Groups, Graphs, and Symmetry-Breaking

Karen S. Potanka

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Mathematics

Dr. Ezra Brown, Chair
Dr. Joseph Ball
Dr. Monte Boisen

April 16, 1998
Blacksburg, Virginia

Keywords: Petersen Graph, Symmetry-Breaking, Graph Theory

Groups, Graphs, and Symmetry-Breaking

Karen S. Potanka

(ABSTRACT)

A labeling of a graph G is said to be r-distinguishing if no automorphism of G preserves all of the vertex labels. The smallest such number r for which there is an r-distinguishing labeling on G is called the *distinguishing number* of G. The *distinguishing set* of a group Γ, $D(\Gamma)$, is the set of distinguishing numbers of graphs G in which $Aut(G) \cong \Gamma$. It is shown that $D(\Gamma)$ is non-empty for any finite group Γ. In particular, $D(D_n)$ is found where D_n is the dihedral group with $2n$ elements. From there, the generalized Petersen graphs, $GP(n, k)$, are defined and the automorphism groups and distinguishing numbers of such graphs are given.

Contents

List of Figures

Chapter 1

Introduction

The concept of symmetry breaking in graphs made its first appearance as Problem 729 in the Journal of Recreational Mathematics, see Rudin [7]. The problem can be summed up as follows: Suppose that Professor X is blind and has a circular key ring with seemingly identical keys which open different doors. Someone suggests to Professor X that he use a variety of handle shapes to help in distinguishing the keys by touch. Assuming that a rotation of the key ring is undetectable from an examination of a key, what is the minimum number of shapes needed so that all keys would be distinguishable from one another?

The question above can be made more general by allowing any particular shape for the key ring. In doing this, the keys become vertices, and two vertices are joined by an edge if the keys are adjacent on the key ring. We will be concerned with finding the minimum number of labels or shapes needed for the vertices, so that all vertices will be distinguishable. This minimum number will be called the distinguishing number of a graph.

This paper begins with an introduction to the representation of graphs and some elementary terminology, followed by a discussion of the symmetry or automorphisms of a given graph. Upon knowing the automorphism group of a graph, the distinguishing number of a graph can be defined. We then discuss the relationship between groups and graphs; in particular, the Cayley graph of a group and the Frucht construction of a graph realizing a particular group. The paper will then continue with the theory developed in Collins [1] on distinguishing the orbits of a graph and how the size and number of orbits can help in distingushing the entire graph. Furthermore, we will present and prove the theorems given in [1] dealing with graphs which realize a dihedral group. In a number of cases, our proofs and discussion fill in many of the details omitted in [1]. Finally, we discuss the automorphism groups of the generalized Petersen graphs and their distinguishing numbers.

Chapter 2

Representation of Graphs

Definitions. A *graph* G consists of a nonempty vertex set $V(G)$ together with an edge set $E(G)$ (possibly empty), where each edge is an unordered pair of vertices. If both the vertex set and edge set are finite, then the graph G is said to be *finite*. We write uv for the edge $\{u, v\}$. If $e = uv \in E(G)$, then we say that u and v are *adjacent* while u and e are *incident*, as are v and e, and we say that the edge $e = uv$ *joins* u and v. A graph is called *simple* if it has no self-loops or multiple edges. In other words, $e = uu \notin E(G)$ and there cannot be distinct e_1 and e_2 in $E(G)$ with both e_1 and e_2 joining u and v. Unless otherwise specified, in what follows all of our graphs will be simple. The *complement* of a graph G, denoted $\overline{G}$, consists of the vertex set $V(\overline{G}) = V(G)$, along with an edge set $E(\overline{G}) = \{uv | uv \notin E(G)\}$. The *degree* of a vertex v in the graph G is the number of edges incident with v. A vertex with degree k is said to be *k-valent*. If all of the vertices have the same degree k, then G is called *regular* of degree k or simply a *k-regular graph*.

Chapter 3

Automorphism Groups and Group Actions

3.1 Automorphisms

Definition. In what follows, we use both σx and $\sigma(x)$ to denote the image of x under the map σ. If G is a graph, then a *symmetry* or *automorphism* of G is a permutation σ on the vertices of G so that for every edge xy of G, $\sigma(xy) = \sigma(x)\sigma(y)$ is an edge of G. Thus, each automorphism of G is a one-to-one and onto mapping of the vertices of G which preserves adjacency. This implies that an automorphism maps any vertex onto a vertex of the same degree. Let G_1 be the graph in Figure 3.1, let σ be the mapping $(13)(24)$ and let τ be the mapping (123). To see that σ is an automorphism of G_1, notice that the images of all the edges are indeed edges of G_1: $\sigma(12) = 34$, $\sigma(23) = 41$, $\sigma(34) = 12$, $\sigma(41) = 23$, and $\sigma(13) = 13$. Now to see that τ is not an automorphism of G_1 notice that $\tau(14) = 24 \notin E(G_1)$.

Lemma 1 *Let $Aut(G)$ be the collection of all automorphisms of G. Then $Aut(G)$ is a group*

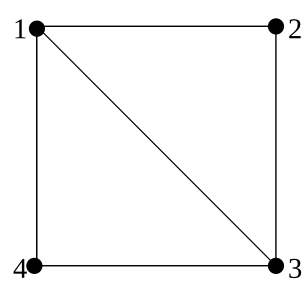

Figure 3.1: G_1

under composition.

Proof:

1. (*Identity*) Clearly, $e \in Aut(G)$.
2. (*Closure*) Suppose $\sigma \in Aut(G)$ and $\tau \in Aut(G)$ and let xy be any edge of G, then $\sigma\tau(xy) = \sigma(\tau(x)\tau(y))$ where $\tau(x)\tau(y)$ is an edge, and $\sigma(\tau(x)\tau(y)) = \sigma\tau(x)\sigma\tau(y)$ which is also an edge of G.
3. (*Associativity*) Associativity follows from the fact that if σ,τ, and γ are all in $Aut(G)$, then they are all permutations of the vertices of G, and we know that composition of permutations is associative.
4. (*Inverses*) Suppose that $\sigma \in Aut(G)$. Then σ is a permutation of the vertices and so is invertible. To show that $\sigma^{-1} \in Aut(G)$, let $xy \in E(G)$ and suppose that $\sigma w = x$ and $\sigma z = y$ (Since σ preserves adjacency, $wz \in E(G)$). Then $\sigma^{-1}(xy) = \sigma^{-1}(x)\sigma^{-1}(y) = wz \in E(G)$. □

Lemma 2 *If G is a graph, then* $Aut(\overline{G}) = Aut(G)$.

Proof: Let $\sigma \in Aut(G)$ and let $xy \in E(\overline{G})$. By definition of the complement of a graph, we have that $xy \notin E(G)$, so $\sigma(x)\sigma(y) \notin E(G)$. (Otherwise, if $\sigma(x)\sigma(y) \in E(G)$, then $\sigma^{-1}(\sigma(x)\sigma(y)) = \sigma^{-1}\sigma(x)\sigma^{-1}\sigma(y) = xy \in E(G)$.) So $Aut(G) \subset Aut(\overline{G})$.

A similar argument shows that $Aut(\overline{G}) \subset Aut(G)$. □

3.2 Group Actions

Definition. We can think of letting the automorphism group of a graph act on the set of vertices and edges of the graph. In doing this, we form *orbits* of both vertices and edges. We say that two vertices v_1 and v_2 of G are in the same orbit if there is an automorphism $\sigma \in Aut(G)$ such that $\sigma v_1 = v_2$. Similarly, we say that two edges e_1 and e_2 of G are in the same orbit if there is an automorphism $\tau \in Aut(G)$ such that $\tau e_1 = e_2$.

Definition. A graph G is said to be *vertex-transitive* if given any two vertices v_1 and v_2 of $V(G)$, there is an automorphism $\sigma \in Aut(G)$ such that $\sigma v_1 = v_2$. In other words, a graph is vertex-transitive if there is only one orbit of vertices under the action of the automorphism group on the set of vertices. Similarly, a graph G is said to be *edge-transitive* if given any two edges e_1 and e_2 of $E(G)$, there is an automorphism $\tau \in Aut(G)$ such that $\tau e_1 = e_2$. So, a graph is edge-transitive if there is only one orbit of edges under the action of the automorphism group on the set of edges.

Lemma 3 *Suppose that the connected graph G is edge-transitive. Then either G is vertex-transitive or there are only two orbits of vertices under the action of the automorphism group on the set of vertices.*

Proof: Suppose that there are three or more orbits of vertices. Then let u_1, u_2, and u_3 be vertices from three different orbits. Now since G is connected, there must be at least one edge incident to each vertex u_1, u_2, and u_3. In particular there are edges u_1v_1, u_2v_2, and $u_3v_3 \in E(G)$. Since G is edge-transitive, there is an automorphism $\sigma \in Aut(G)$ such that $\sigma(u_1v_1) = u_2v_2$. This can be done in only one way: $\sigma u_1 = v_2$ and $\sigma v_1 = u_2$, since $\sigma u_1 \neq u_2$ and $\sigma u_2 \neq u_1$.

Similarly, there exists $\tau \in Aut(G)$ with $\tau(u_2v_2) = u_3v_3$. Since u_2 and u_3 are in different orbits, we must have $\tau u_2 = v_3$ and $\tau v_2 = u_3$. But then we would have $\tau(\sigma(u_1)) = \tau(v_2) = u_3$ and this says that u_1 and u_3 are in the same orbit. □

Definition. Suppose that V(G) is the vertex set of the graph G, and let $Aut(G)$ be the automorphism group of the graph. For each $v \in V(G)$ we define the *stabilizer of v in $Aut(G)$* to be the set of elements in $Aut(G)$ which fix the vertex v or $\{\sigma \in Aut(G) | \sigma v = v\}$. The stabilizer of the vertex v is denoted St_v, and it is straightforward to show that St_v is a subgroup of $Aut(G)$. It is also important to note that the number of elements in St_v is equal to the order of the group divided by the number of elements in the orbit of v (provided that the orbit is finite):

$$|St_v| = \frac{|Aut(G)|}{|O_v|}.$$

We now prove two results involving the stabilizer subgroup of a vertex which will be of use later in the paper:

Lemma 4 *Suppose that u and v are vertices in the same orbit under the action of the automorphism group of G on the set of vertices, and let St_u and St_v be their respective stabilizer subgroups. Then there is some element $g \in Aut(G)$ with*

$$g(St_v)g^{-1} = St_u.$$

Proof: Let $St_v = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be the stabilizer subgroup of the vertex v, and let $St_u = \{\beta_1, \beta_2, \ldots, \beta_n\}$ be the stabilizer subgroup of the vertex u, where u and v are in the same vertex orbit. Then there is some $\varphi \in Aut(G)$ with $\varphi(u) = v$ and $\varphi^{-1}(v) = u$. We want to find some $g \in Aut(G)$ with $g(St_v)g^{-1} = St_u$. Let $\alpha_i \in St_v$, then

$$\varphi^{-1}\alpha_i\varphi(u) = \varphi^{-1}\alpha_i(v) = \varphi^{-1}(v) = u.$$

Thus, $\varphi^{-1}\alpha_i\varphi \in St_u$ for each i, so $\varphi^{-1}St_v\varphi \subset St_u$.

Now let $\beta_j \in St_u$. We want to express β_j as $\varphi^{-1}\alpha_i\varphi$ for any $\alpha_i \in St_v$. It is true that $\varphi\beta_j\varphi^{-1} \in St_v$ for $\varphi\beta_j\varphi^{-1}(v) = \varphi\beta_j(u) = \varphi(u) = v$. So

$$\beta_j = \varphi^{-1}(\varphi\beta_j\varphi^{-1})\varphi$$

where $\varphi\beta_j\varphi^{-1} \in St_v$. Thus $St_u \subset \varphi^{-1}(St_v)\varphi$. □

Corollary 5 *If O is an orbit under the action of the automorphism group of G on the set of vertices, and if $v \in O$ with St_v not normal in $Aut(G)$, then for any vertex $u \in O$, St_u is not normal in G.*

Proof: If St_u is the stabilizer subgroup of vertex $u \neq v \in O$, then by the previous lemma we have that there is some $g \in Aut(G)$ with $g(St_v)g^{-1} = St_u$. If, for instance, St_u is a normal subgroup of $Aut(G)$, then we have $g(St_u)g^{-1} = St_u$ for every $g \in Aut(G)$. Thus $St_u = St_v$. But this contradicts the fact that St_v is not normal. □

Chapter 4

Distinguishing Number of a Graph

Definition. If G is a graph then we can think of assigning to each vertex of the graph a color or label. With each labeling or coloring of a graph, we associate a function

$$\phi : V(G) \to \{1, 2, 3, \ldots, r\}$$

where $\{1, 2, 3, \ldots, r\}$ are the sets of labels. We say that a labeling is *r-distinguishing* if no automorphism of G preserves all of the vertex labels. In other words, for every automorphism $\sigma \in Aut(G)$ there is at least one vertex $v \in V(G)$ with $\phi(v) \neq \phi(\sigma(v))$. Furthermore, if there is a labeling on graph G which is r-distinguishing, we say that G is *r-distinguishable.* The smallest such number r for which G is r-distinguishable is called the *distinguishing number of G*, and is denoted $D(G)$. This idea is due to Albertson and Collins (see [1]).

It should be clear that the automorphism group of any labeled graph is a subgroup of the automorphism group of the unlabeled graph. In some sense, the labels are "breaking the symmetry" of the graph. The goal will be to break all of the symmetries of a particular graph so that the automorphism group of the labeled graph contains only the identity automorphism.

Using this terminology, we can now restate the key problem discussed in the introduction. Finding the minimum number of shapes for the keys so that each key can be distinguished from the others is the same as finding the distinguishing number of C_n, where C_n is the cycle with n vertices. It turns out that for $n = 3, 4, 5$, the distinguishing number for C_n is 3, while for $n \geq 6$, the distinguishing number of C_n is 2. This can be seen in the following labeling ψ where the vertices of C_n are denoted $v_1, v_2, \ldots, v_n$ in order: $\psi(v_1) = 1$, $\psi(v_2) = 2$, $\psi(v_3) = 1$, $\psi(v_4) = 1$, $\psi(v_i) = 2$ for $5 \leq i \leq n$.

It turns out that two graphs with the same automorphism group may have different distinguishing numbers. This idea is illustrated in the next example.

Example. Suppose we consider the distinguishing numbers of the two graphs K_n, the complete graph with n vertices, and the graph W_n with $2n$ vertices obtained by attaching a single pendant vertex to each vertex in K_n.

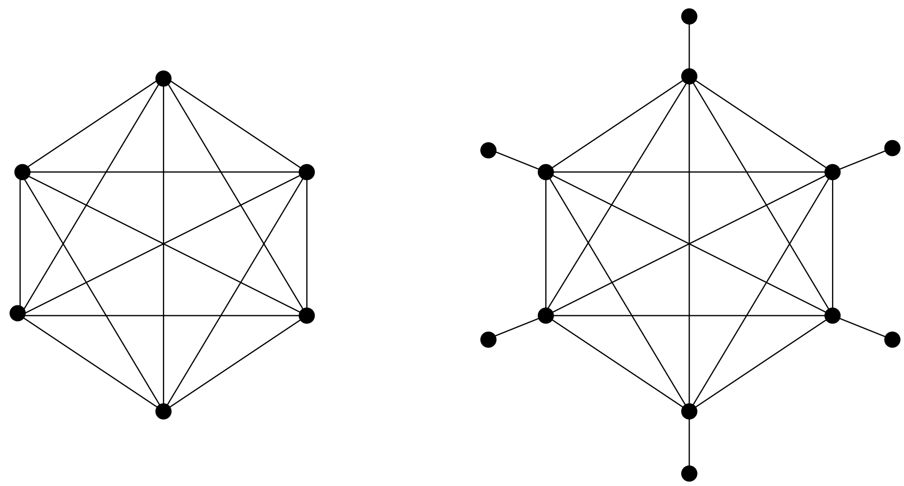

Figure 4.1: K_6 and W_6

See Figure 4.1 for the graphs of K_6 and W_6. It should be clear to the reader that $Aut(K_n) \cong Aut(W_n) \cong S_n$, the permutation group on n elements. It should also be clear that the distinguishing number of K_n is n. Now consider W_n. It turns out that there are n ordered pairs of vertices consisting of a vertex of K_n and its pendant neighbor ((v_i, u_i), $i = 1, 2, \ldots, n$, v_i is a vertex of K_n, and u_i is the pendant vertex adjacent to v_i.) In order for W_n to be distinguished, we must have that each ordered pair be different. If we use k labels for the vertices in W_n, then there are k^2 possible ordered labels for the pairs (k choices for v_i's and k for u_i.) We need for $n \leq k^2$. The distinguishing number will be the smallest such k satisfying the inequality. Thus $D(W_n) = \lceil \sqrt{n}\, \rceil$.

Example. Because a graph G and its complement $\overline{G}$ have the same vertex set, and because each automorphism in $Aut(G)$ has the same action on a given vertex in both G and $\overline{G}$, $D(G) = D(\overline{G})$. To illustrate this idea, Figure 4.2 contains a graph G and its complement both of which have distinguishing number 2.

Definition. Suppose that Γ is a group. We say that the graph G *realizes* Γ if $Aut(G) = \Gamma$. Furthermore, we define the *distinguishing set of a group* by

$$D(\Gamma) = \{D(G) \,|\, G \textit{ realizes } \Gamma\}.$$

In other words, although two graphs with the same automorphism group Γ may have different distinguishing numbers, the possible distinguishing numbers are limited to the set $D(\Gamma)$.

A natural question to ask now is this: given an arbitrary group Γ, is $D(\Gamma) \neq \emptyset$? In other

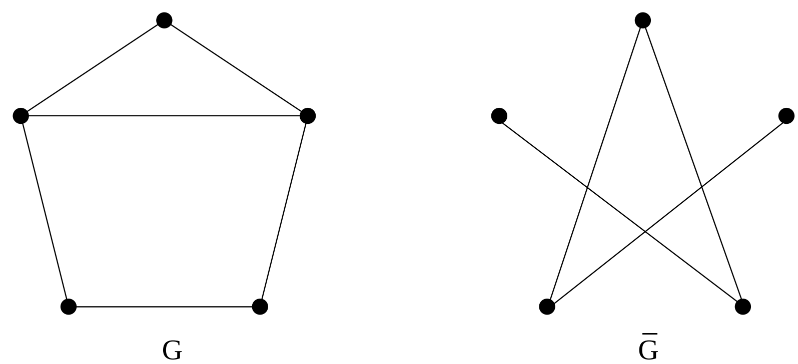

Figure 4.2: G and $\overline{G}$

words, given a group Γ, how do we know that there is even one graph G which realizes Γ? We discuss these questions in the following chapter.

