Hurwitz Equivalence in Tuples of Dihedral Groups, Dicyclic Groups, and Semidihedral Groups

Charmaine Sia
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139-4307, USA
sia@mit.edu

Submitted: Dec 27, 2008; Accepted: Jul 27, 2009; Published: Aug 7, 2009
Mathematics Subject Classification: 20F36, 20F05

Abstract

Let $D_{2N}$ be the dihedral group of order $2N$, $Dic_{4M}$ the dicyclic group of order $4M$, $SD_{2m}$ the semidihedral group of order $2^m$, and $M_{2m}$ the group of order $2^m$ with presentation $M_{2m} = \langle \alpha, \beta | \alpha^{2^{m-1}} = \beta^2 = 1, \beta \alpha \beta^{-1} = \alpha^{2^{m-2}+1} \rangle$. We classify the orbits in $D_{2N}^n$, $Dic_{4M}^n$, $SD_{2m}^n$, and $M_{2m}^n$ under the Hurwitz action.

1 Introduction

Let $B_n$ denote the braid group on $n$ strands, which is given by the presentation

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} | \sigma_i \sigma_j = \sigma_j \sigma_i, \ |i-j| \geq 2; \ \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \ 1 \leq i \leq n-2 \rangle.$$

For an arbitrary group $G$ and $n \geq 2$, there is an action of $B_n$ on $G^n$, called the Hurwitz action, which is defined by

$$\sigma_i(a_1, \ldots, a_n) = (a_1, \ldots, a_{i-1}, a_{i+1}, a_i^{-1} a_{i+1}, a_{i+2}, \ldots, a_n)$$

for every $1 \leq i \leq n-1$ and $(a_1, \ldots, a_n) \in G^n$. Note that

$$\sigma_i^{-1}(a_1, \ldots, a_n) = (a_1, \ldots, a_{i-1}, a_i a_{i+1} a_i^{-1}, a_i, a_{i+2}, \ldots, a_n).$$

Hence, if we write $a = (a_1, \ldots, a_n) \in G^n$ and define $\pi(a) = a_1 \cdots a_n \in G$, then $\pi(a)$ is an invariant of the Hurwitz action on $G^n$. An action by $\sigma_i$ or $\sigma_i^{-1}$ on $G^n$ is called a Hurwitz move. Two tuples $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G^n$ are said to be (Hurwitz) equivalent, denoted $(a_1, \ldots, a_n) \sim (b_1, \ldots, b_n)$, if they lie in the same $B_n$-orbit.

The problem of classifying the orbits in $G^n$ under the Hurwitz action arose from the study of braid monodromy factorization (see, e.g., Kulikov and Teicher [5]). Clearly, this
problem is trivial for any abelian group $G$: two $n$-tuples $\mathbf{a}, \mathbf{b} \in G^n$ are equivalent if and only if one is a permutation of the other. However, there are few results on the classification of $B_n$-orbits in $G^n$ for nonabelian groups $G$. Ben-Itzhak and Teicher [1] determined all $B_n$-orbits in $S^n_m$ represented by $(t_1, \ldots, t_n)$, where $S_m$ is the symmetric group of order $m!$, each $t_i$ is a transposition, and $t_1 \cdots t_n = 1$. Recently, Hou [3] determined completely the $B_n$-orbits in $Q^m_2$ and $D^m_2$, where $Q^m_2$ is the generalized quaternion group of order $2^m$ and $D^m_2$ is the dihedral group of order $2p^m$ for some prime $p$. Clearly, if $a_1, \ldots, a_n \in G$ generate a finite subgroup, then the $B_n$-orbit of $(a_1, \ldots, a_n)$ in $G^n$ is finite. Humphries [4] and Michel [6] proved a partial converse when $G$ is the general linear group $\text{GL}(\mathbb{R}^n)$: if $s_1, \ldots, s_n \in \text{GL}(\mathbb{R}^n)$ are reflections such that the $B_n$-orbit of $(s_1, \ldots, s_n)$ is finite, then the group generated by $s_1, \ldots, s_n$ is finite.

In this paper, we determine completely the $B_n$-orbits in $G^n$ for four families of groups $G$: the dihedral group $D_{2N}$ of order $2N$, the dicyclic group $\text{Dic}_{4M}$ of order $4M$, the semidihedral group $SD_{2m}$ of order $2^m$, and the group $M_{2m} = \langle \alpha, \beta \mid \alpha^{2^{m-1}} = \beta^2 = 1, \beta \alpha \beta^{-1} = \alpha^{2^{m-2}+1} \rangle$ of order $2^m$. Our method is to find a number of invariants of the Hurwitz action and show that these invariants completely determine the Hurwitz equivalence classes. The invariants and the strategies used to find a canonical representative equivalent to each tuple are essentially the same as those in [3]. The novel element of the present paper is the idea that when performing a series of Hurwitz moves to normalize a tuple in $D^n_{2N}$, with respect to a prime factor of $N$, we can preserve certain congruence properties with respect to other factors of $N$ that were obtained in earlier moves.

This paper is organized as follows. In Section 2, we develop some preliminary results regarding the Hurwitz action on $D^n_{2N}$. In Section 3, we classify the orbits in $D^n_{2N}$ under the Hurwitz action. In Section 4, we classify the Hurwitz equivalence classes in $\text{Dic}^n_{4M}$, $SD^n_{2m}$, and $M^n_{2m}$.

## 2 The Hurwitz Action on $D^n_{2N}$

In this section, we develop some preliminary results regarding the Hurwitz action on $D^n_{2N}$. With the exception of Lemma 2.1(iv), the results presented in this section are similar to those in [3, Section 2].

We use the following generators and relations for the dihedral group $D_{2N}$ of order $2N$:

$$D_{2N} = \langle \alpha, \beta \mid \alpha^N = \beta^2 = 1, \beta \alpha \beta^{-1} = \alpha^{-1} \rangle.$$  

Each element of $D_{2N}$ can be uniquely written in the form $\alpha^i \beta^j$, where $0 \leq i < N$ and $0 \leq j \leq 1$. Conjugating one element of $D_{2N}$ by another gives

$$\begin{align*}
(\alpha^k \beta^l)^{-1}(\alpha^i \beta^j)(\alpha^k \beta^l) &= \alpha^{(-1)^i(i-2kj)} \beta^j, \\
(\alpha^i \beta^j)(\alpha^k \beta^l)^{-1}(\alpha^i \beta^j)^{-1} &= \alpha^{(-1)^i k+2il} \beta^l.
\end{align*}$$

Therefore, a Hurwitz move in $D^n_{2N}$ yields one of the following two equivalences:

$$(\cdots, \alpha^i \beta^j, \alpha^k \beta^l, \cdots) \sim (\cdots, \alpha^k \beta^l, \alpha^{(-1)^i(i-2kj)} \beta^j, \cdots),$$

$$(\cdots, \alpha^i \beta^j, \alpha^k \beta^l, \cdots) \sim (\cdots, \alpha^{(-1)^i k+2il} \beta^l, \alpha^i \beta^j, \cdots).$$
To direct the reader’s attention to the Hurwitz moves that we consider, we shall occasionally omit common terms from two equivalent $n$-tuples $a, b \in G^n$ if there is a sequence of moves transforming $a$ to $b$ that does not involve any of those terms. For example, setting $(j, l) = (0, 0), (0, 1), (1, 0)$, and $(1, 1)$ respectively in the above equivalences and omitting common terms, we obtain

\[
\left\{ \begin{array}{l}
(\alpha^i, \alpha^k) \sim (\alpha^k, \alpha^i), \\
(\alpha^i, \alpha^k \beta) \sim (\alpha^k \beta, \alpha^{-i}), \\
(\alpha^i, \alpha^k \beta) \sim (\alpha^{k+2i} \beta, \alpha^i),
\end{array} \right.
\]

\[\alpha^{i+2} \sim (\alpha^{i+2k} \beta), \alpha^{i+2} \sim (\alpha^{-k}, \alpha^i)\]

The following lemma sets forth some key equivalences that can be obtained through a sequence of Hurwitz moves.

**Lemma 2.1** (see Hou [3, Lemma 2.1]). (i) $(\alpha^i, \alpha^j) \sim (\alpha^{-i}, \alpha^{+2i})$ for all $i, j \in \mathbb{Z}$.

(ii) $(\alpha^i \beta, \alpha^j \beta) \sim (\alpha^{i+h(j-i)} \beta, \alpha^{j+h(j-i)} \beta)$ for all $h, i, j \in \mathbb{Z}$.

