Hurwitz Equivalence in Dihedral Groups

Emily Berger

Massachusetts Institute of Technology

ERB90@mit.edu

Submitted: Nov 18, 2009; Accepted: Jan 25, 2010; Published: Feb 21, 2011

Mathematics Subject Classification: 20F36, 20F55

Abstract

In this paper we determine the orbits of the braid group B_n action on G^n when G is a dihedral group and for any $T \in G^n$. We prove that the following invariants serve as necessary and sufficient conditions for Hurwitz equivalence. They are: the product of its entries, the subgroup generated by its entries, and the number of times each conjugacy class (in the subgroup generated by its entries) is represented in T.

Introduction

Let G be a group and G^n be the cartesian product of G with itself n times. The braid group B_n acts on G^n by Hurwitz moves. We study the orbits of this action when G is a dihedral group. When the tuple $T \in G^n$ consists only of reflections, the orbits are determined by the following invariants: the product of the entries, the subgroup generated by the entries, and the number of times each conjugacy class (in the subgroup generated by its entries) is represented in T.

Our study of Hurwitz equivalence in the dihedral group was inspired by the paper [1], which gives a simple criterion for Hurwitz equivalence in the symmetric group analogous to our Main Theorem. That paper studies tuples of transpositions in the symmetric group, which is the reason why we originally chose to restrict to reflections in the dihedral group. (Recall that the symmetric group $\mathfrak{S}_m$ acts on $\mathbb{R}^{m-1}$ in such a way that every transposition acts by a Euclidean reflection.) Utlimately, we extend these results to include rotations as well.

After the bulk of this work was completed we discovered the paper [3] that considers, using a different method, the case of a dihedral group of order $2p^\alpha$ where p is prime. Our results were obtained independently and cover the case of dihedral groups of any order. In addition, after this paper was finished, [5] was published, extending the results of [3]. The results of our paper are complementary to the work in [5], since our results are derived from first principles using what is perhaps a more intuitive approach.

1 Definitions

1.1 The Braid Group

The braid group on n strands, B_n, may be described by $n-1$ generators $\sigma_1, ..., \sigma_{n-1}$ and the following defining relations.

$$\sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{if} \quad |i-j| \geq 2$$

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$$

1.2 Hurwitz Moves

Consider G^n, the set of tuples of length n with entries in G. The braid group acts on G^n by Hurwitz moves. Let $T = (a_1, a_2, ..., a_n)$ with $a_i \in G$. In this sense, σ_i, a Hurwitz move, may be realized as the following.

$$\sigma_i T = (a_1, ..., a_i a_{i+1} a_i^{-1}, a_i, ..., a_n)$$

It must be shown that the defining relations as seen in the presentation of B_n hold. Clearly, σ_i and σ_j commute when $|j-i| \geq 2$. The second relation is more subtle. Assume T has length three for simplicity.

$$\begin{aligned} \sigma_1 \sigma_2 \sigma_1 T &= \left(\left(a_1 a_2 a_1^{-1}\right) \left(a_1 a_3 a_1^{-1}\right) \left(a_1 a_2 a_1^{-1}\right)^{-1}, a_1 a_2 a_1^{-1}, a_1 \right) \\ &= \left(a_1 a_2 a_3 a_2^{-1} a_1^{-1}, a_1 a_2 a_1^{-1}, a_1\right) \\ &= \sigma_2 \sigma_1 \sigma_2 T \end{aligned}$$

Also, inverse Hurwitz moves are defined by $\sigma_i^{-1}(...a_i, a_{i+1}, ...) \to (...a_{i+1}, a_{i+1}^{-1} a_i a_{i+1}...)$. With this action, we may study the orbits of the elements of G^n, motivating the following definition.

1.3 Hurwitz Equivalence

Two elements $T, T' \in G^n$ are defined to be Hurwitz equivalent if there exists a finite sequence of Hurwitz moves transforming T into T'. Equivalently, $T \sim T'$ if both are contained in the same orbit.

2 Necessary Conditions for Hurwitz Equivalence

Let $T = (a_1, ..., a_n)$ and $T' = (a'_1, ..., a'_n)$ be elements of G^n. Certain properties of T are invariant under Hurwitz moves. These properties will serve as necessary conditions for Hurwitz Equivalence.

2.1 Product of the Elements T

Define $\prod T = a_1 a_2 ... a_n$, then $T \sim T'$ implies $\prod T = \prod T'$.

Proof. Any σ_i transforms $T = (..., a_i, a_{i+1}, ...)$ to $\tilde{T} = (..., a_i a_{i+1} a_i^{-1}, a_i, ...)$.

$$\prod \tilde{T} = a_1 ... a_i a_{i+1} a_i^{-1} a_i ... a_n = a_1 ... a_i a_{i+1} ... a_n = \prod T$$

Therefore, any Hurwitz move preserves $\prod T$, so $T \sim T'$ implies $\prod T = \prod T'$. □

2.2 Subgroup Generated by Elements in T

Suppose T and T' generate subgroups S and S' respectively, if $T \sim T'$ then $S = S'$.

Proof. $T \sim T'$ implies there exists some sequence of Hurwitz moves transforming T into T'. If a and b are in S, so is aba^{-1}, so $S \subseteq S'$. By symmetry and the use of inverse Hurwitz moves, $S' \subseteq S$, so $S = S'$. □

2.3 The number of times each conjugacy class of S occurs in T

$T \sim T'$ implies the number of times each conjugacy class with respect to the subgroup $S = S'$ appears in T is the same as in T'.