Chapter 5

Groups and Graphs

5.1 Cayley Graphs

During the nineteenth century, a mathematician named Cayley invented the technique of representing a group with a graph, where vertices correspond to the elements of a group and the edges correspond to multiplication by group generators and their inverses.

As a preliminary example, consider the the group C_5. Suppose that we let the elements of $C_5 = \{e, a, a^2, a^3, a^4\}$ be vertices. Now a generator for the group is multiplication on the right by the element a. So two vertices v_i and v_j will be joined by a directed edge from v_i to v_j if $v_i a = v_j$. The resulting graph (Figure 5.1) is called the Cayley color graph for C_5.

Definition. Let Γ be a group and let

$$\Psi = \{\psi_1, \psi_2, \ldots, \psi_n\}$$

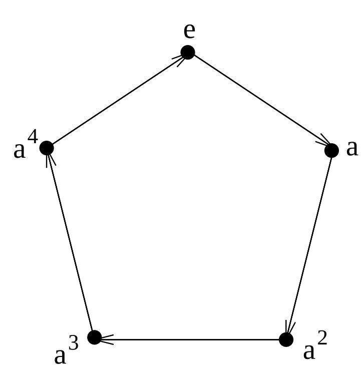

Figure 5.1: The Cayley color graph for C_5

be a generating set for Γ. The *Cayley color graph*, denoted $C(\Gamma, \Psi)$ has as its vertex set the group elements of Γ, and as its edge set the cartesian product $\Gamma \times \Psi$. The edge (σ, ψ_i) has as its endpoints the group elements σ and $\sigma\psi_i$ with direction from σ to $\sigma\psi_i$. To each generator we assign a color or other devices to distinguish one class of edges from another such as dashed lines, bold lines, etc.

As an example of a Cayley color graph for a group with more than one generator, let us consider the group

$$S_3 = \{(1), (123), (132), (12), (13), (23)\}.$$

The set of generators for this group are the elements (123) and (12). If multiplication on the right by (123) is represented by a solid line and (12) by a dashed line, then Figure 5.2 contains the Cayley color graph of this group.

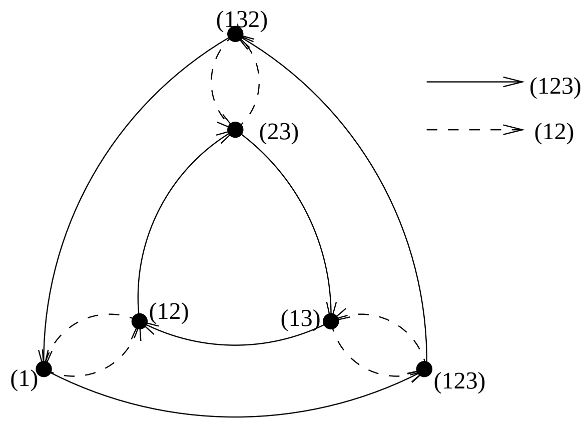

Figure 5.2: Cayley color graph for S_3

The graphs for which we have defined an automorphism to this point have been only simple, nondirected graphs. In order to define an automorphism on a Cayley color graph, we would need to eliminate the directions on the edges and to collapse any multiple edges to one. The resulting graph is defined to be the *Cayley graph*. Note that multiple edges occur when we have a generator of order 2, called an *involution*, as we had in Figure 5.2 with the generator (12). See Figure 5.3 for the Cayley graph of S_3.

5.2 Frucht's Construction

Frucht shows that every finite group is isomorphic to the automorphism group of some graph (See [3], page 70 or White [8]). The graph which Frucht constructs to realize a given group Γ is the Cayley graph of Γ with modifications on each edge of the Cayley graph so that the automorphisms of the modified graph are forced to respect the direction and colors on

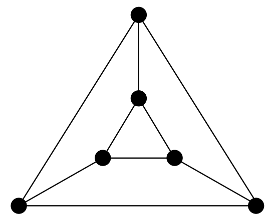

Figure 5.3: Cayley graph for S_3

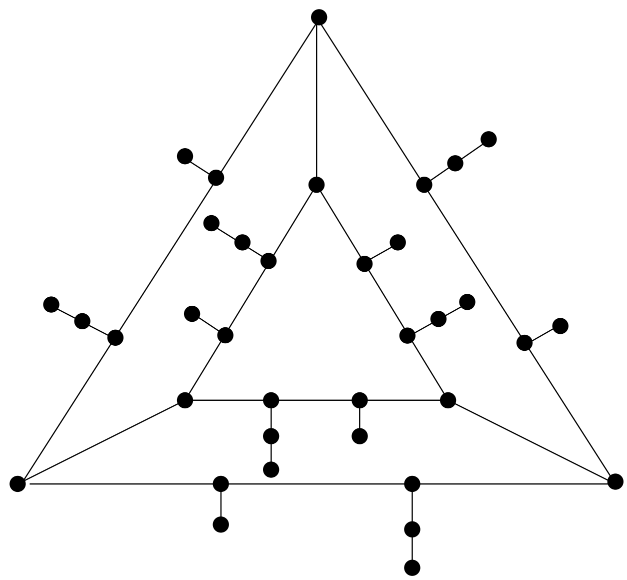

Figure 5.4: The Frucht graph of S_3 whose automorphism group is isomorphic to S_3

the edges of the Cayley color graph. These modifications are done on every edge except those edges resulting from an involution. The first modification to the Cayley graph is the insertion of two new vertices on each edge. For each edge corresponding to the generator ψ_i, attach to the new vertex near the initial end of the directed edge in the Cayley color graph a path of length $2i - 1$ and attach to the other new vertex near the terminal end a path of length $2i$. The resulting graph is called the *Frucht graph of* Γ, denoted $F(\Gamma)$, and it turns out that the automorphism group of this resulting Frucht graph is isomorphic to the group Γ. See Figure 5.4 for the modified graph of S_3 described above.

In the case where none of the generators for a group is an involution, the graphs constructed above have $h(n+1)(2n+1)$ vertices where h is the order of the group and n is the number of generators for the group. Frucht proves even further in [2] that given any finite group Γ of order $h \geq 3$ which is generated by n of its elements, it is always possible to find a 3-regular graph with $2(n+2)h$ vertices that has Γ as its automorphism group. Now we have that each group Γ has at least one graph that realizes it, and in most cases there will be a 3-regular graph which realizes it. Hence we now know that $D(\Gamma)$ will be a nonempty set. In fact, because there is a 3-regular graph that realizes a given group, we will see in the following theorem from [1] that $2 \in D(\Gamma)$ for any finite group Γ.

Theorem 6 *For any finite group* Γ, $2 \in D(\Gamma)$.

Proof: It is known that for any finite group Γ there is a connected 3-regular graph G which realizes Γ (see Frucht [2]). If G is a graph with n vertices, then construct a new graph from G by attaching to each vertex of G a path of length $\lceil log_2 n \rceil$. It should be clear that each automorphism of G is an automorphism of the new graph. Now to see that each automorphism of the new graph is also an automorphism of G, note that each vertex originally in G now has degree 4 and all the other vertices added to G have degree less than or equal to 2. Since automorphisms take vertices to vertices of the same degree. We have that a vertex v originally in G must go to another vertex u originally in G under this automorphism of the new graph. The path attached to this vertex v has only one place to go, namely the path attached to u.

Now there are $2^{\lceil log_2 n \rceil} \geq n$ labelings of these paths using 2 labels. If we color each path differently, then we have distinguished the new graph using 2 colors. $\square$

Chapter 6

Distinguishing the Orbits of a Graph

If O_v is the orbit containing the vertex v in a given graph G, then any automorphism must send v to another vertex in O_v. Thus, vertices in different orbits will be distinguished from one another. One approach to distinguish a graph would be to distinguish each orbit separately. In other words, one could say that an orbit is r-distinguishable if every automorphism that acts nontrivially on the orbit sends at least one vertex to another vertex with a different label. Though it may be easier to distinguish orbits separately than distinguishing the entire graph, the number of labels needed to distinguish the entire graph may be less than the number of labels needed to distinguish the orbits separately. For instance, consider the following example:

Example. The automorphism group of the graph in Figure 6.1 is isomorphic to the cyclic group of order 3. It turns out that there are three orbits of vertices in this graph: $0_1 = \{1, 2, 3\}$, $0_4 = \{4, 6, 8\}$, and $0_5 = \{5, 7, 9\}$. The distiguishing number for any of the orbits is three while the distiguishing number of the entire graph is just two. Figure 6.2 includes the labeling used to distinguish the orbits separately (note that this labeling distinguishes the entire graph as well) and also includes the labeling used to distinguish the entire graph with only two colors.

As illustrated in the previous example, it is not necessary for a labeling to distinguish every orbit separately in order to distinguish the entire graph. It is worth pointing out that it might be beneficial to know the distinguishing number of a given orbit. We see in the next section that if a graph satisfies certain properties, then the distinguishing number of the graph is the distinguishing number of an orbit.

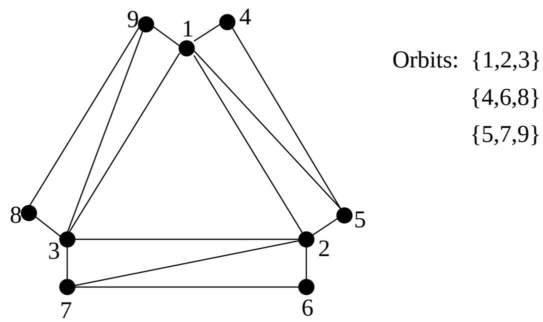

Figure 6.1: This graph has distinguishing number two while the minimum number of labels needed to distinguish each orbit separately is three

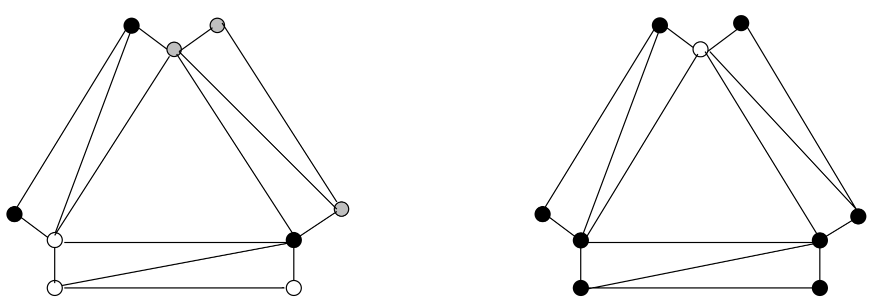

Figure 6.2: The graph on the left is labeled to distinguish each orbit separately while the graph on the right is labeled to distinguish the entire graph

6.1 Distinguishing the Orbits

The following theorem as seen in [1] states a very nice case in which an orbit of a graph can be distinguished with two labels.

Theorem 7 *For a given graph G, if the stabilizer subgroup of a vertex v is normal in $Aut(G)$, then the orbit of v can be distinguished with two colors.*

Proof: Label the vertex v red and the rest of the vertices in O_v blue. We will show that every nontrivial automorphism $\sigma \in Aut(G)$ distinguishes O_v. Suppose there is a nontrivial automorphism h which does not distinguish O_v. In other words, h must preserve colors and so must send one blue vertex $x \in V(G)$ to another blue vertex $y \in V(G)$. In symbols, we have $h(x) = y$. It also must be true that $h(v) = v$ since h preserves colors, and so $h \in St_v$. Now because $x, y \in O_v$, there must be elements $g_1, g_2 \in Aut(G)$ with $g_1(v) = x$ and $g_2(v) = y$. So we have

$$h(g_1(v)) = h(x) = y.$$

Because St_v is normal in $Aut(G)$, there must be some element $h' \in St_v$ with $g_1^{-1}hg_1 = h'$ which implies that $hg_1 = g_1h'$. This would give

$$x = g_1(v) = g_1(h'(v)) = h(g_1(v)) = y.$$

This contradicts the fact that h is nontrivial. □

We define a *hamiltonian* group to be one in which each subgroup is normal. Thus, an immediate consequence of this theorem is that if the automorphism group of a graph is abelian or hamiltonian, then the stabilizer subgroup of each vertex in each orbit is normal and so each orbit can be distinguished with two colors. Hence the entire graph can be distinguished with two colors.

Another interesting result given in [1] says that if we know the distinguishing number of a particular orbit is k, and we know that the intersection of the stabilizer subgroups of all of the vertices in that orbit is simply the identity, then the entire graph can be distinguished with k colors.

Theorem 8 *Let G be a graph with $Aut(G) = \Gamma$. If G has an orbit $O = \{v_1, v_2, \ldots, v_s\}$ that can be distinguished with k colors and $\cap_{i=1}^{s} St_{v_i} = \{e\}$, then G can be distinguished with k colors.*

Proof: If we label G so that O is k-distinguishing, then any nontrivial automorphism will act nontrivially on the orbit O, since the only element in $Aut(G)$ which stabilizes everything in O is the identity automorphism. □

6.2 Size of the Orbit

In [1], we find that having an orbit of vertices large enough can force a graph to be 2-distinguishable. Recall the Orbit-Stabilizer Theorem which states that the size of an orbit of a vertex v is equal to the order of the automorphism group divided by the size of the stabilizer subgroup of v. Thus, if a graph G has an orbit O the size of the automorphism group $Aut(G)$, then every vertex in O has a stabilizer subgroup of size 1. In other words, the element $\{e\}$ is the only automorphism to stabilize all of the vertices in O and so by the above theorem, the distinguishing number of the graph will be the distinguishing number of O. Now if we color one vertex of O red and the rest blue, then it follows that every nontrivial automorphism sends the red vertex to a blue vertex. Hence, G can be distinguished with two colors and we have the following corollary:

Corollary 9 *A graph which has an orbit the size of the automorphism group of the graph can be distinguished with two colors.*

6.3 Number of Orbits

The following result from [1] says that having a large number of orbits can also force a graph to be distinguished with two colors, provided that a few conditions are met.

Theorem 10 *Suppose G is a graph with t orbits and the vertices v_1, v_2, …, v_t are from the t different orbits with respective stabilizer subgroups St_{v_1}, St_{v_2}, …, St_{v_t}. If $\cap_{i=1}^{t} St_{v_i} = \{e\}$, then $D(G) = 2$.*

Proof: Define the labeling φ as follows:

$$\phi(v) = \begin{cases} \text{red, if } v \in \{v_1, v_2, \ldots, v_t\} \\ \text{blue, otherwise.} \end{cases}$$

We want to show that for any nontrivial automorphism $\sigma \in Aut(G)$, there is at least one vertex $x \in V(G)$ such that $\phi(\sigma(x)) \neq \phi(x)$. Let σ be a nontrivial automorphism of G. Since the intersection of the stabilizer subgroups of v_1, v_2, …, v_t is the identity, σ must map at least one v_i, $1 \leq i \leq t$, to another vertex in O_{v_i}, which by the definition of ϕ is blue. Thus, we have distinguished G with two colors. $\square$

Chapter 7

Dihedral Groups

The dihedral groups arise as an important family of groups whose elements are the symmetries of geometric objects. The simplest of such objects are the regular n-gons which can be easily represented with a graph. We define D_n $(n \geq 3)$ to be the set of n rotations about the center of the n-gon along with the set of n reflections through the n lines of symmetry. More precisely,

$$D_n =< \sigma, \tau | \sigma^n = \tau^2 = e, \tau\sigma = \sigma^{-1}\tau >= \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}\}.$$

It is easy to see that the order of D_n is $2n$. Furthermore, the set of involutions, or elements of order 2, include only $\mathcal{I} = \{\tau\sigma^i \, for \, 0 \leq i \leq n-1\}$ if n is odd, and $\mathcal{I}$ along with $\sigma^{\frac{n}{2}}$ if n is even.

7.1 Subgroups of D_n

7.1.1 Types of Subgroups of D_n

It turns out that there are only three types of nontrivial subgroups of D_n:

1. A subgroup of $< \sigma >$, the cyclic half of D_n ,
2. A subgroup isomorphic to D_m, where $m|n$, and
3. $\{e, \tau\sigma^i\}$ where $0 \leq i < n$.

It is obvious that sets of types 1 and 3 are subgroups of D_n. Below we will show that a set of type 2 is a subgroup of D_n . Since D_n is a finite group, to show that a set A of type 2 is a subgroup, it is only necessary to show that for any two elements $\beta, \rho \in A$, $\beta\rho^{-1} \in A$. Now if $A \cong D_m$ where $m|n$, then

$$A = \{e, \sigma^k, \sigma^{2k}, \ldots, \sigma^{(m-1)k}, \tau\sigma^i, \tau\sigma^{k+1}, \tau\sigma^{2k+i}, \ldots, \tau\sigma^{(m-1)k+i}\}$$

where $mk = n$. We need to check several cases:

1. If $\beta = \sigma^{kj}$ and $\rho = \sigma^{kl}$, then
$$\beta\rho^{-1} = \sigma^{kj}(\sigma^{kl})^{-1} = \sigma^{kj}\sigma^{-kl} = \sigma^{k(j-l)} \in A.$$
2. If $\beta = \sigma^{kj}$ and $\rho = \tau\sigma^{kl+i}$, then
$$\beta\rho^{-1} = \sigma^{kj}(\tau\sigma^{kl+i})^{-1} = \sigma^{kj}\sigma^{-kl-i}\tau = \sigma^{k(j-l)-i}\tau = \tau\sigma^{k(l-j)+i} \in A.$$
3. If $\beta = \tau\sigma^{kl+i}$, $\rho = \sigma^{kj}$, then
$$\beta\rho^{-1} = \tau\sigma^{kl+i}(\sigma^{kj})^{-1} = \tau\sigma^{kl+i}\sigma^{-kj} = \tau\sigma^{k(l-j)+i} \in A.$$
4. If $\beta = \tau\sigma^{kl+i}$, $\rho = \tau\sigma^{kj+i}$, then
$$\beta\rho^{-1} = \tau\sigma^{kl+i}(\tau\sigma^{kj+i})^{-1} = \tau\sigma^{kl+i}\sigma^{-kj-i}\tau = \tau\sigma^{k(l-j)}\tau = \sigma^{k(j-l)} \in A.$$

To see why these are the only types of nontrivial subgroups, suppose that H is a nontrivial subgroup of D_n. We break the argument down into three cases depending on the number of elements of the type $\tau\sigma^i$. First suppose that H contains no elements of the type $\tau\sigma^i$. Then H must be a subgroup of $\{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}\} =< \sigma >$. Thus $H =< \sigma^d >$ for some d which divides n.