(iii) Let $p_1, \ldots, p_t$ be distinct prime divisors of $N$ (not necessarily all the prime divisors of $N$) such that $\prod_{r=1}^{t} p_r^k \parallel N$ for $r = 1, \ldots, t$, and let $0 \leq \nu_r \leq k_r - 1$ for $r = 1, \ldots, t$. Let $e, f \in \mathbb{Z}$ such that $e \neq f \pmod{p_r}$ for $r = 1, \ldots, t$. Then for all $g \in \mathbb{Z}$ such that $g \equiv 0 \pmod{N/\prod_{r=1}^{t} p_r^k}$ and $\tau \in \mathbb{Z}$, we have

\[
\prod_{r=1}^{t} p_r^\nu_r \beta, \alpha^{\tau+\nu_r} \beta) \sim (\alpha^{\tau+(e+g)\prod_{r=1}^{t} p_r^\nu_r} \beta, \alpha^{\tau+(f+g)\prod_{r=1}^{t} p_r^\nu_r} \beta).
\]

(iv) Let $p_1, \ldots, p_t$ be distinct prime divisors of $N$ (not necessarily all the prime divisors of $N$) such that $\prod_{r=1}^{t} p_r^k \parallel N$ for $r = 1, \ldots, t$, and let $0 \leq \nu_r \leq k_r - 1$ for $r = 1, \ldots, t$. Then for all $e \neq f \pmod{p_r}$, there exists $g \in \mathbb{Z}$ such that

(a) $(\alpha^{\tau+e\prod_{r=1}^{t} p_r^\nu_r} \beta, \alpha^{\tau+f\prod_{r=1}^{t} p_r^\nu_r} \beta) \sim (\alpha^{\tau+(e+g)\prod_{r=1}^{t} p_r^\nu_r} \beta, \alpha^{\tau+(f+g)\prod_{r=1}^{t} p_r^\nu_r} \beta),$

(b) $p_r^{\nu_r - \nu_r} \mid f + g$, and

(c) if $p_{\nu_r}$ is another prime divisor of $N$, then $f + g \equiv f \pmod{p_r^{\nu_r - \nu_r}}$.

In particular, $\prod_{r=1}^{t} p_r^k \mid (f + g)\prod_{r=1}^{t} p_r^\nu_r$, and if $p_{\nu_r}$ is another prime divisor of $N$ such that $p_r^{k_{\nu_r}} \mid f \prod_{r=1}^{t} p_r^\nu_r$, then $p_r^{k_{\nu_r}} \mid (f + g)\prod_{r=1}^{t} p_r^\nu_r$.

**Proof.** (i) We have

\[
(\alpha^i, \alpha^j \beta) \sim (\alpha^j \beta, \alpha^{-i}) \quad \text{(using the first equivalence in (2.4))}
\]

\[
\sim (\alpha^{-i}, \alpha^{j+2i} \beta) \quad \text{(using the first equivalence in (2.5))}.
\]
(ii) This follows from (2.6).

(iii) Setting \( i = \tau + e \prod_{r=1}^t p_r^{v_r} \) and \( j = \tau + f \prod_{r=1}^t p_r^{v_r} \) in (ii), we see that it suffices to find \( h \in \mathbb{Z} \) satisfying \( h(f - e)^{-1} \equiv g \prod_{r=1}^t p_r^{v_r} \pmod{N} \). This can be achieved by using the Chinese Remainder Theorem to choose \( h \) such that

\[
h \equiv g(f - e)^{-1} \pmod{p_r^{k_r - v_r}} \quad \text{for } r = 1, \ldots, t,
\]

\[
h \equiv 0 \pmod{N/\prod_{r=1}^t p_r^{v_r}}.
\]

(iv) Setting \( i = \tau + e \prod_{r=1}^t p_r^{v_r} \) and \( j = \tau + f \prod_{r=1}^t p_r^{v_r} \) in (ii), we see that it suffices to find \( g, h \in \mathbb{Z} \) satisfying the following system of congruences:

\[
h(f - e) \prod_{i=1}^t p_i^{v_i} \equiv g \prod_{i=1}^t p_i^{v_i} \pmod{N},
\]

\[
g \equiv -f \pmod{p_r^{k_r - v_r}},
\]

\[
g \equiv 0 \pmod{p_r^{k_r - v_r}} \quad \text{for all other primes } p_r \text{ dividing } N.
\]

This can be achieved by using the Chinese Remainder Theorem to choose \( h \) such that

\[
h \equiv -f(f - e)^{-1} \pmod{p_r^{k_r - v_r}},
\]

\[
h \equiv 0 \pmod{p_r^{k_r - v_r'}} \quad \text{for all other primes } p_r' \text{ dividing } N.
\]

It is easy to see that corresponding to any choice of \( h \), there is a unique value of \( g \) modulo \( N/\prod_{r=1}^t p_r^{v_r} \) that satisfies the conditions in (iv). This proves the lemma.

\[\square\]

### 3 \( B_n \)-orbits in Tuples of Dihedral Groups

In this section, we classify the orbits in \( D_{2N}^n \) under the Hurwitz action. The main idea behind our proof is as follows. First, we partition \( D_{2N}^n \) into subsets, each of which is invariant under the Hurwitz action. We then find a number of invariants of the Hurwitz action and show that these invariants completely determine the equivalence classes within each subset.

For \( a = (\alpha^{i_1} \beta^{j_1}, \ldots, \alpha^{i_n} \beta^{j_n}) \in D_{2N}^n \), where \( 0 \leq i_k < N \) and \( 0 \leq j_k \leq 1 \), let

\[
\Lambda(a) = \text{the multiset } \{ \min\{i_k, N - i_k\} : j_k = 0 \}
\]

and

\[
\Gamma(a) = \{ i_k : j_k = 1 \}.
\]

For example, if \( a = (\alpha^{12}, \alpha^{11} \beta, \alpha^4, \alpha^3) \in D_{30}^4 \), then \( \Lambda(a) = \{3, 4, 3\} \) and \( \Gamma(a) = \{11\} \). It is easy to see that \( \Lambda(a) \) is invariant under each of the Hurwitz moves in (2.3)–(2.6), hence it is an invariant of the Hurwitz action.
We fix a notational convention here. If $N$ is odd, we write its prime factorization as $N = p_1^{k_1} \cdots p_m^{k_m}$; if $N$ is even, we write its prime factorization as $N = 2^{k_0} p_1^{k_1} \cdots p_m^{k_m}$ (i.e., we set $p_0 = 2$). Let $v_{p_r}(i)$ denote the $p_r$-adic order of a number $i$. We partition $D_{2N}^n$ into subsets as follows. Let

$$
A = \{ a \in D_{2N}^n : \Gamma(a) = \emptyset \}.
$$

For each odd prime divisor $p_r$ of $N$, for each $0 \leq \nu_r \leq k_r$ and $0 \leq \tau_r < p_r^{\nu_r}$, let

$$
B_{\nu_r, \tau_r}^{p_r} = \{ a \in D_{2N}^n : \min(\{v_{p_r}(i) : i \in \Lambda(a)\} \cup \{k_r\}) = \nu_r, \emptyset \neq \Gamma(a) \subset \tau_r + p_r^{\nu_r} \mathbb{Z} \},
$$

and for each $0 \leq \nu_r \leq k_r - 1$ and $0 \leq \tau_r < p_r^{\nu_r}$, let

$$
C_{\nu_r, \tau_r}^{p_r} = \{ a \in D_{2N}^n : \min(\{v_{p_r}(i) : i \in \Lambda(a)\} \cup \{k_r\}) \geq \nu_r + 1, \emptyset \neq \Gamma(a) \subset \tau_r + p_r^{\nu_r} \mathbb{Z}, \\
\exists j, j' \in \Gamma(a) \text{ such that } v_{p_r}(j - j') = \nu_r \}.
$$

Then, for any odd prime divisor $p_r$ of $N$, we have

$$
D_{2N}^n = A \sqcup \left( \bigcup_{0 \leq \nu_r \leq k_r} \bigcup_{0 \leq \tau_r < p_r^{\nu_r}} B_{\nu_r, \tau_r}^{p_r} \right) \sqcup \left( \bigcup_{0 \leq \nu_r \leq k_r - 1} \bigcup_{0 \leq \tau_r < p_r^{\nu_r}} C_{\nu_r, \tau_r}^{p_r} \right). \quad (3.1)
$$

It is easy to check that each of $A$, $B_{\nu_r, \tau_r}^{p_r}$, and $C_{\nu_r, \tau_r}^{p_r}$ is invariant under the Hurwitz moves in (2.3)–(2.6). Thus $A$, $B_{\nu_r, \tau_r}^{p_r}$, and $C_{\nu_r, \tau_r}^{p_r}$ are invariant under the Hurwitz action.

