Cyclotomic factors of the descent set polynomial

Denis Chebikin [a], Richard Ehrenborg [b], Pavlo Pylyavskyy [c], Margaret Readdy [b]

[a] Department of Mathematics, MIT, Cambridge, MA 02139, United States
[b] Department of Mathematics, University of Kentucky, Lexington, KY 40506, United States
[c] Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, United States

ARTICLE INFO

ABSTRACT

We introduce the notion of the descent set polynomial as an alternative way of encoding the sizes of descent classes of permutations. Descent set polynomials exhibit interesting factorization patterns. We explore the question of when particular cyclotomic factors divide these polynomials. As an instance we deduce that the proportion of odd entries in the descent set statistics in the symmetric group $\mathfrak{S}_n$ only depends on the number on 1's in the binary expansion of n. We observe similar properties for the signed descent set statistics.

© 2008 Elsevier Inc. All rights reserved.

1. Introduction

The study of the behavior of the descent sets of permutations in the symmetric group $\mathfrak{S}_n$ on n elements usually involves such questions as maximizing the descent set or determining inequalities which hold among the entries [4,8–10,14–16]. The usual way to encode the descent statistic information is via the *Eulerian polynomial* $A_n(t) = \sum_S \beta_n(S) \cdot t^{|S|+1}$, where S runs over all subsets of $[n-1] = \{1, \ldots, n-1\}$, and $\beta_n(S)$ denotes the number of permutations of size n with descent set S. We instead introduce the descent set polynomial where the statistic of interest appears in the exponent of the variable t rather than as a coefficient. That is, the *nth descent set polynomial* is defined by

$$Q_n(t) = \sum_S t^{\beta_n(S)},$$

where S ranges over all subsets of $[n-1]$.

The degree of the descent set polynomial is given by the nth Euler number, which grows faster than exponential. Despite this, these polynomials appear to have curious factorization properties,

Table 1
The proportion $\rho(n)$ for at most five 1's in the binary expansion of n

k	$n = 2^k - 1$	$\rho(n)$	$1/2 - \rho(n)$
1	1	1	$-1/2$
2	3	$1/2$	0
3	7	$1/2$	0
4	15	$29/2^6$	$3/2^6$
5	31	$3991/2^{13}$	$3 \cdot 5 \cdot 7/2^{13}$

in particular, having factors which are *cyclotomic polynomials*; see Table 2. This paper explains the occurrence of certain cyclotomic factors. We have displayed these in boldface in the tables. Both combinatorial and number-theoretic properties (for example, the number of 1's in the binary expansion of n and the prime factorization of n) are involved in our investigations.

The divisibility by cyclotomic factors is related to the remainders of sizes of descent classes modulo certain integers. As a simplest example, $Q_n(t)$ is divisible by the second cyclotomic polynomial Φ_2 if and only if the number of even descent set classes is equal to the number of odd descent set classes. In other words, the proportion of even and odd entries in the descent set statistics is the same (in the notation below, $\rho(n) = 1/2$) if and only if -1 is a root of the descent set polynomial. Somewhat surprisingly, whether or not n has this property depends only on the number of 1's in the binary expansion of n.

The paper proceeds as follows. In Section 2 we look at the proportion of odd entries in the descent set statistics. In Section 3 we discuss this result from the viewpoint of quasisymmetric functions related to posets. We consider similar properties for the signed descent set statistics in Section 4. The natural setting for this question is to look at flag vectors of zonotopes. In Section 5 we explore patterns of descent statistics modulo $2p$ where p is a prime. Here we introduce the descent set polynomial and consider divisibility by cyclotomic polynomials. In Section 7 we explore when the descent set polynomial is divisible by the quadratic factors Φ_2^2, Φ_4^2 and Φ_{2p}^2. In Section 8 we introduce type B quasisymmetric functions and the *signed descent set polynomials*. We use the former to describe divisibility patterns of the latter. Finally, in the concluding remarks we make a number of observations on the data presented in Tables 2 and 3.

2. The proportion of odd entries

For $\pi = \pi_1 \cdots \pi_n$ a permutation in $\mathfrak{S}_n$, recall that the *descent set* of π is the subset of $[n-1]$ given by $\{i: \pi_i > \pi_{i+1}\}$. For a subset S of $[n-1]$ the number of permutations in $\mathfrak{S}_n$ with descent set S is denoted by $\beta_n(S)$.

