, and $D_3 = S_3$. ¿From the key problem, $3 \in D(D_4), D(D_5)$. Now D_{2m} has center $C = \{e, \sigma^m\}$, and $D_{2m}/C \cong D_m$ when m is odd by $\sigma \dashrightarrow (\sigma, \tau)$ and $\tau \dashrightarrow (e, \tau)$. Hence $K_{3,2}$, which requires 3 colors to distinguish, realizes D_6, and $C_5 \vee K_2$ realizes D_{10}.

It remains to be shown that if $n = 3, 4, 5, 6, 10$, every graph with automorphism group D_n can be distinguished with 3 colors. Let $u_1, u_2, \ldots, u_t$ be vertices from the t different vertex orbits of G with $H_1, H_2, \ldots, H_t$ their respective stabilizing subgroups. By Lemma 1, $< \sigma > \cap H_1 \cap H_2 \cap \cdots \cap H_t = \{e\}$.

Therefore the subgroup $\cap_{l=1}^{t} H_l$ is of the third type, so $\cap_{l=1}^{t} H_l =< \tau\sigma^i >$, for some $0 \leq i \leq n-1$. Color $u_1, u_2, \ldots, u_t$ red, and choose one vertex v which is not fixed by $\tau\sigma^i$ (all of $u_1, u_2, \ldots, u_t$ are fixed by $\tau\sigma^i$) and color v green. Color the rest of the vertices in G blue. Then every automorphism either moves a red vertex to a vertex which is not red, except for $\tau\sigma^i$ which fixes all the red vertices, but moves the unique green vertex to either a red or a blue vertex. Thus every graph that realizes D_n can be 3-distinguished.

Lemma 5 Suppose O is an orbit of G and for every other orbit O' of G, $G[O'] \ncong G[O]$. Furthermore suppose that each bipartite graph formed by the vertices in O, O' and the edges between these two orbits is either empty or complete. Then $Aut(G) = Aut(G[O]) \times Aut(G[V-O])$.

Proof Let $v \in V$, $h_1 \in Aut(G[O])$, and $h_2 \in Aut(G[V-O])$. We define $\omega : Aut(G[O]) \times Aut(G[V-O]) \to Aut(G)$ by

$$\omega(h_1, h_2)(v) = \begin{cases} (v)h_1 \text{ if } v \in O \\ (v)h_2 \text{ if } v \in V - O \end{cases}$$

Then $\omega(h_1, h_2)$ is an automorphism of G, because it preserves the adjacencies in O, in $V-O$, and between O and $V-O$. Conversely, any automorphism of G, when restricted to O is an automorphism of $G[O]$, and when restricted to $V-O$ is an automorphism of $G[V-O]$.

5 The symmetric group

Before proceeding to our principal result of this section (determining $D(S_4)$), we present an argument (due to Lovasz [12]) to show that if $n \geq 6$, then $D(L(K_n)) = 2$. Since $Aut(L(K_n)) = Aut(K_n) = S_n$, it is enough to show that by 2-coloring the edges of K_n we can break every vertex automorphism of K_n, since every automorphism of the vertices of K_n is an automorphism of the edges as well. Let G consist of a path of n vertices with one additional edge joining the second and fourth vertex. If $n \geq 6$, then G is rigid. Thus if we color the edges of a copy of G in K_n red and all the complementary edges blue, we have destroyed all the automorphisms.

Theorem 7 $D(S_4) = \{2, 4\}$. Furthermore, if G is a graph such that $D(G) = 4$, then G has exactly one 4-orbit and every other vertex is fixed by every automorphism of G.

Outline of Proof Let G realize S_4. Every orbit size must divide 24. By Corollary 4.1, if G has a 24 orbit, then G can be 2-distinguished. It is not hard to show that any orbit with 8 or 12 vertices can be 2-distinguished. From Theorem 4 it follows that if G has an orbit of size 8 or 12, then G can be 2-distinguished. The rest of the argument falls into two cases depending on whether or not G has an orbit of size 4.