Now suppose that H contains only one element of the type $\tau\sigma^i$. Then H must not contain σ^j for any $0 < j < n$. Otherwise, $\tau\sigma^i\sigma^j \in H$ and so $\tau\sigma^{i+j} \in H$. But this contradicts that $\tau\sigma^i$ is the only element of its type in H. Therefore $\tau\sigma^i$ and e are the only elements in H.

Finally suppose that H contains two or more elements of the type $\tau\sigma^i$. Then there must be $\tau\sigma^i \in H$ and $\tau\sigma^j \in H$ with $i \neq j$ and $0 \leq i, j < n$. Because H is a subgroup we must have that $\tau\sigma^i\tau\sigma^j = \tau^2\sigma^{j-i} = \sigma^{j-i} \in H$. (Note that $\sigma^{j-i} \neq e$ since $i \neq j$.) Thus H must contain at least one element σ^p for some $0 \leq p < n$. Let d be the smallest positive integer with $\sigma^d \in H$. If $d = 1$, then $< \sigma >\subset H$ which implies that $H = D_n$. So assume that $d > 1$; then d must divide n. Certainly $< \sigma^d >$ is a subgroup of H; if $\sigma^a \in H$ and $a = qd + r$ with $0 \leq r < d$, then $\sigma^r = \sigma^{a-qd} = \sigma^a(\sigma^d)^{-q} \in H$ since both $\sigma^a \in H$ and $\sigma^d \in H$. By the minimality of d it follows that $r = 0$ or $a = qd$ so $\sigma^a = (\sigma^d)^q \in< \sigma^d >$. Thus the only elements from the cyclic half contained in H are in the set $< \sigma^d >$. So we must have that if $\tau\sigma^i \in H$ and $\tau\sigma^j \in H$, then d must divide $i-j$ or $i = dk+j$ for some integer k with $0 \leq k < \frac{n}{d}$. Thus $\tau\sigma^i = \tau\sigma^{dk+j}$. So H must contain $\frac{n}{d}$ elements of the form σ^{dk} for $0 \leq k < \frac{n}{d}$ and $\frac{n}{d}$ elements of the form $\tau\sigma^{dk}$ for $0 \leq k < \frac{n}{d}$. So

$$H = \{e, \sigma^d, \sigma^{2d}, \ldots, \sigma^{(\frac{n}{d}-1)d}, \tau\sigma^i, \tau\sigma^{i+d}, \tau\sigma^{i+2d}, \ldots, \tau\sigma^{i+(\frac{n}{d}-1)d}\} \cong D_{\frac{n}{d}}.$$

7.1.2 Properties of Subgroups of D_n

Now for each type of subgroup of D_n, it will be useful to know the representation of the subgroup using generators, the subgroups conjugate to it, and the orbit of a vertex which has that subgroup as its stabilizer subgroup. This information is contained in the following table and is discussed below:

Type of Subgroup	Conjugate Subgroups	Intersection of Conjugate Subgroups	Orbit of vertex v with stabilizer subgroup of this type
$<\sigma^k>$ where $k\|n$	$<\sigma^k>$	$<\sigma^k>$	$\{v, \sigma(v), \sigma^2(v), \ldots, \sigma^{k-1}(v), \tau(v), \tau\sigma(v), \tau\sigma^2(v), \ldots, \tau\sigma^{k-1}(v)\}$
$<\sigma^k, \tau\sigma^i>$	$<\sigma^k, \tau\sigma>, <\sigma^k, \tau\sigma^2>, \ldots, <\sigma^k, \tau\sigma^{k-1}>$	$<\sigma^k>$	$\{v, \sigma(v), \sigma^2(v), \ldots, \sigma^{k-1}(v)\}$
$<\tau>$	$<\tau\sigma>, <\tau\sigma^2>, \ldots, <\tau\sigma^{n-1}>$	$\{e\}$	$\{v, \sigma(v), \sigma^2(v), \ldots, \sigma^{n-1}(v)\}$

Type 1. Because $<\sigma^k>$ is a normal subgroup of D_n, we know that for any $g \in D^n$, $g <\sigma^k> g^{-1} = <\sigma^k>$. So $<\sigma^k>$ is its only conjugate and therefore the intersection of the conjugate subgroups is $<\sigma^k>$. Now if a vertex v has $<\sigma^k>$ as its stabilizer subgroup, then clearly the orbit of v will be the set

$$O_v = \{v, \sigma(v), \sigma^2(v), \ldots, \sigma^{k-1}(v), \tau(v), \tau\sigma(v), \ldots, \tau\sigma^{k-1}(v)\}.$$

This is because $\sigma^p(v) = \sigma^{kl+j}(v) = \sigma^j\sigma^{kl}(v) = \sigma^j(v) \in O_v$ where $p = kl + j$ and $0 \le j < k$, and $\tau\sigma^p(v) = \tau\sigma^{kl+j}(v) = \tau\sigma^j\sigma^{kl}(v) = \tau\sigma^j(v) \in O_v$ where $p = kl + j$ and $0 \le j < k$.

Type 2. Now consider a subgroup of the second type, $<\sigma^k, \tau\sigma^i>$ where $km = n$. To find the conjugate subgroups, choose an element $g = \sigma^p$ or $g = \tau\sigma^p$ and compute $g <\sigma^k, \tau\sigma^i> g^{-1}$. In the first case we have:

$$\sigma^p <\sigma^k, \tau\sigma^i> \sigma^{-p} = \sigma^p\{\sigma^k, \sigma^{2k}, \ldots, \sigma^{(m-1)k}, \tau\sigma^i, \tau\sigma^{k+i}, \tau\sigma^{2k+i}, \ldots, \tau\sigma^{(m-1)k+i}\}\sigma^{-p}$$

where $p = kl + j$ and $0 \le j < k$. But $\sigma^p\sigma^{ks}\sigma^{-p} = \sigma^{ks}$ and $\sigma^p\tau\sigma^{ks+i}\sigma^{-p} = \tau\sigma^{ks-2p+i}$ where $0 \le s < m$. Thus in this case we have $\sigma^p <\sigma^k, \tau\sigma^i> \sigma^{-p} = <\sigma^k, \tau\sigma^{i-2p}>$.

In the second case we have:

$$\tau\sigma^p <\sigma^k, \tau\sigma^i> \sigma^{-p}\tau = \tau\sigma^p\{\sigma^k, \sigma^{2k}, \ldots, \sigma^{(m-1)k}, \tau\sigma^i, \tau\sigma^{k+i}, \tau\sigma^{2k+i}, \ldots, \tau\sigma^{(m-1)k+i}\}\sigma^{-p}\tau$$

where $p = kl + j$ and $0 \le j < k$. But $\tau\sigma^p\sigma^{ks}\sigma^{-p}\tau = \tau\sigma^{ks}\tau = \sigma^{-ks}$ and $\tau\sigma^p\tau\sigma^{ks+i}\sigma^{-p}\tau = \sigma^{ks-2p+i}\tau = \tau\sigma^{2p-ks+i}$ where $0 \le s < m$. Thus we have $\tau\sigma^p <\sigma^k, \tau\sigma^i> \sigma^{-p}\tau = <\sigma^k, \tau\sigma^{i+2p}>$.

Clearly the intersection of these conjugate subgroups is $< \sigma^k >$. Now suppose that a vertex v has $< \sigma^k, \tau\sigma^i >$ as its stabilizer subgroup. Then the orbit of v will be the set $O_v = \{v, \sigma(v), \sigma^2(v), \ldots, \sigma^{k-1}(v)\}$. This is because $\sigma^p(v) = \sigma^{kl+j}(v) = \sigma^j\sigma^{kl}(v) = \sigma^j(v) \in O_v$ where $p = kl + j$ and $0 \leq j < k$, and $\tau\sigma^p(v) = \tau\sigma^{kl+j}(v) = \tau\sigma^{kl+(j-i)+i}(v) = \sigma^{i-j}\tau\sigma^{kl+i}(v) = \sigma^{i-j}(v) \in O_v$ where $p = kl + j$ and $0 \leq j < k$.

Type 3. Finally, consider a subgroup of the last type, $< \tau >$. To find the subgroups conjugate to $< \tau >$, choose an element $g = \sigma^p$ or $g = \tau\sigma^p$ and compute $g < \sigma^k, \tau\sigma^i > g^{-1}$. In the first case we have:

$$\sigma^p < \tau > \sigma^{-p} = \sigma\{e, \tau\}\sigma^{-p} = \{e, \tau\sigma^{-2p}\}$$

where $p = kl + j$ and $0 \leq j < k$.

In the second case we have:

$$\tau\sigma^p < \tau > \sigma^{-p}\tau = \tau\sigma^p\{e, \tau > \sigma^{-p}\tau = \{e, \tau\sigma^p\tau\sigma^{-p}\tau\} = \{e, \sigma^{-2p}\tau\} = \{e, \tau\sigma^{2p}\}.$$

Clearly the intersection of the conjugate subgroups is just the identity. Now suppose that a vertex v has $< \tau >$ as its stabilizer subgroup. Then the orbit of v will be the set $\{v, \sigma(v), \sigma^2(v), \ldots, \sigma^{n-1}(v)\}$. This is because $\tau\sigma^p(v) = \sigma^{-p}\tau(v) = \sigma^{-p}(v)$.

7.2 Distinguishing number of graphs which realize D_n

We are now ready to find the distinguishing number of graphs which realize D_n . We can do this by looking at the orbits of vertices and the stabilizer subgroups of the vertices. For instance, we will see from the results in [1] that if there is vertex in the graph with a stabilizing subgroup of Type 1, then the graph is automatically 2-distinguishable. If the graph has no vertex with stabilizing subgroup of Type 1, but does have an orbit with more than 6 elements, then we will see that the graph is 2-distinguishable. The case in which the graph satisfies neither of the above conditions will be handled by the last theorem in this section. In any case, a graph which realizes D_n will have a distinguishing number of either 2 or 3.

Two lemmas are extremely useful in obtaining the results described above. One is Lemma 4 in Chapter 3, and the other is the following result given in [1]:

Lemma 11 *Let G be a graph which realizes D_n , and suppose that G has t orbits of vertices. If St_{v_1}, St_{v_2}, …, St_{v_t} are the respective stabilizer subgroups of vertices v_1, v_2, …, v_t from the t different orbits, then $St_{v_1} \cap St_{v_2} \cap \ldots \cap St_{v_t} \cap < \sigma >= \{e\}$.*

Proof: Consider the conjugates of $\sigma^k \in D_n$. First, $\sigma^l \sigma^k \sigma^{-l} = \sigma^k$ for $0 \leq l < n$. Second, $\tau\sigma^i\sigma^k(\tau\sigma^i)^{-1} = \tau\sigma^i\sigma^k\sigma^{-i}\tau = \tau\sigma^k\tau = \sigma^{-k}$. So the conjugacy class of σ^k is $\{\sigma^k, \sigma^{-k}\}$.

Now if σ^k is an element of any subgroup H, then so is σ^{-k}. Let gHg^{-1} be any subgroup conjugate to H. If $g = \sigma^l$ for some $0 \leq l < n$, then $g\sigma^k g^{-1} = \sigma^k \in gHg^{-1}$. On the other hand, if $g = \tau\sigma^l$ for some $0 \leq l < n$, then $g\sigma^k g^{-1} = \tau\sigma^l\sigma^{-k}\sigma^{-l}\tau = \tau\sigma^{-k}\tau = \sigma^k \in gHg^{-1}$. So if $\sigma^k \in H$ then σ^k is an element of any subgroup conjugate to H.

If $\sigma^k \in St_{v_1} \cap St_{v_2} \cap \ldots \cap St_{v_t}$, then σ^k is in the conjugate of all of these subgroups. That would mean that σ^k is in the stabilizer subgroup for every vertex of G by Lemma 4. So σ^k would have to fix every element of G, and since G realizes D_n, $\sigma^k = e$ and $k = n$. Thus $< \sigma > \cap St_{v_1} \cap St_{v_2} \cap \ldots \cap St_{v_t} = \{e\}$ and so nothing in the cyclic half of D_n can stabilize every vertex of G. □

7.2.1 Graphs with a stabilizer subgroup of Type 1

Theorem 12 *Let G realize D_n. If G has a vertex whose stabilizer subgroup is of type 1, then G can be distinguished with 2 colors.*

Proof: Suppose that the vertex v has stabilizer subgroup St_v of type 1. Then $St_v =< \sigma^j >$ for some $0 \leq j \leq n$ where $j|n$. Now let $v_1, v_2, \ldots, v_t$ be vertices from all the other different orbits of G where $St_{v_1}, St_{v_2}, \ldots, St_{v_t}$ are their respective stabilizer subgroups. By lemma 11, we have that $< \sigma > \cap St_v \cap St_{v_1} \cap \ldots \cap St_{v_t} = \{e\}$. But $< \sigma > \cap < \sigma^j > = < \sigma^j >$, thus we have $< \sigma^j > \cap St_{v_1} \cap \ldots \cap St_{v_t} = St_v \cap St_{v_1} \cap \ldots \cap St_{v_t} = \{e\}$. So by Theorem 10, $D(G) = 2$. □

7.2.2 Graphs with a stabilizer subgroup of Type 2 or 3

Lemma 13 *Let G realize D_n. If G has a vertex v whose stabilizer subgroup St_v is of type 2 or 3, and if the orbit of v, O_v, has more than six elements, the O_v can be distinguished with 2 colors.*

Proof: From the table above we see that $O_v = \{v, \sigma(v), \sigma^2(v), \ldots, \sigma^{j-1}(v)\}$ where $0 < j \leq n$ and in the case that $St_v =< \tau\sigma^i >$, we have $j = n$. We may assume that $j \geq 6$ since $|O_v| \geq 6$. Let $A = \{v, \sigma^2(v), \sigma^3(v)\}$; color the vertices in A red and the rest of the vertices in O_v blue. Our goal is to show that this is a 2-distinguishing coloring of O_v. In other words, we need to show that every automorphism which acts nontrivially on O_v must send at least one vertex in A to vertex not in A.

Suppose that the automorphism $g \in D_n$ fixes A setwise. Then g must send v to v, $\sigma^2(v)$, or $\sigma^3(v)$. Now if g were to fix v, then $g \in St_v$. Similarly, if $g(v) = \sigma^2(v)$ then $g \in \sigma^2 St_v$ and if

$g(v) = \sigma^3(v)$ then $g \in \sigma^3 St_v$. Hence in order to show that g distinguishes O_v, we must show that g either acts trivially on A or does not fix A for all the cases of g listed above. So we need to look at the image of A under all of those automorphisms.

To rule out the case that g acts trivially on O_v, note that if an automorphism acts trivially on O_v, then it is contained in the intersection of the stabilizer subgroups of each element in O_v. But by Lemma 4, we know that stabilizer subgroups of vertices in the same orbit are conjugate to one another. So the automorphisms which act trivially on A are in the intersection of such stabilizer subgroups. If $St_v =< \sigma^k, \tau\sigma^i >$, then the intersection is just $< \sigma^k >$, and if $St_v =< \tau\sigma^i >$, the intersection is simply $\{e\}$.

First suppose $St_v =< \sigma^k, \tau\sigma^i >= \{e, \sigma^k, \sigma^{2k}, \ldots, \sigma^{(\frac{n}{k}-1)k}, \tau\sigma^i, \tau\sigma^{k+i}, \ldots, \tau\sigma^{(\frac{n}{k}-1)k+i}\}$. Then if $0 \leq d < \frac{n}{k}$ we have:

1. $\sigma^{dk}A = \{\sigma^{dk}(v), \sigma^{dk}\sigma^2(v), \sigma^{dk}\sigma^3(v)\} = \{v, \sigma^2(v), \sigma^3(v)\} = A$,
2. $\tau\sigma^{dk+i}A = \{\tau\sigma^{dk+i}(v), \tau\sigma^{dk+i}\sigma^2(v), \tau\sigma^{dk+i}\sigma^3(v)\} = \{v, \sigma^{n-2}(v), \sigma^{n-3}(v)\}$,
3. $\sigma^2\sigma^{dk}A = \{\sigma^2\sigma^{dk}(v), \sigma^2\sigma^{dk}\sigma^2(v), \sigma^2\sigma^{dk}\sigma^3(v)\} = \{\sigma^2(v), \sigma^4(v), \sigma^5(v)\}$,
4. $\sigma^2\tau\sigma^{dk+i}A = \{\sigma^2\tau\sigma^{dk+i}(v), \sigma^2\tau\sigma^{dk+i}\sigma^2(v), \sigma^2\tau\sigma^{dk+i}\sigma^3(v)\} = \{\sigma^2(v), v, \sigma^{n-1}(v)\}$,
5. $\sigma^3\sigma^{dk}A = \{\sigma^3\sigma^{dk}(v), \sigma^3\sigma^{dk}\sigma^2(v), \sigma^3\sigma^{dk}\sigma^3(v)\} = \{\sigma^3(v), \sigma^5(v), \sigma^6(v)\}$,
6. $\sigma^3\tau\sigma^{dk+i}A = \{\sigma^3\tau\sigma^{dk+i}(v), \sigma^3\tau\sigma^{dk+i}\sigma^2(v), \sigma^3\tau\sigma^{dk+i}\sigma^3(v)\} = \{\sigma^3(v), \sigma(v), v\}$.

So since $n \geq 6$, we see that only σ^{dk} preserves A, but $\sigma^{dk} \in < \sigma^k >$ which acts trivially on O_v.

Now suppose that $St_v =< \tau\sigma^i >= \{e, \tau\sigma^i\}$. Then the action of $\tau\sigma^i$, $\sigma^2\tau\sigma^i$, and $\sigma^3\tau\sigma^i$ on A is as follows:

1. $\tau\sigma^i A = \{\tau\sigma^i(v), \tau\sigma^i\sigma^2(v), \tau\sigma^i\sigma^3(v)\} = \{v, \sigma^{n-2}(v), \sigma^{n-3}(v)\}$,
2. $\sigma^2\tau\sigma^i A = \{\sigma^2\tau\sigma^i(v), \sigma^2\tau\sigma^i\sigma^2(v), \sigma^2\tau\sigma^i\sigma^3(v)\} = \{\sigma^2(v), v, \sigma^{n-1}(v)\}$,
3. $\sigma^3\tau\sigma^i A = \{\sigma^3\tau\sigma^i(v), \sigma^3\tau\sigma^i\sigma^2(v), \sigma^3\tau\sigma^i\sigma^3(v)\} = \{\sigma^3(v), \sigma(v), v\}$.