For $a \in C_{\nu_r, \tau_r}^{p_r}$, collect the components of $a$ of the form $\alpha^i \beta$ from left to right and let the result be $(\alpha^{i_1} \beta, \ldots, \alpha^{i_t} \beta)$, where $0 \leq i_k < N$. Let $e_s \in \mathbb{Z}_{p_r}, 1 \leq s \leq t$, be defined by $i_s \equiv \tau_r + p_r^{\nu_r} e_s \pmod{p_r^{\nu_r+1}}$. Define

$$
s_{p_r}(a) = \sum_{s=1}^{t} (-1)^{s-1} e_s.
$$

For example, let $N = 135 = 3^3 \cdot 5$, $p_r = 3$, $\nu_r = 2$, $\tau_r = 3$, $n = 4$, and let

$$
a = (\alpha^{7+3^2 \cdot 13} \beta, \alpha^{3^2 \cdot 6}, \alpha^{7+3^2 \cdot 2} \beta, \alpha^{7+3^2 \cdot 11} \beta) \in C_{2,7}^3.
$$

Then $s_{p_r}(a) = 13 - 2 + 11 = 1 \in \mathbb{Z}_3$. It is easy to see from (2.3)–(2.6) that $s(a)$ is also an invariant under the Hurwitz equivalence. This allows us to further partition $C_{\nu_r, \tau_r}^{p_r}$ into two invariant subsets

$$
C_{\nu_r, \tau_r, 0}^{p_r} = \{ a \in C_{\nu_r, \tau_r}^{p_r} : s_{p_r}(a) = 0 \}
$$

and

$$
C_{\nu_r, \tau_r, 1}^{p_r} = \{ a \in C_{\nu_r, \tau_r}^{p_r} : s_{p_r}(a) \neq 0 \}.
$$

Thus, the partition (3.1) can be further refined into

$$
D_{2N}^n = A \sqcup \left( \bigcup_{0 \leq \nu_r \leq k_r} \bigcup_{0 \leq \tau_r < p_r^{\nu_r}} B_{\nu_r, \tau_r}^{p_r} \right) \sqcup \left( \bigcup_{0 \leq \nu_r \leq k_r - 1} \bigcup_{0 \leq \tau_r < p_r^{\nu_r}} C_{\nu_r, \tau_r, 0}^{p_r} \right) \sqcup \left( \bigcup_{0 \leq \nu_r \leq k_r - 1} \bigcup_{0 \leq \tau_r < p_r^{\nu_r}} C_{\nu_r, \tau_r, 1}^{p_r} \right) \quad (3.2)
$$

THE ELECTRONIC JOURNAL OF COMBINATORICS 16 (2009), #R95
for odd primes $p_r$ dividing $N$.

If $N$ is even, we require some additional definitions. For each $0 \leq \nu_0 \leq k_0$ and $0 \leq \tau_0 < 2^{\nu_0}$, let

$$B^2_{\nu_0, \tau_0} = \{ a \in D^2_{2N} : \min(\{v_2(i) : i \in \Lambda(a)\} \cup \{k_0 - 1\}) = \nu_0, \emptyset \neq \Gamma(a) \subset \tau_0 + 2^{\nu_0} \mathbb{Z} \},$$

and for each $0 \leq \nu_0 \leq k_0 - 1$ and $0 \leq \tau_0 < 2^{\nu_0}$, let

$$C^2_{\nu_0, \tau_0} = \{ a \in D^2_{2N} : \min(\{v_2(i) : i \in \Lambda(a)\} \cup \{k_0 - 1\}) \geq \nu_0 + 1, \emptyset \neq \Gamma(a) \subset \tau_0 + 2^{\nu_0} \mathbb{Z} \}
\exists j, j' \in \Gamma(a) \text{ such that } v_2(j - j') = \nu_0 \}.$$

Then $A, B^2_{\nu_0, \tau_0}$, and $C^2_{\nu_0, \tau_0}$ are all invariant under the Hurwitz equivalence and

$$D^2_{2N} = A \sqcup \left( \bigcup_{0 \leq \nu_0 \leq k_0} B^2_{\nu_0, \tau_0} \right) \sqcup \left( \bigcup_{0 \leq \nu_0 \leq k_0 - 1} C^2_{\nu_0, \tau_0} \right). \quad (3.3)$$

For $a = (\alpha_1 \beta_1, \ldots, \alpha_n \beta_n) \in C^2_{\nu_0, \tau_0}$, where $0 \leq i_k \leq N$ and $0 \leq j_k \leq 1$, let

$$u(a) = \# \{ k : j_k = 1 \text{ and } i_k \equiv \tau_0 + 2^{\nu_0} \pmod{2^{\nu_0 + 1}} \}.$$

It is easy to check that $u(a)$ is also invariant under the Hurwitz action.

Having set up this framework, we are now ready to define our desired partition $P$ of $D^2_{2N}$. Let $Q$ be the common refinement of the partitions (3.2) as $p_r$ varies over all the odd prime factors of $N$. If $N$ is odd, then we take $P = Q$, so that any block of the partition $P$ is either $A$ or has the form

$$\chi^{p_1}_{\nu_1, \tau_1} \cap \chi^{p_2}_{\nu_2, \tau_2} \cap \cdots \cap \chi^{p_m}_{\nu_m, \tau_m},$$

where each $\chi^{p_r}_{\nu_r, \tau_r}$ stands for one of $B^{p_r}_{\nu_r, \tau_r}$, $C^{p_r}_{\nu_r, \tau_r, 0}$, or $C^{p_r}_{\nu_r, \tau_r, 1}$. If $N$ is even, we take $P$ to be the common refinement of $Q$ and (3.3). Let $R \sqcup S_0 \sqcup S_1 \sqcup T \sqcup U$ be a partition of the set of prime divisors of $N$, with the restriction that $2 \not\in R \cup S_0 \cup S_1$, and either $T = U = \emptyset$, $(T, U) = (\{2\}, \emptyset)$, or $(T, U) = (\emptyset, \{2\})$. For convenience, we will denote the block

$$\left( \bigcap_{p_r \in R} B^{p_r}_{\nu_r, \tau_r} \right) \cap \left( \bigcap_{p_r \in S_0} C^{p_r}_{\nu_r, \tau_r, 0} \right) \cap \left( \bigcap_{p_r \in S_1} C^{p_r}_{\nu_r, \tau_r, 1} \right) \cap \left( \bigcap_{p_r \in T} B^{p_r}_{\nu_r, \tau_r} \right) \cap \left( \bigcap_{p_r \in U} C^{p_r}_{\nu_r, \tau_r} \right)$$

by $\Pi(R, S_0, S_1, T, U)(\nu_r)(\tau_r)$, where $(\nu_r)$ and $(\tau_r)$ represent vectors that record the numbers $\nu_r$ and $\tau_r$ for each prime $p_r$. For example, if $p_0 = 2$, $p_1 = 3$, $p_2 = 5$, and $p_3 = 7$, then

$$\Pi(\{5, 7\}, \{3\}, \emptyset, \emptyset, \{2\})(1, 2, 1, 1)(1, 8, 4, 0) = C^2_{1,1} \cap C^3_{2,8,0} \cap B^5_{1,4} \cap B^7_{1,0}.$$

By our remarks above, each block of $P$ is invariant under the Hurwitz action, hence it suffices to find a set of representatives of the $B_n$-orbits in $A$ and in each of the blocks $\Pi(R, S_0, S_1, T, U)(\nu_r)(\tau_r)$. This is achieved in Theorem 3.1 below.

6
Theorem 3.1. (i) The $B_n$-orbits in $A$ are represented by

$$\langle \alpha^i_1, \ldots, \alpha^i_n \rangle,$$

where $0 \leq i_1 \leq \cdots \leq i_n < N$.