Proof. Notice that σ_i acts as the transposition $(i\ i{+}1)$ on conjugacy classes in T. Without loss of generality, let $i = 1$ and $n = 2$.

$$\sigma_1(a_1, a_2) = (a_1 a_2 a_1^{-1}, a_1)$$

Clearly, a_1 is in the conjugacy class of a_1 and $a_1 a_2 a_1^{-1}$ in that of a_2. Therefore, σ_i only transposes elements of conjugacy classes, and thus leaves the number of elements in each conjugacy class fixed. □

2.4 Main Theorem

Theorem 2.1. *Let G be a dihedral group of order $2m$ and T, T' tuples of length N whose entries are elements of D_m. The necessary conditions stated above for an arbitrary group G serve as sufficient conditions for $T \sim T'$.*

We first prove the main theorem for T containing only reflections, we call this the reflection main theorem. We then generalize to all $T \in D_m^n$.

3 Preliminaries and the Main Lemma

Before proving the reflection main theorem, we fix notation and present elementary facts about the dihedral group. In addition, we prove the main lemma which will be used in Section 4.

3.1 Notation

We define notation by labeling the vertices and edges of a polygon. Firstly, alter the polygon by adjoining a vertex to the mid-point of each edge. Begin by labeling some adjoined vertex 1 and continue in the counterclockwise direction alternately numbering adjoined vertices and regular vertices 1 through m twice. Images of the numbering for $m = 5$ and $m = 6$ are below.

Define the line connecting the pair of vertices (adjoined or normal) labeled i to be l_i and the reflection fixing l_i to be r_{l_i}, or simply r_i. In addition, define the distance between two reflections $d(r_i, r_j)$ to be the length of the minimal path through adjoined and regular vertices connecting some vertex on l_i to some vertex on l_j.

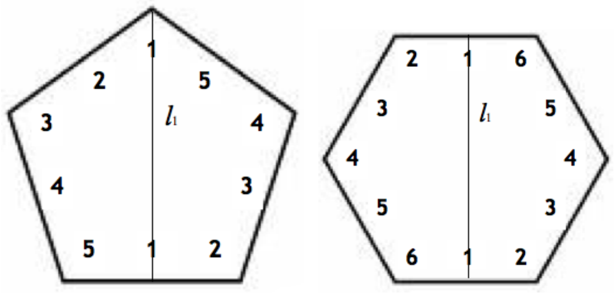

Figure 1: Numbering of reflections

3.2 Conjugation and Products in the Dihedral Group

In order to understand the action of B_n, conjugation of reflections by reflections and products of reflections must be explained.

3.2.1 Conjugation of reflections by reflections

In general, conjugation by a reflection has the following formula

$$r_i r_j r_i = r_{r_i(l_j)}$$

where $r_i(l_j)$ represents the line to which r_i maps l_j. Geometrically, $r_i(l_j)$ is the line symmetric to l_j with respect to reflecting about l_i, namely l_k where $k - i = i - j$ or $k = i + (i - j)$.

Lemma 3.1.

$$r_i r_j r_i = r_{i+(i-j)}$$

Corollary 3.2. *The product $r_i r_j r_i$ may also be written as $r_{j+2(i-j)}$ which shows that when m is even, not all reflections are conjugate to each other. They are split into edge-edge refections and vertex-vertex reflections because r_k and $r_{k'}$ are conjugate if and only if $k' - k \equiv 0$ (mod 2).*

3.2.2 Product of two reflections

Consider the product of two reflections, say $r_i r_j$. The product of any two reflections must be some rotation. By definition, r_j fixes l_j, so the rotation is determined by which line l_j gets mapped to by r_i. Geometrically, it is clear that this line is l_k where $i - j = k - i$. Therefore, if we fix counterclockwise to be the positive direction, $r_i r_j$ is a rotation through $(i-j)\frac{2\pi}{m}$.

Lemma 3.3.

$$\textit{The product } r_i r_j \textit{ is a rotation through } (i-j)\frac{2\pi}{m}.$$

Lemma 3.4. *The the orbit of* (r_i, r_j) *is* $O = \{(r_{i+k(i-j)}, r_{i+(k-1)(i-j)}) \mid k \in \mathbb{Z}_m\}$

Proof. By Lemma 3.1,

$$(r_i, r_j) \sim \sigma(r_i, r_j) = (r_i r_j r_i, r_i) = (r_{i+(i-j)}, r_i).$$

Since $i + (i-j) - i = i - j$, the above shows σ_i does not change the the difference between the i^{th} and $i + 1^{st}$ entries. For fixed k we have

$$\sigma(r_{i+k(i-j)}, r_{i+(k-1)(i-j)}) = (r_{i+(k+1)(i-j)}, r_{i+(k)(i-j)})$$

since

$$i + (k+1)(i-j) = i + k(i-j) + \Big(i + k(i-j)\Big) - \Big(i + (k-1)(i-j)\Big).$$

We apply σ (at times we will omit the i attached to σ_i) in repetition to obtain the orbit O of (r_i, r_j).

$$O = \{(r_{i+k(i-j)}, r_{i+(k-1)(i-j)}) \mid k \in \mathbb{Z}_m\}$$

□

We remark that the size of the orbit is determined by the smallest $k > 0$ *such that* $k(i-j) \equiv 0 \pmod m$*. At this time, the first entry of the pair has returned to* r_i*, causing the second to return to* r_j*.*

Remark 1. The subgroups of D_m including reflections are isomorphic to D_k where k divides m.

