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

1 Introduction

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

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

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

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

for every $1 \leqslant i \leqslant n-1$ 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 $\boldsymbol{a} = (a_1, \ldots, a_n) \in G^n$ and define $\pi(\boldsymbol{a}) = a_1 \cdots a_n \in G$, then $\pi(\boldsymbol{a})$ is an invariant of the Hurwitz action on G^n. An action by σ_i or σ_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 $\boldsymbol{a}$, $\boldsymbol{b} \in G^n$ 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_m^n 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 $Q_{2^m}^n$ and $D_{2p^m}^n$, where Q_{2^m} is the generalized quaternion group of order 2^m and D_{2p^m} 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-orb! it 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 $\mathrm{GL}(\mathbb{R}^n)$: if $s_1, \ldots, s_n \in \mathrm{GL}(\mathbb{R}^n)$ 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 Dic_{4M} of order $4M$, the semidihedral group SD_{2^m} of order 2^m, and the group $M_{2^m} = \langle \alpha, \beta \mid \alpha^{2^{m-1}} = \beta^2 = 1,\ \beta\alpha\beta^{-1} = \alpha^{2^{m-2}+1} \rangle$ 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_{2N}^n 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_{2N}^n. In Section 3, we classify the orbits in D_{2N}^n under the Hurwitz action. In Section 4, we classify the Hurwitz equivalence classes in Dic_{4M}^n, $SD_{2^m}^n$, and $M_{2^m}^n$.

2 The Hurwitz Action on D_{2N}^n

In this section, we develop some preliminary results regarding the Hurwitz action on D_{2N}^n. 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 $0 \leqslant i < N$ and $0 \leqslant j \leqslant 1$. Conjugating one element of D_{2N} by another gives

$$(\alpha^k\beta^l)^{-1}(\alpha^i\beta^j)(\alpha^k\beta^l) = \alpha^{(-1)^l(i-2kj)}\beta^j, \tag{2.1}$$

$$(\alpha^i\beta^j)(\alpha^k\beta^l)(\alpha^i\beta^j)^{-1} = \alpha^{(-1)^j k+2il}\beta^l. \tag{2.2}$$

Therefore, a Hurwitz move in D_{2N}^n yields one of the following two equivalences:

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

To direct the reader's attention to the Hurwitz moves that we consider, we shall occasionally omit common terms from two equivalent n-tuples $\boldsymbol{a}$, $\boldsymbol{b} \in G^n$ if there is a sequence of moves transforming $\boldsymbol{a}$ to $\boldsymbol{b}$ 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

$$(\alpha^i, \alpha^k) \sim (\alpha^k, \alpha^i), \tag{2.3}$$

$$\begin{cases} (\alpha^i, \alpha^k\beta) \sim (\alpha^k\beta, \alpha^{-i}), \\ (\alpha^i, \alpha^k\beta) \sim (\alpha^{k+2i}\beta, \alpha^i), \end{cases} \tag{2.4}$$

$$\begin{cases} (\alpha^i\beta, \alpha^k) \sim (\alpha^k, \alpha^{i-2k}\beta), \\ (\alpha^i\beta, \alpha^k) \sim (\alpha^{-k}, \alpha^i\beta), \end{cases} \tag{2.5}$$

$$\begin{cases} (\alpha^i\beta, \alpha^k\beta) \sim (\alpha^k\beta, \alpha^{-i+2k}\beta) = (\alpha^{i+(k-i)}\beta, \alpha^{k+(k-i)}\beta), \\ (\alpha^i\beta, \alpha^k\beta) \sim (\alpha^{-k+2i}\beta, \alpha^i\beta) = (\alpha^{i-(k-i)}\beta, \alpha^{k-(k-i)}\beta). \end{cases} \tag{2.6}$$

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)* $(\alpha^i, \alpha^j\beta) \sim (\alpha^{-i}, \alpha^{j+2i}\beta)$ *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* $p_r^{k_r} \| N$ *for* $r = 1, \ldots, t$, *and let* $0 \leqslant \nu_r \leqslant k_r - 1$ *for* $r = 1, \ldots, t$. *Let* $e, f \in \mathbb{Z}$ *such that* $e \not\equiv f \pmod{p_r}$ *for* $r = 1, \ldots, t$. *Then for all* $g \in \mathbb{Z}$ *such that* $g \equiv 0 \pmod{N/\prod_{r=1}^t p_r^{k_r}}$ *and* $\tau \in \mathbb{Z}$, *we have*

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

(iv) Let $p_1, \ldots, p_t$ *be distinct prime divisors of* N *(not necessarily all the prime divisors of* N*) such that* $p_r^{k_r} \| N$ *for* $r = 1, \ldots, t$, *and let* $0 \leqslant \nu_r \leqslant k_r - 1$ *for* $r = 1, \ldots, t$. *Then for all* $e \not\equiv f \pmod{p_r}$, *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) $p_r^{k_r-\nu_r} \mid f+g$, *and*

(c) if $p_{r'}$ *is another prime divisor of* N, *then* $f+g \equiv f \pmod{p_{r'}^{k_{r'}-\nu_{r'}}}$.

In particular, $p^{k_r} \mid (f+g)\prod_{r=1}^t p_r^{\nu_r}$, *and if* $p_{r'}$ *is another prime divisor of* N *such that* $p_{r'}^{k_{r'}} \mid f\prod_{r=1}^t p_r^{\nu_r}$, *then* $p_{r'}^{k_{r'}} \mid (f+g)\prod_{r=1}^t p_r^{\nu_r}$.

