Major Indices and Perfect Bases for Complex Reflection Groups

Robert Shwartz*
Department of Mathematics
Bar-Ilan University
Ramat-Gan 52900, Israel
shwartr1@math.biu.ac.il

Ron M. Adin
Department of Mathematics
Bar-Ilan University
Ramat-Gan 52900, Israel
radin@math.biu.ac.il

Yuval Roichman
Department of Mathematics
Bar-Ilan University
Ramat-Gan 52900, Israel
yuvalr@math.biu.ac.il

Submitted: Aug 16, 2007; Accepted: Apr 8, 2008; Published: Apr 18, 2008
Mathematics Subject Classification: Primary 05E15, 20F55;
Secondary 20F05, 13A50.

Abstract

It is shown that, under mild conditions, a complex reflection group $G(r,p,n)$ may be decomposed into a set-wise direct product of cyclic subgroups. This property is then used to extend the notion of major index and a corresponding Hilbert series identity to these and other closely related groups.

1 Introduction

1.1 The Major Index

Let S_n be the symmetric group on n letters. S_n is a Coxeter group with respect to the Coxeter generating set $S = \{s_i \,|\, 1 \le i < n\}$, where $s_i := (i, i+1)$ $(1 \le i < n)$ are the adjacent transpositions. Let $\ell(\pi)$ be the *length* of $\pi \in S_n$ with respect to S, let

$$\mathrm{Des}(\pi) := \{1 \le i < n \,|\, \ell(\pi s_i) < \ell(\pi)\}$$

*Research of all authors was supported in part by the Israel Science Foundation, grant no. 947/04.

be the *descent set* of π (where permutations are multiplied from right to left), and let

$$\mathrm{maj}(\pi) := \sum_{i \in \mathrm{Des}(\pi)} i$$

be the *major index* of π. It is well known that

$$\ell(\pi) = \#\{i < j \mid \pi(i) > \pi(j)\},$$

the number of inversions in π, and that

$$\mathrm{Des}(\pi) = \{1 \leq i \leq n-1 \mid \pi(i) > \pi(i+1)\}.$$

The major index is involved in many classical identities on the symmetric group; see, for example, [15, 11, 12, 8]. The search for an extended major index and corresponding identities on other groups, initiated by Foata in the early nineties, turned out to be successful for the classical Weyl groups and some wreath products. In particular, the Hilbert series of the coinvariant algebra of the symmetric group S_n and of the wreath products $\mathbf{Z}_r \wr S_n$ may be expressed as generating functions for the *flag major index* on these groups [3, 5, 1]. A generalization of this result to complex reflection groups, involving the notion of *basis* for a group, is suggested in this paper. This generalization extends previous results of [3].

1.2 Bases

The concept of basis for a group [18, 16] extends the classical Fundamental Theorem for Finitely Generated Abelian Groups to the non-abelian case.

Definition 1.1. *Let G be a finite group. A sequence $\mathbf{a} = (a_1, \ldots, a_n)$ of elements of G is called a* basis *(or a* starred ordered generating system, OGS* *) for G if there exist positive integers $m_1, \ldots, m_n$ such that every element $g \in G$ has a unique presentation in the form*

$$g = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n},$$

with $0 \leq k_i < m_i$ for every $1 \leq i \leq n$.

If $m_i = o(a_i)$ (the order of the element a_i) for every $1 \leq i \leq n$ then $\mathbf{a}$ is a perfect basis *(or an* ordered generating system, OGS*) for G.*

A finite group G has a perfect basis if and only if G has a decomposition into a set-wise direct product of cyclic subgroups. Namely, a group G has a perfect basis if and only if there exist subgroups $C_1, \ldots, C_n$ of G such that

(i) $$C_i \text{ is cyclic} \qquad (\forall i),$$

(ii) $$G = C_1 \cdots C_n, \text{ and}$$

(iii) $$C_i \cap \left(C_1 \cdots \hat{C}_i \cdots C_n\right) = \{1\} \qquad (\forall i).$$

Examples:

1. pq-groups (p, q distinct primes) have a perfect basis [18].

2. The group of quaternions Q_8 has a basis, but **not** a perfect basis [18].

The major index of a permutation has an algebraic interpretation in terms of a perfect basis. The following observation is a reformulation of [3, Claim 2.1].

Observation 1.2. *Let* $s_i := (i, i+1) \in S_n$ $(1 \le i < n)$ *and*

$$t_i := s_i s_{i-1} \cdots s_1 \qquad (1 \le i < n).$$

Then $(t_{n-1}, t_{n-2}, \ldots, t_1)$ *is a perfect basis for* S_n*; namely, every permutation* $\pi \in S_n$ *has a unique presentation*

$$\pi = {t_{n-1}}^{k_{n-1}} \cdots {t_1}^{k_1},$$

where $0 \le k_i < o(t_i) = i+1$ $(1 \le i < n)$*. In this notation,*

$$\mathrm{maj}(\pi) = \sum_{i=1}^{n-1} k_i.$$

This observation was applied in [3] to solve a problem of Foata regarding the hyperoctahedral group. In this paper, this approach is extended to complex reflection groups.