Theorem 3.5. *Define* $D = gcd(i-j, m)$*. The size of* O *is* $\frac{m}{D}$ *and the reflections of* O *generate a subgroup with index* D *in* D_m*, isomorphic to* $D_{\frac{m}{D}}$*.*

Corollary 3.6. *If the* $gcd(i-j, m) = 1$*, the orbit of* (r_i, r_j) *is of size* m *and contains all pairs* $(r_{i'}, r_{j'})$ *where* $i' - j' = i - j$*. In otherwords,* $(r_k, r_{k-(i-j)}) \in O$ *for all* k*. The reflections in* O *generate* D_m*.*

3.3 Main Lemma

Lemma 3.7. *Given a tuple T of length greater than two whose entries generate D_m, we may pull a pair of reflections $(r, r') \in D_m^2$ to the left most or right most positions of T given gcd$(d(r, r'), m) = 1$.*

Proof. The case in which T is constant is trivial, so assume otherwise. Consider all the pairwise distances of reflections, choose the pair with the smallest positive difference, say (r_i, r_j). Using Hurwitz moves, we may move any reflection rightward leaving it unchanged. Suppose r_i is to the left of r_j in T, move r_i rightward until r_i and r_j are adjacent. We have altered T using Hurwitz moves to form some equivalent but likely different tuple $\tilde{T}$. Consider the orbit O of (r_i, r_j). The subgroup generated by O is the subgroup S generated by r_i and r_j. There are two cases, either there exist reflections in $\tilde{T}$ outside of S, or there do not. We discuss both cases separately.

If there do not exist reflections in $\tilde{T}$ outside of S, then $\tilde{T}$ generates S, which implies T does as well. By assumption, T generates D_m so S must be D_m, and therefore $\gcd(d(r_i, r_j), m) = 1$. Assume there is a reflection r_k immediately to the left of the pair (r_i, r_j) (if there is not move the pair (r_i, r_j) to the right so that there is). Because $\gcd(d(r_i, r_j), m) = 1$, we may transform (r_i, r_j) into $(r_{i'}, r_{j'})$ so that $d(r_k, r_{i'},) = d(r, r')$ with the correct orientation so that $r_k r_{i'} = rr'$. Move the pair $(r_k, r_{i'})$ to the left-most or right-most positions unchanged and apply Hurwitz moves to transform $(r_k, r_{i'})$ into (r, r').

On the other hand, suppose now that there does exist some reflection R in $\tilde{T}$ outside of S. Suppose S has index D in D_m. R must lie between some $s, s' \in S$ of distance D apart with $D \leq d(r_i, r_j)$. Apply Hurwitz moves to (r_i, r_j) until s or s' is in the tuple, creating a pair of reflections with distance strictly less than D. Continue to reduce D in this manner until the current pair generates D_m as in the above case. This must occur eventually because when $D = 1$, D_m is generated.

□

4 Proof of the Reflection Main Theorem

4.1 Proof Structure

We prove the reflection main theorem for the case when T generates the whole group D_m. If it does not, it must generate some subgroup isomorphic to D_k for some k. Applying the reflection main theorem to T as if the group in question is in fact D_k is sufficient. We begin by proving the theorem for when $\prod T = I$ and later extend it to arbitrary products of T. Recall in this case, T may only contain reflections.

4.2 Hurwitz Equivalence when $\prod T = I$

4.2.1 Canonical forms

We will prove our claim by using Hurwitz moves to transform any T into a particular canonical form. In the case where m is odd, this form is $(r_0, ..., r_0, r_1, r_1)$.

The canonical form chosen for even m differs slightly from the odd case. When m is even, we will use the following lemma to motivate the choice of canonical form.

Lemma 4.1. *Let m be even. If $\prod T = I$, then the number of reflections from each conjugacy class must be even.*

Proof. Assume for the sake of contradiction the numbers of reflections from each conjugacy class in T are odd. Transform T into an equivalent $\tilde{T}$ with all edge-edge reflections to the left and all vertex-vertex reflections to the right. We have

$$T \sim \tilde{T} = (\Delta, \Delta') \text{ with } \prod \tilde{T} = I$$

The product of an odd number of edge-edge reflections must be an edge-edge reflection and the analogous is true for vertex-vertex reflections. Therefore, $\prod \Delta \neq \prod \Delta'$, but $\prod \Delta \prod \Delta' = I$. There do not exist a pair of distinct reflections whose product is I, which is a contradiction. □

Suppose T contains $2n_v$ vertex-vertex reflections and $2n_e$ edge-edge reflections. Both n_v and $n_e > 0$, else T does not generate D_m. T will be transformed into $(r_0, ..., r_0, r_1, ..., r_1)$ with exactly $2n_v$ r_0 reflections and $2n_e$ r_1 reflections.

4.2.2 Transformation moves

We show we may transform T into the canonical forms described above using the following moves.