Proof. (i) We have

$$\begin{aligned} (\alpha^i, \alpha^j\beta) &\sim (\alpha^j\beta, \alpha^{-i}) && \text{(using the first equivalence in (2.4))} \\ &\sim (\alpha^{-i}, \alpha^{j+2i}\beta) && \text{(using the first equivalence in (2.5)).} \end{aligned}$$

(ii) This follows from (2.6).

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

$$\begin{aligned} h &\equiv g(f-e)^{-1} && \pmod{p_r^{k_r-\nu_r}} \text{ for } r = 1, \ldots, t, \\ h &\equiv 0 && \left(\operatorname{mod} N/\textstyle\prod_{r=1}^{t} p_r^{k_r}\right). \end{aligned}$$

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

$$\begin{aligned} h(f-e)\prod_{i=1}^{t} p_r^{\nu_r} \equiv g\prod_{i=1}^{t} p_r^{\nu_r} && \pmod N, \\ g \equiv -f && \pmod{p_r^{k_r-\nu_r}}, \\ g \equiv 0 && \pmod{p_{r'}^{k_{r'}-\nu_{r'}}} \text{ for all other primes } p_{r'} \text{ dividing } N. \end{aligned}$$

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

$$\begin{aligned} h &\equiv -f(f-e)^{-1} && \pmod{p_r^{k_r-\nu_r}}, \\ h &\equiv 0 && \pmod{p_{r'}^{k_{r'}-\nu_{r'}}} \text{ for all other primes } p_{r'} \text{ dividing } N. \end{aligned}$$

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

□

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

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

and

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

For example, if $\boldsymbol{a} = (\alpha^{12}, \alpha^{11}\beta, \alpha^4, \alpha^3) \in D_{30}^4$, then $\Lambda(\boldsymbol{a}) = \{3, 4, 3\}$ and $\Gamma(\boldsymbol{a}) = \{11\}$. It is easy to see that $\Lambda(\boldsymbol{a})$ 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

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

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

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

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

$$\begin{aligned}\mathcal{C}_{\nu_r,\tau_r}^{p_r} = \{\boldsymbol{a} \in D_{2N}^n : &\min(\{v_{p_r}(i) : i \in \Lambda(\boldsymbol{a})\} \cup \{k_r\}) \geqslant \nu_r + 1,\ \emptyset \neq \Gamma(\boldsymbol{a}) \subset \tau_r + p_r^{\nu_r}\mathbb{Z},\\ &\exists j, j' \in \Gamma(\boldsymbol{a}) \text{ such that } v_{p_r}(j - j') = \nu_r\}.\end{aligned}$$

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

$$D_{2N}^n = \mathcal{A} \sqcup \left(\bigsqcup_{\substack{0 \leqslant \nu_r \leqslant k_r \\ 0 \leqslant \tau_r < p_r^{\nu_r}}} \mathcal{B}_{\nu_r,\tau_r}^{p_r} \right) \sqcup \left(\bigsqcup_{\substack{0 \leqslant \nu_r \leqslant k_r - 1 \\ 0 \leqslant \tau_r < p_r^{\nu_r}}} \mathcal{C}_{\nu_r,\tau_r}^{p_r} \right). \tag{3.1}$$

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

For $\boldsymbol{a} \in \mathcal{C}_{\nu_r,\tau_r}^{p_r}$, collect the components of $\boldsymbol{a}$ 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 $0 \leqslant i_k < N$. Let $e_s \in \mathbb{Z}_{p_r}$, $1 \leqslant s \leqslant t$, be defined by $i_s \equiv \tau_r + p_r^{\nu_r} e_s \pmod{p_r^{\nu_r+1}}$. Define

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

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

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

Then $\sigma_3(\boldsymbol{a}) = 13 - 2 + 11 = 1 \in \mathbb{Z}_3$. It is easy to see from (2.3)–(2.6) that $\sigma(\boldsymbol{a})$ is also an invariant under the Hurwitz equivalence. This allows us to further partition $\mathcal{C}_{\nu_r,\tau_r}^{p_r}$ into two invariant subsets

$$\mathcal{C}_{\nu_r,\tau_r,0}^{p_r} = \{\boldsymbol{a} \in \mathcal{C}_{\nu_r,\tau_r}^{p_r} : \sigma_{p_r}(\boldsymbol{a}) = 0\}$$

and

$$\mathcal{C}_{\nu_r,\tau_r,1}^{p_r} = \{\boldsymbol{a} \in \mathcal{C}_{\nu_r,\tau_r}^{p_r} : \sigma_{p_r}(\boldsymbol{a}) \neq 0\}.$$

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

$$D_{2N}^n = \mathcal{A} \sqcup \left(\bigsqcup_{\substack{0 \leqslant \nu_r \leqslant k_r \\ 0 \leqslant \tau < p_r^{\nu_r}}} \mathcal{B}_{\nu_r,\tau_r}^{p_r} \right) \sqcup \left(\bigsqcup_{\substack{0 \leqslant \nu_r \leqslant k_r - 1 \\ 0 \leqslant \tau < p_r^{\nu_r}}} \mathcal{C}_{\nu_r,\tau_r,0}^{p_r} \right) \sqcup \left(\bigsqcup_{\substack{0 \leqslant \nu_r \leqslant k_r - 1 \\ 0 \leqslant \tau < p_r^{\nu_r}}} \mathcal{C}_{\nu_r,\tau_r,1}^{p_r} \right) \tag{3.2}$$

for odd primes p_r dividing N.