2 Concepts and Results

2.1 Background: Wreath Products

The colored permutation group $G(r, n)$ is the wreath product of the cyclic group $\mathbf{Z}_r$ by the symmetric group S_n. Namely,

$$G(r,n) = \mathbf{Z}_r \wr S_n := \{((c_1, \ldots, c_n);\, \pi) \,|\, c_i \in \mathbf{Z}_r,\, \pi \in S_n\}$$

with group operation

$$((c_1, \ldots, c_n);\, \pi) \cdot ((c'_1, \ldots, c'_n);\, \pi') := ((c_1 + c'_{\pi^{-1}(1)}, \ldots, c_n + c'_{\pi^{-1}(n)});\, \pi\pi').$$

Proposition 2.1. *Let* $\tau_i := ((1, 0, \ldots, 0); t_i)$ $(0 \le i < n)$*, where* $t_i := s_i \cdots s_1 \in S_n$ $(1 \le i < n)$*, as in Observation 1.2 above, and* $t_0 = Id \in S_n$*, the identity permutation. Then* $(\tau_{n-1}, \ldots, \tau_0)$ *is a perfect basis for* $G(r, n)$*, i.e., every element* $\pi \in G(r, n)$ *has a unique presentation*

$$\pi = {\tau_{n-1}}^{k_{n-1}} \cdots {\tau_1}^{k_1} \tau_0^{k_0}, \tag{1}$$

where $0 \le k_i < o(\tau_i) = r(i+1)$ $(0 \le i < n)$.

Proposition 2.1 generalizes the first part of Observation 1.2, which concerns the special case $G(1,n) = S_n$. It is a slightly modified version of a result described in [3], where the basis elements are $\tau_0^{-1}\tau_i\tau_0$ instead of our τ_i.

Given the unique presentation (1), define the *flag major index* of a colored permutation $\pi \in G(r,n)$ by

$$\mathrm{fmaj}_{G(r,n)}(\pi) := \sum_{i=0}^{n-1} k_i,$$

the sum of exponents in (1).

2.2 General Concepts

Given a (perfect) basis $\mathbf{a} = (a_1, \ldots, a_n)$ for a group G, define the $(G, \mathbf{a})$ *flag major index* as follows. For every $g \in G$ let

$$\mathrm{fmaj}_{(G,\mathbf{a})}(g) := \sum_{i=1}^{n} k_i, \tag{2}$$

where k_i $(1 \le i \le n)$ are the exponents in the unique presentation

$$g = a_1^{k_1} \cdots a_n^{k_n} \qquad (0 \le k_i < m_i).$$

Let

$$\mathrm{Fmaj}_{(G,\mathbf{a})}(q) := \sum_{g \in G} q^{\mathrm{fmaj}_{(G,\mathbf{a})}(g)}$$

be the corresponding generating function.

By definition,

$$\mathrm{Fmaj}_{(G,\mathbf{a})}(q) = \prod_{i=1}^{n} [m_i]_q, \tag{3}$$

where

$$[m_i]_q := \frac{q^{m_i} - 1}{q - 1}.$$

Given a group G with a set of generators S, let $\ell_{(G,S)}(\cdot)$ denote the length function on G with respect to S, that is,

$$\ell_{(G,S)}(g) := \min\{\ell : g = s_1 s_2 \cdots s_\ell \text{ for some } s_i \in S\};$$

and let the Poincaré series of G (with respect to S) be the corresponding generating function

$$\mathrm{Poin}_{(G,S)}(q) := \sum_{g \in G} q^{\ell_{(G,S)}(g)}.$$

The case where (G, S) is a Coxeter system has been extensively studied (see, e.g., [14]). If G is a Coxeter group we will always assume that S is the Coxeter generating set.

Motivated by Observation 1.2 we define a *(perfect) Mahonian basis* for G as follows.

Definition 2.2. *Let* $\mathbf{a}$ *be a (perfect) basis for a group* G *and let* S *be a generating set of* G. *Then* $\mathbf{a}$ *is a (perfect)* Mahonian basis *for* G *with respect to* S *if*

$$\mathrm{Fmaj}_{(G,\mathbf{a})}(q) = \mathrm{Poin}_{(G,S)}(q);$$

namely, if the $(G, \mathbf{a})$ *flag major index is equidistributed with length (with respect to* S*).*

Let V be an n-dimensional vector space over a field $\boldsymbol{F}$ of characteristic zero, and let G be a subgroup of the general linear group $GL(V)$. Then G acts naturally on the symmetric algebra $S(V^*)$, which may be identified with the polynomial ring $P_n = \boldsymbol{F}[x_1, \ldots, x_n]$. Let Λ^G be the subalgebra of G-invariant polynomials, I_n^G the ideal (of P_n) generated by the G-invariant polynomials without constant term, and $R^G := P_n/I_n^G$ the associated coinvariant algebra. The coinvariant algebra is a direct sum of its homogeneous components, graded by degree: $R^G = \oplus_k R_k^G$. Let

$$\mathrm{Hilb}_G(q) := \sum_{k\geq 0} \dim R_k^G q^k$$

be the corresponding Hilbert series.

Definition 2.3. *Let* $\mathbf{a}$ *be a (perfect) basis for a group* $G \subset GL(V)$. *Then* $\mathbf{a}$ *is a (perfect)* Hilbertian basis *for* G *if*

$$\mathrm{Fmaj}_{(G,\mathbf{a})}(q) = \mathrm{Hilb}_G(q).$$

2.3 Main Result

Let r be a positive integer and let p be a divisor of r. The complex reflection group $G(r,p,n)$ is defined in [19] as the following subgroup of index p of the wreath product $G(r,n) = \mathbf{Z}_r \wr S_n$:

$$G(r,p,n) := \{g = ((c_1, \ldots, c_n);\ \pi) \in G(r,n) \,|\, \sum_{i=1}^{n} c_i \equiv 0 \pmod p\}.$$

For more information on these groups the reader is referred to [13]. For the coinvariant algebra and flag major index on these groups see [4].