Suppose that G does have a 4-orbit U. The stabilizer of any vertex in U must be isomorphic to S_3. There are four copies of S_3 in S_4, which are all conjugate, so each is the stabilizer of exactly one vertex in U. The induced subgraph $G[U]$ on U must be a vertex transitive graph on 4 vertices. Since the stabilizer of each vertex in U contains a 3-cycle, $G[U]$ cannot be a matching or a 4-cycle, Thus $G[U]$ is either 4 independent vertices or K_4.

If every orbit besides U has size 1, then by Lemma 5, $Aut(G) = Aut(G[U]) = S_4$, hence four colors are necessary to distinguish the four vertices in U and sufficient to distinguish G. If there exists an orbit W besides U which has size greater than 1, then the proof proceeds by providing a 2 coloring of the graph between U and W which must be 2-distinguishing of G.

Suppose that G has no orbit of size 4. Then the possible orbit sizes for G are $1, 2, 3$, or 6. The rest of the argument proceeds by analyzing the stabilizers of the possible orbits and providing 2-distinguishing colorings for graphs with 6-orbits, and graphs without 6-orbits, but with 3-orbits. Clearly graphs with largest orbit size 2 can be 2-distinguished. The authors will be happy to provide details of the proof upon request.

6 Conjectures

Conjecture 1 There does not exist a group Γ such that $D(\Gamma) = \{2, 3, 4\}$.

Conjecture 2 If $n \geq 4$, then $n - 1$ is not in $D(S_n)$. In particular this would imply that $D(S_5) = \{2, 3, 5\}$. We further conjecture that for $6 \leq n \leq 9, D(S_n) = \{2, 3, n\}$.

Conjecture 3 If G realizes S_n and $D(G) = n$, then G consists of K_n or its complement together with vertices in 1- orbits.

References

[1] Bela Bollobas, *Graph Theory*, Springer-Verlag, New York, 1979, Graduate Texts in Mathematics.

[2] N. L. Biggs and A. T. White, *Permutation Groups and Combinatorial Structures*, Cambridge Univ. Press, New York, 1979, London Math. Soc. Lect. Notes Ser. 33.

[3] V. Chvatal, *Tough graphs and Hamiltonian circuits*, Disc. Math. 5 (1973), 215-228.

[4] H. S. M. Coxeter, *Regular Polytopes*, Dover, New York, 1973.

[5] H. S. M. Coxeter and W. O. Moser, *Generators and Relations for Discrete Groups*, Springer-Verlag, Berlin, 1957.

[6] R. Frucht, *Graphs of Degree Three with a Given Abstract Group*, Canadian J. Math. 1 (1949) 365-378.

[7] J. L. Gross and T. W. Tucker, *Topological Graph Theory*, Wiley, Inc., New York, 1987.

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

[9] Christoph Hoffmann, *Group Theoretic Algorithms and Graph Isomorphism*, Springer Verlag, New York, 1982 (Lecture Notes in Computer Science 136).

[10] D. A. Holton and J. Sheehan, *The Petersen Graph*, Cambridge University Press, New York, 1993.

[11] J. Kobler, U. Schoning, and J.Toran, *The Graph Isomorphism Problem*, Its Structural Complexity, Birkhauser, Boston, 1993.

[12] L. Lovasz, personal communication.

[13] J. Konhauser, D. Velleman, and S. Wagon, *Which Way Did the Bicycle Go?*, Dolciani series, Mathematical Association of America, Washington, D.C. (1996).

[14] Joseph J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, New York, 1995.

[15] Frank Rubin, Problem 729 in Journal of Recreational Mathematics, volume 11, (solution in volume 12, 1980), p. 128, 1979.

[16] Arthur T. White, *Graphs, Groups and Surfaces*, North Holland, New York, 1984, North Holland Math Studies 8.