(ii) For each odd prime divisor $p_r$ of $N$, let $0 \leq \nu_r \leq k_r$ and $0 \leq \tau_i < p^\nu_r$; if $N$ is even, further let $1 \leq \nu_0 \leq k_0$ and $0 \leq \tau_0 < 2^{k_0}$. The $B_n$-orbits in $\Pi(R, S_0, S_1, T, U)(\nu_r)(\tau_r)$ are represented by

$$\langle \alpha^i_1, \ldots, \alpha^i_s, \alpha^\tau \beta, \alpha^\tau \beta \alpha^\tau G \beta \alpha^\tau G \beta, \ldots, \alpha^\tau G \beta \alpha^\tau \beta, \ldots, \alpha^\tau \beta \rangle,$$

where

(a) $0 \leq s < n$ and $0 \leq i_1 \leq \cdots \leq i_s \leq N/2$,

(b) $\tau$ is the unique integer such that $0 \leq \tau < \prod_{p_r \mid N} p^{\nu_r}_r$ and $\tau \equiv \tau_r$ (mod $p^{\nu_r}_r$) for each prime $p_r$ dividing $N$,

(c) for each $p_r \in R$, we have $\min\{v_{p_r}(i_1), \ldots, v_{p_r}(i_s), k_r\} = \nu_r$, $n - s - 1 \geq 0$, $p^{\nu_r}_r \mid E$, $p^{k_r}_r \mid F$, and $p^{\nu_r}_r \mid G$,

(d) for each $p_r \in S_0$, we have $\min\{v_{p_r}(i_1), \ldots, v_{p_r}(i_s), k_r\} \geq \nu_r + 1$, $n - s - 1 \geq 1$,

$$E \equiv p^{\nu_r}_r \pmod{p^{\nu_r + 1}_r}, \quad F \equiv p^{\nu_r}_r \pmod{p^{k_r}_r}, \quad \text{and} \quad p^{\nu_r}_r \mid G,$$

(e) for each $p_r \in S_1$, we have $\min\{v_{p_r}(i_1), \ldots, v_{p_r}(i_s), k_r\} \geq \nu_r + 1$, $n - s - 1 \geq 1$,

$$p^{\nu_r}_r \mid E, \quad p^{k_r}_r \mid F, \quad \text{and} \quad p^{\nu_r}_r \mid G,$$

(f) if $2 \in T$, then $\min\{v_2(i_1), \ldots, v_2(i_s), k_0 - 1\} = \nu_0 - 1$, $n - s - 1 \geq 0$, $2^{\nu_0} \mid E$, $2^{k_0} \mid F$, and $2^{\nu_0} \mid G$,

(g) if $2 \in U$, then $\min\{v_2(i_1), \ldots, v_2(i_s), k_0 - 1\} \geq \nu_0$, $2^{\nu_0} \mid E, \quad G \equiv 2^{\nu_0} \pmod{2^{k_0}}$, and either

1. $2^{k_0} \mid F$ and $w = 0$ (so $u(\mathbf{a}) = 1$) or
2. $F \equiv 2^{\nu_0} \pmod{2^{k_0}}$ and $n - s - 1 \geq w + 2$ (so $u(\mathbf{a}) \geq 2$).

There are certain degenerate cases where terms of the form $\alpha^\tau + F$ or $\alpha^\tau + G$ do not appear in (3.4); this occurs exactly when conditions (c)–(g) force $F \equiv G \equiv 0$ (mod $N$).

The reason for our final comment is that a term of the form $\alpha^\tau + F$ arises only when $S_0 \cup U$ is nonempty, while terms of the form $\alpha^\tau + G$ arise only when $U$ is nonempty.

Let $\varphi : D_{2N} \to D_{2N}/\langle \alpha^{N/p_r^{k_r}} \rangle \cong D_{2p^{k_r}_r^{k_r}}$ be the canonical projection. We remark that under the map $\vartheta : D_{2N}^n \to D_{2p^{k_r}_r^{k_r}}^n$, $\vartheta(\mathbf{a}) = (\varphi(a_1), \ldots, \varphi(a_n))$, the images of the representatives in (3.4) agree with the representatives in [3, Theorems 3.1 and 4.2] up to the ordering of $\alpha^{i_1}, \ldots, \alpha^{i_s}$. Thus Theorem 3.1 can be viewed as a generalization of the results in [3].

Before proceeding with the proof of Theorem 3.1, we give two examples to familiarize the reader with the content of parts (ii)(b)–(g). Suppose $N = 225 = 3^2 \cdot 5^2$, $p_1 = 3$, $p_2 = 5$, $\nu_1 = 5$,
Proof of Theorem 3.1.  (i) This is clear.

(ii) First, we observe that different tuples in (3.4) have different combinations of invariants \( \Lambda(a) \), \( \pi(a) \), \( \sigma_{p_r}(a) \), and \( u(a) \) (whenever these invariants are defined for \( a \)). Thus, different tuples in (3.4) are inequivalent.

Next, we show that every \( a \in \Pi(R, S_0, S_1, T, U)(\nu_r)(\tau_r) \) is equivalent to one of the tuples in (3.4). Since we can use a sequence of Hurwitz moves to shift all the terms of the form \( \alpha^i \) to the front, we may as well assume that \( a \) has the form

\[
a = (\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{i_{s+1}} \beta, \ldots, \alpha^{i_r} \beta).
\]

The general idea behind our proof is to write \( a \) in the form

\[
a = (\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{\tau + e_1} \Pi_{p_r \mid N} p_r^{v_r \tau} \beta, \ldots, \alpha^{\tau + e_t} \Pi_{p_r \mid N} p_r^{v_r \tau} \beta)
\]

and consider the effects of Hurwitz moves on the numbers \( e_1, \ldots, e_t \) modulo \( p_r^{k_r - \nu_r} \) for each prime \( p_r \) dividing \( N \). To avoid cluttering up expressions, we shall use the notation \( \Pi p_r^{v_r} \) to mean \( \Pi_{p_r \mid N} p_r^{v_r} \) in the sequel; if a different product is intended, it will be specified in the subscript of the product symbol. Note that the existence and uniqueness of \( \tau \) is a direct consequence of the Chinese Remainder Theorem. Because the case \( p_r = 2 \) must be handled differently from the case of odd \( p_r \), we shall first prove the theorem for odd values of \( N \), and then show how the proof can be modified to work for even values of \( N \). Observe that it suffices to prove that we can obtain the conditions in parts (c)–(g), since we can then use (2.3) and Lemma 2.1(i) repeatedly to ensure that part (a) is also satisfied.
First suppose that \( N \) is odd, so that we only need to prove that we can obtain the conditions in parts (c)–(e). We proceed by induction on \( t \), the number of terms of the form \( \alpha^i \beta \) in \( a \). The case \( t = 1 \) is trivial. Suppose \( t = 2 \). Write \( a \) in the form

\[
a = (\alpha^{t_1}, \ldots, \alpha^{t_9}, \alpha^{\tau+e_1} \Pi \nu^{i_1} \beta, \alpha^{\tau+e_2} \Pi \nu^{i_2} \beta).
\]

Note that by the definition of \( C^p_{\nu r, \tau r, 0} \), we cannot have \( a \in C^p_{\nu r, \tau r, 0} \) for any prime divisor \( p_r \) of \( N \) (because \( t = 2 \)). Hence, we must have \( e_1 \not\equiv e_2 \pmod{p_r} \) for every prime \( p_r \in S_0 \cup S_1 \). Suppose that \( p_r \in R \). By the definition of \( B^p_{\nu r, \tau r} \), either \( \Lambda(a) \neq \emptyset \) and at least one of \( v_{p_r}(i_1'), \ldots, v_{p_r}(i_9') \), say \( v_{p_r}(i_k') \), is equal to \( \nu r \), or \( \Lambda(a) = \emptyset \). First suppose that we are in the former case. Applying (2.3) and (2.4) multiple times, we can shift the term \( \alpha^{t_6} \) to the right until the last three terms of \( a \) are

\[
(\alpha^{t_6}, \alpha^{\tau+e_1} \Pi \nu^{i_1} \beta, \alpha^{\tau+e_2} \Pi \nu^{i_2} \beta).
\]

If \( e_1 \equiv e_2 \pmod{p_r} \), then applying Lemma 2.1(i) to the first two terms yields

\[
(\alpha^{-t_6}, \alpha^{\tau+e_1} \Pi \nu^{i_1} \beta, \alpha^{\tau+e_2} \Pi \nu^{i_2} \beta),
\]

where \( e_1' \not\equiv e_2' \pmod{p_r} \). Thus we may assume that \( e_1 \not\equiv e_2 \pmod{p_r} \) for all prime divisors \( p_r \) of \( N \). Now, by Lemma 2.1(iv), we have

\[
(\alpha^{\tau+e_1} \Pi \nu^{i_1} \beta, \alpha^{\tau+e_2} \Pi \nu^{i_2} \beta) \sim (\alpha^{\tau+f_1} \Pi \nu^{i_1} \beta, \alpha^{\tau+f_2} \Pi \nu^{i_2} \beta)
\]

for some \( f_2 \) such that if \( p_{r'} \) is another prime divisor of \( N \) such that \( p_{r'} \mid e_2 \), then \( p_{r'} \mid f_2 \) also. If \( \Lambda(a) = \emptyset \) instead, then \( \nu r = k_r \) by definition of \( B^p_{\nu r, \tau r} \) and we obtain (3.5) without any additional work. Repeating this argument for each prime \( p_r \) dividing \( N \), we have

\[
(\alpha^{\tau+e_1} \Pi \nu^{i_1} \beta, \alpha^{\tau+e_2} \Pi \nu^{i_2} \beta) \sim (\alpha^{\tau+E} \beta, \alpha^\tau \beta).
\]

This completes the case \( t = 2 \).