The main result of this paper states:

Theorem 2.4. *Every complex reflection group* $G(r,p,n)$ *with parameters satisfying* $gcd(n,p,r/p) = 1$ *has a perfect Hilbertian basis.*

See Theorem 3.3 and Corollary 4.1 below. The special case $p = 1$ (wreath product) was established in [21, 2, 3].

It follows that all classical Weyl groups have perfect Hilbertian-Mahonian bases (Corollaries 4.2 and 4.3 below) and that the alternating subgroup of a Weyl group of type B has a Mahonian basis (Proposition 4.5 below). On the other hand, if $gcd(n,p,r/p) > 1$ then $G(r,p,n)$ does not necessarily have a Hilbertian basis; see Section 5 below.

3 A Perfect Basis for Complex Reflection Groups

Let $\mathbf{u} = (u_{n-1}, \ldots, u_0)$ be the following sequence of n elements in $G(r, p, n)$:

$$u_i := (\bar{c}_i;\ t_i) \qquad (0 \le i \le n-1),$$

where $t_0 \in S_n$ is the identity permutation,

$$t_i := s_i s_{i-1} \cdots s_1 = (i+1, i, \ldots, 1) \in S_n \qquad (1 \le i \le n-1),$$

$$\bar{c}_i := (1, 0, \ldots, 0, \alpha p - 1) \in \mathbf{Z}_r^n \qquad (0 \le i \le n-2),$$

and

$$\bar{c}_{n-1} := (1, 0, \ldots, 0, p-1).$$

The integer $0 \le \alpha < r/p$ will be chosen later.

Remark 3.1. *All the results below still hold if we define, more generally,*

$$\bar{c}_{n-1} := (1, 0, \ldots, 0, \beta p - 1),$$

where β is any integer satisfying $\gcd(\beta, r/p) = 1$.

Remark 3.2. *If $r = p$ then one can also take $\bar{c}_{n-1} := (0, \ldots, 0)$.*

The main result of this section is the following.

Theorem 3.3. *If $gcd(n, p, r/p) = 1$ then there exists $0 \le \alpha < r/p$ such that* $\mathbf{u}$ *above is a perfect basis for $G(r, p, n)$.*

The rest of this section is devoted to proving this result, using the Chinese Remainder Theorem and the Principle of Inclusion-Exclusion. For a discussion of the extent to which the condition $\gcd(n, p, r/p) = 1$ can be relaxed, see Section 5 below.

Lemma 3.4. *Let H be the subgroup of $G(r, p, n)$ generated by the elements $\{u_i \,|\, 0 \le i \le n-2\}$. Then H is isomorphic to $G(r, n-1)$.*

Proof of Lemma 3.4. Define a map $\phi : H \to G(r, n-1)$ by erasing, from each $\pi = (\bar{c};\, t) \in H$, the last coordinate of $\bar{c}$. Let $\psi(\pi)$ be that coordinate, so that $\psi : H \to \mathbf{Z}_r$. Since every $\pi \in H$ satisfies $|\pi(n)| = n$, it follows that ϕ and ψ are group homomorphisms. Moreover, for each $\pi = ((c_1, \ldots, c_{n-1}, c_n);\, t) \in H$:

$$c_n = (\alpha p - 1) \sum_{i=1}^{n-1} c_i,$$

since this property holds for the generators, and is invariant under the group operation in H. It follows that

$$c_1 = \ldots = c_{n-1} = 0 \Longrightarrow c_n = 0,$$

namely: ϕ is injective. It is also surjective, since

$$\{((1,0,\ldots,0);\, t_i) \,:\, 0 \le i \le n-2\}$$

is a perfect basis for $G(r,n-1)$, by Proposition 2.1 above. Thus ϕ is a group isomorphism. $\square$

Consider now the sequence $\mathbf{u} = (u_{n-1},\ldots,u_0)$ defined above. Clearly

$$o(u_i) = (i+1)r \qquad (0 \le i \le n-2)$$

and

$$o(u_{n-1}) = nr/p.$$

(The latter equality holds also if we use the definitions in Remark 3.1 or 3.2.)

The product of all these orders is $n!r^n/p = |G(r,p,n)|$. If we show that all the products

$$u_{n-1}^{k_{n-1}} \cdots u_0^{k_0} \qquad (0 \le k_i < o(u_i))$$

are distinct, then it will follow that $\mathbf{u}$ is a perfect basis for $G(r,p,n)$.

Assume that

$$u_{n-1}^{k'_{n-1}} \cdots u_0^{k'_0} = u_{n-1}^{k''_{n-1}} \cdots u_0^{k''_0} \qquad (0 \le k'_i, k''_i < o(u_i)).$$

We want to show that $k'_i = k''_i$ $(\forall i)$. It suffices to show that $k'_{n-1} = k''_{n-1}$, since then

$$u_{n-2}^{k'_{n-2}} \cdots u_0^{k'_0} = u_{n-2}^{k''_{n-2}} \cdots u_0^{k''_0}$$

and, by (the proof of) Lemma 3.4 and Proposition 2.1, this implies $k'_i = k''_i$ $(0 \le i \le n-2)$.