Again we see that because $n \geq 6$, none of these preserves A. $\square$

Example. One motivation of this lemma is the original key problem with n keys on a circular ring. It was stated in Chapter 4 that for $n \geq 6$, all keys could be distinguished using 2 colors. This is because there is only one orbit of vertices, $O = \{v_1, v_2, \ldots, v_n\}$, of size ≥ 6 and the stabilizer subgroup of any vertex, v_i, will be of type 3, $\tau\sigma^j$. Thus labeling the set $A = \{v_i, v_{i+2}, v_{i+3}\}$ red and the rest of the vertices on the cycle blue distinguishes $O_{v_i} = V(G)$.

Theorem 14 *Let G realize D_n. If G has a vertex v whose stabilizer subgroup St_v is of type 2 or 3, and if the orbit of v, O_v, has more than six elements, the G can be distinguished with 2 colors.*

Proof: In the case that $St_v =< \tau\sigma^i >$, the intersection of the subgroups conjugate to St_v is just the identity. In other words, the identity is the only element in D_n which fixes every vertex in O_v. Furthermore, by the previous lemma, O_v can be distinguished with 2 colors. Thus by Theorem 8, we have that G can be distinguished with 2 colors.

If $St_v =< \sigma^k, \tau\sigma^i >$, then again by the previous lemma, O_v can be distinguished with 2 colors. With this coloring, every automorphism which acts nontrivially on O_v must send a red vertex to a blue vertex, distinguishing the graph.

What about the automorphisms which act trivially on O_v? We know that these are the automorphisms in the intersection of the stabilizer subgroups of the vertices in O_v. From the table above, we see that this intersection is just $< \sigma^k >$. If we let $< \sigma^k >$ act on the vertices of G, then $< \sigma^k >$ makes vertex orbits $V_1, V_2, \ldots, V_s$ which are contained in the vertex orbits of G under the action of D_n. Since $< \sigma^k >$ stabilizes each vertex in O_v, O_v is broken into 1-orbits under the action of $< \sigma^k >$. Consider the orbits V_i with $|V_i| > 1$. In each orbit of this type, choose a vertex $v_j \in V_i$ and color it red and color the rest of the vertices in V_i blue.

Suppose that with this coloring, $< \sigma^k >$ fixes each v_j which we colored red. We have $< \sigma^k >= \{e, \sigma^k, \sigma^{2k}, \ldots, \sigma^{(\frac{n}{k}-1)k}\}$ and so if $0 \leq d < \frac{n}{k}$, then $\sigma^{dk}(v_j) = v_j$. Now if u_t is any other vertex in V_i , then there must be some number $0 \leq r < \frac{n}{k}$ with $\sigma^{rk}(v_j) = u_t$. So

$$\sigma^{dk}(u_t) = \sigma^{dk}(\sigma^{rk}(v_j)) = \sigma^{rk}(\sigma^{dk}(v_j)) = \sigma^{rk}(v_j) = u_t.$$

Thus σ^{dk} fixes every element in V_i for $1 \leq i \leq s$ and so σ^{dk} fixes all of G. This contradicts that G realizes D_n. Thus $< \sigma^k >$ must send at least one vertex to a blue vertex. So $D(G) = 2$. □

Example. To illustrate this theorem, let $G = GP(7, 2)$ be the graph in Figure 7.1. It turns out that this graph realizes D_7 (see Chapter 8.) For any vertex in $GP(7, 2)$, the stabilizer subgroup includes the identity automorphism and an involution (reflection through line through the vertex) and so is of type $< \tau\sigma^i >$. Furthermore, under the action of the automorphism group, the vertices are partitioned into two orbits, $U = \{u_1, u_2, \ldots, u_7\}$ and $V = \{v_1, v_2, \ldots, v_7\}$. Thus $GP(7, 2)$ satifies the conditions of Theorem 11. The coloring described in the proof of the theorem is shown in the figure.

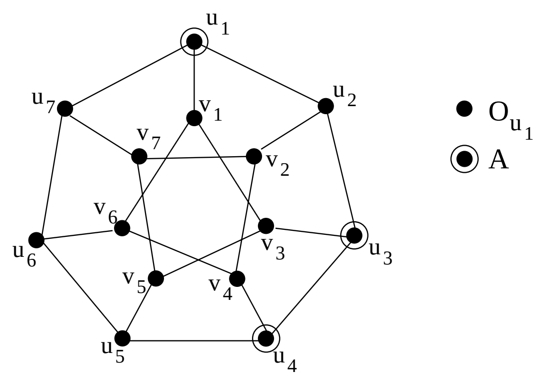

Figure 7.1: This graph illustrates the coloring in Lemma 10

Lemma 15 *If G realizes D_n, and p^α is the largest power of p that divides n, then there is a vertex orbit O of size p^α in G.*

Proof: Let p be a prime divisor of n, and suppose that p^α is the largest power of p that divides n. Certainly there is a subgroup $\Lambda =< \sigma^{\frac{n}{p^\alpha}} >$ which is cyclic. Note that there are only p^α elements in Λ, so if $v \in V(G)$ then by the Orbit-Stabilizer Theorem, $|O_v||St_v| = |\Lambda| = p^\alpha$. Thus, the size of the orbit of any vertex must divide p^α and so must be one of $1, p, p^2, \ldots, p^\alpha$.

Let $v \in V(G)$, and let d be the smallest positive integer such that $\sigma^{d(\frac{n}{p^\alpha})}(v) = v$. Then d is the size of the Λ-orbit that contains v. By the argument in the previous paragraph, d divides p^α. It must be the case that there is an orbit O under the action of Λ of size p^α. If not, then for each $v \in V(G)$ we have $\sigma^{d(\frac{n}{p^\alpha})}(v) = v$ and $d = p^\beta$ for some $\beta < \alpha$. So $d\frac{n}{p^\alpha} = p^\beta \frac{n}{p^\alpha} = \frac{n}{p^{(\alpha-\beta)}}$ and $(\alpha - \beta) \geq 1$. Thus, $\sigma^{(\frac{n}{p^{(\alpha-\beta)}})}(v) = v$ and so $\sigma^{\frac{n}{p}}(v) = v$ for each $v \in V(G)$. In other words, we have found some $\sigma^{\frac{n}{p}}$ which fixes each vertex of G, contradicting the fact that G realizes D_n. So we conclude that there must be a Λ-orbit of size p^α. Because the orbits under the action of D_n are at least as large as the Λ-orbit, we are guaranteed to have an orbit of size p^α under the action of D_n. □

This lemma is extremely useful in the proof of the following theorem, for it limits the cases needed to be considered.

Theorem 16 $D(D_n) = \{2\}$ *unless* $n = 3, 4, 5, 6, 10$ *in which case* $D(D_n) = \{2, 3\}$.

Proof: By Theorem 12, if there is a vertex with stabilizer subgroup of type $< \sigma^k >$, then the graph is 2-distinguishable. So we may assume that G does not have a vertex with stabilizer subgroup of type 1. Similarly, by Theorem 14, if a vertex has a stabilizer of type 2 or 3, and the orbit of that vertex has size greater than or equal to 6, then the graph is 2-distinguishable. So we may assume that for any $v \in V(G)$, $|O_v| < 6$.

By the previous lemma, there must be an orbit of size p^α where p^α is the largest power of p which divides n. To have $|O_v| < 6$ for any vertex $v \in V(G)$, we only need to handle now the cases in which $p^\alpha < 6$. So clearly, $p \leq 5$ and n can have at most one factor of 5, one factor of 3, and two factors of 2. With this in mind, we need only consider the cases when $n = 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

The cases when $n \geq 12$ will be considered first. If the stabilizer subgroup of a vertex in G is of the type $< \tau\sigma^i >$, then the orbit of v contains $\frac{2n}{2} = n$ elements by the Orbit-Stabilizer Theorem. For $n \geq 12$, this would give an orbit of size greater than or equal to 12. So we may assume that the stabilizer subgroup of any vertex in G is of type $< \sigma^k, \tau\sigma^i >$.

Choose a vertex $v \in V(G)$ and suppose that $|O_v| = d$ ($d =$ 1,2,3,4, or 5 and d divides n) and $|St_v| = \frac{2n}{d}$. Then $St_v =< \sigma^d, \tau\sigma^i >$ for some $1 \leq i < d$. Now the stabilizer subgroups of the vertices in O_v are conjugate to St_v and their intersection is simply $< \sigma^d >$ which means that $< \sigma^d >$ fixes O_v. If v' is a vertex in another orbit $O_{v'}$ of size d_2 with $St_{v'} =< \sigma^{d_2}, \tau\sigma^{i'} >$, then the intersection of stabilizer subgroups of vertices in $O_{v'}$ is just $< \sigma^{d_2} >$. Now if $l = lcm(d, d_2)$ then clearly $< \sigma^l >$ fixes both O_v and $O_{v'}$. If we do this for each orbit O_1, O_2, …, O_s of sizes d, d_2, …, d_s respectively, then if $L = lcm(d, d_1, \ldots, d_s)$, then $< \sigma^L >$ will fix every vertex in the graph. Now the only automorphism in D_n that stabilizes the entire graph is $e = \sigma^n$. So in order for G to realize D_n , G must have orbits with sizes whose least common multiple is n.

The following table contains the values for n, and the possible sizes for the orbits so that their least common multiple is n.

n	Possible size of orbits
12	2,3,4
15	3,5
20	2,4,5
30	2,3,5
60	2,3,4,5

We first show that when there are orbits of sizes which are not pairwise relatively prime, then the graph can be 2-distinguished. This can happen in the cases listed above when there are two orbits of the same size, or we have both a 2-orbit and a 4-orbit. To motivate this, consider the following example.

Example. Consider a graph G which realizes D_{12}. Listed below are the possible stabilizer subgroups of a vertex with orbit size either 2,3 or 4:

Orbit Size	Possible Stabilizer Subgroup	List of elements
2	$<\sigma^2, \tau>$	$\{e, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}, \tau, \tau\sigma^2, \tau\sigma^4, \tau\sigma^6, \tau\sigma^8, \tau\sigma^{10}\}$
	$<\sigma^2, \tau\sigma>$	$\{e, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}, \tau\sigma, \tau\sigma^3, \tau\sigma^5, \tau\sigma^7, \tau\sigma^9, \tau\sigma^{11}\}$
3	$<\sigma^3, \tau>$	$\{e, \sigma^3, \sigma^6, \sigma^9, \tau, \tau\sigma^3, \tau\sigma^6, \tau\sigma^9\}$
	$<\sigma^3, \tau\sigma>$	$\{e, \sigma^3, \sigma^6, \sigma^9, \tau\sigma, \tau\sigma^4, \tau\sigma^7, \tau\sigma^{10}\}$
	$<\sigma^3, \tau\sigma^2>$	$\{e, \sigma^3, \sigma^6, \sigma^9, \tau\sigma^2, \tau\sigma^5, \tau\sigma^8, \tau\sigma^{11}\}$
4	$<\sigma^4, \tau>$	$\{e, \sigma^4, \sigma^8, \tau, \tau\sigma^4, \tau\sigma^8\}$
	$<\sigma^4, \tau\sigma>$	$\{e, \sigma^4, \sigma^8, \tau\sigma, \tau\sigma^5, \tau\sigma^9\}$
	$<\sigma^4, \tau\sigma^2>$	$\{e, \sigma^4, \sigma^8, \tau\sigma^2, \tau\sigma^6, \tau\sigma^{10}\}$
	$<\sigma^4, \tau\sigma^3>$	$\{e, \sigma^4, \sigma^8, \tau\sigma^3, \tau\sigma^7, \tau\sigma^{11}\}$

So in order for G to realize D_{12}, G must have orbits with sizes whose least commmon multiple is 12. In other words, there must be an orbit of size 3 and 4. From the table above, we see that each of the possible stabilizer subgroups for a vertex in the 4-orbit intersects each of the possible stabilizer subgroups for a vertex in the 3-orbit at the identity and a non-cyclic automorphism $\tau\sigma^h$ where $0 \leq h \leq 11$. What happens if there is an orbit of size 2 as well? We see that we can choose a stabilizer subgroup from the 2-orbit, say $<\sigma^2, \tau\sigma>$, and a stabilizer subgroup from the 4-orbit, say $<\sigma^4, \tau>$, whose intersection is $<\sigma^4>$. Thus $<\sigma^4> \cap \{e, \tau\sigma^h\} = \{e\}$. So by Theorem 10, the graph can be distinguished with 2 colors. A similar argument can be made if we have two orbits of the same size.

Resume proof of Theorem 16: As seen in the example, if we have two orbits O_1 and O_2 in which $|O_1| = |O_2|$ or $|O_1| = 2$ and $|O_2| = 4$, then the stabilizer subgroups from these orbits can be chosen so that their intersection is a subgroup of $<\sigma>$. If we throw in an orbit O_3 with size relatively prime to $|O_1|$ or $|O_2|$, then no matter which stabilizer subgroup St_3 we choose for a vertex in O_3, the intersection of St_3 with a subgroup of $<\sigma>$ will be the identity. From Theorem 10, we have then that $D(G) = 2$.

Now we must consider the cases when $n \geq 12$ and the orbits of G have sizes which are pairwise relatively prime. Hence if $n = 12$, the orbits sizes are 3 and 4; $n = 15$, 3 and 5; $n = 20$, 4 and 5; $n = 30$, 2,3 and 5; $n = 60$, 3,4, and 5. The goal is to show that there cannot possibly be orbits of G with sizes which are pairwise relatively prime. This will be done in three steps:

1. Show that the bipartite graphs formed by vertices in two separate orbits and the edges between them is either complete or empty.

2. Show that D_n will be equal to the product of the automorphism groups of the orbits.

3. Consider the product of all vertex-transitive graphs of sizes 3,4 and 5.

Step 1. We say that a graph G is a *bipartite graph*, if the set of vertices of G can be partitioned into 2 nonempty sets V_1 and V_2 such that any edge of G joins a vertex in V_1 to

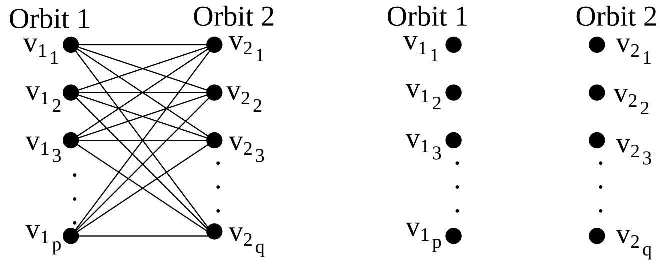

Figure 7.2: The bipartite graph on the left is complete while the one on the right is empty

a vertex in V_2. Furthermore, we say that a bipartite graph is *complete*, if given any pair of vertices, one from V_1 and the other from V_2, there is an edge joining them. We want to consider the bipartite graph formed by using vertices from 2 different orbis and the edges of G between them. We will show that this bipartite graph will either be complete or empty (see Figure 7.2).

Form the bipartite graph described above where $O_1 = \{v_{1_1}, \ldots, v_{1_p}\}$ and $O_2 = \{v_{2_1}, \ldots, v_{2_q}\}$ are the two orbits and p and q are relatively prime. Suppose now that there is an edge in the bipartite graph. Without loss of generality, say an edge between v_{1_1} and v_{2_1}. Now choose any other vertex v_{1_l} and v_{2_m} from orbits 1 and 2 respectively. It must be shown that there is an automorphism that maps v_{1_1} to v_{1_l} and v_{2_1} to v_{2_m}.

We see that $|O_1| = p$ and $|O_2| = q$. Thus $St_{v_{1_1}} =< \sigma^p, \tau\sigma^i >$ for some $1 \leq i < d_1$ and $St_{v_{2_1}} =< \sigma^q, \tau\sigma^j >$ for some $1 \leq j < d_2$. With this in mind, we can rewrite the orbits as follows:

$$O_1 = \{v_{1_1}, \sigma(v_{1_1}), \sigma^2(v_{1_1}), \ldots, \sigma^{p-1}(v_{1_1})\}$$

and

$$O_2 = \{v_{2_1}, \sigma(v_{2_1}), \sigma^2(v_{2_1}), \ldots, \sigma^{q-1}(v_{2_1})\}.$$

Since v_{1_1} and v_{1_l} are in O_1, then there is an automorphism σ^s such that $\sigma^s(v_{1_1}) = v_{1_l}$ where $0 \leq s < p$. Similarly, there is some σ^t with $0 \leq t < q$ such that $\sigma^t(v_{2_1}) = v_{2_m}$. We need to find some σ^r such that $\sigma^r(v_{1_1}) = v_{1_l}$ and $\sigma^r(v_{2_1}) = v_{2_m}$. In other words we need to find the solution of

$$r \equiv s\,(mod\, p)$$

$$r \equiv t\,(mod\, q).$$

By the Chinese Remainder Theorem, such a solution exists modulo pq. Because of the sizes of p and q, we have that $pq \leq n$; thus there is some automorphism in D_n which takes v_{1_1} to v_{1_l} and v_{2_1} to v_{2_m}. So if there is an edge between v_{1_1} and v_{2_1}, then there is an edge between any other pair of vertices, v_{1_i} and v_{2_j}. Similarly, no edge between v_{1_1} and v_{2_1} means there is no edge between any other pair v_{1_i} and v_{2_j}.

Step 2. We now show that if for every pair of orbits O and O' in the graph with $G[O] \ncong G[O']$ the bipartite graph formed by the vertices in O and O' and the edges between these orbits is either empty or complete, then $Aut(G) = Aut(G[O]) \times Aut(G[V-O])$. Here we use the notation $G[O]$ to mean the *subgraph of G induced by O* or the subgraph containing the vertices in O and all the edges in G which join two vertices in O. Suppose that $v \in V(G)$ and $h_1 \in Aut(G[O])$ and $h_2 \in Aut(G[V-O])$. Define $\omega : Aut(G[O]) \times Aut(G[V-O]) \to Aut(G)$ by

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

We want to show that ω is an automorphism of G. So we must show that ω preserves adjacency in G. It turns out that there are 3 kinds of edges in G:

1. edges in $G[O]$,
2. edges in $G[V-O]$, and
3. edges between O and $V-O$.