Proof. The way we transform T into its canonical from depends on m. For m odd, we show that we may transform T into the following

$$T \sim (r_0, r_0, T').$$

When m is even and T contains more than two vertex-vertex reflections, we show

$$T \sim (r_0, r_0, T').$$

Similarly, when m is even and T contains more than two edge-edge reflections, we show

$$T \sim (T', r_1, r_1).$$

In each case, T' is arbitrary except that we require the entries of T' to generate D_m. Assuming we may apply the transformations above (we will prove that we may in Lemma 4.2), we show how to transform T into the desired canonical form.

When m is odd we continue pulling out pairs (r_0, r_0) left, leaving a tuple of four rightward entries.

When m is even, while the number of vertex-vertex reflections is greater than two, we move pairs (r_0, r_0) leftward and while the number of edge-edge reflections is greater than two, we move pairs (r_1, r_1) rightward. At the end of this process, we are left with a tuple of length four.

In each case, call the remaining tuple of length four τ. When m is odd, τ consists of the four right-most reflections of T. When m is even, τ may lie in the middle of T as well. By the way we transformed T, we know that $\prod \tau = 1$ and the entries of τ generate D_m. We transform τ into the canonical form (r_0, r_0, r_1, r_1).

Proof.

$$\tau \sim (r_0, r_1, r_k, r_{k-1}) \sim (r_0, r_1, r_2, r_1) \sim (r_0, r_0, r_1, r_1)$$

The main lemma may be used to fix the first two entries as (r_0, r_1). The last two entries must then differ by one, since $\prod \tau = I$. A sequence of σ_3's and σ_2's are then applied to arrive at the canonical form (r_0, r_0, r_1, r_1). □

In both m odd and m even cases, we have arrived at our described canonical form. □

Lemma 4.2. *We may transform T in the ways described by* 4.2.2.

Proof. Suppose T has length greater than 4, by Lemma 3.7 we may transform T into the following

$$T \sim (r_0, r_1, \Delta)$$

and continue by moving r_1 to the right to obtain

$$T \sim (r_0, r_1, \Delta) \sim (r_0, \Delta', r_1).$$

We have $\prod(\Delta') = r_0 r_1$ is a rotation through $\frac{2\pi}{m}$ by Lemma 3.3, which implies the subgroup generated by Δ' is D_m. Applying Lemma 3.7 again,

$$T \sim (r_0, \Delta', r_1) \sim (r_0, r_0, r_{-1}, \Delta'', r_1)$$

T has now been reduced to a pair (r_0, r_0) and the tuple $T' = (r_{-1}, \Delta'', r_1)$.

When m is odd, the reflections in T' must generate D_m because r_{-1} and $r_1 \in T'$ and are distance two apart, which is relatively prime to m.

When m is even and T contains more than two vertex-vertex reflections, while the orbit of r_{-1}, r_1 only contains edge-edge reflections, it contains all of them. We have Δ'' must contain a vertex-vertex reflection, which must be distance one from some edge-edge reflection, all of which are generated. Therefore T' generates D_m and we are done.

At this point we have shown that when m is odd or m is even and T contains more than two vertex-vertex reflections, we may transform T into a pair (r_0, r_0) and T' such that $\prod T' = I$ and the entries of T' generate D_m.

Below we briefly show without explanation how to remove a pair (r_1, r_1) to the right leaving some T' which satisfies the same conditions as above for the case where m is even and T contains more than two edge-edge reflections.

$$T \sim (\Delta, r_0, r_1) \sim (r_0, \Delta', r_1) \sim (r_0, \Delta'', r_2, r_1, r_1).$$

This concludes the proof. □

4.3 Arbitrary Products

To prove the entirety of the reflection main theorem, cases in which $\prod T \neq I$ must be resolved. Before proceeding, we prove the following lemma.

4.4 Number Theory Lemmas

Lemma 4.3. *Number Theory Lemma*

Let m be some odd positive integer. Given a fixed k with $0 \leq k < m$, there exist q, q' such that $q + q' \equiv k$ (mod m) with $gcd(q, m) = gcd(q', m) = 1$.

Proof. Consider the prime factorization $m = p_1^{\alpha_1} p_2^{\alpha_2} ... \, p_n^{\alpha_n}$. Suppose k satifies the set of congruence relations $k \equiv b_i \pmod{p_i^{\alpha_i}}$ for all $i \leq n$ while q, q' satisfy the analogous congruence relations a_i, a_i' respectively.

We examine two cases: fix i, if $b_i \not\equiv 1 \pmod{p_i}$, choose $a_i = 1$ which leaves $a_i' = b_i - 1 \not\equiv 0 \pmod{p_i}$ and hence is relatively prime to $p_i^{\alpha_i}$. In the case of $b_i \equiv 1 \pmod{p_i}$, choose $a_i = 2$, $a_i' = b_i - 2 \not\equiv 0 \pmod{p_i}$. Then a_i and a_i' are both relatively prime to $p_i^{\alpha_i}$.