Indeed, by assumption

$$u_{n-1}^{k'_{n-1}-k''_{n-1}} = [u_{n-2}^{k''_{n-2}} \cdots u_0^{k''_0}][u_{n-2}^{k'_{n-2}} \cdots u_0^{k'_0}]^{-1} \in H.$$

Let $k := k'_{n-1} - k''_{n-1}$; working modulo $o(u_{n-1})$, we can assume that $0 \le k < nr/p$. $u_{n-1}^k \in H$ implies that $|u_{n-1}^k(n)| = n$ and therefore, by considering the S_n-component of u_{n-1}, $n|k$. Denote $\tilde{k} := k/n$. Then

$$u_{n-1}^k = u_{n-1}^{n\tilde{k}} = ((\tilde{k}p,\ldots,\tilde{k}p); Id),$$

where $Id \in S_n$ is the identity permutation and $0 \le \tilde{k} < r/p$. (If we use the definition in Remark 3.1 then $\tilde{k}p$ should be replaced here by $\tilde{k}\beta p$. If we use the definition in Remark 3.2 then $o(u_{n-1}) = n$, and the proof ends here.)

On the other hand, we can present $u_{n-1}^k \in H$ in the form

$$u_{n-1}^k = u_{n-2}^{k_{n-2}} \cdots u_0^{k_0} \qquad (0 \le k_i < o(u_i)).$$

The natural projection $T : H \to S_{n-1}$, defined by $T((\bar{c};\, t)) := t$, is a group homomorphism mapping the perfect basis $(u_{n-2},\ldots,u_0)$ of H onto the perfect basis $(t_{n-2},\ldots,t_0)$ of

S_{n-1}. Since $T(u_{n-1}^k) = Id$, it follows that $o(t_i) = i+1$ divides k_i; let $\tilde{k}_i := k_i/(i+1)$ $(0 \le i \le n-2)$. Now

$$u_i^{i+1} = (v_i; Id) \qquad (0 \le i \le n-2)$$

where

$$v_i := (\underbrace{1, \ldots, 1}_{i+1}, 0, \ldots, 0, (\alpha p - 1)(i+1)) \in \mathbf{Z}_r^n. \tag{4}$$

Thus

$$u_{n-1}^k = u_{n-2}^{(n-1)\tilde{k}_{n-2}} \cdots u_1^{2\tilde{k}_1} u_0^{\tilde{k}_0} = (\sum_{i=0}^{n-2} \tilde{k}_i v_i; Id).$$

So far we have

$$\sum_{i=0}^{n-2} \tilde{k}_i v_i = (\tilde{k}p, \ldots, \tilde{k}p) \in \mathbf{Z}_r^n \qquad (0 \le \tilde{k}_i < \frac{o(u_i)}{i+1} = r,\ 0 \le i \le n-2).$$

Since $v_0, \ldots, v_{n-2} \in \mathbf{Z}_r^n$ are linearly independent, we conclude that

$$\tilde{k}_{n-2} = \tilde{k}p$$

while

$$\tilde{k}_i = 0 \qquad (0 \le i \le n-3).$$

Thus

$$\tilde{k}p v_{n-2} = (\tilde{k}p, \ldots, \tilde{k}p).$$

Comparing the last coordinate on each side, we get by (4):

$$\tilde{k}p(\alpha p - 1)(n-1) = \tilde{k}p \qquad (\text{in } \mathbf{Z}_r).$$

(Multiply both sides by β for Remark 3.1.) Rewriting $(\alpha p - 1)(n-1) - 1 = (n-1)\alpha p - n$, this is equivalent to

$$\tilde{k}[(n-1)\alpha p - n] = 0 \qquad (\text{in } \mathbf{Z}_{r/p}), \tag{5}$$

where $0 \le \tilde{k} < r/p$ and $0 \le \alpha < r/p$. (Same equation for Remark 3.1, since $\gcd(\beta, r/p) = 1$.)

We want to show that there exists $0 \le \alpha < r/p$ such that (5) necessarily implies $\tilde{k} = 0$. Equivalently, we must find α such that

$$\gcd(r/p, (n-1)\alpha p - n) = 1.$$

If $r/p = 1$, every α will do. In general, we want to show that the following "False Assumption" leads to a contradiction.

False Assumption: For every $0 \le \alpha < r/p$,

$$\gcd(r/p, (n-1)\alpha p - n) > 1.$$

Lemma 3.5. *If $q > 1$ is a common divisor of r/p, $(n-1)\alpha p - n$ and $(n-1)\alpha' p - n$, where $\alpha \neq \alpha'$ and $gcd(\alpha' - \alpha, q) = 1$, then q divides* $\gcd(n, p, r/p)$.

Proof of Lemma 3.5. By assumption, q divides $((n-1)\alpha' p - n) - ((n-1)\alpha p - n) = (n-1)(\alpha' - \alpha)p$. Since $gcd(\alpha' - \alpha, q) = 1$, q divides $(n-1)p$. Thus q divides $\alpha(n-1)p - ((n-1)\alpha p - n) = n$, so that $gcd(q, n-1) = 1$. Hence q divides p as well, completing the proof of the lemma. $\square$

By the "False Assumption" above there exists, for each $0 \leq \alpha < r/p$, a common (prime) divisor of r/p and $(n-1)\alpha p - n$.

Lemma 3.6. *Assume that* $\gcd(n, p, r/p) = 1$, *and denote*

$$Q := \{q \textit{ prime} \,|\, q \textit{ divides } r/p \textit{ and } (n-1)\alpha p - n \textit{ for some } 0 \leq \alpha < r/p\}.$$

Then, for any number of distinct primes $q_1, \ldots, q_t \in Q$, the number of integers $0 \leq \alpha < r/p$ such that $(n-1)\alpha p - n$ is divisible by all of $q_1, \ldots, q_t$ is $r/(pq_1 \cdots q_t)$.