Now assume \( t > 2 \). Again, we write \( a \) in the form

\[
a = (\alpha^{t_1}, \ldots, \alpha^{t_9}, \alpha^{\tau+e_1} \Pi \nu^{i_1} \beta, \ldots, \alpha^{\tau+e_1} \Pi \nu^{i_2} \beta).
\]

First consider \( p_r \in R \). As before, we wish to apply a sequence of Hurwitz moves to obtain an \( n \)-tuple

\[
a' = (\alpha^{t_1}, \ldots, \alpha^{t_9}, \alpha^{\tau+f_1} \Pi \nu^{i_1} \beta, \ldots, \alpha^{\tau+f_1} \Pi \nu^{i_2} \beta, \alpha^{\tau+f_1} \Pi \nu^{i_2} \beta) \sim a
\]

such that if \( p_{r'} \) is another prime divisor of \( N \) such that \( p_{r'} \mid e_1 \), then \( p_{r'} \mid f_1 \) also. Using a similar argument as above, we may assume that \( e_{t-1} \not\equiv e_t \pmod{p_r} \) for every \( p_r \in R \), and hence by Lemma 2.1(iv), we have

\[
(\alpha^{\tau+e_1} \Pi \nu^{i_1} \beta, \alpha^{\tau+e_1} \Pi \nu^{i_2} \beta) \sim (\alpha^{\tau+f_1} \Pi \nu^{i_1} \beta, \alpha^{\tau+f_1} \Pi \nu^{i_2} \beta)
\]
for some \( f \), such that if \( p^j \) is another prime divisor of \( N \) such that \( p^j \mid e_\ell \), then \( p^j \mid f \) also. Repeating this argument for each prime \( p_r \in R \), we have

\[
\alpha = (\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{r+e_1} p^i \beta, \ldots, \alpha^{r+e_s} p^i \beta)
\]

\[
\sim (\alpha^{j_1}, \ldots, \alpha^{j_s}, \alpha^{r+g_1} p^i \beta, \ldots, \alpha^{r+g_1} p^i \beta, \alpha^{r+g_1} p^i \beta),
\]

where \( p^i \mid g_t \) for every prime \( p_r \in R \).

Now consider \( p_r \in S_0 \cup S_1 \). Assume that \( g_t \neq g_{t+1} \equiv \cdots \equiv g_t \mod p_r \). By (2.6) and Lemma 2.1(iv), we have

\[
(\alpha^{r+g_1} p^i \beta, \alpha^{r+g_1} p^i \beta, \ldots, \alpha^{r+g_1} p^i \beta)
\]

\[
\sim (\alpha^{r+g_1} p^i \beta, \alpha^{r+g_1} p^i \beta, \ldots, \alpha^{r+g_1} p^i \beta)
\]

\[
\sim \cdots
\]

\[
\sim (\alpha^{r+g_1} p^i \beta, \ldots, \alpha^{r+g_1} p^i \beta, \alpha^{r+g_1} p^i \beta, \alpha^{r+g_1} p^i \beta)
\]

\[
\sim (\alpha^{r+g_1} p^i \beta, \ldots, \alpha^{r+g_1} p^i \beta, \alpha^{r+g_1} p^i \beta, \alpha^{r+g_1} p^i \beta),
\]

for some \( h_t \) such that if \( p^j \) is another prime divisor of \( N \) such that \( p^j \equiv p^j \mod p_r \), then \( p^j \equiv h_t \mod p_r \) also. Repeating this argument for each prime \( p_r \in S_0 \cup S_1 \), we obtain

\[
\alpha = (\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{r+e_1} p^i \beta, \ldots, \alpha^{r+e_s} p^i \beta)
\]

\[
\sim (\alpha^{j_1}, \ldots, \alpha^{j_s}, \alpha^{r+e_1} p^i \beta, \ldots, \alpha^{r+e_s} p^i \beta, \alpha^{r+e_1} p^i \beta, \alpha^{r+e_s} p^i \beta) = \beta.
\]

If \( h_1, \ldots, h_{t-1} \) are not all the same modulo \( p_r \) for any prime divisor \( p_r \) of \( N \), then the induction hypothesis applies to \( b = (\alpha^{j_1}, \ldots, \alpha^{j_s}, \alpha^{r+h_1} p^i \beta, \ldots, \alpha^{r+h_1} p^i \beta, \alpha^{r} \beta) \).

So assume that the set \( I \) of prime divisors \( p_r \) of \( N \) such that \( h_1 \equiv \cdots \equiv h_{t-1} \equiv 0 \mod p_r \) is nonempty. Let \( J \) be the set of prime divisors of \( N \) that are not in \( I \).

By the Chinese Remainder Theorem, we can find an integer \( M \) satisfying the system of congruences

\[
M \equiv 0 \mod p^k \quad \text{for each } p_s \in J,
\]

\[
M \prod_{p_r \notin I} p \equiv 1 \mod p^k \quad \text{for each } p_r \in I.
\]

Write \( b \) as \( (\alpha^{j_1}, \ldots, \alpha^{j_s}, \alpha^{r+h_1} p^i \beta, \ldots, \alpha^{r+h_1} p^i \beta, \alpha^{r} \beta) \). Let \( x \in \mathbb{Z} \) be such that \( x \equiv -h_1 \mod p_r \) for each \( p_r \in I \) and \( x \equiv 0 \mod p^k \) for each \( p_s \in J \). Then, using Lemma 2.1(iii) repeatedly, we have

\[
(\alpha^{r+h_1} p^i \beta, \alpha^{r+h_1} p^i \beta, \alpha^{r} \beta)
\]

\[
\sim (\alpha^{r+h_1} p^i \beta, \alpha^{r+(h_1+1)} p^i \beta, \alpha^{r+M} p^i \beta, \alpha^{r+M} p^i \beta)
\]

\[
\sim (\alpha^{r+(h_1+x+1)} p^i \beta, \alpha^{r+(h_1+x+1)} p^i \beta, \alpha^{r+M} p^i \beta, \alpha^{r+M} p^i \beta)
\]

\[
\sim (\alpha^{r+(h_1+x+1)} p^i \beta, \alpha^{r+(h_1+x+1)} p^i \beta, \alpha^{r+M} p^i \beta, \alpha^{r+M} p^i \beta).
\]

(3.6)
If \( t = 3 \), use the Chinese Remainder Theorem to choose \( x \) such that

\[
(h'_t + x) \left( \prod_{i \in I} p_i^{\nu_i} \right) \equiv 1 \pmod{p_r^{k_r-\nu_r}}
\]

for each \( p_r \in I \) and \( x \equiv 0 \pmod{p_r^{k_r}} \) for each \( p_r \in J \). Then the middle term becomes \( \alpha^{\tau + F'} \), where \( F' \equiv \nu_r \pmod{p_r^{k_r}} \) for each \( p_r \in I \). Since \( S_0 \subseteq I \) in this case because \( h_1 - h_2 \equiv 0 \pmod{p_r} \) for each \( p_r \in I \), condition (d) holds. Applying (3.5) to the first two terms in (3.6) for each prime \( p_r \in R \cup S_1 \), we can also get conditions (c) and (e) to hold. Hence \( \alpha \) is equivalent to the tuple in (3.4).