If v_1v_2 is an edge in $G[O]$, then both $v_1, v_2 \in O$. So $\omega(h_1,h_2)(v_1) = h_1(v_1)$ and $\omega(h_1,h_2)(v_2) = h_1(v_2)$. Now h_1 preserves adjacency in $G[O]$, so $\omega(h_1,h_2)(v_1)\omega(h_1,h_2)(v_2)$ is an edge of $G[O]$. Similarly, we have that $\omega(h_1,h_2)$ preserves adjacency in $V-O$. $\omega(h_1,h_2)$ also preserves adjacency between O and $V-O$ since the graph formed by the vertices in O and $V-O$ and the edges between them is either complete or empty. Thus

$$Aut(G[O]) \times Aut(G[V-O]) \subset Aut(G).$$

Now conversely, if we have any automorphism of G, when restricted to O, is an automorphism of $G[O]$ and when restricted to $V-O$ is an automorphism of $G[V-O]$. Thus we have shown containment both ways.

From the above discussion, we have that

$$D_n = Aut(G[O]) \times Aut(G[V-O])$$

where O is an orbit. In other words, D_n is the product of the automorphism group of each orbit considered as a subgroup of G.

Step 3. Now, each orbit must form a vertex-transitive graph. So we must consider all orbits of sizes 3,4, and 5 which are vertex-transitive. The only graphs with 3 vertices which are vertex-transitive are C_3 and $\overline{C_3}$ and both have the same automorphism group S_3. The only

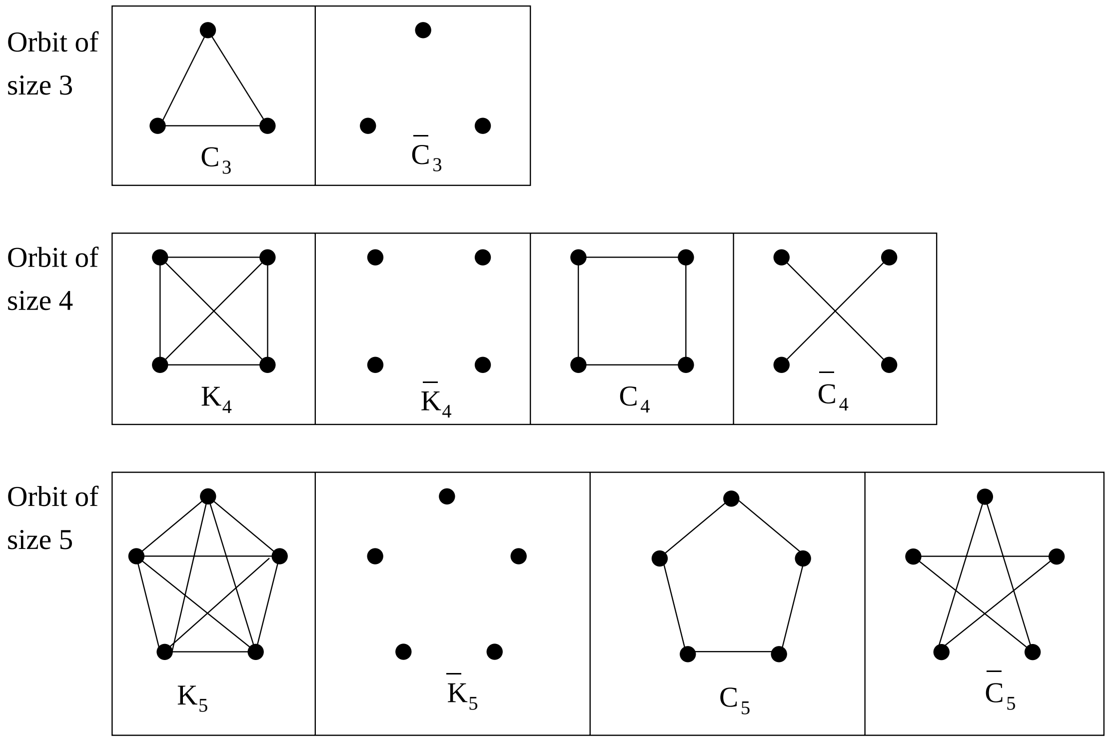

Figure 7.3: Vertex-transitive graphs with sizes 3,4 and 5

graphs with 4 vertices which are vertex-transitive are K_4, $\overline{K_4}$, C_4, and $\overline{C_4}$. The automorphism group of K_4 and its complement is S_4, while the automorphism group of C_4 and its complement is D_4. The only graphs with 5 vertices which are vertex-transitive are K_5, $\overline{K_5}$, C_5 and $\overline{C_5}$. The automorphism group of K_5 and its complement is S_5 and the automorphism group of C_5 and its complement is D_5. These graphs are seen in Figure 7.3.

1. For $n = 12$, $|D_{12}| = 24$. Now $|S_3| = 6$, $|S_4| = 24$ and $|D_4| = 8$, so the size of product of the automorphism groups for orbits of size 3 and 4 is at least 48.

2. For $n = 15$, $|D_{15}| = 30$. Now $|S_3| = 6$, $|S_5| = 120$ and $|D_5| = 10$, so the size of product of the automorphism groups for orbits of size 3 and 5 is at least 60.

3. For $n = 20$, $|D_{20}| = 40$. The size of product of the automorphism groups for orbits of size 4 and 5 is at least 80.

4. For $n = 30$, $|D_{30}| = 60$. The size of product of the automorphism groups for orbits of size 2, 3 and 5 is at least 120.

5. For $n = 60$, $|D_{60}| = 120$. The size of product of the automorphism groups for orbits of size 3, 4 and 5 is at least 480.

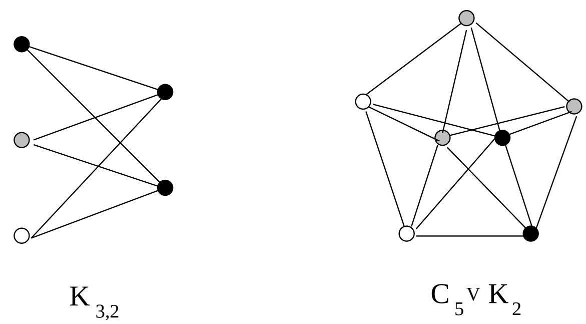

Figure 7.4: $K_{3,2}$ and $C_5 \vee K_2$

Thus we see that we cannot have orbits of G with sizes which are relatively prime. Since we have exhausted all of the cases for $n \geq 12$, we see that $D(D_n) = \{2\}$.

Now we will show that for the cases $n = 3, 4, 5, 6, 10$, $D(D_n) = \{2, 3\}$. We know that $2 \in D(G)$ for any graph G. So we will find a graph in each case with distinghuishing number 3, and then we will show that every graph which realizes D_n can be distinguished with 3 colors (or less.)

As observed in the original key problem when n=3,4,or 5, then it required 3 colors to disinguish the keys. Thus we have $3 \in D(D_3), D(D_4)$ and $D(D_5)$. It turns out that the complete bipartite graph $K_{3,2}$ realizes D_6 and requires 3 colors to be distinguished while the graph $C_5 \vee K_2$ realizes D_{10} and also requires 3 colors to distinguish. See Figure 7.4 for the distinguishing coloring of each graph.

It remains to be shown that any graph which realizes D_n for $n = 3, 4, 5, 6, 10$ can be distinguished with 3 colors. Suppose that $v_1, v_2, \ldots, v_t$ are vertices from the t different orbits of such a graph and $St_{v_1}, St_{v_2}, \ldots, St_{v_t}$ are their respective stabilizer subgroups. By Lemma 11, we have $< \sigma > \cap St_{v_1} \cap St_{v_2} \cap \ldots \cap St_{v_t} = \{e\}$ which means that $St_{v_1} \cap St_{v_2} \cap \ldots \cap St_{v_t} = \cap_{j=1}^{t} St_{v_j}$ is of the third type. So we have $\cap_{j=1}^{t} St_{v_j} =< \tau\sigma^i >$ for some $0 \leq i < n$. Color the vertices $v_1, v_2, \ldots, v_t$ red. Choose one vertex v which is not fixed by $\tau\sigma^i$ and color v green. Note that such a vertex exists, otherwise $\tau\sigma^i$ would fix every vertex in G, and because G realizes D_n this cannot happen. Color the rest of the vertices in G blue. Thus every automorphism moves a red vertex to a vertex which is not red, except for the automorphism $\tau\sigma^i$ which fixes all of the red vertices but moves the green vertex v to a blue vertex. Thus every graph can be distinguished with 3 colors. □

Chapter 8

Generalized Petersen Graphs

Having read Collins and Albertson's paper, it became of interest to find the distinguishing numbers of the generalized Petersen graphs. Before attempting to solve this problem, it was necessary to find the automorphism groups of these graphs. In this chapter, I will discuss my attempts in identifying these automorphism groups as well as the results published by Frucht in 1971 on the groups of the generalized Petersen graphs (see [3]).

Definition. The *generalized Petersen graph* $GP(n,k)$ for positive integers n and k with $2 \leq 2k < n$ is defined to have vertex set

$$V(GP(n,k)) = \{u_0, u_2, \ldots, u_{n-1}, v_0, v_1, v_2, \ldots, v_{n-1}\}$$

and edge set

$$E(GP(n,k)) = \{u_i u_{i+1}, v_i v_{i+k}, u_i v_i \,|\, i = 0, 1, \ldots, n-1\}$$

where addition in the subscripts is modulo n. Notice that $GP(n,k)$ is a regular 3-valent graph for any pair (n,k).

We have already seen the generalized Petersen graph $GP(7,2)$ in Figure 7.1. The most familiar generalized Petersen graph is $GP(5,2)$, otherwise known as simply the *Petersen graph.* This graph can be found in Figure 8.1.

As seen in the definition of the generalized Petersen graph, there are 3 types of edges: those edges between u_i and u_{i+1} called *outer edges*, those between v_i and v_{i+k} called *inner edges*, and those between u_i and v_i called *spokes.* Since $i = 0, 1, \ldots, n-1$, we see that there are n edges of each type and the symbols Ω, I, and Σ will be used to denote the set of outer edges, inner edges, and spokes respectively. If we first join the n outer edges appropriately, we see that we form an n-circuit which will be called the *outer rim.* Similarly, if $d = gcd(n,k)$, then by joining the n inner edges appropriately, we see that we form d pairwise-disjoint $\frac{n}{d}$-circuits called *inner rims.* Notice that when n and k are relatively prime, then there will be only one inner rim of length n as seen in Figure 7.1 and Figure 8.1 with $GP(7,2)$ and $GP(5,2)$

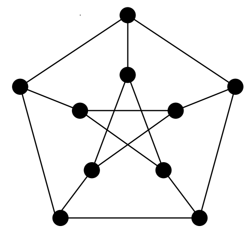

Figure 8.1: The Petersen Graph

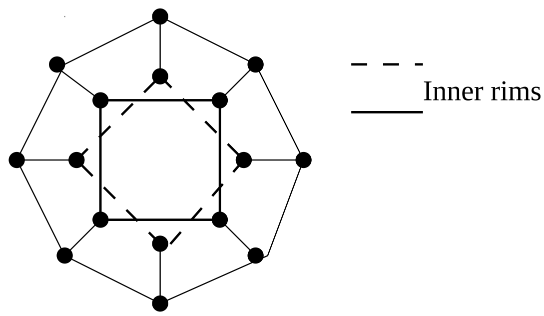

Figure 8.2: GP(8,2)

respectively. Figure 8.2 contains the graph of $GP(8,2)$. Notice that because 8 and 2 are not relatively prime, there are 2 inner rims of length 4.

8.1 Automorphism Groups of the Generalized Petersen Graphs

In finding the automorphism groups of the generalized Petersen graphs, it is important to notice that $D_n \subseteq Aut(GP(n,k))$ for all positive integers n and k. For some n and k, D_n is not the entire automorphism group of the graph. So finding the automorphism groups of the graphs now becomes a problem of seeing when there are automorphisms other than the basic rotations and reflections.

The first question I wanted to answer was this: When is there an automorphism which switches the outer and inner rims? Clearly, if n and k are not relatively prime, then there would be no such automorphism since automorphisms must take n-circuits to n-circuits. So my attention turned to the cases when n and k were relatively prime.

Lemma 17 *Suppose that n and k are relatively prime. Then there is an automorphism $\alpha \in Aut(GP(n,k))$ which switches the outer and inner rim if and only if $k^2 \equiv \pm 1 \,(mod\, n)$.*

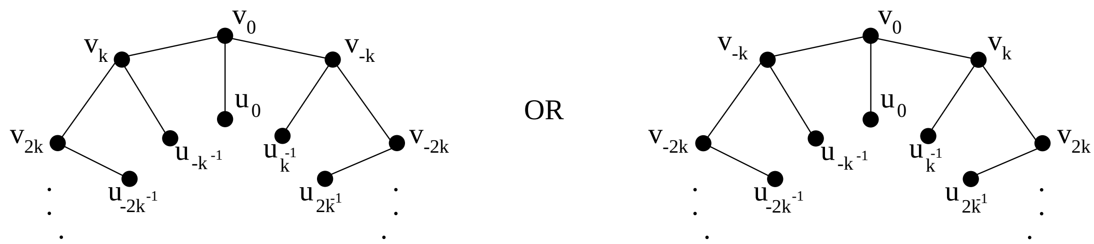

Figure 8.3: Two cases for the action of α

Proof: Switching the outer rim and the inner rim if at all possible could be done in one of several ways. Without loss of generality, the only case needed to be considered is the one in which $\alpha(u_0) = v_0$ and $\alpha(v_0) = u_0$. Again, we can assume without loss of generality that $\alpha(u_1) = v_k$. Now the outer rim is the n-circuit $u_0u_1u_2 \ldots u_{n-1}$ which must go to the inner rim if α is to be an automorphism. Since $\alpha(u_1) = v_k$, we must have that $\alpha(u_i) = v_{ik}$ for $i = 0, 1, \ldots, n-1$ (Remember that subscripts are read modulo n.) In other words, what gets mapped to $v_1, v_2, \ldots, v_{n-1}$ are the vertices $u_{k^{-1}}, u_{2k^{-1}}, \ldots, u_{-k^{-1}}$. Similarly, the inner rim is the n-circuit $v_0v_kv_{2k} \ldots v_{-k}$ which must get mapped to the outer rim. This can be done in one of two ways. Either $\alpha(v_k) = u_1$ or $\alpha(v_k) = u_{-1}$. More generally, either $\alpha(v_{ik}) = u_i$ or $\alpha(v_{ik}) = u_{-i}$. See Figure 8.3 for these two cases.

Now α will be an automorphism if it preserves adjacency. We have already fixed the vertices so that the adjacency of vertices in the inner and outer rims were preserved, so now we need to check the spokes. In the first case α will be an automorphism if and only if lk and $-lk^{-1}$ differ by n for $l = 0, 1, \ldots, n-1$; in other words, if and only if $lk \equiv -lk^{-1} \, (mod\, n)$ or

$$k \equiv -k^{-1} \, (mod\, n).$$

In the second case α will be an automorphism if and only if lk and lk^{-1} differ by n; in other words, if and only if $lk \equiv lk^{-1} \, (mod\, n)$ or

$$k \equiv k^{-1} \, (mod\, n).$$

Thus we see that α will be an automorphism if and only if $k^2 \equiv \pm 1 \, (mod\, n)$. □

Corollary 18 *If $k^2 \equiv \pm 1 \, (mod\, n)$, then $GP(n, k)$ is vertex-transitive.*

Proof: If $k^2 \equiv \pm 1 \, (mod\, n)$, then $\alpha \in Aut(GP(n, k))$, so vertices on the outer rim can be mapped to vertices on the inner rims and vice versa. Vertex-transitivity follows immediately. □

Appendix A contains two tables, one of which contains values of n and k with $n \leq 150$ and for which $k^2 \equiv 1 \, (mod\, n)$, and the other of which contains values of n and k with $n \leq 150$

and for which $k^2 \equiv -1 \,(mod\, n)$. These would be the only cases in which there would be an automorphism which switches the outer and inner rims (given that $n \leq 150$.)

The next natural question to ask is this: Are there other symmetries of $GP(n,k)$ other than those of D_n and other than α? My idea to answer this question was to look at possible images of the outer rim and then work from there. Before doing this, I used Mathematica and Groups and Graphs to generate a large number of these generalized Petersen graphs and to find the order of their automorphism groups. A table of the results I generated can be found in Appendix B.

It should be clear to the reader that if the order of $Aut(GP(n,k))$ is greater than $2n$, then there must be an automorphism in $Aut(GP(n,k))$ which is not in D_n. Thus, these automorphisms not in D_n must take a vertex from the outer rim to a vertex in the inner rim and vice versa. Looking at the table from Appendix B, I noticed that the only time the order of $Aut(GP(n,k))$ was greater than $2n$ was when $k^2 \equiv \pm 1 \,(mod\, n)$. In other words, I saw that if the graph $GP(n,k)$ were vertex-transitive, then α would be in $Aut(GP(n,k))$. This lead to the conjecture that if $GP(n,k)$ is vertex-transitive, then $k^2 \equiv \pm 1 \,(mod\, n)$ (hence the converse to the corollary above.) The proof of this is found in Frucht [3].

How Frucht proves that $GP(n,k)$ is vertex-transitive if and only if $k^2 \equiv \pm 1 \,(mod\, n)$ is to first consider the subgroup $B(n,k)$ of $Aut(GP(n,k))$ which fixes the set Σ set-wise. As we have already seen, the dihedral group D_n is a subgroup of $Aut(GP(n,k))$ but it is also contained in $B(n,k)$. He then defines another mapping α of the vertices of $GP(n,k)$ by:

$$\alpha(u_i) = v_{ki}, \;\; \alpha(v_i) = u_{ki}$$

for all i. Notice that this mapping exchanges Ω and I set-wise and is the same α which was defined above. Now we saw that α will be an automorphism of $GP(n,k)$ if and only if $k^2 \equiv \pm 1 \,(mod\, n)$. For a different approach to see why this is true, notice that α must map the spoke $u_i v_i$ onto the spoke $v_{ik} u_{ik}$, the outer edge $u_i u_{i+1}$ onto the inner edge $u_{ki} u_{ki+k}$, and the inner edge $v_i v_{i+k}$ onto the pair $u_{ki} u_{ki+k^2}$. Now this pair will be an edge if and only if their indices differ by ± 1. Thus we have an edge and hence an automorphism if and only if $k^2 \equiv \pm 1 \,(mod\, n)$ as we expected.