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

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

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

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

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

$$D^n_{2N} = \mathcal{A} \sqcup \left(\bigsqcup_{\substack{0 \leqslant \nu_0 \leqslant k_0 \\ 0 \leqslant \tau_0 < 2^{\nu_0}}} \mathcal{B}^2_{\nu_0,\tau_0} \right) \sqcup \left(\bigsqcup_{\substack{0 \leqslant \nu_0 \leqslant k_0 - 1 \\ 0 \leqslant \tau_0 < 2^{\nu_0}}} \mathcal{C}^2_{\nu_0,\tau_0} \right). \tag{3.3}$$

For $\boldsymbol{a} = (\alpha^{i_1}\beta^{j_1}, \dots, \alpha^{i_n}\beta^{j_n}) \in \mathcal{C}^2_{\nu_0,\tau_0}$, where $0 \leqslant i_k \leqslant N$ and $0 \leqslant j_k \leqslant 1$, let

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

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

Having set up this framework, we are now ready to define our desired partition $\mathcal{P}$ of D^n_{2N}. Let $\mathcal{Q}$ 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 $\mathcal{P} = \mathcal{Q}$, so that any block of the partition $\mathcal{P}$ is either $\mathcal{A}$ or has the form

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

where each $\mathcal{X}^{p_r}_{\nu_r,\tau_r}$ stands for one of $\mathcal{B}^{p_r}_{\nu_r,\tau_r}$, $\mathcal{C}^{p_r}_{\nu_r,\tau_r,0}$, or $\mathcal{C}^{p_r}_{\nu_r,\tau_r,1}$. If N is even, we take $\mathcal{P}$ to be the common refinement of $\mathcal{Q}$ 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 $2 \notin R \cup S_0 \cup S_1$, and either $T = U = \emptyset$, $(T, U) = (\{2\}, \emptyset)$, or $(T, U) = (\emptyset, \{2\})$. For convenience, we will denote the block

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

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

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

By our remarks above, each block of $\mathcal{P}$ is invariant under the Hurwitz action, hence it suffices to find a set of representatives of the B_n-orbits in $\mathcal{A}$ 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.

Theorem 3.1. *(i) The B_n-orbits in $\mathcal{A}$ are represented by*

$$(\alpha^{i_1}, \ldots, \alpha^{i_n}),$$

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

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

$$(\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{\tau+E}\beta, \underbrace{\alpha^{\tau+F}\beta, \overbrace{\alpha^{\tau+G}\beta, \ldots, \alpha^{\tau+G}\beta}^{w}, \alpha^{\tau}\beta, \ldots, \alpha^{\tau}\beta}_{n-s-1}), \tag{3.4}$$

where

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

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

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

(d) for each $p_r \in S_0$, we have $\min\{v_{p_r}(i_1), \ldots, v_{p_r}(i_s), k_r\} \geqslant \nu_r + 1$, $n - s - 1 \geqslant 2$, $E \equiv p_r^{\nu_r} \pmod{p_r^{\nu_r+1}}$, $F \equiv p_r^{\nu_r} \pmod{p_r^{k_r}}$, and $p_r^{k_r} \mid G$,

(e) for each $p_r \in S_1$, we have $\min\{v_{p_r}(i_1), \ldots, v_{p_r}(i_s), k_r\} \geqslant \nu_r + 1$, $n - s - 1 \geqslant 1$, $p_r^{\nu_r} \| E$, $p_r^{k_r} \mid F$, and $p_r^{k_r} \mid G$,

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

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

(1) $2^{k_0} \mid F$ and $w = 0$ (so $u(\boldsymbol{a}) = 1$) or

(2) $F \equiv 2^{\nu_0} \pmod{2^{k_0}}$ and $n - s - 1 \geqslant w + 2$ (so $u(\boldsymbol{a}) \geqslant 2$).

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 $F \equiv G \equiv 0 \pmod{N}$.

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 $\varphi : D_{2N} \to D_{2N}/\langle \alpha^{N/p_i^{k_i}} \rangle \cong D_{2p_i^{k_i}}$ be the canonical projection. We remark that under the map $\vartheta : D_{2N}^n \to D_{2p_i^{k_i}}^n$, $\vartheta(\boldsymbol{a}) = (\varphi(a_1), \ldots, \varphi(a_n))$, 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 $N = 225 = 3^2 \cdot 5^2$, $p_1 = 3$, $p_2 = 5$,

$n = 2$, and consider the block $\Pi(\{3,5\}, \emptyset, \emptyset, \emptyset, \emptyset)(1,1)(2,3)$. Since $S_0 = S_1 = T = U = \emptyset$, only the conditions in parts (a)–(c) apply; furthermore, there are no terms of the form $\alpha^{\tau+F}$ or $\alpha^{\tau+G}$. From (ii)(b), we have $0 \leqslant \tau < 15$, $\tau \equiv 2 \pmod 3$, and $\tau \equiv 3 \pmod 5$, so $\tau = 8$. From (ii)(c), $\min\{v_3(i_1), \ldots, v_3(i_s), 2\} = 1$ and $\min\{v_5(i_1), \ldots, v_5(i_s), 2\} = 1$, so we must have $s = 1$ and $v_3(i_s) = v_5(i_s) = 1$; also, $3 \mid E$ and $5 \mid E$, so $15 \mid E$. Finally, from (ii)(a), $0 \leqslant i_1 \leqslant 225/2$. Thus, by (3.4), the equivalence classes in this block are represented by

$$(\alpha^{15i}, \alpha^{8+15e}\beta),$$

where $\gcd(15, i) = 1$, $1 \leqslant i \leqslant 15/2$, and $e \in \mathbb{Z}$.