By the Chinese Remainder Theorem, there exists some q which satisfies $q \equiv a_i \pmod{p_i^{\alpha_i}}$ for all i. Choose $q' = k - q$, $q' \equiv a_i' \pmod{p_i^{\alpha_i}}$ by construction. Since both a_i and a_i' are relatively prime to $p_i^{\alpha_i}$ for all i, $\gcd(q, m) = \gcd(q', m) = 1$ and $q + q' \equiv k \pmod{m}$. □

4.4.1 Generalization of the Number Theory Lemma

Lemma 4.4. *Suppose m is even and $0 \leq k < m$. When k is even, the above result still holds, namely there exist q, q' such that $q+q' \equiv k$ (mod m) with $gcd(q, m) = gcd(q', m) = 1$.*

Proof. Let $m = 2^{\alpha_1} p_2^{\alpha_2} ... \, p_n^{\alpha_n}$ where $\alpha_1 > 0$ and let $k \equiv b_1 \pmod{2^{\alpha_1}}$. Fix $a_1 \equiv 1 \pmod{2^{\alpha_1}}$ and $a_1' \equiv b_1 - 1 \pmod{2^{\alpha_1}}$ so that $a_1 + a_1' \equiv b_1 \pmod{2^{\alpha_1}}$. Since k is even, $b_1 - 1$ is relatively prime to 2^{α_1}. Combining this with the relations discussed in the m odd case and applying the Chinese Remainder Theorem results in q, q' relatively prime to m such that $q + q' \equiv k \pmod{m}$. □

Lemma 4.5. *Suppose m is even and $0 \leq k < m$. When k is odd, there exist q, q' such that $q + q' \equiv k$ (mod m) with $gcd(q, m) = gcd(\frac{q'}{2}, m) = 1$.*

Proof. Since k is odd, we know $k \equiv b_1 \pmod{2^{\alpha_1}}$ for some odd b_1. Using the same method as in the m odd case, choose a_i and a'_i for all $i > 1$. Define $c_i \equiv 2^{-1}a'_i \pmod{p_i^{\alpha_i}}$ for all $i > 1$ (by 2^{-1} we mean the multiplicative inverse of two $\pmod{p_i^{\alpha_i}}$ for each i). Now define $a_1 \equiv b_1 - 2 \pmod{2^{\alpha_1}}$, $c_1 \equiv 1 \pmod{2^{\alpha_1}}$, and finally $a'_i \equiv 2 \pmod{2^{\alpha_1}}$. Since b_1 is odd, $b_1 - 2$ is relatively prime to (2^{α_1}) and by applying the Chinese Remainder Theorem, we obtain q, q' such that $\gcd(q, m) = 1$ and $q + q' \equiv k \pmod{m}$. Applying the CRT to the c_i congruences, we get $\frac{q'}{2}$ relatively prime to m since $c_1 = 1$ which is relatively prime to (2^{α_1}) and c_i is relatively prime to $p_i^{\alpha_i}$ for all $i > 1$. □

4.5 Canonical Forms

As before, we choose canonical forms for each distinct case, first considering the case when $N > 4$.

When $\prod T = r_k$, a reflection, we transform T into a tuple of the form (Λ, r_k). When $\prod T = r_0 r_j$, a rotation, we transform T into a tuple of the form (r_0, Λ, r_j). In each case, Λ represents some tuple T' whose entries generate a subgroup that is maximal (to be described in detail below), $\prod \Lambda = I$, and Λ is in the appropriate canonical form as defined in 4.2.1. When $N = 3$, we choose the canonical form to be (r_{k-1}, r_{k-1}, r_k). When $N = 4$, and m is odd we have the canonical form $(r_0, r_{j-1}, r_{j-1}, r_j)$. When m is even, depending on the number of elements from each conjugacy class, we either have $(r_0, r_{j-1}, r_{j-1}, r_j)$ or $(r_0, r_{j-2}, r_{j-2}, r_j)$.

4.5.1 $\prod T = r_k$

Proof. When $N = 3$, we would like to transform T into (r_{k-1}, r_{k-1}, r_k). Use Lemma 3.7 to fix the right-most entries as (r_{k-1}, r_k) and $\prod T = r_k$ implies the left-most entry is r_{k-1}.

Consider the case where $\prod T = r_k$ and $N > 3$. By assumption, the entries in T must generate D_m, so we may use Lemma 3.7 to transform T in the following way.

$$T \sim (r_{k-1}, \Delta) \sim (r_{k-1}, \Delta', r_{k+1}, r_k) \sim (\Lambda, r_k)$$

We were able to use Lemma 3.7 for the second transformation because $\prod \Delta = r_{k-1} r_k$ is a rotation through $\frac{2\pi}{m}$, and therefore Δ generates D_m. We now consider T'.

In the case where m is odd, since $T' = (r_{k-1}, \Delta', r_{k+1})$, its entries generate D_m because r_{k-1} and $r_{k+1} \in T'$ and are distance two, which is relatively prime to m. Since $\prod T' = I$, we may transform T' into its canonical form, from 4.2.1, Λ and this case is complete.

When m is even, if T contains more than one reflection in k's conjugacy class, then T' generates D_m. This is true because we get the entirety of r_{k-1}'s conjugacy class from the pair (r_{k-1}, r_{k+1}) and one of these reflections must be distance one from a reflection in the conjugacy class of r_k. Again, since $\prod T' = I$, we may transform T' into its canonical form, from 4.2.1, Λ and this case is complete.