Our first goal is to find $B(n,k)$ for the three cases: $k^2 \not\equiv \pm 1 \,(mod\, n)$, $k^2 \equiv 1 \,(mod\, n)$, and $k^2 \equiv -1 \,(mod\, n)$. We begin with the following two results found in [3]:

Lemma 19 *If $\lambda \in Aut(GP(n,k))$ fixes set-wise any of the sets Ω, I, or Σ, then either it fixes all three sets or fixes Σ set-wise and interchanges Ω and I.*

Proof: Suppose that an outer edge e gets mapped to a spoke. Then one of the two outer edges adjacent to e must get mapped to an outer edge while the other outer edge adjacent to e must go to an inner edge (see Figure 8.4). Thus if the automorphism does not preserve Σ

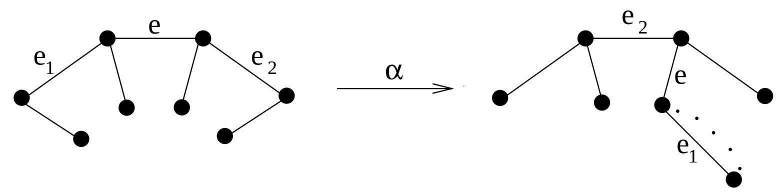

Figure 8.4: The action of α if an outer edge e is sent to a spoke

set-wise, then it cannot preserve either of the other sets Ω or I. Since the set of outer edges and the set of inner edges are both separate components, any automorphism which fixes Σ set-wise must fix Ω and hence I as well, or map Ω onto I and hence I onto Ω. $\square$

Theorem 20 *1. If $k^2 \not\equiv \pm 1\,(mod\, n)$ then $B(n,k) = D_n$ with*

$$\sigma^n = \tau^2 = 1, \;\; \tau\sigma\tau = \sigma^{-1}.$$

2. If $k^2 \equiv 1\,(mod\, n)$, then $B(n,k) = <\sigma, \tau, \alpha>$ with

$$\sigma^n = \tau^2 = \alpha^2 = 1, \;\; \tau\sigma\tau = \sigma^{-1}, \;\; \alpha\tau = \tau\alpha, \;\; \alpha\sigma\alpha = \sigma^k.$$

3. If $k^2 \equiv -1\,(mod\, n)$, then $B(n,k) = <\sigma, \alpha>$ with

$$\sigma^n = \alpha^4 = 1, \;\; \alpha\sigma\alpha^{-1} = \sigma^k.$$

In this case, $\tau = \alpha^2$. Hence, we can omit τ as a generator.

Proof: Suppose that $\lambda \in B(n,k)$. Then λ fixes Σ set-wise, and so by Lemma 19 λ either fixes Ω and I set-wise as well or λ interchanges Σ and I.

For $k^2 \not\equiv \pm 1\,(mod\, n)$, we saw that there was no such automorphism which exchanged the sets Ω and I. So in this case, any automorphism must fix all three sets. Suppose λ fixes all three of the sets Ω, Σ, and I. The set of edges in Ω form an n-circuit whose automorphism group is D_n. It is not hard to see that any automorphism $\lambda \in Aut(GP(n,k))$ is uniquely determined by its action on Ω. Thus $\lambda \in D_n = <\sigma, \tau>$. It is well known that the relations of the elements in the dihedral group are $\sigma^n = \tau^2 = 1$ and $\tau\sigma\tau = \sigma^{-1}$.

For $k^2 \equiv \pm 1\,(mod\, n)$, we saw that there is an automorphism α which exchanges Ω and I. Now suppose that λ is another automorphism which fixes Σ but interchanges Ω and I. If we compose λ with an appropriate power of σ, then we can force u_0 and v_0 to be switched. Furthermore, by composing this automorphism with τ (if necessary), we can insist that u_1 get mapped to v_k. Thus since the outer rim is being mapped to the inner rim, the inner rim must also be an n-circuit. With u_0 and u_1 going to v_0 and v_k respectively, we must also have u_i going to v_{ik} for all $i = 0, 1, \ldots, n-1$. Now since the set of spokes is being preserved set-wise, we must have the spoke u_iv_i going to $u_{ik}v_{ik}$. This forces v_i to go to u_{ik}. Thus we have the the composition of τ, a power of σ, and λ is just the automorphism α.

Thus we have that every element in $B(n, k)$ which is not in D_n interchanges Ω and I and can be written as the composition of any number of σ's and τ with the automorphism α. Since composing any two of these automorphism fixes each set Ω, Σ, and I, it is in D_n. Thus D_n has index 2 within $B(n, k)$ and $B(n, k)$ has order $4n$. (Notice that this says that the order of $Aut(GP(n, k))$ is at least $4n$. There could be other automorphisms which do not fix the set Σ set-wise. We will soon see when this is true.)

It remains to be shown the defining relations for $B(n, k)$ for $k^2 \equiv \pm 1 \,(mod\, n)$. The easiest way to do this is to consider the action of $B(n, k)$ on the set of spokes $\{s_0, s_1, \ldots, s_{n-1}\}$ where s_i is the edge u_iv_i. Notice that $\sigma(s_i) = s_{i+1}$, $\tau(s_i) = s_{-i}$, and $\alpha(s_i) = s_{ik}$.

First suppose that $B(n, k)$ is not faithful on the set Σ. Then there must be a nontrivial automorphism $\lambda \in B(n, k)$ which fixes each spoke. Certainly, the only automorphism fixing all sets Ω, Σ, and I while fixing each spoke s_i is the identity automorphism, so λ must interchange Ω and I. This can happen if and only if $k = 1$. In this case we have $B(n, 1) \cong D_n \times S_2$. The remaining relations are $\alpha^2 = \alpha\sigma\alpha\sigma^{-1} = (\tau\alpha)^2 = 1$.

Now assume that $k > 1$. We've already seen that $B(n, k)$ acts faithfully on Σ. First suppose that $k^2 \equiv 1 \,(mod\, n)$. For any $s_i \in \Sigma$, we have

$$\alpha^2(s_i) = \alpha(s_{ik}) = s_{ik^2} = s_i.$$

Thus α^2 fixes every vertex and so $\alpha^2 = 1$. Similarly,

$$\alpha\tau\alpha(s_i) = \alpha\tau(s_{ik}) = \alpha(s_{-ik}) = s_{-ik^2} = s_{-i} = \tau(s_i),$$

$$\alpha\sigma\alpha(s_i) = \alpha\sigma(s_{ik}) = \alpha(s_{ik+1}) = s_{ik^2+k} = s_{i+k} = \sigma^k(s_i).$$

Thus we have proved the second part of the theorem.

Now suppose that $k^2 \equiv -1 \,(mod\, n)$. For any $s_i \in \Sigma$, we have

$$\alpha^2(s_i) = \alpha(s_{ik}) = s_{ik^2} = s_{-i} = \tau(s_i),$$

$$\alpha\sigma\alpha^{-1}(s_i) = \alpha\sigma(s_{-ik}) = \alpha(s_{1-ik}) = s_{k-ik^2} = s_{k+i} = \sigma^k(s_i).$$

Now because $1 = \tau^2 = (\alpha^2)^2 = \alpha^4$, we may omit τ as a generator and thus we have proved the theorem. $\square$

To this point we can conclude that $B(n, k)$ acts transitively on the vertices if and only if $k^2 \equiv \pm 1 \,(mod\, n)$. From this we can deduce that if $k^2 \equiv \pm 1 \,(mod\, n)$, then $GP(n, k)$ is vertex-transitive. In order to prove the converse, it will be necessary to find $Aut(GP(n, k))$ for each pair (n, k). We do this by first enumerating the cases in which $B(n, k)$ is a proper subgroup of the automorphism group of $GP(n, k)$. We begin with the straight-forward result given in [3].

Lemma 21 *The following are equivalent:*

1. *$GP(n, k)$ is edge-transitive*
2. *There is an automorphism $\lambda \in Aut(GP(n, k))$ which maps some spoke onto an edge which is not a spoke.*
3. *$B(n, k)$ is a proper subgroup of $Aut(GP(n, k))$.*

Proof: Suppose that $GP(n, k)$ is edge-transitive; then clearly there must be some automorphism λ which maps some spoke onto an edge which is not a spoke. It is also clear by the definition of $B(n, k)$ that λ is not contained in $B(n, k)$ and so $B(n, k)$ is a proper subgroup of $Aut(GP(n, k))$.

Now suppose that $GP(n, k)$ were not edge-transitive. Thus there must be at least two orbits of edges under the action of $Aut(GP(n, k))$ on the edges. But there are no more than three orbits of edges, since the set of outer edges are contained in one orbit, the set of spokes are contained in one, and the set of inner edges are contained in one orbit. Since $B(n, k) \subseteq Aut(GP(n, k))$, if we let $B(n, k)$ act on the set of edges, then the edge-orbits we obtain will be subsets of the edge-orbits obtained by letting $Aut(GP(n, k))$ act on the edges. Now because $B(n, k)$ has either 2 or 3 edge-orbits ($B(n, k)$ fixes Σ set-wise and thus Ω and I are either in separate orbits or one together), $Aut(GP(n, k))$ and $B(n, k)$ must have at least one edge-orbit in common. It turns out the $Aut(GP(n, k))$ must fix one of Ω, Σ, or I, but by Lemma 19, $Aut(GP(n, k))$ must fix Σ, and so $Aut(GP(n, k)) = B(n, k)$ contrary to part 3 of the theorem. $\square$

Before proving the next theorem, we need some new notation. In particular if C is an arbitrary circuit in $GP(n, k)$, let $r(C)$ be the number of outer edges in C, $s(C)$ be the number of spokes in C, and $t(C)$ be the number of inner edges in C. Now if C_j is the set of j-circuits in $GP(n, k)$, then let

$$R_j = \sum_{C \in C_j} r(C),$$

$$S_j = \sum_{C \in C_j} s(C), \text{ and}$$

$$T_j = \sum_{C \in C_j} t(C).$$

The following lemma given in [3] is a very useful tool in showing that the entire automorphism group of $GP(n, k)$ is equal to the subgroup $B(n, k)$ for certain pairs of n and k. In particular, we have:

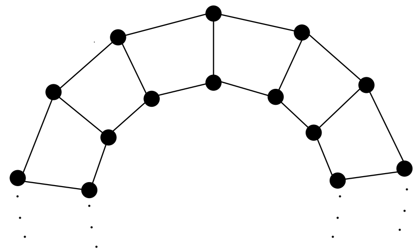

Figure 8.5: For $k = 1$, there are only n 4-circuits in $GP(n, 1)$

Lemma 22 *If $B(n,k) \neq Aut(GP(n,k))$, then $R_j = S_j = T_j$ for $j = 3, 4, 5, \ldots$.*

Proof: Because $\sigma \in Aut(GP(n,k))$, then if any given outer edge e is in c j-circuits, then every outer edge is contained in c j-circuits. Thus we have $R_j = nc$. Similarly, there are constants c' and c'' such that if s is a spoke contained in c' different j-circuits, then $S_j = nc'$ and if f is an inner edge contained in c'' j-circuits, then $T_j = nc''$. If $B(n,k) \neq Aut(GP(n,k))$, then $GP(n,k)$ is edge-transitive by Lemma 21, and so if any edge in the graph is contained in c j-circuits, then they all are, so $c = c' = c''$. Thus $R_j = S_j = T_j$. □

Note that this lemma says that if we can find some j for which $R_j \neq S_j$, $R_j \neq T_j$, or $S_j \neq T_j$, then $B(n,k) = Aut(GP(n,k))$. The use of this lemma is illustrated in the following two lemmas from [3]. In particular, we will see that $B(n,k) = Aut(GP(n,k))$ except for the following pairs of n and k: $(4,1)$, $(5,2)$, $(8,3)$, $(10,2)$,$(10,3)$,$(12,5)$,$(24,5)$. We will begin with the case $k = 1$:

Lemma 23 *If $n \neq 4$, then $B(n,1) = Aut(GP(n,1))$*

Proof: The method of proof will be that described above. In particular, we look at all of the possible 4-circuits in $GP(n,1)$. If $n \neq 4$, then the only possible 4-circuit will be of the form $u_i u_{i+1} v_{i+1} v_i$ (See Figure 8.5), and there are exactly n of these. Note that in a circuit of this type, there is exactly one outer edge, one inner edge, and two spokes, so that $R_4 = n$, $S_4 = 2n$ and $T_4 = n$. Thus by the previous lemma, $B(n,1) = Aut(GP(n,1))$. □

Lemma 24 *If $n \neq 5$ or 10, then $B(n,2) = Aut(GP(n,2))$*

Proof: If $n \neq 5$ *or* 10, then the outer rim would be an n-circuit and the inner rims would be circuits of length $\frac{n}{gcd(n,2)}$. Now because $gcd(n,2) = 1$ *or* 2, the only time $\frac{n}{gcd(n,2)} = 5$ is when $n = 5$ *or* 10. Thus the only 5-circuits in $GP(n,k)$ will be those with $s(C) = 2$ and either $r(C) = 1$ and $t(C) = 2$ or $r(C) = 2$ and $t(C) = 1$. The former case is impossible since $s(C) = 2$ forces the inner edges to be adjacent, yielding the circuit of type $u_0 v_0 v_2 v_4 u_4$

which is not a circuit. Thus $GP(n, 2)$ contains n 5-circuits of the form $u_i u_{i+1} u_{i+2} v_{i+2} v_i$. It follows that $R_5 = S_5 = 2n$ and $T_5 = n$. By Lemma 22 we have $B(n, 2) = Aut(GP(n, 2))$ for $n \neq 5\,or\,10$. □

It turns out that by considering all of the possible 8-circuits in $GP(n, k)$ for $k > 2$ and $n > 5$ most of the other cases fall out. We do this by looking at all possible cases for $r(C)$, where C is an 8-circuit. First note that any circuit C in $GP(n, k)$ must have an even number of spokes. Suppose that C is an 8-circuit:

1. Suppose $r(C) = 8$. Then there is only one possible way for this to happen: $n = 8$.

2. Suppose $r(C) = 7$. Then the other edge of the circuit would be either a spoke or an inner edge. Thus since there has to be an even number of spokes, the other edge would be an inner edge. The union of 7 outer edges with an inner edge can never be a circuit.

3. Suppose $r(C) = 6$, then we could have either $s(C) = 2$ and $t(C) = 0$ or $s(C) = 0$ and $t(C) = 2$. Note that in either case, the union of the 6 outer edges with the other two would not be a circuit.

4. Suppose $r(C) = 5$, then we must have $s(C) = 2$ and $t(C) = 1$. (The only other possible combination would be $s(C) = 0$ and $t(C) = 3$, but by the same reasoning used in (3), this would not be a circuit.) Now because $s(C) = 2$, the 5 outer edges are forced to be adjacent to obtain a circuit. Thus this type of 8-circuit would be $u_0 u_1 u_2 u_3 u_4 u_5 v_5 v_0$ and this is only possible if $k = 5$ or $n - k = 5$.

5. Suppose $r(C) = 4$, then we must have $s(C) = 2$ and $t(C) = 2$. Again because $s(C) = 2$, the 4 outer edges are forced to be adjacent and the 2 inner edges are forced to be adjacent. This type of 8-circuit would be $u_0 u_1 u_2 u_3 u_4 v_4 v_{\frac{1}{2}(n+4)} v_0$ and this is only possible when $k = \frac{1}{2}(n + 4) - 4 = \frac{n}{2} - 2$ or $2k + 4 = n$.

6. Suppose $r(C) = 3$, then either $s(C) = 2$ and $t(C) = 3$ or $s(C) = 4$ and $t(C) = 1$. Note that the latter case cannot happen because we have 4 endpoints of the 4 spokes to be joined by one inner edge. Thus since $s(C) = 2$ this forces the 3 outer edges to be adjacent and the 3 inner edges to be adjacent. This type of 8-circuit would be $u_0 u_1 u_2 u_3 v_3 v_{3+k} v_{3+2k} v_0$ or $u_0 u_1 u_2 u_3 v_3 v_{3-k} v_{3-2k} v_0$ and these are possible when $n = 3+3k$ or $3 - 3k = -n$ respectively since $2k < n$ and $\frac{n}{2} \geq 3 \Rightarrow 3 + 3k < 3 + \frac{3}{2}n \Rightarrow 3 + 3k < 2n$ and $2k < n \Rightarrow 3 - 3k > 3 - \frac{3}{2}n \Rightarrow 3 - 3k \geq -n$.

7. Suppose $r(C) = 2$, then we can have $s(C) = 2$ and $t(C) = 4$ or $s(C) = 4$ and $t(C) = 2$. In the first case, because $s(C) = 2$, this forces the 2 outer edges to be adjacent and the 4 inner edges to be adjacent. This type of 8-circuit would be $u_0 u_1 u_2 v_2 v_{2+k} v_{2+2k} v_{2+3k} v_0$ which occurs when $n = 2 + 4k$ or $2n = 2 + 4k$ since $2k < n \Rightarrow 2 + 4k < 2 + 2n \Rightarrow 2 + 4k = n$ or $2 + 4k = 2n$ or it could be $u_0 u_1 u_2 v_2 v_{2-k} v_{2-2k} v_{2-3k} v_0$ which occurs when $2 - 4k = -n$ since $2k < n \Rightarrow -4k > 2n \Rightarrow 2 - 4k > 2 - 2n \Rightarrow 2 - 4k = -n$

In the second case, because $s(C) = 4$, we cannot have the 2 outer edges adjacent, nor can we have the 2 inner edges adjacent. Each outer and inner edge must join two endpoints of a spoke, so that this type of 8-circuit is $u_0u_1v_1v_{1+k}u_{1+k}u_{2+k}v_{2+k}v_0$ which occurs when $2 + 2k = n$ or it is $u_0u_1v_1v_{1+k}u_{1+k}u_kv_kv_0$ which occurs for all $n \geq 4$. Note that the case $u_0u_1v_1v_{1-k}u_{1-k}u_{2-k}v_{2-k}v_0$ can never happen and the case $u_0u_1v_1v_{1-k}u_{1-k}u_{-k}v_{-k}v_0$ is analogous to the second circuit. Thus we have exhausted all cases.

8. Suppose $r(C) = 1$, then it must be true that $s(C) = 2$ which leaves $t(C) = 5$. This type of 8-circuit will be $u_0u_1v_1v_{1+k}v_{1+2k}v_{1+3k}v_{1+4k}v_0$ which occurs when $n = 1 + 5k$ or $2n = 1 + 5k$ since $2k < n$ and $\frac{n}{2} \geq 3 \Rightarrow 1 + 5k < 1 + \frac{5}{2}n \Rightarrow 1 + 5k < 3n$. This type of 8-circuit could also be $u_0u_1v_1v_{1-k}v_{1-2k}v_{1-3k}v_{1-4k}v_0$ which occurs when $1 - 5k = -n$ or $1 - 5k = -2n$ since $2k < n$ and $\frac{n}{2} \geq 3 \Rightarrow 1 - 5k > 1 - \frac{5}{2}n \Rightarrow 1 - 5k \geq -2n$.