Proof of Lemma 3.6. Let $q \in Q$, and assume that it divides $(n-1)\alpha p - n$. If $\alpha' - \alpha$ is divisible by q, then clearly q divides also $(n-1)\alpha' p - n$. Conversely, if $\alpha' - \alpha$ is not divisible by the prime q then $\gcd(\alpha' - \alpha, q) = 1$. By Lemma 3.5, and since $\gcd(n, p, r/p) = 1$ by assumption, q does not divide $(n-1)\alpha' p - n$. It follows that the number of $0 \leq \alpha < r/p$ divisible by any $q \in Q$ is exactly $r/(pq)$.

We now consider any number of distinct primes $q_1, \ldots, q_t \in Q$. Suppose that q_i divides $(n-1)\alpha_i p - n$ $(1 \leq i \leq t)$. By the above argument, an integer α has the property that $(n-1)\alpha p - n$ is divisible by all of the q_i if and only if α solves the t simultaneous modular equations

$$\alpha \equiv \alpha_i \pmod{q_i} \qquad (1 \leq i \leq t).$$

A solution exists, and is unique (mod $q_1 \cdots q_t$), by the Chinese Remainder Theorem. It follows that the number of $0 \leq \alpha < r/p$ divisible by all of $q_1, \ldots, q_t$ is exactly $r/(pq_1 \cdots q_t)$. $\square$

We shall now wrap up, by counting the integers $0 \leq \alpha < r/p$ according to which primes $q \in Q$ divide $(n-1)\alpha p - n$. According to the "False Assumption", each α has at least one such q. By Lemma 3.6 and the Principle of Inclusion-Exclusion, counting gives

$$\frac{r}{p} = \sum_{q \in Q} \frac{r}{pq} - \sum_{q_1 < q_2} \frac{r}{pq_1 q_2} + \sum_{q_1 < q_2 < q_3} \frac{r}{pq_1 q_2 q_3} - \cdots.$$

Rearrangement gives

$$\frac{r}{p} \cdot \prod_{q \in Q} \left(1 - \frac{1}{q}\right) = 0,$$

which is clearly a contradiction, since Q is a finite set of integers greater than 1. This completes the proof of Theorem 3.3.

4 Identities

4.1 A Flag Major Index for $G(r,p,n)$

$G(r,p,n)$ is a subgroup of $G(r,n) = \mathbf{Z}_r \wr S_n$, and thus acts naturally on the polynomial ring $P_n = \mathbf{C}[x_1,\ldots,x_n]$; here S_n acts by permuting the variables $x_1,\ldots,x_n$, while each copy of $\mathbf{Z}_r$ acts by multiplying a suitable x_i by a complex r-th root of unity. Denote the ring of $G(r,p,n)$-invariant polynomials in P_n by $\Lambda_{r,p,n}$. Let $I_{r,p,n}$ be the ideal of P_n generated by the elements of $\Lambda_{r,p,n}$ without constant term. The quotient $R_{r,p,n} := P_n/I_{r,p,n}$ is the *coinvariant algebra* of $G(r,p,n)$. Each complex reflection group $G(r,p,n)$ acts naturally on its coinvariant algebra. Let $R^{(k)}_{r,p,n}$ be the k-th homogeneous component of the coinvariant algebra, $R_{r,p,n} = \oplus_k R^{(k)}_{r,p,n}$, and let

$$\mathrm{Hilb}_{r,p,n}(q) := \sum_{k\geq 0} \dim R^{(k)}_{r,p,n} q^k$$

be the corresponding Hilbert series. $\mathrm{Hilb}_{r,p,n}(q)$ was expressed in [4] as a generating function for $\mathrm{fmaj}_{G(r,n)}$ on a certain subset of the wreath product $G(r,n)$. Using Theorem 3.3 it will be shown that $\mathrm{Hilb}_{r,p,n}(q)$ may be expressed as a generating function for a natural flag major index on the group $G(r,p,n)$ itself. This generalizes results for $G(r,1,n)$ which were proved in [21, 2, 3].

Let $G := G(r,p,n)$ with $gcd(n,p,r/p) = 1$. Recall the perfect basis $\mathbf{u}$ for G from Theorem 3.3 and the flag major index $\mathrm{fmaj}_{(G,\mathbf{u})}$ from Definition (2).

Corollary 4.1. *If $gcd(n,p,r/p) = 1$ then $\mathbf{u}$ is a perfect Hilbertian basis for $G(r,p,n)$; namely,*

$$\mathrm{Hilb}_{r,p,n}(q) = \mathrm{Fmaj}_{(G(r,p,n),\mathbf{u})}(q),$$

where $\mathrm{Fmaj}_{(G(r,p,n),\mathbf{u})}(q) := \sum_{\pi\in S_n} q^{\mathrm{fmaj}_{(G(r,p,n),\mathbf{u})}(\pi)}$.

Proof. By Theorem 3.3 and identity (3),

$$\sum_{\pi\in S_n} q^{\mathrm{fmaj}_{G(r,p,n)}(\pi)} = [r]_q[2r]_q\cdots[(n-1)r]_q[nr/p]_q$$

where $[m]_q := \frac{q^m-1}{q-1}$. On the other hand, it is known (see, e.g., [4]) that

$$\mathrm{Hilb}_{r,p,n}(q) = [r]_q[2r]_q\cdots[(n-1)r]_q[nr/p]_q, \tag{6}$$

completing the proof. □

4.2 Classical Weyl Groups

Recall the three infinite series of classical Weyl group: the symmetric groups S_n (Weyl groups of type A), the signed permutation groups (sometimes called hyperoctahedral groups) B_n (Weyl groups of type B), and the even signed permutation groups D_n (Weyl groups of type D). We shall use here square brackets for the one-line notation of permutations, namely write

$$\pi = [\pi(1), \ldots, \pi(n)]$$

for π in S_n, B_n or D_n; round parentheses will be used for the cycle notation.