Finally, when m is even but T only contains one element from r_k's conjugacy class, we have that the entries of T' generate $D_{\frac{m}{2}}$. A reasonable canonical form to choose is that which would result from reducing the entries in T' to elements of $D_{\frac{m}{2}}$ and then transforming T' into what would be its canonical form with respect to $D_{\frac{m}{2}}$. Following this transformation, we once again view the reflections as elements of D_m and arrive at Λ. This would result in Λ containing either only reflections r_{-1} and r_1 (if k is even) or r_0 and r_2 (if k is odd), as opposed to the reflections r_0 and r_1 as in the more general cases. □

4.5.2 $\prod T = r_0 r_j$

Proof. Suppose $\prod T = r_0 r_j$. When $N = 2$, the two reflections in T must generate D_m by assumption and therefore the first entry may be made r_0 implying the second to be r_j. In the case where $N > 3$ (clearly N may not be equal to 3). By 4.4 and 4.4.1, we have given j, there exist q and q' such that q is relatively prime to m and depending on the case, either q' or $\frac{q'}{2}$ is relatively prime to m as well. Either way, we require that $q + q' \equiv j \pmod{m}$. Using Lemma 3.7 we have the following transformation.

$$T \sim (r_0, r_q, \Delta)$$

In the case where q' is relatively prime to m, namely when m is odd or m is even and j is even, we have that q was chosen so that $q' \equiv j - q \pmod{m}$ is relatively prime to m, and $T' = (r_q, \Delta)$ is such that $\prod T' = r_j$. Because r_q is in T' and $\prod T' = r_j$, we know that T' generates D_m since $d(r_q, r_j) = \pm q' \pmod{m}$ and thus $\gcd(d(r_q, r_j), m) = 1$. Therefore, we have reduced this cause to the previous one in which $\prod T' = r_j$ and therefore by 4.5.1 we have: When $N > 4$,

$$T \sim (r_0, \Lambda, r_j)$$

and where Λ has the appropriate form from 4.2.1. When $N = 4$, this reduces to 4.5.1 with product r_j. Therefore, the canonical form is $(r_0, r_{j-1}, r_{j-1}, r_j)$.

In the case where q' is not relatively prime to m, namely when m is even and j is odd, we may choose q, q' so that $\gcd(q, m) = \gcd(\frac{q'}{2}, m) = 1$ and $q + q' \equiv j$ by 4.4.1. We still have

$$T \sim (r_0, r_q, \Delta)$$

and $T' = (r_q, \Delta)$. There are two options for the subgroup generated by T'. In either case, the pair (r_q, r_j) generates the entirety of the conjugacy class of r_j because $\frac{q'}{2}$ and m are relatively prime. If there exists some $r_i \in T'$ not in the conjugacy class of r_j, then T' generates D_m. On the other hand, if there does not, T' generates the conjugacy class of r_j. If $N > 4$, this reduces to some case in 4.5.1 and we may transform T' into the appropriate Λ.

For $N = 4$, depending on the number of elements from each conjugacy class, we either have $(r_0, r_{j-1}, r_{j-1}, r_j)$ or $(r_0, r_{j-2}, r_{j-2}, r_j)$. □

5 A generalization including rotations

In the second part of the paper, we show that the necessary conditions mentioned at the start are sufficient conditions for Hurwitz equivalence for tuples whose entries are any elements of dihedral groups, including rotations.

5.1 Rotation preliminaries

Define p_i (as an element of D_m) to be the counterclockwise rotation through $i\frac{2\pi}{m}$. We say p_i has degree i. All rotations commute with each other. In order to work with rotations, we must understand the orbit of a rotation and a reflection. Conjugating any rotation p_i by a reflection results in the rotation's inverse p_{m-i}. Conjugating a reflection by a rotation is more subtle. We work out the details for each case below.

5.2 Orbit of (r_i, p_j)

We enumerate the orbit of (r_i, p_j) to describe conjugation of reflections by rotations and vice versa. In the most general case, the orbit has four distinct pairs.

Lemma 5.1. *The orbit of (r_i, p_j) consists of the following pairs*

$$(r_i, p_j) \sim (p_{m-j}, r_i) \sim (r_{i+2(m-j)}, p_{m-j}) \sim (p_j, r_{i+2(m-j)}).$$

Proof. We begin by showing

$$\sigma_1(r_i, p_j) = (r_i p_j r_i, r_i) = (p_{m-j}, r_i).$$

To see this equivalence, suppose $r_i p_j = r_k$ for some k. We then have $p_h r_i = r_k$ for some h. Therefore, $p_j = r_i r_k$ and $p_h = r_k r_i$, but $r_i r_k r_k r_i = I$, which implies $h = m-j$. We remark that this implies that the conjugacy class of a rotation is the rotation and its inverse since rotations themselves commute.

We also must show

$$\sigma_1(p_j, r_i) = (p_j r_i p_{j-m}, p_j) = (r_{i+2j}, p_j).$$

To see this, first notice that p_i takes the k^{th} index of the polygon to the $k+2i^{th}$ (mod m). To determine the h for which $p_j r_i p_{m-j} = r_h$, we look for the index fixed by the reflection $p_j r_i p_{m-j}$. We have that r_h fixes the h^{th} index and therefore if $p_j r_i p_{m-j} = r_h$, then $p_j r_i p_{m-j}(h) = h$. It follows that $r_i p_{m-j}(h) = p_{m-j}(h)$ and therefore, $r_i(h + (2m-2j)) = (h + (2m-2j))$ or $r_i(h-2j) \equiv h - 2j \pmod m$. Since r_i fixes i, we have that $i = h-2j$ and hence $h = i + 2j$. □

6 Proof of the Main Theorem

As in the proof of the reflection main theorem, if T contains at least one reflection, we assume the subgroup S generated by the entries of T is the entire group D_m, if not we reduce to $D_{m'}$. We will see when T consists only of rotations the orbits are trivial. As well, we assume that T contains at least one rotation, otherwise we have already handled this case.