Let $\rho(n)$ denote the proportion of odd entries in the descent statistics in the symmetric group $\mathfrak{S}_n$, that is,

$$\rho(n) = \frac{|\{S \subseteq [n-1]: \ \beta_n(S) \equiv 1 \bmod 2\}|}{2^{n-1}}.$$

For instance, $\rho(3) = 1/2$ since in the data $\beta_3(\varnothing) = \beta_3(\{1,2\}) = 1$ and $\beta_3(\{1\}) = \beta_3(\{2\}) = 2$ exactly half of the entries are odd.

The first few values of the proportion $\rho(n)$ are shown in Table 1. In this section we prove the following result.

Theorem 2.1. *The proportion of odd entries in the descent set statistics $\rho(n)$ only depends on the number of 1's in the binary expansion of the integer n.*

Recall that a composition of n is a list $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m)$ of positive integers such that $\gamma_1 + \gamma_2 + \cdots + \gamma_m = n$. The multinomial coefficient is defined by

$$\binom{n}{\gamma} = \frac{n!}{\gamma_1! \cdot \gamma_2! \cdots \gamma_m!}.$$

Define a bijection D between subsets of the set $[n-1]$ and compositions of n by sending the set $\{s_1 < s_2 < \cdots < s_{m-1}\}$ to the composition $(s_1, s_2 - s_1, s_3 - s_2, \ldots, n - s_{m-1})$. Let $\alpha_n(S)$ denote the multinomial coefficient $\binom{n}{D(S)}$. The following is a classic result due to MacMahon.

Lemma 2.2. *Let S be a subset of $[n-1]$. Then the number of permutations in $\mathfrak{S}_n$ with descent set contained in S is $\alpha_n(S)$, and we have*

$$\beta_n(S) = \sum_{T \subseteq S} (-1)^{|S-T|} \cdot \alpha_n(T).$$

We need Kummer's theorem for the multinomial coefficient version.

Theorem 2.3. *For a prime p and a composition $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m)$ of n, the largest power d such that p^d divides the multinomial coefficient $\binom{n}{\gamma}$ is equal to the number of carries when adding $\gamma_1 + \gamma_2 + \cdots + \gamma_m$ in base p.*

As a corollary we can determine whether a multinomial coefficient is even or odd. This corollary also follows from Lucas' congruence for binomial coefficients.

Corollary 2.4. *For a composition $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m)$ of n, the multinomial coefficient $\binom{n}{\gamma}$ is odd if and only if there are no carries when adding $\gamma_1 + \gamma_2 + \cdots + \gamma_m$ in base 2, that is, for all $i \neq j$, the binary expansions of γ_i and γ_j have no powers of 2 in common.*

Let the binary expansion of n be $n = 2^{j_1} + 2^{j_2} + \cdots + 2^{j_k}$, where $j_1 > j_2 > \cdots > j_k$. Call an element of $[n-1]$ *essential* if it can be expressed as $\sum_{i \in B} 2^{j_i}$ for some nonempty proper subset B of $[k]$; otherwise, call this element *nonessential*.

Lemma 2.5. *If $S \subseteq [n-1]$ contains a nonessential element s_i, then $\alpha_n(S)$ is even, that is, $\alpha_n(S) \equiv 0 \bmod 2$.*

Proof. Let $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m)$ be the associated composition $D(S)$. Notice in the addition $(\gamma_1 + \cdots + \gamma_i) + (\gamma_{i+1} + \cdots + \gamma_m) = s_i + (n - s_i) = n$ there is a carry in base 2. Hence it follows from Corollary 2.4 that $\alpha_n(S)$ is even. $\square$