9. Finally, suppose $r(C) = 0$, then we must also have $s(C) = 0$, which forces $t(C) = 8$. Thus we have an 8-circuit of type $v_0v_kv_{2k}v_{3k}v_{4k}v_{5k}v_{6k}v_{7k}$ which occurs if $n = 8k$. Now since $2k < n$, we have that $8k < 4n$ which tells us that this type of circuit could occur if $3n = 8k$ as well.

The above information is summarized in the following table:

Type	Cycle representation	Conditions	Number	$r(C)$	$s(C)$	$t(C)$
1	$u_0u_1u_2u_3u_4u_5u_6u_7$	$n = 8$	1	8	0	0
2	$u_0u_1u_2u_3u_4u_5v_5v_0$	$k = 5$ or $n - k = 5$	n	5	2	1
3	$u_0u_1u_2u_3u_4v_4v_{\frac{1}{2}(n+4)}v_0$	$n = 2k + 4$	n	4	2	2
4	$u_0u_1u_2u_3v_3v_{3+k}v_{3+2k}v_0$	$n = 3k + 3$	n	3	2	3
4'	$u_0u_1u_2u_3v_3v_{3-k}v_{3-2k}v_0$	$n = 3k - 3$	n	3	2	3
5	$u_0u_1u_2v_2v_{2+k}v_{2+2k}v_{2+3k}v_0$	n *or* $2n = 4k + 2$	n	2	2	4
5'	$u_0u_1u_2v_2v_{2-k}v_{2-2k}v_{2-3k}v_0$	$n = 4k - 2$	n	2	2	4
6	$u_0u_1v_1v_{1+k}u_{1+k}u_{2+k}v_{2+k}v_0$	$n = 2k + 2$	$\frac{1}{2}n$	2	4	2
7	$u_0u_1v_1v_{1+k}u_{1+k}u_kv_kv_0$	$n \geq 4$	n	2	4	2
8	$u_0u_1v_1v_{1+k}v_{1+2k}v_{1+3k}v_{1+4k}v_0$	n *or* $2n = 5k + 1$	n	1	2	5
8'	$u_0u_1v_1v_{1-k}v_{1-2k}v_{1-3k}v_{1-4k}v_0$	n *or* $2n = 5k - 1$	n	1	2	5
9	$v_0v_kv_{2k}v_{3k}v_{4k}v_{5k}v_{6k}v_{7k}$	$n = 8k$	k	0	0	8
9'	$v_0v_kv_{2k}v_{3k}v_{4k}v_{5k}v_{6k}v_{7k}$	$3n = 8k$	$\frac{1}{8}n$	0	0	8

We have already seen that when $n \neq 4$ $B(n, 1) = Aut(GP(n, 1))$, and when $n \neq 5$ or 10 $B(n, 2) = Aut(GP(n, 2))$. We now use the 8-circuits in $GP(n, k)$ for $k > 2$ to show that when (n, k) is not one of six pairs, we definitely have $B(n, k) = Aut(GP(n, k))$.

Lemma 25 *$B(n, k) = Aut(GP(n, k))$ if $k > 2$ and if (n, k) is not one of the pairs: $(8, 3)$, $(10, 3)$, $(12, 5)$, $(13, 5)$, $(24, 5)$, or $(26, 5)$*

Proof: Since $(8,1)$, $(8,2)$, and $(8,3)$ have already been excluded, we may assume that $n \neq 8$. We first consider the case when $n = 8k$ and $k > 2$. The types of 8-circuits contained in $GP(8k,k)$ are 7 and 9 as well as type 2 if $k = 5$. Thus there are two cases to consider. Suppose that $k = 5$, then $R_8 = 5n+0+2n = 7n$ while $S_8 = 2n+0+4n = 6n$. Now suppose that $k \neq 5$, then similarly $R_8 = 0+2n = 2n$ and $S_8 = 0+4n = 4n$. Thus in both cases we have $B(8k,k) = Aut(GP(8k,k))$ by Lemma 22.

Now suppose that $n \neq 8k$. Note that because n cannot be equal to $3k+3$ and $3k-3$ simultaneously, there cannot be 8-circuits of types 4 and 4' simultaneously. A similar statement can be made of 8-circuits of types 5 and 5', 8 and 8', and 9 and 9'. What we will do next is sum up the total number of outer edges in any 8-circuit, the total number of spokes in any 8-circuit, and the total number of inner edges in any 8-circuit. Before doing this, let $x_i = 1$ if there are circuits of type i or i' in $GP(n,k)$ and let $x_i = 0$ otherwise. Then we have:

$$R_8 = 5nx_2 + 4nx_3 + 3nx_4 + 2nx_5 + nx_6 + 2n + nx_8,$$

$$S_8 = 2nx_2 + 2nx_3 + 2nx_4 + 2nx_5 + 2nx_6 + 4n + 2nx_8,$$

$$T_8 = nx_2 + 2nx_3 + 3nx_4 + 4nx_5 + nx_6 + 2n + 5nx_8 + nx_9.$$

We want to find the cases when $B(n,k) \neq Aut(GP(n,k))$. Suppose that $B(n,k) \neq Aut(GP(n,k))$. By Lemma 22 we would have $\frac{(R_8-T_8)}{n} = 0$ or $4x_2 + 2x_3 - 2x_5 - x_9 - 4x_8 = 0$ which gives

$$4x_2 + 2x_3 = 2x_5 + x_9 + 4x_8.$$

Since the left side is always even, we must have that $x_9 = 0$. Furthermore, it should be clear that $x_2 = x_8$ and $x_3 = x_5$. If $x_2 = x_8 = 1$, then we must have $k = 5$ and $n = 12, 12, 24$, or 26 all of which are excluded in the hypothesis. Now if $x_3 = x_5$, then intersecting the conditions gives $2k+4 = 4k+4$ which cannot happen, $4k+8 = 4k+2$ which cannot happen, and $2k+4 = 4k-2 \Rightarrow 2k = 6 \Rightarrow k = 3 \Rightarrow n = 10$ which is also an excluded case. Thus we may assume that $x_2 = x_3 = x_5 = x_8 = 0$.

We can similarly look at when $\frac{(R_8-S_8)}{n} = 0$. This occurs when $3x_2+2x_3+x_4-x_6-2-x_8 = 0$ or when

$$3x_2 + 2x_3 + x_4 = x_6 + 2 + x_8.$$

But since $x_2 = x_3 = x_5 = x_8 = 0$, we have $x_4 = x_6 + 2$. Because x_i is either 0 or 1, the condition has no solution. $\square$

The next lemma gives two more cases in which $B(n,k) = Aut(GP(n,k))$. For an alternate proof of the second part of the lemma, please refer to [3], page 216.

Lemma 26 $B(13,5) = Aut(GP(13,5))$ *and* $B(26,5) = Aut(GP(26,5))$.

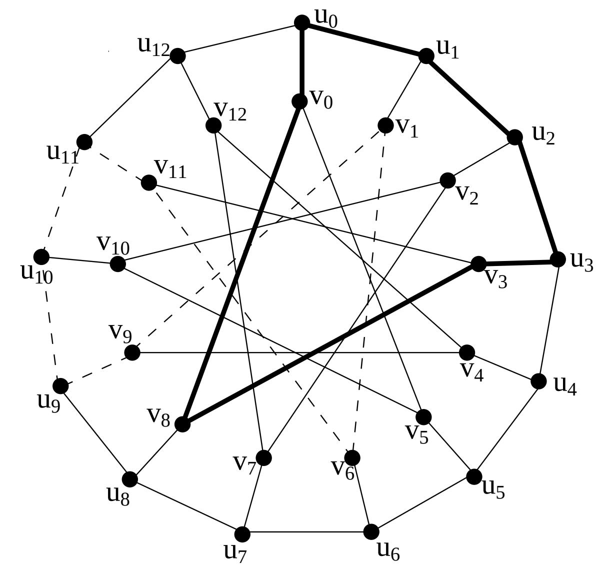

Figure 8.6: $GP(13, 5)$

Proof: First consider $GP(13, 5)$ as seen in Figure 8.7 and suppose that we look at all possible 7-circuits. Clearly there are no 7-circuits with 7,6, or 5 outer edges. All other cases are summarized in the following table:

$r(C)$	$s(C)$	$t(C)$	Circuit representation	Circuit?
4	2	1	$u_0u_1u_2u_3u_4v_4v_0$	No
3	2	2	$u_0u_1u_2u_3v_3v_8v_0$	Yes
3	2	2	$u_0u_1u_2u_3v_3v_{11}v_0$	No
2	2	3	$u_0u_1u_2v_2v_7v_{12}v_0$	No
2	2	3	$u_0u_1u_2v_2v_{10}v_5v_0$	Yes
1	2	4	$u_0u_1v_1v_6v_{11}v_3v_0$	No
1	2	4	$u_0u_1v_1v_9v_4v_{12}v_0$	No

It should be clear to the reader that the cases in which $s(C) = 4$ is impossible since it would leave $r(C) = 2$ and $t(C) = 1$ or $r(C) = 1$ and $t(C) = 2$. In either case, we would have to have one outer or inner edge joining the 4 endpoints of the spokes.

From the table above, we see that there are only 2 types of 7-circuits in $GP(13, 5)$ each type occuring $n = 13$ times. This leads to the calculations $R_7 = 5 \times 13 = 65$, $S_7 = 4 \times 13 = 52$, and so by Lemma 22, we have that $B(13, 5) = Aut(GP(13, 5))$.

It turns out that in $GP(26, 5)$ there are only two types of 10-circuits (See Appendix C for justification of this statement.) One type is $u_0u_1u_2v_2v_7u_7u_6u_5v_5v_0$ while the other is

$u_0u_1v_1v_6v_{11}u_{11}u_{10}v_{10}v_5v_0$. Note that in the first type $r(C) = 4$, $s(C) = 4$, and $t(C) = 2$ and there are 26 circuits of this type. In the second type, $r(C) = 2$, $s(C) = 4$, and $t(C) = 4$ and there are also 26 circuits of this type so that $R_{10} = 4 \times 26 + 2 \times 26 = 156$ and $S_{10} = 4 \times 26 + 4 \times 26 = 208$. Thus by lemma 23 , $B(26, 5) = Aut(GP(26, 5))$. □

We are now in a position to prove the converse of Corollary 18, namely:

Theorem 27 *If $GP(n, k)$ is vertex-transitive, then $k^2 \equiv \pm 1 \, (mod\, n)$ or the graph is $GP(10, 2)$.*

Proof: As seen in the previous lemmas, there are only seven cases when $B(n, k) \neq Aut(GP(n, k))$, namely $GP(4, 1)$, $GP(5, 2)$, $GP(8, 3)$, $GP(10, 2)$, $GP(10, 3)$, $GP(12, 5)$, and $GP(24, 5)$. We have also seen that $B(n, k)$ acts transitively on the vertices if and only if $k^2 \equiv \pm 1 \, (mod\, n)$ for graphs not in this list. Since $Aut(GP(n, k)) = B(n, k)$ except for the seven cases, we have that if $Aut(GP(n, k))$ acts transitively on the vertices then $k^2 \equiv \pm 1 \, (mod\, n)$. To complete the proof we need to show the statement is true for the seven exceptional cases.

Consider first the graphs $GP(4, 1)$, $GP(8, 3)$, $GP(12, 5)$, and $GP(24, 5)$. It is shown in [3] that if we define λ on $V(GP(n, k))$ for these four cases by

$$\lambda(u_{4i}) = u_{4i}, \ \lambda(v_{4i}) = u_{4i+1},$$

$$\lambda(u_{4i+1}) = u_{4i-1}, \ \lambda(u_{4i-1}) = v_{4i},$$

$$\lambda(u_{4i+2}) = v_{4i-1}, \ \lambda(v_{4i-1}) = v_{4i+5},$$

$$\lambda(v_{4i+1}) = u_{4i-2}, \ \lambda(v_{4i+2}) = v_{4i-6}$$

for all i then $Aut(GP(n, k)) =< \sigma, \tau, \lambda >$ with

$$\sigma^n = \tau^2 = \lambda^3 = 1,$$

$$\tau\sigma\tau = \sigma^{-1},$$

$$\tau\lambda\tau = \lambda^{-1},$$

$$\lambda\sigma\lambda = \sigma^{-1},$$

$$\lambda\sigma^4 = \sigma^4\lambda.$$

Thus α as defined earlier in the paper is given by

$$\alpha = \lambda^{-1}\sigma\lambda^{-1} = \tau\lambda^{-1}\sigma\lambda^{-1}.$$

So clearly in these four cases, the graph is vertex-transitive, and it can be verified that in each case $k^2 \equiv 1 \, (mod\, n)$. Note that in each case $|Aut(GP(n, k))| = 12n$ as seen in Appendix A.

Now consider the graphs $GP(5,2)$ and $GP(10,3)$. It has been shown that $Aut(GP(5,2))$ is isomorphic to S_5 while $Aut(GP(10,3))$ is isomorphic to $S_5 \times S_2$. As given in [3], both graphs can be generated by σ and μ defined by

$$(u_2v_1)(u_3v_4)(u_7v_6)(u_8v_3)(v_2v_8)(v_3v_7)$$

for $GP(10,3)$ and

$$(u_2v_1)(u_3v_4)(v_2v_3)$$

for $GP(5,2)$. The defining relations for $GP(10,3)$ are

$$\sigma^{10} = \mu^2 = (\mu\sigma^2)^4 = (\sigma^2\mu\sigma^{-2}\mu)^3 = (\sigma\mu\sigma^{-1}\mu)^2 = (\sigma^5\mu\sigma^{-5}\mu) = 1$$

and those for $GP(5,2)$ are

$$\sigma^5 = \mu^2 = (\mu\sigma^2)^4 = (\sigma^2\mu\sigma^{-2}\mu)^3 = (\sigma^5\mu\sigma^{-5}\mu) = 1.$$

In either case we find that $|Aut(GP(n,k))| = 24n$ and $Aut(GP(n,k))$ acts transitively on the vertices of $GP(n,k)$. It can be verified that $k^2 \equiv -1\,(mod\,n)$.

The last case to consider is the graph $GP(10,2)$ which is seen to be the graph of the regular dodecahedron. Its automorphism group is found to have order 120 and can be represented by $Aut(GP(10,2)) =< \sigma, \zeta >$ where ζ is defined by

$$\zeta = (u_0v_2v_8)(u_1v_4u_8)(u_2v_6u_9)(u_3u_6v_9)(u_4u_7v_1)(u_5v_7v_3).$$

The defining relations for $Aut(GP(10,2))$ are given by

$$\sigma^{10} = \zeta^3 = (\zeta\sigma^2)^2 = \sigma^5\zeta\sigma^{-5}\zeta^{-1} = 1.$$

$GP(10,2)$ is seen to be vertex-transitive although $k^2 \not\equiv \pm 1\,(mod\,n)$. Thus the theorem is proved. □

8.2 Distinguishing Numbers of Generalized Petersen Graphs

Now that the automorphism groups of all of the generalized Petersen graphs have been defined, we can now find the distinguishing numbers for these graphs.

Theorem 28 *$D(GP(n,k)) = 2$ except for the pairs $(4,1)$ and $(5,2)$ in which case $D(GP(n,k)) = 3$.*

Proof: Let's first suppose that $k^2 \not\equiv \pm 1\,(mod\,n)$. In this case it must follow that $n \geq 6$ and we know from the discussion above that $Aut(GP(n,k) \cong D_n$ except for the pair $(10,2)$. Excluding the pair $(10,2)$, we must have that there are two orbits of vertices each of size n. Besides the identity automorphism, there is only one other automorphism, namely $\tau\sigma^i$ for some $0 \leq i < n$, which stabilizes any given vertex in $GP(n,k)$. Thus by Theorem 14 we have that $GP(n,k)$ can be distinguished with two colors in these cases.

We defined $Aut(GP(10,2)) =< \sigma, \zeta >$ where ζ and the relations are given above. We can think of $Aut(GP(10,2))$ as consisting of the rotations σ^i, the reflections $\tau\sigma^i$, the order 3 rotations about the axis through antipodal vertices (i.e. u_0 and u_5), and the order 2 automorphism represented by $\zeta\sigma^2$. If we color u_0, u_2 and u_3 red and the rest of the vertices in $GP(10,2)$ blue then clearly we have broken the symmetries including all of the rotations and reflections as well as all of the order 3 rotations about axes through opposite vertices. All that needs to be checked is that this coloring breaks the order 2 automorphisms described above. Using this coloring in Groups and Graphs, we can see that indeed all symmetries of $GP(10,2)$ are broken.

Now consider the case when $k^2 \equiv \pm 1\,(mod\,n)$. It was shown above that the automorphism groups of the graphs $GP(n,k)$ included the rotations, reflections, and the automorphism α switching the outer rim and the inner rim except for the cases $(4,1)$, $(5,2)$, $(8,3)$, $(10,3)$, $(12,5)$, and $(24,5)$. Excluding these cases, if we color u_0, u_2, and u_3 red and the rest of the vertices blue, then clearly we see that all of the symmetries are broken.

Using Groups and Graphs, it is possible to show that for the cases $GP(8,3)$, $GP(10,3)$, $GP(12,5)$, and $GP(24,5)$, $D(GP(n,k)) = 2$. In particular, if we color the vertices u_0, u_2 and u_3 red and the rest of the vertices in $GP(n,k)$ blue as above then it turns out that this is a 2-distinguishing coloring for the cases $GP(8,3)$, $GP(10,3)$, $GP(12,5)$, and $GP(24,5)$.

We can think of $GP(4,1)$ as the three dimensional cube. It is known that there are 48 automorphisms in $Aut(GP(4,1))$. These can be described in terms of the cube so that there are 12 rotations about an axes through the center of a face (4 rotations in each of the 3 dimensions), 12 reflections about lines through two opposite vertices on a face or through the center of two opposite edges of a face (4 reflections in each of the three dimenstions), 12 rotations about axes through antipodal vertices in the cube (3 rotations for each of the 4 pairs of antipodal vertices), and 12 symmetries exchanging antipodal vertices and then rotating about axes through antipodal vertices (3 rotations for each of the 4 pairs of antipodal vertices.)