Now, suppose instead that $N = 36 = 2^2 \cdot 3^2$, $p_0 = 2$, $p_1 = 3$, $n = 2$, and consider the block $\Pi(\{3\}, \emptyset, \emptyset, \emptyset, \{2\})(1,2)(0,7)$. From (ii)(b), we have $0 \leqslant \tau < 18$, $\tau \equiv 0 \pmod 2$, and $\tau \equiv 7 \pmod 9$, so $\tau = 16$. From (ii)(g), we have $2 \| E$. Now, (ii)(g)(2) would require that $n \geqslant 3$, so we only need to consider (ii)(g)(1); this condition implies that there are no terms of the form $\alpha^{\tau+F}$ or $\alpha^{\tau+G}$. Moreover, since $2 \in U$, both terms must be of the form $\alpha^i\beta$. Finally, from (ii)(c), we have $3^2 \mid E$, so $E \equiv 18 \pmod{36}$. Thus, the (unique) equivalence class in this block is represented by

$$(\alpha^{34}\beta, \alpha^{16}\beta).$$

Proof of Theorem 3.1. (i) This is clear.

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

Next, we show that every $\boldsymbol{a} \in \Pi(R, S_0, S_1, T, U)(\nu_r)(\tau_r)$ 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 α^i to the front, we may as well assume that $\boldsymbol{a}$ has the form

$$\boldsymbol{a} = (\alpha^{i'_1}, \ldots, \alpha^{i'_s}, \alpha^{i'_{s+1}}\beta, \ldots, \alpha^{i'_n}\beta).$$

The general idea behind our proof is to write $\boldsymbol{a}$ in the form

$$\boldsymbol{a} = (\alpha^{i'_1}, \ldots, \alpha^{i'_s}, \alpha^{\tau+e_1\prod_{p_r|N} p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+e_t\prod_{p_r|N} p_r^{\nu_r}}\beta)$$

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 $\prod p_r^{\nu_r}$ to mean $\prod_{p_r|N} p_r^{\nu_r}$ 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 τ 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 $\boldsymbol{a}$. The case $t=1$ is trivial. Suppose $t=2$. Write $\boldsymbol{a}$ in the form

$$\boldsymbol{a} = (\alpha^{i'_1}, \ldots, \alpha^{i'_s}, \alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_2\prod p_r^{\nu_r}}\beta).$$

Note that by the definition of $\mathcal{C}^{p_r}_{\nu_r,\tau_r,0}$, we cannot have $\boldsymbol{a} \in \mathcal{C}^{p_r}_{\nu_r,\tau_r,0}$ 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 $\mathcal{B}^{p_r}_{\nu_r,\tau_r}$, either $\Lambda(\boldsymbol{a}) \neq \emptyset$ and at least one of $v_{p_r}(i'_1), \ldots, v_{p_r}(i'_s)$, say $v_{p_r}(i'_k)$, is equal to ν_r, or $\Lambda(\boldsymbol{a}) = \emptyset$. First suppose that we are in the former case. Applying (2.3) and (2.4) multiple times, we can shift the term $\alpha^{i'_k}$ to the right until the last three terms of $\boldsymbol{a}$ are

$$(\alpha^{i'_k}, \alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_2\prod p_r^{\nu_r}}\beta).$$

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

$$(\alpha^{-i'_k}, \alpha^{\tau+e'_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_2\prod p_r^{\nu_r}}\beta),$$

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

$$(\alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_2\prod p_r^{\nu_r}}\beta) \sim (\alpha^{\tau+f_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_2 p_r^{k_r-\nu_r}\prod p_r^{\nu_r}}\beta) \tag{3.5}$$

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

$$(\alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_2\prod p_r^{\nu_r}}\beta) \sim (\alpha^{\tau+E}\beta, \alpha^{\tau}\beta).$$

This completes the case $t=2$.

Now assume $t>2$. Again, we write $\boldsymbol{a}$ in the form

$$\boldsymbol{a} = (\alpha^{i'_1}, \ldots, \alpha^{i'_s}, \alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+e_t\prod p_r^{\nu_r}}\beta).$$

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

$$\boldsymbol{a}' = (\alpha^{j_1}, \ldots, \alpha^{j_s}, \alpha^{\tau+f_1\prod p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+f_{t-1}\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_t\prod p_r^{\nu_r}}\beta) \sim \boldsymbol{a}$$

such that if $p_{r'}$ is another prime divisor of N such that $p_{r'}^{k_{r'}-\nu_{r'}} \mid e_t$, then $p_{r'}^{k_{r'}-\nu_{r'}} \mid f_t$ 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

$$(\alpha^{\tau+e_{t-1}\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_t\prod p_r^{\nu_r}}\beta) \sim (\alpha^{\tau+f_{t-1}\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_t p_r^{k_r-\nu_r}\prod p_r^{\nu_r}}\beta)$$

for some f_t such that if $p_{r'}$ is another prime divisor of N such that $p_{r'}^{k_{r'}-\nu_{r'}} \mid e_t$, then $p_{r'}^{k_{r'}-\nu_{r'}} \mid f_t$ also. Repeating this argument for each prime $p_r \in R$, we have

$$\begin{aligned}\boldsymbol{a} &= (\alpha^{i'_1}, \ldots, \alpha^{i'_s}, \alpha^{\tau+e_1 \prod p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+e_t \prod p_r^{\nu_r}}\beta) \\ &\qquad \sim (\alpha^{j_1}, \ldots, \alpha^{j_s}, \alpha^{\tau+g_1 \prod p_r^{\nu_r} g_1}\beta, \ldots, \alpha^{\tau+g_{t-1} \prod p_r^{\nu_r}}\beta, \alpha^{\tau+g_t \prod p_r^{\nu_r}}\beta),\end{aligned}$$

where $p_r^{k_r-\nu_r} \mid g_t$ for every prime $p_r \in R$.