Corollary 4.2.

1. *Let*

$$\alpha_i := (i, i-1, \ldots, 1) = [i, 1, 2, \ldots, i-1, i+1, i+2, \ldots, n] \qquad (2 \le i \le n)$$

be permutations in S_n. *Then* $\mathbf{a} = (\alpha_n, \alpha_{n-1}, \ldots, \alpha_2)$ *is a perfect Hilbertian basis for the symmetric group* S_n.

2. *Let*

$$\beta_i := [-i, 1, 2, \ldots, i-1, i+1, i+2, \ldots, n] \qquad (1 \le i \le n)$$

be signed permutations in B_n. *Then* $\mathbf{b} = (\beta_n, \beta_{n-1}, \ldots, \beta_1)$ *is a perfect Hilbertian basis for the hyperoctahedral group* B_n.

3. *Let*

$$\delta_i := [-i, 1, 2, \ldots, i-1, i+1, i+2, \ldots, -n] \qquad (1 \le i \le n-1)$$

and

$$\delta_n := [n, 1, 2, \ldots, n-1]$$

be signed permutations in D_n. *Then* $\mathbf{d} = (\delta_n, \delta_{n-1}, \ldots, \delta_1)$ *is a perfect Hilbertian basis for the group of even signed permutations* D_n.

Proof. By Theorem 3.3 and Remark 3.2, $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{d}$ are perfect bases for $S_n = G(1,1,n)$, $B_n = G(2,1,n)$ and $D_n = G(2,2,n)$, respectively (using $\alpha = 1$ for B_n and D_n, with Remark 3.2 for D_n). By Corollary 4.1, these bases are Hilbertian. $\square$

Corollary 4.3. 1. *The sequence* $\mathbf{b}$ *is a perfect Mahonian basis for* B_n *(with respect to the Coxeter generating set* S*). Namely, the resulting flag major index* $\mathrm{fmaj}_{(B_n,\mathbf{b})}$ *is equidistributed with the length function* $\ell_{(B_n,S)}$ *over* D_n.

2. *The sequence* $\mathbf{d}$ *is a perfect Mahonian basis for* D_n *(with respect to the Coxeter generating set* S'*). Namely, the resulting flag major index* $\mathrm{fmaj}_{(D_n,\mathbf{d})}$ *is equidistributed with the length function* $\ell_{(D_n,S')}$ *over* D_n.

Proof. It is well known that for every Weyl group W, the Hilbert series of the coinvariant algebra of W is equal to the Poincaré series of W, namely to the generating function for length with respect to the Coxeter generators; see, e.g., [14, §3.15]. Combining this with Corollary 4.1 gives the desired result. $\square$

While the statements on types A and B are not new, see [3], the statements on type D (Corollary 4.2(3) and Corollary 4.3(2)) are new. In particular, note that $\mathrm{fmaj}_{(D_n,\mathbf{u})}$ is equidistributed with, but different from, the flag major index for D_n which was introduced by Biagioli and Caselli [5].

4.3 The Alternating Subgroup of B_n

Let B_n^+ be the alternating subgroup of the Coxeter group of type B; namely, the subgroup consisting all elements in B_n of even length.

Let $r_1 := [2, -1, 3, \ldots, n]$ and $r_i := [-1, 2, \ldots, i+1, i, i+2, i+3, \ldots, n]$ $(2 \le i \le n-1)$. $R := \{r_i \,|\, 1 \le i \le n-1\}$ is a set of generators for B_n^+ with Coxeter-like relations [9, Chapter IV Section 1 Exercise 9]. The defining relations are:

$$r_1^4 = 1$$

$$r_i^2 = 1 \qquad (1 < i < n)$$
$$(r_i r_{i+1})^3 = 1 \qquad (1 \le i < n).$$
$$(r_i r_j)^2 = 1 \qquad (|i-j| > 1)$$

Let $\ell_{(B_n^+, R\cup R^{-1})}(\pi)$ be the length of $\pi \in B_n^+$ with respect to $R \cup R^{-1}$. Let

$$v_n := ((0, \ldots, 0, 1);\ Id) = [1, 2, \ldots, -n] \in B_n,$$

and define a map $\psi : D_n \mapsto B_n^+$ by

$$\psi(w) := \begin{cases} w & \text{if } w \in B_n^+; \\ w v_n & \text{if } w \notin B_n^+. \end{cases}$$

Namely, ψ switches the sign of the last letter of w if $w \notin B_n^+$.