If \( t > 3 \), choose \( x \) such that \( x \not\equiv -h'_t, 0 \pmod{p_r} \) for each \( p_r \in I \). Then the induction hypothesis applies to

\[
(\alpha^{\tau_1}, \ldots, \alpha^{\tau_t}, \alpha^{\tau+\nu_t} \prod_{\nu_r \in r} \nu_r, \ldots, \alpha^{\tau+\nu_t} \prod_{\nu_r \in r} \nu_r, \beta, \ldots, \alpha^{\tau} \beta).
\]

This concludes the induction and completes the proof in the case that \( N \) is odd.

Now, we describe how the proof above can be modified to work for even \( N \). If \( a \in B_{\nu_0, \tau_0}^2 \) for some \( \nu_0 \) and \( \tau_0 \), then the technique for primes \( p_r \in R \) carries over almost exactly to the case \( p_r = 2 \). In what follows, we concentrate on the case \( a \in C_{\nu_0, \tau_0}^2 \).

First observe that the proof for odd \( N \) can be carried out in steps: we change terms in the \( n \)-tuple to \( \alpha^\tau \beta \) one-by-one, starting from the rightmost element and working our way left until we reach the third element of the form \( \alpha^t \beta \) from the left. We shall use a similar approach when \( N \) is even, except that we wish to obtain one of the following two tuples after changing all but the first three elements of the form \( \alpha^t \beta \):

\[
\begin{align*}
&\left(\alpha^{\tau + f_1} \prod p_i^{\nu_i} \beta, \alpha^{\tau + e_1} \prod p_i^{\nu_i} \beta, \alpha^{\tau + f_2} \prod p_i^{\nu_i} \beta, \alpha^{\tau + \beta}, \ldots, \alpha^{\tau} \beta\right), \quad \text{if } u(a) = 1, \\
&\left(\alpha^{\tau + e_1} \prod p_i^{\nu_i} \beta, \alpha^{\tau + e_2} \prod p_i^{\nu_i} \beta, \alpha^{\tau + f_1} \prod p_i^{\nu_i} \beta, \alpha^{\tau + \beta}, \ldots, \alpha^{\tau - g} \beta, \alpha^{\tau} \beta, \ldots, \alpha^{\tau} \beta\right), \quad \text{if } u(a) \geq 2,
\end{align*}
\]

(3.7)

where \( e_1 \) and \( e_2 \) are odd, \( f_1 \) and \( f_2 \) are even, and \( g \) satisfies the congruences

\[
\begin{align*}
g &\equiv 0 \pmod{N/2^{k_0}}, \\
g &\equiv 2^{\nu_0} \pmod{2^{k_0}}.
\end{align*}
\]

(3.8)

This can be achieved as follows. Consider the first term from the right that does not agree with the form mentioned above; let it be \( \alpha^{\tau + z} \prod p_i^{\nu_i} \beta \). Observe that by the definition of \( u(a) \) and the form of the \( n \)-tuples in (3.7), there exists a term of the form \( \alpha^{\tau + y} \prod p_i^{\nu_i} \beta \), where \( y \) has different parity from \( z \), occurring before \( \alpha^{\tau + z} \prod p_i^{\nu_i} \beta \).
Using the second equivalence in (2.6), we can shift $\alpha^{r+y} \Pi^{\nu_{\nu}} \beta$ to the right until we have an adjacent pair

$$(\alpha^{r+y} \Pi^{\nu_{\nu}} \beta, \alpha^{r+z} \Pi^{\nu_{\nu}} \beta).$$

Now, using Lemma 2.1(iii), we can find an equivalent pair

$$(\alpha^{r+y'} \Pi^{\nu_{\nu}} \beta, \alpha^{r+z' \Pi^{\nu_{\nu}} \beta}),$$

where $z' \prod_{p_{\nu}}^{\nu_{\nu}} \equiv -2^{\nu_{\nu}}$ or 0 (mod $2^{\nu_{\nu}}$) as desired. We can then use Lemma 2.1(iv) again for all the odd primes $p_{\nu}$, as in the case where $N$ is odd, so that the term that was previously $\alpha^{r+z} \Pi^{\nu_{\nu}} \beta$ now has the correct form. Finally, by performing Hurwitz moves on the 3 leftmost terms, we can ensure that $e_1, e_2, f_1,$ and $f_2$ have the correct parity.

At this stage, consider the first three terms of the form $\alpha^i \beta$ in the resulting $n$-tuple. If $u(a) = 1$, we want to show that

$$(\alpha^{r+e_1} \Pi^{\nu_{\nu}} \beta, \alpha^{r+e_2} \Pi^{\nu_{\nu}} \beta, \alpha^{r+f_1} \Pi^{\nu_{\nu}} \beta) \sim (\alpha^{r+E}, \alpha^{r+F}, \alpha^r),$$

where $E$ and $F$ satisfy the conditions in Theorem 3.1; if $u(a) \geq 2$, we want to show that

$$(\alpha^{r+e_1} \Pi^{\nu_{\nu}} \beta, \alpha^{r+e_2} \Pi^{\nu_{\nu}} \beta, \alpha^{r+f_1} \Pi^{\nu_{\nu}} \beta) \sim (\alpha^{r+E}, \alpha^{r+F}, \alpha^r).$$

First suppose $u(a) = 1$. Using the same technique as above, we can obtain

$$(\alpha^{r+e_1} \Pi^{\nu_{\nu}} \beta, \alpha^{r+e_2} \Pi^{\nu_{\nu}} \beta, \alpha^{r+f_1} \Pi^{\nu_{\nu}} \beta) \sim (\alpha^{r+e'} \beta, \alpha^{r+e''} \beta, \alpha^r),$$

where $e'$ is even, $e''$ is odd, and $e' \equiv p_{\nu}^{\nu_{\nu}}$ (mod $p_{\nu}^{\nu_{\nu}+1}$), $e'' \equiv p_{\nu}^{\nu_{\nu}}$ (mod $p_{\nu}^{\nu_{\nu}}$) for each $p_{\nu} \in S_0$. Applying (3.5) to the second tuple in (3.9) for every prime $p_{\nu} \in R \cup S_1 \cup T \cup U$, we see that $a$ is equivalent to the tuple in (3.4).

Now suppose $u(a) \geq 2$. Notice that in $(\alpha^{r+e_1} \Pi^{\nu_{\nu}} \beta, \alpha^{r+e_2} \Pi^{\nu_{\nu}} \beta, \alpha^{r+f_1} \Pi^{\nu_{\nu}} \beta)$, we never have $x \equiv y \equiv z$ (mod $p_{\nu}$) for any $p_{\nu}$ (because $x-y+z \equiv 0$ (mod $p_{\nu}$)). Therefore, using Lemma 2.1(iv) repeatedly to adjust the middle term, we obtain

$$(\alpha^{r+e_1} \Pi^{\nu_{\nu}} \beta, \alpha^{r+e_2} \Pi^{\nu_{\nu}} \beta, \alpha^{r+f_1} \Pi^{\nu_{\nu}} \beta) \sim (\alpha^{r+e''} \Pi^{\nu_{\nu}} \beta, \alpha^{r+F} \beta, \alpha^{r+f''} \Pi^{\nu_{\nu}} \beta)$$

$$(\alpha^{r+e''} \Pi^{\nu_{\nu}} \beta, \alpha^{r+F} \beta, \alpha^{r+f''} \Pi^{\nu_{\nu}} \beta) \sim (\alpha^{r+e''} \Pi^{\nu_{\nu}} \beta, \alpha^{r+f''} \Pi^{\nu_{\nu}} \beta, \alpha^{r-F} \beta)$$

(3.10)

where $e''$ is odd, $f''$ and $f'''$ are even, and $f'' \equiv 0$ (mod $p_{\nu}^{\nu_{\nu}+1}$) for every $p_{\nu} \in S_0$. Now, we concentrate on the first two terms $(\alpha^{r+e''} \Pi^{\nu_{\nu}} \beta, \alpha^{r+f''} \Pi^{\nu_{\nu}} \beta)$. Returning to the definitions of $B^{(p_{\nu}, r, \tau)}$, $C^{(p_{\nu}, r, \tau)}$, and $C^{(p_{\nu}, r, \tau, 0)}$ (for odd $p_{\nu}$), we see that we have $e'' \neq f''$ (mod $p_{\nu}$) for any prime $p_{\nu}$ dividing $N$. Therefore, we can use Lemma 2.1(iv) repeatedly for every prime $p_{\nu}$ to obtain

$$(\alpha^{r+e''} \Pi^{\nu_{\nu}} \beta, \alpha^{r+f''} \Pi^{\nu_{\nu}} \beta) \sim (\alpha^{r+E} \beta, \alpha^r),$$

(3.11)
Combining (3.7), (3.10), and (3.11), we obtain
\[ a \sim (\alpha^{\tau+E}\beta, \alpha^{\tau-F}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta, \alpha^{\tau}\beta, \ldots, \alpha^{\tau}\beta). \] (3.12)

Finally, applying (2.6) repeatedly to \((\alpha^{\tau}\beta, \alpha^{\tau-F}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta)\), we obtain
\[ (\alpha^{\tau}\beta, \alpha^{\tau-F}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta) \sim (\alpha^{\tau}\beta, \alpha^{\tau+G}\beta, \alpha^{\tau}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta) \sim \ldots \sim (\alpha^{\tau}\beta, \alpha^{\tau+G}\beta, \alpha^{\tau}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta) \] (3.13)

Combining (3.12) and (3.13), we see that \(a\) is equivalent to an \(n\)-tuple of the form (3.4), as desired. This concludes the proof of the theorem.