Now consider $p_r \in S_0 \cup S_1$. Assume that $g_l \not\equiv g_{l+1} \equiv \cdots \equiv g_t \pmod{p_r}$. By (2.6) and Lemma 2.1(iv), we have

$$\begin{aligned}&(\alpha^{\tau+g_l \prod p_r^{\nu_r}}\beta, \alpha^{\tau+g_{l+1} \prod p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+g_t \prod p_r^{\nu_r}}\beta) \\ \sim\, &(\alpha^{\tau+g'_l \prod p_r^{\nu_r}}\beta, \alpha^{\tau+g_l \prod p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+g_t \prod p_r^{\nu_r}}\beta) \\ \sim\, &\cdots \\ \sim\, &(\alpha^{\tau+g'_l \prod p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+g'_{t-2} \prod p_r^{\nu_r}}\beta, \alpha^{\tau+g_l \prod p_r^{\nu_r}}\beta, \alpha^{\tau+g_t \prod p_r^{\nu_r}}\beta) \\ \sim\, &(\alpha^{\tau+g'_l \prod p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+g'_{t-2} \prod p_r^{\nu_r}}\beta, \alpha^{\tau+h_{t-1} \prod p_r^{\nu_r}}\beta, \alpha^{\tau+h_t \prod p_r^{k_r}}\beta),\end{aligned}$$

for some h_t such that if $p_{r'}$ is another prime divisor of N such that $p_{r'}^{k_{r'}-\nu_{r'}} \mid g_t$, then $p_{r'}^{k_{r'}-\nu_{r'}} \mid h_t$ also. Repeating this argument for each prime $p_r \in S_0 \cup S_1$, we obtain

$$\begin{aligned}\boldsymbol{a} &= (\alpha^{i'_1}, \ldots, \alpha^{i'_s}, \alpha^{\tau+e_1 \prod p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+e_t \prod p_r^{\nu_r}}\beta) \\ &\qquad \sim (\alpha^{j_1}, \ldots, \alpha^{j_s}, \alpha^{\tau+h_1 \prod p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+h_{t-1} \prod p_r^{\nu_r}}, \alpha^{\tau}\beta) = \boldsymbol{b}.\end{aligned}$$

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 $\boldsymbol{b} = (\alpha^{j_1}, \ldots, \alpha^{j_s}, \alpha^{\tau+h_1 p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+h_{t-1} p_r^{\nu_r}}, \alpha^{\tau}\beta)$. So assume that the set I of prime divisors p_r of N such that $h_1 \equiv \cdots \equiv h_{t-1} \not\equiv 0 \pmod{p_r}$ 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

$$\begin{aligned} M &\equiv 0 \pmod{p_s^{k_s}} \quad \text{for each } p_s \in J, \\ M \prod_{\substack{p \in I \\ p \neq p_r}} p &\equiv 1 \pmod{p_r^{k_r}} \quad \text{for each } p_r \in I.\end{aligned}$$

Write $\boldsymbol{b}$ as $(\alpha^{j_1}, \ldots, \alpha^{j_s}, \alpha^{\tau+h'_1 \prod_{r\in I} p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+h'_{t-1} \prod_{r\in I} p_r^{\nu_r}}, \alpha^{\tau}\beta)$. Let $x \in \mathbb{Z}$ be such that $x \not\equiv -h'_{t-1} \pmod{p_r}$ for each $p_r \in I$ and $x \equiv 0 \pmod{p_s^{k_s}}$ for each $p_s \in J$. Then, using Lemma 2.1(iii) repeatedly, we have

$$\begin{aligned}&(\alpha^{\tau+h'_{t-2} \prod_{p_r\in I} p_r^{\nu_r}}\beta, \alpha^{\tau+h'_{t-1} \prod_{p_r\in I} p_r^{\nu_r}}\beta, \alpha^{\tau}\beta) \\ \sim\, &(\alpha^{\tau+h'_{t-2} \prod_{p_r\in I} p_r^{\nu_r}}\beta, \alpha^{\tau+(h'_{t-1}+M) \prod_{p_r\in I} p_r^{\nu_r}}\beta, \alpha^{\tau+M \prod_{p_r\in I} p_r^{\nu_r}}\beta) \\ \sim\, &(\alpha^{\tau+(h'_{t-2}+x) \prod_{p_r\in I} p_r^{\nu_r}}\beta, \alpha^{\tau+(h'_{t-1}+x+M) \prod_{p_r\in I} p_r^{\nu_r}}\beta, \alpha^{\tau+M \prod_{p_r\in I} p_r^{\nu_r}}\beta) \\ \sim\, &(\alpha^{\tau+(h'_{t-2}+x) \prod_{p_r\in I} p_r^{\nu_r}}\beta, \alpha^{\tau+(h'_{t-1}+x) \prod_{p_r\in I} p_r^{\nu_r}}\beta, \alpha^{\tau}\beta).\end{aligned} \tag{3.6}$$