Let the number of reflections be denoted by N_r. We begin by describing the case where $N_r = 0$ which is trivial, followed by $N_r = 1$, $N_r = 2$, and finally $N_r > 2$.

6.1 $N_r = 0$

When T contains only rotations, all of its entries commute and therefore two tuples are Hurwitz equivalent if and only if they are permutations of each other. This is consistent with our three invariants since with respect the the subgroup generated by the entries of T, some cyclic group, each rotation is its own conjugacy class. Therefore two tuples are Hurwitz equivalent if and only if the conjugacy class condition is satisfied, which in this case implies the subgroup and product conditions.

6.2 $N_r = 1$

The canonical form will only include rotations whose degree is $\leq \frac{m}{2}$ since any rotation may be turned into its inverse via Hurwitz moves. As well, we will order these rotations with their degrees increasing from left to right. The right-most entry of the tuple will be the reflection resulting from this particular ordering of rotations and fixed product. Given this canonical form can be reached, which we will show below, it is clear that the neccesary conditions for Hurwitz equivalence are indeed sufficient. Equivalently, the canonical form described above is uniquely determined by the number of entries from each conjugacy class and the product of the entries. Since we only have one reflection, the number of entries from each conjugacy class determines the subgroup generated by the tuple, so this is a weaker condition.

Proof. Use the reflection to perturb each rotation so that its degree $k \leq \frac{m}{2}$. By 'use' we mean apply Hurwitz moves to a rotation reflection pair so that the rotation has been transformed into its inverse if necessary. Following this, the reflection may be moved through the rotation from either the right or the left without changing the degree of the rotation by applying σ or σ^{-1} respectively (we omit the index of σ). We then order the rotations so that they are increasing in degree from left to right. This results in the described canonical form and only depends on the conjugacy classes of the rotations in the tuple and the original product, which determines the final reflection. □

Lemma 6.1. *Suppose T has at least two reflections and $S = D_m$. If we write T in the form (Δ, r_i), then for every k, there exists Δ' such that*

$$(\Delta, r_i) \sim (\Delta', r_{i'}).$$

where $i' \equiv i + 2k \pmod{m}$.

Proof. Begin by moving all reflections rightward, we will also call this new tuple T since it is equivalent to our original. In this position, let S_{rot} and S_{ref} be the subgroups generated by the rotations in T and reflections in T respectively. Let i_{rot} be the index of S_{rot} in C_m and i_{ref} the index of S_{ref} in D_m. We remark that S_{ref} and thus i_{ref} are dependent on the positions of the entries and may change under Hurwitz moves. As well, we always define S_{ref} and i_{ref} with respect to an initial position with all reflections rightward.

Observe that in order for $S = D_m$, it is necessary that the $\gcd(i_{rot}, i_{ref}) = 1$, (otherwise S will not contain p_1).

Given i_{rot}, there exists some product of the rotations in T, perhaps including some rotations more than once, equal to $p_{i_{rot}}$ since the index in C_m corresponds to the smallest positive degree of a rotation in S_{rot}. Equivalently, the sum of their degrees is i_{rot}.

For i_{ref}, first consider the case where T has two reflections. Suppose r_i and r_j are the two reflections used to determine i_{ref}, then the $\gcd(d(r_i, r_j), m) = i_{ref}$ and therefore there exists a such that

$$a \cdot d(r_i, r_j) \equiv i_{ref} \pmod{m}.$$

When the number of reflections in T is greater than two, by Lemma 3.7 we may pull a pair of reflections whose distance (mod m) is i_{ref} to the left-most positions amongst the reflections (who are all to the right of the rotations). We say (mod m) for the case in which all reflections are the same and therefore the index is m but the distance is zero. The main lemma actually shows that in the case were $S_{ref} = D_m$, we may extract a pair whose distance is one, but the above claim follows by reducing to $D_{m'}$ if needed. In this case, we will still label the pair (r_i, r_j) and we have $d(r_i, r_j) \equiv i_{ref} \pmod{m}$ (in this case $a = 1$).

Since i_{rot} and i_{ref} are relatively prime, we may find n_1 and n_2 such that

$$2 \cdot n_1 \cdot i_{rot} + n_2 \cdot i_{ref} \equiv 2 \pmod{m}.$$

Therefore, we have

$$2 \cdot k \cdot n_1 \cdot i_{rot} + k \cdot n_2 \cdot i_{ref} \equiv 2k \pmod{m}.$$

We use k, n_1, and n_2 to transform r_i into r_{i+2k}. Suppose we have the pair (r_i, r_j) in the left-most positions within the set of reflections (either r_i and r_j are the two reflections, or when there are more than two, this pair has been generated using the algorithm from Lemma 3.7). Without loss of generality, let $i > j$. Apply σ to (r_i, r_j) exactly $k \cdot n_2 \cdot a + 1$ times so that the right-most entry is now $r_{i+k\cdot n_2 \cdot a \cdot (i-j)} = r_{i+k\cdot n_2 \cdot i_{ref}}$.