The following corollary is a direct consequence of Theorem 3.1.

Corollary 3.2. (i) Two \(n\)-tuples \(a, b \in A\) are equivalent if and only if \(a\) is a permutation of \(b\).

(ii) Two \(n\)-tuples \(a, b \in \Pi(R, S_0, S_1, T, U)(\nu_r)(\tau_r)\) are equivalent if and only if \(\Lambda(a) = \Lambda(b), \pi(a) = \pi(b), \sigma_p(a) = \sigma_p(b)\) for each odd prime \(p \mid N\) such that \(a, b \in C_{\nu, \tau}^p\), and \(u(a) = u(b)\) if \(2 \mid N\).

4 \(B_n\)-orbits in Tuples of Dicyclic and Semidihedral Groups

The results in the previous section can also be applied to classify the \(B_n\)-orbits in dicyclic groups, which are closely related to dihedral groups. The similarity between dihedral groups and dicyclic groups can be seen from the presentation of the dicyclic group \(\text{Dic}_{4M}\) of order \(4M\):
\[ \text{Dic}_{4M} = \langle \alpha, \beta \mid \alpha^{2M} = 1, \alpha^M = \beta^2, \beta\alpha\beta^{-1} = \alpha^{-1} \rangle. \]

Analogous to elements of \(D_{2N}\), each element of \(\text{Dic}_{4M}\) can be uniquely written in the form \(\alpha^i\beta^j\), where \(0 \leq i < 2M\) and \(0 \leq j \leq 1\). It is easy to check that equations (2.1) and (2.2), and hence (2.3)–(2.6), also hold for \(\text{Dic}_{4M}\). In these equations, the only difference between \(D_{2N}\) and \(\text{Dic}_{4M}\) that affects the Hurwitz action is that the element \(\alpha\) has order \(N\) in \(D_{2N}\), but order \(2M\) in \(\text{Dic}_{4M}\). If \(N = 2M\), then there is no difference. Therefore, under the bijection \(D_{4M} \rightarrow \text{Dic}_{4M}\), \(\alpha^i\beta^j \rightarrow \alpha^i\beta^j\) for \(0 \leq i < 2M\), \(0 \leq j \leq 1\), the Hurwitz action on \(D_{4M}^n\) is identical to that on \(\text{Dic}_{4M}^n\). It follows that all results in Section 3 continue to hold with \(D_{4M}^n\) replaced by \(\text{Dic}_{4M}^n\).

Hou [3] determined the \(B_n\)-orbits in the generalized quaternion group \(Q_{2m}^n\) of order \(2^m\) and in \(D_{2m}^n\). These two families of groups share the property that for every \(m \geq 4\),...
there exists a maximal cyclic subgroup of index 2. There are exactly two other families of groups of order $2^m$ that possess this property. Following Gorenstein [2], we call one of these groups the semidihedral group and denote it by $SD_{2^m}$. It has the presentation

$$SD_{2^m} = \langle \alpha, \beta \mid \alpha^{2^{m-1}} = \beta^2 = 1, \beta\alpha\beta^{-1} = \alpha^{2^{m-2} - 1} \rangle.$$  

We denote the other group by $M_{2^m}$; it has the presentation

$$M_{2^m} = \langle \alpha, \beta \mid \alpha^{2^{m-1}} = \beta^2 = 1, \beta\alpha\beta^{-1} = \alpha^{2^{m-2} + 1} \rangle.$$  

In this section, we classify the $B_n$-orbits in $SD_{2^m}^n$ and $M_{2^m}^n$. The proofs of our results are very similar to those in [3] and in Section 3, hence we omit them.

### 4.1 $B_n$-orbits in $SD_{2^m}^n$

The semidihedral group $SD_{2^m}$ of order $2^m$ is defined for any $m \geq 3$. When $m = 3$, $SD_8$ is isomorphic to the abelian group $\mathbb{Z}_2 \times \mathbb{Z}_4$, so the problem of determining the $B_n$-orbits in $SD_8$ is trivial. In what follows, we concentrate on the case $m \geq 4$. Like the dihedral group and the dicyclic group, every element of $SD_{2^m}$ can be uniquely written in the form $\alpha^i\beta^j$, where $0 \leq i < 2^{m-1}$ and $0 \leq j \leq 1$.

For $a = (\alpha^{i_1}\beta^{j_1}, \ldots, \alpha^{i_n}\beta^{j_n}) \in SD_{2^m}^n$, where $0 \leq i_k < 2^{m-1}$ and $0 \leq j_k \leq 1$, let

$$\lambda(a) = \text{the multiset } \{ \min\{i_k, (2^{m-2} - 1)i_k \text{ mod } 2^{m-1} \} : j_k = 0 \}$$

and

$$\gamma(a) = \{ i_k : j_k = 1 \}.$$  

Let

$$A = \{ a \in SD_{2^m}^n : \gamma(a) = \emptyset \}.$$  

For each $1 \leq \nu \leq m - 1$ and $0 \leq \tau < 2^\nu$, let

$$B_{\nu,\tau} = \{ a \in SD_{2^m}^n : \min(\{v_2(i) : i \in \lambda(a)\} \cup \{m - 2\}) = \nu - 1, \emptyset \neq \gamma(a) \subset \tau + 2^\nu \mathbb{Z}, \}$$

where $v_2(i)$ is the 2-adic order of $i$. For each $0 \leq \nu \leq m - 2$ and $0 \leq \tau < 2^\nu$, let

$$C_{\nu,\tau} = \{ a \in SD_{2^m}^n : \min(\{v_2(i) : i \in \lambda(a)\} \cup \{m - 2\}) \geq \nu, \gamma(a) \subset \tau + 2^\nu \mathbb{Z}, \exists j, j' \in \Gamma(a) \text{ such that } v_2(j - j') = \nu \}.$$  

Then

$$SD_{2^m}^n = A \sqcup \left( \bigsqcup_{1 \leq \nu \leq m-1} \bigsqcup_{0 \leq \tau < 2^\nu} B_{\nu,\tau} \right) \sqcup \left( \bigsqcup_{0 \leq \nu \leq m-2} \bigsqcup_{0 \leq \tau < 2^\nu} C_{\nu,\tau} \right).$$  

As in Section 3, it is easy to see that each of $A$, $B_{\nu,\tau}$, and $C_{\nu,\tau}$ is invariant under the Hurwitz action, so that it suffices to find a set of representatives of the $B_n$-orbits in each of $A$, $B_{\nu,\tau}$, and $C_{\nu,\tau}$.
For \( \mathbf{a} = (\alpha^{i_1} \beta^{j_1}, \ldots, \alpha^{i_n} \beta^{j_n}) \in \mathcal{C}_{\nu, \tau} \), where \( 0 \leq i_k < 2^{m-1} \) and \( 0 \leq j_k \leq 1 \), let
\[
\nu(\mathbf{a}) = \# \{ k : j_k = 1 \text{ and } i_k \equiv \tau \pmod{2^{v+1}} \}.
\]

Again, it is easy to see that \( \nu(\mathbf{a}) \) is an invariant of the Hurwitz action.

The following theorem classifies the \( B_n \)-orbits in \( SD_{2^m}^n \).

**Theorem 4.1.** Let \( m \geq 4 \), and let the semidihedral group \( SD_{2^m} \) be partitioned into sets \( \mathcal{A} \), \( \mathcal{B}_{\nu, \tau} \), and \( \mathcal{C}_{\nu, \tau} \) as above.