If $t = 3$, use the Chinese Remainder Theorem to choose x such that

$$(h'_{t-1} + x)\left(\frac{\prod_{p_{r'} \in I} p_{r'}^{\nu_{r'}}}{p_r^{\nu_r}}\right) \equiv 1 \pmod{p_r^{k_r - \nu_r}}$$

for each $p_r \in I$ and $x \equiv 0 \pmod{p_s^{k_s}}$ for each $p_s \in J$. Then the middle term becomes $\alpha^{\tau+F'}$, where $F' \equiv p_r^{\nu_r} \pmod{p_r^{k_r}}$ 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 $\boldsymbol{a}$ is equivalent to the tuple in (3.4).

If $t > 3$, choose x such that $x \not\equiv -h'_{t-1}, 0 \pmod{p_r}$ for each $p_r \in I$. Then the induction hypothesis applies to

$$\begin{aligned}(\alpha^{i'_1}, \ldots, \alpha^{i'_s}, \alpha^{\tau+h'_1 \prod_{p_r \in I} p_r^{\nu_r}}\beta, \ldots, \alpha^{\tau+h'_{t-3} \prod_{p_r \in I} p_r^{\nu_r}}\beta,&\\ \alpha^{\tau+(h'_{t-2}+x) \prod_{p_r \in I} p_r^{\nu_r}}\beta, \alpha^{\tau+(h'_{t-1}+x) \prod_{p_r \in I} p_r^{\nu_r}}\beta, \alpha^{\tau}\beta).&\end{aligned}$$

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 $\boldsymbol{a} \in \mathcal{B}^2_{\nu_0,\tau_0}$ for some ν_0 and τ_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 $\boldsymbol{a} \in \mathcal{C}^2_{\nu_0,\tau_0}$.

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 $\alpha^i\beta$ 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 $\alpha^i\beta$:

$$\begin{cases} (\alpha^{\tau+f_1 \prod p_r^{\nu_r} f_1}\beta, \alpha^{\tau+e_1 \prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_2 \prod p_r^{\nu_r}}\beta, \underbrace{\alpha^\tau\beta, \ldots, \alpha^\tau\beta}_{t-3}), & \text{if } u(\boldsymbol{a}) = 1, \\ (\alpha^{\tau+e_1 \prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_2 \prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_1 \prod p_r^{\nu_r}}\beta, \underbrace{\alpha^{\tau-g}\beta, \ldots, \alpha^{\tau-g}\beta}_{u-2}, \underbrace{\alpha^\tau\beta, \ldots, \alpha^\tau\beta}_{t-u-1}), & \\ & \text{if } u(\boldsymbol{a}) \geqslant 2, \end{cases} \tag{3.7}$$

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

$$\begin{aligned} g &\equiv 0 \pmod{N/2^{k_0}}, \\ g &\equiv 2^{\nu_0} \pmod{2^{k_0}}. \end{aligned} \tag{3.8}$$

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 $\alpha^{\tau+z \prod p_r^{\nu_r}}\beta$. Observe that by the definition of $u(\boldsymbol{a})$ and the form of the n-tuples in (3.7), there exists a term of the form $\alpha^{\tau+y \prod p_r^{\nu_r}}\beta$, where y has different parity from z, occurring before $\alpha^{\tau+z \prod p_r^{\nu_r}}\beta$.

Using the second equivalence in (2.6), we can shift $\alpha^{\tau+y\prod p_r^{\nu_r}}\beta$ to the right until we have an adjacent pair

$$(\alpha^{\tau+y\prod p_r^{\nu_r}}\beta, \alpha^{\tau+z\prod p_r^{\nu_r}}\beta).$$

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

$$(\alpha^{\tau+y'\prod p_r^{\nu_r}}\beta, \alpha^{\tau+z'\prod p_r^{\nu_r}}\beta),$$

where $z'\prod p_r^{\nu_r} \equiv -2^{\nu_0}$ or $0 \pmod{2^{k_0}}$ as desired. We can then use Lemma 2.1(iv) again for all the odd primes p_r, as in the case where N is odd, so that the term that was previously $\alpha^{\tau+z\prod p_r^{\nu_r}}\beta$ 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 $u(\boldsymbol{a}) = 1$, we want to show that

$$(\alpha^{\tau+f_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_2\prod p_r^{\nu_r}}\beta) \sim (\alpha^{\tau+E}, \alpha^{\tau+F}, \alpha^{\tau}),$$

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

$$(\alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_2\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_1\prod p_r^{\nu_r}}\beta) \sim (\alpha^{\tau+E}, \alpha^{\tau+F}, \alpha^{\tau}).$$

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

$$(\alpha^{\tau+f_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_2\prod p_r^{\nu_r}}\beta) \sim (\alpha^{\tau+f'}\beta, \alpha^{\tau+e'}\beta, \alpha^{\tau}\beta), \tag{3.9}$$