From this point on, we distinguish between the reflections starting in the positions of r_i and r_j and will call them r and r' respectively (at this time $r' = r_{i+k\cdot n_2\cdot i_{ref}}$). We are no longer concerned with which reflection r specifically is and therefore we may use r to perturb rotations freely. We use the rotations described earlier whose degrees sum to i_{rot} and apply σ^2 to the pair (p, r') for each p included in the sum the correct number of times. After applying this once, we ought to have $r_{i+k\cdot n_2\cdot i_{ref}+2\cdot i_{rot}}$. We remark that once a rotation is used in this way, it becomes its inverse in the tuple. If we wish to use it more than one, we perturb it back to its original state with r. We preform this $k \cdot n_1$ times and obtain $r_{i+k\cdot n_2 \cdot i_{ref}+2\cdot k\cdot n_1\cdot i_{rot}} = r_{i+2k}$. This leaves us with $T \sim (\Delta', r_{i+2k})$. □

6.3 $N_r = 2$

In this case, we choose our canonical form to be (Δ, r, r_0) (or (Δ, r, r_1) if m is even and both reflections are edge-edge reflections). We require that Δ contains only rotations of degree $\leq \frac{m}{2}$ increasing from left to right and we observe that r is uniquely determined by $\prod T$. When $N_r = 2$, we do not necessarily have by assumption that $S_{rot} = C_m$. Once we include the reflections however, we must have that $S = D_m$. We show that there exists Δ' such that $T \sim (\Delta', r_0)$ (or (Δ', r_1) in the aforementioned special case), both of which reduce to the case where $N_r = 1$.

Proof. By Lemma 6.1, given a reflection r_i in T, we may transform r_i into r_{i+2k} for all k. When m is odd, there exists k such that $i + 2k \equiv 0 \pmod{m}$ for all i and so we may obtain an r_0. On the other hand, when m is even, there exists k such that $i+2k \equiv 0 \pmod{m}$ for all i even (so we may get r_0) and there exists k such that $i + 2k \equiv 1 \pmod{m}$ for all j odd (so we may get r_1). In terms of reflections, as long as there is one vertex-vertex reflection, we have one r_i such that i is even and for edge-edge reflections we have r_i such that i is odd. □

6.4 $N_r > 2$

Our goal here is to transform the collection of reflections so that the subgroup generated by this collection is maximal. When m is odd, D_m will always be maximal. When m is even however, if all reflections belong to one conjugacy class, $D_{\frac{m}{2}}$ is maximal. We then choose a reflection from the transformed collection that will not disrupt the previous condition to perturb the rotations so that they are of the form of the case $N_r = 1$. Finally, we transform the reflections into the canonical form described in the reflection only case, section 4. The configuration of the rotations and $\prod T$ fix the product of the reflections and the number from each conjugacy class is fixed from the start. The only work needed is to show that we may transform the reflections into a collection whose subgroup is maximal.

Proof. By the proof of Lemma 6.1 in the case where there are more than two reflections, we see that only the pair (r_i, r_j) is involved in the proof after it has been specified. Therefore, at least one reflection may stay fixed when transforming r_i to r_{i+2k}. Choose a reflection to be fixed, move it to the right-most position of the tuple, and label this reflection r_h.

When m is odd, there exists some k such that $i + 2k \equiv h + 1 \pmod{m}$ and therefore we have a pair of reflections whose distance is one, meaning the reflections generate D_m.

When m is even, there exists k such that either $i + 2k \equiv h + 1 \pmod{m}$ (if $i - h$ odd) or $i + 2k \equiv h + 2 \pmod{m}$ (if $i - h$ even). If we may obtain $h + 1$ we generate D_m and we are done, so assume we are in the $h + 2$ case. If there do exist both vertex-vertex and edge-edge reflections, by applying Hurwitz moves to (r_{h+2}, r_h) we enumerate either all vertex-vertex or edge-edge reflections (depending on the parity of h), one of which must be distance one from some reflection in the tuple lying not in the conjugacy class of r_h. In this case, we are done.

Finally assume there are only vertex-vertex or edge-edge reflections, then r_h and r_{h+2} generate all of them. The subgroup $D_{\frac{m}{2}}$ is maximal in this case, and we may transfrom the collection of reflections into its appropriate canonical form as if they were elements of $D_{\frac{m}{2}}$. This concludes the proof. □

Future Work

There exist many other reflection groups in higher dimensions. Similar problems could be studied involving a number of these different groups. As well, one need not restrict oneself to reflection groups.

Acknowledgments

This research was done at the Massachusetts Institute of Technology, SPUR 2009, which is run by David Jerison. The author would like to thank James Pascaleff for suggesting the problem, describing the basic invariants from section two, and always offering encouragement. Finally, the author wishes to thank Adrian Liu for helpful conversations.

References

[1] T. Ben-Itzhak and M. Teicher, *Graph Theoretic Method for Determining non-Hurwitz Equivalence in the Braid Group and Symmetric group*, Available at *http://arxiv.org/abs/math/0110110*, 2001

[2] Joan S. Birman and Tara E. Brendle, *Braids: A Survey*, Available at *http://arxiv.org/abs/math/0409205v2*, 2004

[3] X Hou, *Hurwitz Equivalence in Tuples of Generalized Quaternion Groups and Dihedral Groups*, The Electronic Journal of Combinatorics, 2008

[4] James E. Humphries, *Reflection Groups and Coxeter Groups*, Cambridge Studies in Advanced Mathematics **29**, Cambridge University Press, 1990

[5] Charmaine Sia, *Hurwitz Equivalence in Tuples of Dihedral Groups, Dicyclic Groups, and Semidihedral Groups*, The Electronic Journal of Combinatorics, 2009