(i) The \( B_n \)-orbits in \( \mathcal{A} \) are represented by
\[
(\alpha^{i_1}, \ldots, \alpha^{i_n}),
\]
where \( 0 \leq i_1 \leq \cdots \leq i_n < 2^{m-1} \).

(ii) Let \( 1 \leq \nu \leq m-1 \) and \( 0 \leq \tau < 2^\nu \). The \( B_n \)-orbits in \( \mathcal{B}_{\nu, \tau} \) are represented by
\[
(\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{\tau+2^\nu e} \beta, \alpha^{\tau} \beta, \ldots, \alpha^{\tau} \beta),
\]
where \( 0 \leq i_1 \leq \cdots \leq i_s < 2^{m-1} \), \( i_k \in \{ \min \{ i, (2^{m-2} - 1) i \pmod{2^{m-1}} \} : 0 \leq i \leq 2^{m-1} \} \), \( \min \{ \nu_2(i_1), \ldots, \nu_2(i_s), m-2 \} = \nu - 1 \), and \( 0 \leq e < 2^{m-1-\nu} \).

(iii) Let \( 1 \leq \nu \leq m-2 \) and \( 0 \leq \tau < 2^\nu \). The \( B_n \)-orbits in \( \mathcal{C}_{\nu, \tau} \) are represented by
\[
(\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{\tau+2^\nu e} \beta, \alpha^{\tau+2^\nu e} \beta, \ldots, \alpha^{\tau+2^\nu e} \beta, \underbrace{\alpha^{\tau} \beta, \ldots, \alpha^{\tau} \beta}_u),
\]
where \( 0 \leq i_1 \leq \cdots \leq i_s < 2^{m-1} \), \( i_k \in \{ \min \{ i, (2^{m-2} - 1) i \pmod{2^{m-1}} \} : 0 \leq i \leq 2^{m-1} \} \), \( \min \{ \nu_2(i_1), \ldots, \nu_2(i_s), m-2 \} \geq \nu \), \( 0 \leq e < 2^{m-1-\nu} \), \( e \equiv 1 \pmod{2} \), and \( u > 0 \).

Analogous to Theorem 3.1, different \( n \)-tuples in (4.1) have different combinations of invariants \( \lambda(\mathbf{a}) \) and \( \pi(\mathbf{a}) \), while different \( n \)-tuples in (4.2) have different combinations of invariants \( \lambda(\mathbf{a}) \), \( \pi(\mathbf{a}) \), and \( u(\mathbf{a}) \). This allows us to establish the following criterion for two \( n \)-tuples in \( SD_{2^m}^n \) to be equivalent.

**Corollary 4.2.** Let \( m \geq 4 \), and let the semidihedral group \( SD_{2^m} \) be partitioned into sets \( \mathcal{A} \), \( \mathcal{B}_{\nu, \tau} \), and \( \mathcal{C}_{\nu, \tau} \) as above.

(i) Two \( n \)-tuples \( \mathbf{a}, \mathbf{b} \in \mathcal{A} \) are equivalent if and only if \( \mathbf{a} \) is a permutation of \( \mathbf{b} \).

(ii) Two \( n \)-tuples \( \mathbf{a}, \mathbf{b} \in \mathcal{B}_{\nu, \tau} \) are equivalent if and only if \( \lambda(\mathbf{a}) = \lambda(\mathbf{b}) \) and \( \pi(\mathbf{a}) = \pi(\mathbf{b}) \).

(iii) Two \( n \)-tuples \( \mathbf{a}, \mathbf{b} \in \mathcal{C}_{\nu, \tau} \) are equivalent if and only if \( \lambda(\mathbf{a}) = \lambda(\mathbf{b}) \), \( u(\mathbf{a}) = u(\mathbf{b}) \), and \( \pi(\mathbf{a}) = \pi(\mathbf{b}) \).
4.2 $B_n$-orbits in $M_{2m}^n$

Let $m \geq 3$. Recall that $M_{2m}^n$ has the following representation in terms of generators and relations:

$$M_{2m}^n = \langle \alpha, \beta \mid \alpha^{2^{m-1}} = \beta^2 = 1, \ \beta\alpha\beta^{-1} = \alpha^{2^{m-2}+1} \rangle.$$

Like the dihedral group, the dicyclic group, and the semidihedral group, every element of $M_{2m}^n$ can be uniquely written in the form $\alpha^i\beta^j$, where $0 \leq i < 2^{m-1}$ and $0 \leq j \leq 1$.

For $a = (\alpha^{i_1}\beta^{j_1}, \ldots, \alpha^{i_n}\beta^{j_n}) \in M_{2m}^n$, let

$$\Phi(a) = \text{the multiset}\{i_k' : j_k = 0\}, \text{ where } i_k' = \begin{cases} i_k, & \text{if } i_k \text{ is even;} \\ i_k \mod 2^{m-2}, & \text{if } i_k \text{ is odd;} \end{cases}$$

and let

$$\Psi(a) = \text{the multiset}\{i_k'' : j_k = 1\}, \text{ where } i_k'' = i_k \mod 2^{m-2}.$$

Then $\Phi(a)$ and $\Psi(a)$ are invariants of the Hurwitz action on $M_{2m}^n$.

Let

$$\mathcal{D} = \{a \in M_{2m}^n : \Phi(a) \subseteq 2\mathbb{Z} \text{ and } \Psi(a) \subseteq \tau \oplus 2\mathbb{Z} \text{ for } \tau = 0 \text{ or } 1\} \cup \{a \in M_{2m}^n : \Psi(a) = \emptyset\}.$$

**Theorem 4.3.** Let $m \geq 3$, and let the group $M_{2m}^n$ be partitioned into sets $\mathcal{D}$ and its complement $\mathcal{D}^c$ as above.

(i) The $B_n$-orbits in $\mathcal{D}$ are represented by

$$(\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{i_{s+1}}\beta, \ldots, \alpha^{i_n}\beta),$$

where $0 \leq s \leq n$, $0 \leq i_1 \leq \cdots \leq i_s < 2^{m-1}$, and $0 \leq i_{s+1} \leq \cdots \leq i_n < 2^{m-1}$, subject to the conditions above.

(ii) The $B_n$-orbits in $\mathcal{D}^c$ are represented by

$$(\alpha^{i_1}, \ldots, \alpha^{i_r}, \alpha^{i_{r+1}}, \ldots, \alpha^{i_s}, \alpha^{i_{s+1}}\beta, \ldots, \alpha^{i_n}\beta),$$

where $0 \leq r \leq s < n$, $\{i_1, \ldots, i_r\} \subseteq 2\mathbb{Z}$, $\{i_{r+1}, \ldots, i_s\} \subseteq 1 + 2\mathbb{Z}$, $0 \leq i_1 \leq \cdots \leq i_r < 2^{m-1}$, $0 \leq i_{r+1} \leq \cdots \leq i_s < 2^{m-2}$, $0 \leq i_{s+1} \leq \cdots \leq i_{n-1} \leq 2^{m-2}$, and $i_{n-1} \leq i_n < 2^{m-1}$.

As before, the invariants $\Phi(a), \Psi(a)$ and $\pi(a)$ show that distinct $n$-tuples in (4.3) are inequivalent. This yields the following criterion for two $n$-tuples in $M_{2m}^n$ to be equivalent.

**Corollary 4.4.** Let $m \geq 3$, and let the group $M_{2m}^n$ be partitioned into sets $\mathcal{D}$ and $\mathcal{D}^c$ as above.

(i) Two $n$-tuples $a, b \in \mathcal{D}$ are equivalent if and only if $a$ is a permutation of $b$.

(ii) Two $n$-tuples $a, b \in \mathcal{D}^c$ are equivalent if and only if $\Phi(a) = \Phi(b)$, $\Psi(a) = \Psi(b)$ and $\pi(a) = \pi(b)$. 


Acknowledgments

This research was carried out at the University of Minnesota Duluth under the supervision of Joseph Gallian. Financial support was provided by the National Science Foundation (grant number DMS 0754106), the National Security Agency (grant number H98230-06-1-001), and the Massachusetts Institute of Technology Department of Mathematics. The author would like to thank Joseph Gallian for his support and encouragement, as well as Ricky Liu for his assistance in proofreading this paper. Finally, the author would like to thank the referee for pointing out an error in Theorem 4.3 in a previous version of this paper, and for several other useful comments and suggestions.

References