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

Now suppose $u(\boldsymbol{a}) \geqslant 2$. Notice that in $(\alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_2\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_1\prod p_r^{\nu_r}}\beta)$, we never have $x \equiv y \equiv z \pmod{p_r}$ for any p_r (because $x-y+z \equiv 0 \pmod{p_r}$). Therefore, using Lemma 2.1(iv) repeatedly to adjust the middle term, we obtain

$$\begin{aligned} &(\alpha^{\tau+e_1\prod p_r^{\nu_r}}\beta, \alpha^{\tau+e_2\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f_1\prod p_r^{\nu_r}}\beta) \\ \sim\ &(\alpha^{\tau+e''\prod p_r^{\nu_r}}\beta, \alpha^{\tau-F}\beta, \alpha^{\tau+f''\prod p_r^{\nu_r}}\beta) \\ \sim\ &(\alpha^{\tau+e''\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f'''\prod p_r^{\nu_r}}\beta, \alpha^{\tau-F}\beta) \quad \text{(using the first equivalence in (2.6))} \end{aligned} \tag{3.10}$$

where e'' is odd, f'' and f''' are even, and $f''' \equiv 0 \pmod{p_r^{k_r-\nu_r}}$ for every $p_r \in S_0$. Now, we concentrate on the first two terms $(\alpha^{\tau+e''\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f'''\prod p_r^{\nu_r}}\beta)$. Returning to the definitions of $\mathcal{B}^{p_r}_{\nu_r,\tau_r}$, $\mathcal{C}^{p_r}_{\nu_r,\tau_r,0}$, and $\mathcal{C}^{p_r}_{\nu_r,\tau_r,1}$ (for odd p_r), we see that we have $e'' \not\equiv f''' \pmod{p_r}$ for any prime p_r dividing N. Therefore, we can use Lemma 2.1(iv) repeatedly for every prime p_r to obtain

$$(\alpha^{\tau+e''\prod p_r^{\nu_r}}\beta, \alpha^{\tau+f'''\prod p_r^{\nu_r}}\beta) \sim (\alpha^{\tau+E}\beta, \alpha^{\tau}\beta). \tag{3.11}$$

Combining (3.7), (3.10), and (3.11), we obtain

$$\boldsymbol{a} \sim (\alpha^{\tau+E}\beta, \alpha^{\tau}\beta, \alpha^{\tau-F}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta, \alpha^{\tau}\beta, \ldots, \alpha^{\tau}\beta). \tag{3.12}$$

Finally, applying (2.6) repeatedly to $(\alpha^{\tau}\beta, \alpha^{\tau-F}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta)$, we obtain

$$\begin{aligned}
&(\alpha^{\tau}\beta, \alpha^{\tau-F}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta)\\
\sim\ &(\alpha^{\tau+F}\beta, \alpha^{\tau}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta)\\
\sim\ &(\alpha^{\tau+F}\beta, \alpha^{\tau+G}\beta, \alpha^{\tau}\beta, \alpha^{\tau-G}\beta, \ldots, \alpha^{\tau-G}\beta)\\
\sim\ &\cdots\\
\sim\ &(\alpha^{\tau+F}\beta, \alpha^{\tau+G}\beta, \ldots, \alpha^{\tau+G}\beta, \alpha^{\tau}\beta)
\end{aligned} \tag{3.13}$$

Combining (3.12) and (3.13), we see that $\boldsymbol{a}$ 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 $\boldsymbol{a}$, $\boldsymbol{b} \in \mathcal{A}$ are equivalent if and only if $\boldsymbol{a}$ is a permutation of $\boldsymbol{b}$.*

(ii) Two n-tuples $\boldsymbol{a}$, $\boldsymbol{b} \in \Pi(R, S_0, S_1, T, U)(\nu_r)(\tau_r)$ are equivalent if and only if $\Lambda(\boldsymbol{a}) = \Lambda(\boldsymbol{b})$, $\pi(\boldsymbol{a}) = \pi(\boldsymbol{b})$, $\sigma_p(\boldsymbol{a}) = \sigma_p(\boldsymbol{b})$ for each odd prime $p \mid N$ such that $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{C}^p_{\nu,\tau}$, and $u(\boldsymbol{a}) = u(\boldsymbol{b})$ 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 Dic_{4M} of order $4M$:

$$Dic_{4M} = \langle \alpha, \beta \mid \alpha^{2M} = 1,\ \alpha^M = \beta^2,\ \beta\alpha\beta^{-1} = \alpha^{-1}\rangle.$$

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

Hou [3] determined the B_n-orbits in the generalized quaternion group $Q^n_{2^m}$ of order 2^m and in $D^n_{2^m}$. These two families of groups share the property that for every $m \geqslant 4$, 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 $SD^n_{2^m}$ and $M^n_{2^m}$. 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 $SD^n_{2^m}$

The semidihedral group SD_{2^m} of order 2^m is defined for any $m \geqslant 3$. 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 $m \geqslant 4$. 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 $0 \leqslant i < 2^{m-1}$ and $0 \leqslant j \leqslant 1$.

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

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

and

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

Let

$$\mathfrak{A} = \{\boldsymbol{a} \in SD^n_{2^m} : \gamma(\boldsymbol{a}) = \emptyset\}.$$

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

$$\mathfrak{B}_{\nu,\tau} = \{\boldsymbol{a} \in SD^n_{2^m} : \min(\{v_2(i) : i \in \lambda(\boldsymbol{a})\} \cup \{m-2\}) = \nu - 1,\ \emptyset \neq \gamma(\boldsymbol{a}) \subset \tau + 2^\nu\mathbb{Z}\},$$