Lemma 2.6. *Let S be a subset of $[n-1]$, and suppose that $i \in [n-1] - S$ is a nonessential element. Then*

$$\beta_n(S) \equiv \beta_n\big(S \cup \{i\}\big) \bmod 2.$$

Proof. By Lemmas 2.2 and 2.5, we have

$$\beta\big(S \cup \{i\}\big) = \sum_{T \subseteq S} (-1)^{|S-T|+1} \cdot \alpha_n(T) + \sum_{T \subseteq S} (-1)^{|S-T|} \cdot \alpha_n\big(T \cup \{i\}\big)$$

$$= -\beta_n(S) + \sum_{T \subseteq S} (-1)^{|S-T|} \cdot \alpha_n\big(T \cup \{i\}\big)$$

$$\equiv \beta_n(S) \bmod 2. \qquad \square$$

Lemma 2.7. *Let $S = \{s_1 < s_2 < \cdots < s_{m-1}\}$ be a subset of $[n-1]$ consisting of essential elements, so that there are nonempty proper subsets $B_1, B_2, \ldots, B_{m-1}$ of $[k]$ such that $s_r = \sum_{i \in B_r} 2^{j_i}$. Then $\alpha_n(S)$ is odd if and only if $B_1 \subseteq B_2 \subseteq \cdots \subseteq B_{m-1}$.*

Proof. Let $B_0 = \varnothing$ and $B_m = [k]$. If $B_1 \subseteq B_2 \subseteq \cdots \subseteq B_{m-1}$ then $\gamma_r = s_r - s_{r-1} = \sum_{i \in B_r - B_{r-1}} 2^{j_i}$. Then there is no carry in the addition $\gamma_1 + \cdots + \gamma_m = n$ and hence $\alpha_n(S)$ is odd. On the other hand, if $\alpha_n(S)$ is odd then there are no carries in the addition $\gamma_1 + \cdots + \gamma_m = n$, so all the 2-powers that appear in

$\gamma_1, \ldots, \gamma_m$ must be disjoint. Since s_r is given by the partial sum $\gamma_1 + \cdots + \gamma_r$, the 2-powers appearing in s_r must be contained among the 2-powers appearing in s_{r+1}, that is, $B_r \subseteq B_{r+1}$. $\quad\square$

Lemma 2.8. *Let n have k 1's in its binary expansion. Let $E = \{e_1, e_2, \ldots, e_{2^k-1}\}$ be the set of essential elements of $[n-1]$, where the e_i's are listed in increasing order: $e_1 < e_2 < \cdots < e_{2^k-1}$. Let $S = \{s_{i_1}, s_{i_2}, \ldots, s_{i_m}\}$ be a subset of E and $\widehat{S}$ be the set of indices of S, that is, $\widehat{S} = \{i_1, i_2, \ldots, i_m\}$. Then the parity of $\beta_n(S)$ is the same as the parity of $\beta_{2^k-1}(\widehat{S})$.*

Proof. From Lemma 2.7 it follows that the parity of $\alpha_n(S)$ is the same as the parity of $\alpha_{2^k-1}(\widehat{S})$. Now the result follows by

$$\beta_n(S) = \sum_{T \subseteq S} (-1)^{|S-T|} \cdot \alpha_n(T) \equiv \sum_{\widehat{T} \subseteq \widehat{S}} (-1)^{|\widehat{S}-\widehat{T}|} \cdot \alpha_{2^k-1}(\widehat{T}) = \beta_{2^k-1}(\widehat{S}) \bmod 2. \quad\square$$

We are now ready to prove Theorem 2.1.

Proof of Theorem 2.1. It follows from Lemma 2.6 that the proportion of odd entries among $\beta_n(S)$ for $S \subseteq [n-1]$ is the same as the proportion of odd entries among $\beta_n(S)$ for $S \subseteq E$. By Lemma 2.8 the proportion of odd entries among $\beta_n(S)$ for $S \subseteq E$ depends on k, the number of 1's in the binary expansion of n. $\quad\square$

3. Quasisymmetric functions and posets

In this section we relate the preceding result to the theory of quasisymmetric functions.

Consider the ring $\mathbb{Z}[\![w_1, w_2, \ldots]\!]$ of power series with bounded degree. A function f in this ring is called *quasisymmetric* if for any sequence of positive integers $\gamma_1, \gamma_2, \ldots, \gamma_m$ we have

$$\left[w_{i_1}^{\gamma_1} \cdots w_{i_k}^{\gamma_m}\right] f = \left[w_{j_1}^{\gamma_1} \cdots w_{j_k}^{\gamma_m}\right] f$$

whenever $i_1 < \cdots < i_m$ and $j_1 < \cdots < j_m$, and where $[w^\gamma]f$ denotes the coefficient of w^γ in f. Denote by QSym $\subseteq \mathbb{Z}[\![w_1, w_2, \ldots]\!]$ the ring of quasisymmetric functions.