It turns out that there is no 2-distinguishing coloring of $GP(4,1)$. Suppose that there were a 2-distinguishing coloring of $GP(4,1)$. Then we must find a set A of the 8 vertices to color red and a set B to color blue such that every nontrivial automorphism sends a red vertex to a blue vertex. Without loss of generality, there are only four cases to consider:

1. Suppose $|A| = 1$ and $|B| = 7$. Without loss of generality, suppose that u_0 is the red vertex. Then every nontrivial automorphism not in St_v sends u_0 to a blue vertex. There is at least one, for example a rotation about the axes through the center of any of the faces.

2. Suppose $|A| = 2$ and $|B| = 6$. Without loss of generality, suppose that u_0 is one of the two red vertices. If the other red vertex is any vertex except the antipodal vertex, then there is a reflection exchanging the two, thus fixing the coloring. If the other vertex is the antipodal one, then there is a symmetry switching them.

3. Suppose $|A| = 3$ and $|B| = 5$. We first consider the case when two of the red vertices are antipodal, say for instance u_0 and v_2. Then the third red vertex will be adjacent to one of u_0 or v_2 and diagonal on a face from the other. Thus there is a (nontrivial) reflection about the line through that diagonal fixing each of the red vertices. Now suppose that none of the three are antipodal but two of them are adjacent, say u_0 and u_1. Then the third vertex cannot be v_2 or v_3 and so the three must lie on the same face. Thus there is a reflection about a line through one of them, switching the other two. Finally, suppose that none of the three are antipodal and none of them are adjacent. If we choose u_0 and u_2 to be red, then the other red vertex is either v_1 ro v_3. In either case, the three red vertices are adjacent to a common vertex (either u_1 or u_3), and there is a rotation about a line through that vertex rotating the three red vertices.

4. Suppose $|A| = 4$ and $|B| = 4$. First suppose that all three red vertices are on the same face. Then clearly any rotation about the axis through the center of that face is a symmetry fixing the red vertices. Now suppose that no more than three red vertices are on the same face. Without loss of generality, suppose that u_0, u_1 and u_2 are red. Then the fourth red vertex could be v_1, but reflecting about the line through u_1 and v_1 fixes the red. The fourth could be v_3, but reflecting through the plane containing u_1, v_1, u_3, and v_3 fixes the red. Finally the fourth could be v_2 or v_0, but in either case the composition of two reflections fixes the red. Now suppose that no more than two red vertices lie on a face and suppose that u_0 is red. Then the second red vertex could be u_1 , in which case the other two red vertices are forced to be v_2 and v_3, but there is a reflection fixing all of these red vertices. (The case in which the second red vertex is u_3 is similar.) If the second red vertex is u_2, then the other two red vertices could be v_0 and v_2 or v_1 and v_3. In the former case, there is a reflection fixing the red, and in the latter, there is a rotation fixing the red. Finally, the case in which a face contains no more than one red vertex is impossible.

Thus we have exhausted all of the cases for a coloring using 2 colors for $GP(4, 1)$ and we must conclude that the disinguishing number of $GP(4, 1)$ must be greater than or equal to 3. Figure 8.7 contains a 3-distinguishing coloring of $GP(4, 1)$ and so $D(GP(4, 1)) = 3$.

It was already noted in [1] that $D(GP(5, 2)) = 3$, thus we have exhausted all of the cases. □

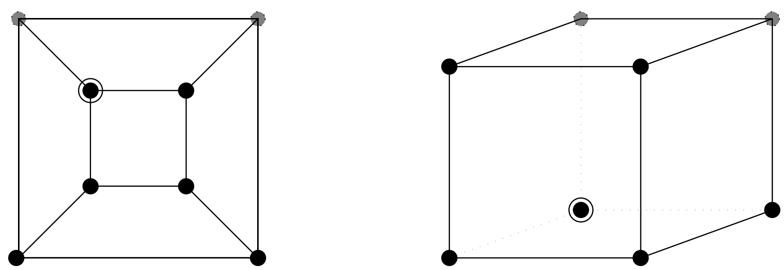

Figure 8.7: A 3-distinguishing coloring of $GP(4, 1)$

Chapter 9

Conclusions and Conjectures

As discovered in the results above, finding the distinguishing number of a given graph is not always a trivial problem. Nonintuitively, it turns out that in several cases the fewer the number of vertices the more colors needed to disinguish the graph. This was seen in the example of the cyclic graph C_n, other graphs which realize D_n, as well as the generalized Petersen graphs.

An interesting idea to consider would be to let a proper nontrivial subgroup H of the automorphism group of a given graph G act on the vertices in G. Knowing that the distinguishing number of G under the action of H is k, then what can be said about the distinguishing number of G under the action of the entire automorphism group? Certainly there are cases in which an automorphism not in the subgroup fixes the coloring disintinguished under the action of the subgroup. Perhaps another coloring exists using the same number of colors such that the graph is disinguished under the action of the entire automorphism group. Perhaps more colors are needed to distinguish the graph under the action of the automorphism group. It would be interesting to see a pattern of such cases. For instance, is there an upper bound on the distinguishing number of a graph knowing the disinguishing number of a graph under the action of a subgroup?

Another interesting idea to consider would be to see if there is a relation between the distinguishing number of two graphs G_1 and G_2 and the distinguishing number of $G_1 \times G_2$, $G_1 \vee G_2$ or $G_1 \wedge G_2$. Before analyzing this idea, it would be necessary to see if there is any relation between the automorphism groups of G_1 and G_2 and the automorphism groups of $G_1 \times G_2$, $G_1 \vee G_2$ or $G_1 \wedge G_2$.

Finally, does the fact that a graph G is edge-transitive have anything to do with the distinguishing number of a graph? If so, does this give us an upper bound on the distinguishing number?

Appendix A

Tables of Congruences

The first table contains values of n and k for which $k^2 \equiv 1 \,(mod\, n)$. The second contains values of n and k for which $k^2 \equiv -1 \,(mod\, n)$.

$$k^2 \equiv 1 \,(mod\, n)$$

n	k	n	k	n	k	n	k	n	k	n	k
8	3	45	19	72	17	93	32	115	24	135	26
12	5	48	7	72	19	95	39	116	57	136	33
15	4	48	17	72	35	96	17	117	53	136	35
16	7	48	23	75	26	96	31	119	50	136	67
20	9	51	16	76	37	96	47	120	11	138	47
21	8	52	25	77	34	99	10	120	19	140	29
24	5	55	21	78	25	100	49	120	29	140	41
24	7	56	13	80	9	102	35	120	31	140	69
24	11	56	15	80	31	104	25	120	41	141	46
28	13	56	27	80	39	104	27	120	49	143	12
30	11	57	20	84	13	104	51	120	59	144	17
32	15	60	11	84	29	105	29	123	40	144	55
33	10	60	19	84	41	105	34	124	61	144	71
35	6	60	29	85	16	105	41	126	55	145	59
36	17	63	8	87	28	108	53	128	63	147	50
39	14	64	31	88	21	110	21	129	44	148	73
40	9	65	14	88	23	111	38	130	51	150	49
40	11	66	23	88	43	112	15	132	23		
40	19	68	33	91	19	112	41	132	43		
42	13	69	22	91	27	112	55	132	65		
44	21	70	29	92	45	114	37	133	20		

$$k^2 \equiv -1 \,(mod\, n)$$

n	k	n	k	n	k
5	2	58	17	106	23
10	3	61	11	109	33
13	5	65	8	113	15
17	4	65	18	122	11
25	7	73	27	125	57
26	5	74	31	130	47
29	12	82	9	130	57
34	13	85	13	137	37
37	6	85	38	145	12
41	9	89	34	145	17
50	7	97	22	146	27
53	23	101	10	149	44

Appendix B

Group Orders

The table on the following page contains the orders of $GP(n, k)$ for $n \leq 27$.

Graph	Order	Graph	Order	Graph	Order
$GP(5,2)$	$120 = 24n$	$GP(19,3)$	$38 = 2n$	$GP(25,3)$	$50 = 2n$
$GP(7,2)$	$14 = 2n$	$GP(19,4)$	$38 = 2n$	$GP(25,4)$	$50 = 2n$
$GP(7,3)$	$14 = 2n$	$GP(19,5)$	$38 = 2n$	$GP(25,6)$	$50 = 2n$
$GP(8,3)$	$96 = 12n$	$GP(19,6)$	$38 = 2n$	$GP(25,7)$	$100 = 4n$
$GP(9,2)$	$18 = 2n$	$GP(19,7)$	$38 = 2n$	$GP(25,8)$	$50 = 2n$
$GP(9,4)$	$18 = 2n$	$GP(19,8)$	$38 = 2n$	$GP(25,9)$	$50 = 2n$
$GP(10,3)$	$240 = 24n$	$GP(19,9)$	$38 = 2n$	$GP(25,11)$	$50 = 2n$
$GP(11,3)$	$22 = 2n$	$GP(20,3)$	$40 = 2n$	$GP(25,12)$	$50 = 2n$
$GP(11,4)$	$22 = 2n$	$GP(20,7)$	$40 = 2n$	$GP(26,3)$	$52 = 2n$
$GP(11,5)$	$22 = 2n$	$GP(20,9)$	$80 = 4n$	$GP(26,5)$	$104 = 4n$
$GP(12,5)$	$144 = 12n$	$GP(21,2)$	$42 = 2n$	$GP(26,7)$	$52 = 2n$
$GP(13,2)$	$26 = 2n$	$GP(21,4)$	$42 = 2n$	$GP(26,9)$	$52 = 2n$
$GP(13,4)$	$26 = 2n$	$GP(21,5)$	$42 = 2n$	$GP(26,11)$	$52 = 2n$
$GP(13,5)$	$52 = 4n$	$GP(21,8)$	$84 = 4n$	$GP(27,2)$	$54 = 2n$
$GP(13,6)$	$26 = 2n$	$GP(21,10)$	$42 = 2n$	$GP(27,4)$	$54 = 2n$
$GP(14,3)$	$28 = 2n$	$GP(22,3)$	$44 = 2n$	$GP(27,5)$	$54 = 2n$
$GP(14,5)$	$28 = 2n$	$GP(22,5)$	$44 = 2n$	$GP(27,7)$	$54 = 2n$
$GP(15,2)$	$30 = 2n$	$GP(22,7)$	$44 = 2n$	$GP(27,8)$	$54 = 2n$
$GP(15,4)$	$60 = 4n$	$GP(22,9)$	$44 = 2n$	$GP(27,10)$	$54 = 2n$
$GP(15,7)$	$30 = 2n$	$GP(23,2)$	$46 = 2n$	$GP(27,11)$	$54 = 2n$
$GP(16,3)$	$32 = 2n$	$GP(23,3)$	$46 = 2n$	$GP(27,13)$	$54 = 2n$
$GP(16,5)$	$32 = 2n$	$GP(23,4)$	$46 = 2n$		
$GP(16,7)$	$64 = 4n$	$GP(23,5)$	$46 = 2n$		
$GP(17,2)$	$34 = 2n$	$GP(23,6)$	$46 = 2n$		
$GP(17,3)$	$34 = 2n$	$GP(23,7)$	$46 = 2n$		
$GP(17,4)$	$68 = 4n$	$GP(23,8)$	$46 = 2n$		
$GP(17,5)$	$34 = 2n$	$GP(23,9)$	$46 = 2n$		
$GP(17,6)$	$34 = 2n$	$GP(23,10)$	$46 = 2n$		
$GP(17,7)$	$34 = 2n$	$GP(23,11)$	$46 = 2n$		
$GP(17,8)$	$34 = 2n$	$GP(24,5)$	$288 = 12n$		
$GP(18,5)$	$36 = 2n$	$GP(24,7)$	$96 = 4n$		
$GP(18,7)$	$36 = 2n$	$GP(24,11)$	$96 = 4n$		
$GP(19,2)$	$38 = 2n$	$GP(25,2)$	$50 = 2n$		

Appendix C

10-circuits in $GP(26, 5)$

Type	$r(C)$	$s(C)$	$t(C)$	Circuit representation	Circuit?
	7	2	1	$u_0u_1u_2u_3u_4u_5u_6u_7v_7v_0$	No
	6	2	2	$u_0u_1u_2u_3u_4u_5u_6v_6v_{11}v_0$	No
	6	2	2	$u_0u_1u_2u_3u_4u_5u_6v_6v_1v_0$	No
	5	2	2	$u_0u_1u_2u_3u_4u_5v_5v_{10}v_{15}v_0$	No
	4	4	2	$u_0u_1u_2u_3v_3v_8u_8u_9v_9v_0$	No
	4	4	2	$u_0u_1u_2u_3v_3v_8u_8u_7v_7v_0$	No
	4	4	2	$u_0u_1u_2u_3v_3v_{24}u_{24}u_{23}v_{23}v_0$	No
	4	4	2	$u_0u_1u_2u_3v_3v_{24}u_{24}u_{25}v_{25}v_0$	No
	4	4	2	$u_0u_1u_2v_2v_7u_7u_8u_9v_9v_0$	No
1	4	4	2	$u_0u_1u_2v_2v_7u_7u_6u_5v_5v_0$	Yes
1’	4	4	2	$u_0u_1u_2v_2v_{23}u_{23}u_{22}u_{21}v_{21}v_0$	Yes
	4	4	2	$u_0u_1u_2v_2v_{23}u_{23}u_{24}u_{25}v_{25}v_0$	No
	4	2	4	$u_0u_1u_2u_3u_4v_4v_9v_{14}v_{19}v_0$	No
	4	2	4	$u_0u_1u_2u_3u_4v_4v_{25}v_{20}v_{15}v_0$	No
	3	4	3	$u_0u_1u_2v_2v_7v_{12}u_{12}u_{13}v_{13}v_0$	No
	3	4	3	$u_0u_1u_2v_2v_7v_{12}u_{12}u_{11}v_{11}v_0$	No
	3	4	3	$u_0u_1u_2v_2v_{23}v_{18}u_{18}u_{17}v_{17}v_0$	No
	3	4	3	$u_0u_1u_2v_2v_{23}v_{18}u_{18}u_{19}v_{19}v_0$	No
	3	4	3	$u_0u_1u_2v_2v_7u_7u_6v_6v_1v_0$	No
	3	4	3	$u_0u_1u_2v_2v_7u_7u_6v_6v_{11}v_0$	No

Type	$r(C)$	$s(C)$	$t(C)$	Circuit representation	Circuit?
	3	4	3	$u_0u_1u_2v_2v_7u_7u_8v_8v_3v_0$	No
	3	4	3	$u_0u_1u_2v_2v_7u_7u_8v_8v_{13}v_0$	No
	3	4	3	$u_0u_1u_2v_2v_{23}u_{23}u_{22}v_{22}v_{17}v_0$	No
	3	4	3	$u_0u_1u_2v_2v_{23}u_{23}u_{22}v_{22}v_1v_0$	No
	3	4	3	$u_0u_1u_2v_2v_{23}u_{23}u_{24}v_{24}v_3v_0$	No
	3	4	3	$u_0u_1u_2v_2v_{23}u_{23}u_{24}v_{24}v_{19}v_0$	No
	2	4	4	$u_0u_1v_1v_6v_{11}v_{16}u_{16}u_{15}v_{15}v_0$	No
	2	4	4	$u_0u_1v_1v_6v_{11}v_{16}u_{16}u_{17}v_{17}v_0$	No
	2	4	4	$u_0u_1v_1v_{22}v_{17}v_{12}u_{12}u_{11}v_{11}v_0$	No
	2	4	4	$u_0u_1v_1v_{22}v_{17}v_{12}u_{12}u_{13}v_{13}v_0$	No
2	2	4	4	$u_0u_1v_1v_6v_{11}u_{11}u_{10}v_{10}v_5v_0$	Yes
	2	4	4	$u_0u_1v_1v_6v_{11}u_{11}u_{10}v_{10}v_{15}v_0$	No
	2	4	4	$u_0u_1v_1v_6v_{11}u_{11}u_{12}v_{12}v_7v_0$	No
	2	4	4	$u_0u_1v_1v_6v_{11}u_{11}u_{12}v_{12}v_{17}v_0$	No
	2	4	4	$u_0u_1v_1v_{22}v_{17}u_{17}u_{16}v_{16}v_{11}v_0$	No
2'	2	4	4	$u_0u_1v_1v_{22}v_{17}u_{17}u_{16}v_{16}v_{21}v_0$	Yes
	2	4	4	$u_0u_1v_1v_{22}v_{17}u_{17}u_{18}v_{18}v_{13}v_0$	No
	2	4	4	$u_0u_1v_1v_{22}v_{17}u_{17}u_{18}v_{18}v_{23}v_0$	No
	2	2	6	$u_0u_1u_2v_2v_7v_{12}v_{17}v_{22}v_1v_0$	No
	2	2	6	$u_0u_1u_2v_2v_{23}v_{18}v_{13}v_8v_3v_0$	No
	1	2	7	$u_0u_1v_1v_6v_{11}v_{16}v_{21}v_0$	No
	1	2	7	$u_0u_1v_1v_{22}v_{17}v_{12}v_7v_2v_{23}v_0$	No

Bibliography

[1] Michael O. Albertson, Karen L. Collins (1996). Symmetry Breaking in Graphs, *The Electronic Journal of Combinatorics 3.*

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

[3] Robert Frucht, J. E. Graver, M. Watkins. The groups of the generalized Petersen graphs, *Proceedings of the Cambridge Philosophical Society* **70**, (1971), 211-218.

[4] Jonathon L. Gross, Thomas W. Tucker. *Topological Graph Theory.* John Wiley & Sons, Inc.: New York, 1987.

[5] Israel Grossman, Wilhelm Magnus. *Groups and their Graphs.* The Mathematical Association of America: Yale University, 1964.

[6] Fred Roberts. *Applied Combinatorics.* Prentice-Hall, Inc.: Englewood Cliffs,NJ, 1984.

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

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

Vita

Karen Sue Potanka was born in New Britain, Connecticut on February 18, 1975. Karen was raised in Cumberland, Maryland until she first attended Virginia Tech in August of 1993. As an undergraduate, she participated in two Research Experience for Undergraduates (REU) programs, one at the University of Oklahoma and the other at Northern Arizona University. Because of her experience in research, she was named a Barry M. Goldwater scholar in 1996 and was asked to present her research in graph theory at two national conferences in 1997. She graduated summa cum laude with an "in Honors" Bachelor of Science degree in Mathematics in May of 1997. She was named Outstanding Graduating Senior and received the Layman Prize for her research in graph theory. As a graduate student, Karen worked on another research project in graph theory. She received a Master of Science in Mathematics from Virginia Tech in 1998 as part of the Five Year Bachelor/Master's program.