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

$$\begin{aligned}\mathfrak{C}_{\nu,\tau} = \{\boldsymbol{a} \in SD^n_{2^m} &: \min(\{v_2(i) : i \in \lambda(\boldsymbol{a})\} \cup \{m-2\}) \geqslant \nu,\ \gamma(\boldsymbol{a}) \subset \tau + 2^\nu\mathbb{Z},\\ &\exists j, j' \in \Gamma(\boldsymbol{a}) \text{ such that } v_2(j-j') = \nu\}.\end{aligned}$$

Then

$$SD^n_{2^m} = \mathfrak{A} \sqcup \left(\bigsqcup_{\substack{1\leqslant\nu\leqslant m-1\\ 0\leqslant\tau<2^\nu}} \mathfrak{B}_{\nu,\tau}\right) \sqcup \left(\bigsqcup_{\substack{0\leqslant\nu\leqslant m-2\\ 0\leqslant\tau<2^\nu}} \mathfrak{C}_{\nu,\tau}\right).$$

As in Section 3, it is easy to see that each of $\mathfrak{A}$, $\mathfrak{B}_{\nu,\tau}$, and $\mathfrak{C}_{\nu,\tau}$ is invariant under the Hurwitz action, so that it suffices to find a set of representatives of the B_n-orbits in each of $\mathfrak{A}$, $\mathfrak{B}_{\nu,\tau}$, and $\mathfrak{C}_{\nu,\tau}$.

For $\boldsymbol{a} = (\alpha^{i_1}\beta^{j_1}, \ldots, \alpha^{i_n}\beta^{j_n}) \in \mathfrak{C}_{\nu,\tau}$, where $0 \leqslant i_k < 2^{m-1}$ and $0 \leqslant j_k \leqslant 1$, let

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

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

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

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

(i) The B_n-orbits in $\mathfrak{A}$ are represented by

$$(\alpha^{i_1}, \ldots, \alpha^{i_n}),$$

where $0 \leqslant i_1 \leqslant \cdots \leqslant i_n < 2^{m-1}$.

(ii) Let $1 \leqslant \nu \leqslant m-1$ and $0 \leqslant \tau < 2^\nu$. The B_n-orbits in $\mathfrak{B}_{\nu,\tau}$ are represented by

$$(\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{\tau+2^\nu e}\beta, \alpha^\tau\beta, \ldots, \alpha^\tau\beta), \tag{4.1}$$

where $0 \leqslant i_1 \leqslant \cdots \leqslant i_s < 2^{m-1}$, $i_k \in \{\min\{i, (2^{m-2}-1)i \bmod 2^{m-1}\} : 0 \leqslant i \leqslant 2^{m-1}\}$, $\min\{\nu_2(i_1), \ldots, \nu_2(i_s), m-2\} = \nu - 1$, and $0 \leqslant e < 2^{m-1-\nu}$.

(iii) Let $1 \leqslant \nu \leqslant m-2$ and $0 \leqslant \tau < 2^\nu$. The B_n-orbits in $\mathfrak{C}_{\nu,\tau}$ are represented by

$$(\alpha^{i_1}, \ldots, \alpha^{i_s}, \alpha^{\tau+2^\nu e}\beta, \alpha^{\tau+2^\nu}\beta, \ldots, \alpha^{\tau+2^\nu}\beta, \underbrace{\alpha^\tau\beta, \ldots, \alpha^\tau\beta}_{u}), \tag{4.2}$$

where $0 \leqslant i_1 \leqslant \cdots \leqslant i_s < 2^{m-1}$, $i_k \in \{\min\{i, (2^{m-2}-1)i \bmod 2^{m-1}\} : 0 \leqslant i \leqslant 2^{m-1}\}$, $\min\{\nu_2(i_1), \ldots, \nu_2(i_s), m-2\} \geqslant \nu$, $0 \leqslant e < 2^{m-1-\nu}$, $e \equiv 1 \pmod 2$, and $u > 0$.

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

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

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

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

(iii) Two n-tuples $\boldsymbol{a}, \boldsymbol{b} \in \mathfrak{C}_{\nu,\tau}$ are equivalent if and only if $\lambda(\boldsymbol{a}) = \lambda(\boldsymbol{b})$, $u(\boldsymbol{a}) = u(\boldsymbol{b})$, and $\pi(\boldsymbol{a}) = \pi(\boldsymbol{b})$.

4.2 B_n-orbits in $M_{2^m}^n$

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

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

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

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

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

and let

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

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

Let

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

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

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

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

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

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

$$(\alpha^{i_1}, \ldots, \alpha^{i_r}, \alpha^{i_{r+1}}, \ldots, \alpha^{i_s}, \alpha^{i_{s+1}}\beta, \ldots, \alpha^{i_n}\beta), \tag{4.3}$$

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

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

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

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

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

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

[1] T. Ben-Itzhak and M. Teicher, Graph theoretic method for determining Hurwitz equivalence in the symmetric group, *Israel J. Math.* **135** (2003) 83–91.

[2] D. Gorenstein, *Finite Groups*, 2nd ed., Chelsea Publishing Company, New York, 1980.

[3] X. Hou, Hurwitz equivalence in tuples of generalized quaternion groups and dihedral groups, *Electron. J. Combin.* **15** (2008) #R80, 10pp.

[4] S. P. Humphries, Finite Hurwitz braid group actions on sequences of Euclidean reflections, *J. Algebra* **269** (2003) 556–558.

[5] V. S. Kulikov, M. Teicher, Braid monodromy factorizations and diffeomorphism types, *Izv. Math.* **64** (2000) 311–341.

[6] J. Michel, Hurwitz action on tuples of Euclidean reflections, *J. Algebra* **295** (2006) 289–292.