For a composition $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m)$ the *monomial quasisymmetric function* M_γ is given by

$$M_\gamma = \sum_{i_1 < \cdots < i_m} w_{i_1}^{\gamma_1} \cdots w_{i_m}^{\gamma_m}.$$

Definition 3.1. Let P be a graded poset with rank function ρ. Define the quasisymmetric function $F(P)$ of the poset P by

$$F(P) = \sum_c M_{\rho(c)},$$

where the sum ranges over all chains $c = \{\hat{0} = x_0 < x_1 < \cdots < x_m = \hat{1}\}$ in P, $\rho(c)$ denotes the composition $(\rho(x_0, x_1), \rho(x_1, x_2), \ldots, \rho(x_{m-1}, x_m))$, and $\rho(x, y)$ denotes the rank difference $\rho(x, y) = \rho(y) - \rho(x)$.

The quasisymmetric function of a poset is multiplicative, that is, for two graded posets P and Q the quasisymmetric function of their Cartesian product is given by the product of the respective quasisymmetric functions:

$$F(P \times Q) = F(P) \cdot F(Q);$$

see Proposition 4.4 in [6]. Recall that the Boolean algebra B_n is the Cartesian power of the chain of two elements B_1, that is, $B_n = B_1^n$ and $F(B_1) = w_1 + w_2 + \cdots$. Hence we have that $F(B_n) = F(B_1)^n = M_{(1)}^n = (w_1 + w_2 + \cdots)^n$.

Let P be a graded poset of rank n. For a subset $S = \{s_1 < s_2 < \cdots < s_{m-1}\}$ of $[n-1]$, define the *flag f-vector* entry f_S to be the number of chains $\{\hat{0} = x_0 < x_1 < \cdots < x_m = \hat{1}\}$ such that $\rho(x_i) = s_i$ for $1 \leqslant i \leqslant m-1$. The *flag h-vector* is defined by the invertible relation

$$h_S = \sum_{T \subseteq S} (-1)^{|S-T|} \cdot f_T.$$

Recall the bijection D between subsets of $[n-1]$ and compositions of n defined in Section 2. By abuse of notation we will write M_S instead of $M_{D(S)}$, where the degree of the quasisymmetric function is understood. Then Lemma 4.2 in [6] states that the quasisymmetric function of a poset encodes the flag f-vector, that is,

$$F(P) = \sum_{S \subseteq [n-1]} f_S \cdot M_S.$$

The *fundamental quasisymmetric function* L_T is given by

$$L_T = \sum_{T \subseteq S} M_S.$$

Note that one can write $F(P)$ in terms of fundamental quasisymmetric functions:

$$F(P) = \sum_{S \subseteq [n-1]} h_S \cdot L_S.$$

If the poset P is a Boolean algebra B_n then $h_S = \beta_n(S)$. This is straightforward to observe using the classical R-labeling of the Boolean algebra [17, Section 3.13] or by direct enumeration [17, Corollary 3.12.2]. The multiplicative property $B_{\ell+m} \cong B_\ell \times B_m$ allows us to compute $F(B_n)$ modulo 2:

Lemma 3.2. *For $m = 2^j$ we have $F(B_m) \equiv M_{(m)}$ mod 2. Consequently, for $n = 2^{j_1} + \cdots + 2^{j_k}$ with $j_1 > \cdots > j_k \geqslant 0$ we have $F(B_n) \equiv \prod_{i=1}^{k} M_{(2^{j_i})}$ mod 2.*

Proof. It is enough to prove the first statement. Recall the congruence $(a+b)^{2^j} \equiv a^{2^j} + b^{2^j}$ mod 2. Now we have

$$F(B_{2^j}) = (w_1 + w_2 + \cdots)^{2^j} \equiv w_1^{2^j} + w_2^{2^j} + \cdots = M_{(2^j)} \text{ mod } 2. \qquad \square$$

An *ordered partition* π of a set $[k]$ is a list of non-empty pairwise disjoint sets $(B_1, B_2, \ldots, B_j)$ such that their union is $[k]$.