Fact 4.4. *ψ is a bijection.*

Recall the basis $\mathbf{d} = (\delta_n, \ldots, \delta_1)$ for D_n from Corollary 4.2(3) and let

$$\gamma_i := \psi(\delta_i) \qquad (1 \le i \le n).$$

Proposition 4.5. *(1). The sequence $\mathbf{c} = (\gamma_1, \ldots, \gamma_n)$ is a Mahonian basis for B_n^+. Namely*

(i) Every element $\pi \in B_n^+$ has a unique presentation

$$\pi = \gamma_n^{k_n} \gamma_{n-1}^{k_{n-1}} \cdots \gamma_1^{k_1} \qquad 0 \le k_i \le 2i \text{ for } 1 \le i < n \text{ and } 0 \le k_n < n. \tag{7}$$

(ii)

$$\sum_{\pi \in B_n^+} q^{\mathrm{fmaj}_{(B_n^+, \mathbf{c})}(\pi)} = \sum_{\pi \in B_n^+} q^{\ell_{(B_n^+, R\cup R^{-1})}(\pi)}. \tag{8}$$

(2). The flag major index is invariant under ψ. Namely, for every $w \in D_n$

$$\mathrm{fmaj}_{(D_n, \mathbf{d})}(w) = \mathrm{fmaj}_{(B_n^+, \mathbf{c})}(\psi(w)). \tag{9}$$

(3). For every $w \in D_n$, $\mathrm{fmaj}_{(D_n,\mathbf{d})}(w) \equiv 0 \pmod 2$ if and only if $w \in D_n \cap B_n^+$. Similarly, for every $w \in B_n^+$, $\mathrm{fmaj}_{(B_n^+,\mathbf{c})}(w) \equiv 0 \pmod 2$ if and only if $w \in D_n \cap B_n^+$.

Proof. Let w be an element in D_n. By Corollary 4.2(3), there exist unique $0 \le k_i < 2i$ $(0 \le i < n)$ and $0 \le k_n < n$ such that $w = \delta_n^{k_n} \cdots \delta_1^{k_1}$. Noticing that v_n commutes with δ_i for $i < n$ we obtain

$$\gamma_n^{k_n} \cdots \gamma_1^{k_1} = (\delta_n v_n)^{k_n} \cdots (\delta_1 v_n)^{k_1} = \delta_n^{k_n} \cdots \delta_1^{k_1} v_n^{\sum_i k_i}$$

$$= w v_n^{\mathrm{fmaj}_{(D_n,\mathbf{d})}(w)} = w v_n^{\mathrm{fmaj}_{(D_n,\mathbf{d})}(w) \bmod 2}.$$

But $\gamma_n^{k_n} \cdots \gamma_1^{k_1} \in B_n^+$ while $v_n \notin B_n^+$.
It follows that $w \in B_n^+$ if and only if $\mathrm{fmaj}_{(D_n,\mathbf{d})}(w) \bmod 2 = 0$. Hence

$$\gamma_n^{k_n} \cdots \gamma_1^{k_1} = w v_n^{\mathrm{fmaj}_{(D_n,\mathbf{d})}(w) \bmod 2} = \psi(w).$$

Since ψ is a bijection this proves (i), (2) and (3).

To prove (ii) recall from [10] the bijection $\theta : B_n^+ \mapsto D_n$

$$\theta(w) := \begin{cases} w & \text{if } w \in B_n^+; \\ ws_0 & \text{if } w \notin B_n^+, \end{cases}$$

which switches the sign of the first letter of w if $w \notin D_n$. By [10, Corollary 5.2(i)], the length is invariant under θ. Namely, for every $w \in B_n^+$

$$\ell_{(B_n^+, R\cup R^{-1})}(w) = \ell_{(D_n,S')}(\theta(w)). \tag{10}$$

Combining (9), (10) with Corollary 4.3(2) and the fact that ψ and θ are bijections we obtain

$$\sum_{\pi \in B_n^+} q^{\mathrm{fmaj}_{(B_n^+,\mathbf{c})}(\pi)} = \sum_{\pi \in B_n^+} q^{\mathrm{fmaj}_{(D_n,\mathbf{d})}(\psi^{-1}(\pi))} = \sum_{w \in D_n} q^{\mathrm{fmaj}_{(D_n,\mathbf{d})}(w)} =$$

$$= \sum_{w \in D_n} q^{\ell_{(D_n,S')}(w)} = \sum_{w \in D_n} q^{\ell_{(B_n^+,R\cup R^{-1})}(\theta^{-1}(w))} = \sum_{\pi \in B_n^+} q^{\ell_{(B_n^+,R\cup R^{-1})}(\pi)}.$$

This completes the proof of (ii). $\square$

Remarks. 1. $(\gamma_n, \ldots, \gamma_1)$ is a perfect Mahonian basis for B_n^+ if and only if n is odd. If n is even then the order of γ_n is $2n$ while k_n is bounded by n in (7), so B_n^+ is not decomposed into a set-wise direct product of the cyclic subgroups generated by $\gamma_n, \ldots, \gamma_1$; in this case $(\gamma_n, \ldots, \gamma_1)$ is a Mahonian basis for B_n^+ which is not perfect.

2. A major index and a Mahonian identity on the alternating subgroup of S_n may be found in [17]. It should be noted that, while the length function is defined there with respect to a generating set analogous to the above $R \cup R^{-1}$, there is apparently no simple interpretation, involving bases, of the major index in this case.

5 Complex Reflection Groups with No Hilbertian Basis

Proposition 5.1. *For any prime p, the group $G(p^2, p, p)$ has no perfect Hilbertian basis.*

Proof. Assume that p is a prime number for which $G(p^2, p, p)$ has a perfect Hilbertian basis. A Hilbert function of the form (6) has a unique decomposition into factors of the form $[m_i]_q$, where m_i are positive integers. It follows that, up to reordering, the p elements $t_0, t_1, \ldots, t_{p-1}$ in a perfect Hilbertian basis for $G(p^2, p, p)$ have orders $o(t_0) = p^2$, $o(t_1) = 2p^2, \ldots, o(t_{p-2}) = (p-1)p^2$ and $o(t_{p-1}) = p^2$. Let $t_i = (v_i;\ \pi_i)$, where $v_i \in (\mathbf{Z}_{p^2})^p$ with sum of entries $\equiv 0 \pmod p$ and $\pi_i \in S_p$ $(0 \le i \le p-1)$.

Both t_0 and t_{p-1} are of order p^2, and therefore neither π_0 nor π_{p-1} contains a cycle of any size $1 < i < p$. Each of them is, therefore, either a p-cycle or the identity permutation. If π_0 is a p-cycle then $t_0^p = (w_0;\ Id)$ where $w_0 = (\alpha, \ldots, \alpha)$, $\alpha \equiv 0 \pmod p$ but $\alpha \not\equiv 0 \pmod{p^2}$. If $\pi_0 = Id$ then $t_0^p = (w_0;\ Id)$ where all the entries of w_0 are $0 \pmod p$ but not all are $0 \pmod{p^2}$, and their sum is $0 \pmod{p^2}$. In both cases, $w_0 \in (p\mathbf{Z}_{p^2})^p$ is a nonzero vector whose sum of entries is $0 \pmod{p^2}$. The same conclusion holds for w_{p-1}, where $t_{p-1}^p = (w_{p-1};\ Id)$

Now let $1 < i < p$. Then $o(t_{i-1}) = ip^2$, and therefore $o(\pi_{i-1}) \mid ip^2$. If π_{i-1} is a p-cycle then $t_{i-1}^{p^3} = Id$; and since $\gcd(i, p) = 1$ this implies $t_{i-1}^{p^2} = Id$, contradicting $1 < i < p$. Thus π_{i-1} is not a p-cycle, and therefore $o(\pi_{i-1}) \mid i$. Denoting $t_{i-1}^{ip} = (w_{i-1};\ Id)$ $(1 < i < p)$, it follows that $w_{i-1} \in (p\mathbf{Z}_{p^2})^p$ is a nonzero vector whose sum of entries is $0 \pmod{p^2}$.

We conclude that all the vectors $w_0, w_1, \ldots, w_{p-2}, w_{p-1}$ belong to

$$V := \{w = (\alpha_1, \ldots, \alpha_p) \in (p\mathbf{Z}_{p^2})^p \mid \alpha_1 + \ldots + \alpha_p = 0\},$$

which is a $(p-1)$-dimensional vector space over the field $\mathbf{Z}_p$. The unique presentation property of the basis $t_0, \ldots, t_{p-1}$ implies that these p vectors are linearly independent over $\mathbf{Z}_p$. This is a contradiction which completes the proof of the proposition. $\square$

References

[1] R. M. Adin, F. Brenti and Y. Roichman, *Descent numbers and major indices for the hyperoctahedral group*, Special issue in honor of Dominique Foata's 65th birthday (Philadelphia, PA 2000), Adv. Appl. Math. **27** (2001), 210–224.

[2] R. M. Adin and Y. Roichman, *A flag major index for signed permutations*, Proc. 11th Conference on Formal Power Series and Algebraic Combinatorics, Universitat Politècnica de Catalunya, Barcelona 1999, 10–17.

[3] R. M. Adin and Y. Roichman, *The flag major index and group actions on polynomial rings*, Europ. J. Combin. **22** (2001), 431–446.

[4] E. Bagno and R. Biagioli, *Colored-descent representations for complex reflection groups*, Isreal J. Math. **160** (2007), 317–347.

[5] R. Biagioli and F. Caselli, *Invariant algebras and major indices for classical Weyl groups*, Proc. London Math. Soc. **88** (2004), 603–631.

[6] R. Biagioli and F. Caselli, *A descent basis for the coinvariant algebra of type D*, J. Algebra **275** (2004), 517-539.

[7] A. Björner and F. Brenti, *Combinatorics of Coxeter Groups*, Graduate Texts in Mathematics, Vol. 231, Springer-Verlag, 2005.

[8] A. Björner and M. L. Wachs, *Permutation statistics and linear extensions of posets*, J. Combin. Theory (Ser. A) **58** (1991), 85–114.

[9] N. Bourbaki, *Lie Groups and Lie Algebras*, English translation by Andrew Pressley, Springer, 2002.

[10] F. Brenti, V. Reiner and Y. Roichman, *On the alternating subgroups of Coxeter groups*, preprint, 2006.

[11] D. Foata and M. P. Schützenberger, *Major index and inversion number of permutations*, Math. Nachr. **83** (1978), 143–159.

[12] A. M. Garsia and I. Gessel, *Permutation statistics and partitions*, Adv. Math. **31** (1979), 288–305.

[13] M. Geck and G. Malle, *Reflection Groups*, Handbook of Algebra, Vol. 4, North-Holland, Amsterdam, to appear.

[14] J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge Studies in Advanced Math., No. 29, Cambridge Univ. Press, Cambridge, 1990.

[15] P. A. MacMahon, *Combinatory Analysis I-II*, Cambridge Univ. Press, London/New-York, 1916. (Reprinted by Chelsea, New-York, 1960.)

[16] A. Muranov, *On torsion-free groups with finite regular file bases*, preprint, 2006.

[17] A. Regev and Y. Roichman, *Permutation statistics on the alternating group*, Adv. Appl. Math. **33** (2004), 676–709.

[18] R. Shwartz, *Ordered generating systems*, preprint, 2006.

[19] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canadian J. Math. **6** (1954), 274–304.

[20] E. Steingrímsson, *Permutation statistics of indexed permutations*, Europ. J. Combin. **15** (1994), 187–205.

[21] J. Stembridge, *On the eigenvalues of representations of reflection groups and wreath products*, Pacific J. Math. **140** (1989), 353–396.