Theorem 3.3. *For positive integers $m_1, m_2, \ldots, m_k$, the product of the quasisymmetric functions $M_{(m_1)} \cdot M_{(m_2)} \cdots M_{(m_k)}$ is given by*

$$M_{(m_1)} \cdot M_{(m_2)} \cdots M_{(m_k)} = \sum_{\pi} M_{S(\pi)}$$

where

$$S(\pi) = D^{-1}\left(\left(\sum_{i \in B_1} m_i, \sum_{i \in B_2} m_i, \ldots, \sum_{i \in B_j} m_i\right)\right),$$

and $\pi = (B_1, B_2, \ldots, B_j)$ ranges over all ordered partitions of the set $[k]$.

Proof. The theorem can be proved by iterating Lemma 3.3 in [6]. $\square$

In view of Lemma 3.2, the following is a restatement of Theorem 2.1 in the language of quasisymmetric functions.

Theorem 3.4. *The proportion of odd coefficients in the quasisymmetric function $f = M_{(2^{j_1})} \cdot M_{(2^{j_2})} \cdots M_{(2^{j_k})}$ when expressed in the L-basis only depends on k.*

Proof. There is a natural partially ordered set Π_k on ordered partitions of $[k]$ with the cover relation $\pi \prec \sigma$ whenever σ is obtained from π by merging two adjacent blocks. Expressing the quasisymmetric function f in terms of the L-basis, we get

$$f = \sum_{\pi \in \Pi_k} M_{S(\pi)} = \sum_{\pi \in \Pi_k} \sum_{T \supseteq S(\pi)} (-1)^{|T - S(\pi)|} \cdot L_T,$$

where $S(\pi)$ is defined as in Theorem 3.3 for $m_i = 2^{j_i}$. Thus the coefficient of L_T is given by the sum

$$\sum_{\pi \in \Pi_k: \ S(\pi) \subseteq T} (-1)^{|T - S(\pi)|}.$$

As in the proof of Theorem 2.1, considering pairs of sets T and $T \cup \{i\}$, where $i \notin T$ is a nonessential element, we conclude that the proportion of odd coefficients in the expansion of f in the L-basis only depends on sets T consisting solely of essential elements. The coefficients corresponding to such T depend only on the poset Π_k, that is, only on k, because of the above expression for the coefficient of L_T. $\quad \square$

Theorem 2.1 implies that for $n = 2^j$ all the entries in the descent set statistics are odd. Hence it is interesting to look at this data modulo 4.

Theorem 3.5. *For $n = 2^j \geqslant 4$ exactly half of the descent set statistics are congruent to 1 modulo 4, and the other half are congruent to 3 modulo 4.*

Proof. First we claim that $F(B_n) \equiv M_{(n)} + 2M_{(n/2, n/2)}$ mod 4. This identity follows from the observation $(a + 2b)^2 \equiv a^2$ mod 4 and by induction on j, where the induction step is

$$F(B_{2n}) \equiv (M_{(n)} + 2M_{(n/2, n/2)})^2 \equiv M_{(n)}^2 \equiv M_{(2n)} + 2M_{(n, n)} \text{ mod 4}.$$

We have the expansion

$$M_{(n)} + 2M_{(n/2, n/2)} = M_\varnothing + 2M_{\{n/2\}}$$

$$= \sum_S (-1)^{|S|} \cdot L_S - 2 \cdot \sum_{n/2 \in S} (-1)^{|S|} \cdot L_S$$

$$= \sum_{n/2 \notin S} (-1)^{|S|} \cdot L_S - \sum_{n/2 \in S} (-1)^{|S|} \cdot L_S.$$

Hence the descent set statistics modulo 4 are given by $\beta_n(S) \equiv (-1)^{|S - \{n/2\}|}$ mod 4. Thus for $1 \notin S$ the values of $\beta_n(S)$ and $\beta_n(S \cup \{1\})$ have the opposite sign modulo 4, proving the result. $\quad \square$

4. The signed descent set statistics

A *signed permutation* of size n is of the form $\pi = \pi_1 \cdots \pi_n$ where each π_i belongs to the set $\{\pm 1, \ldots, \pm n\}$ and $|\pi_1| \cdots |\pi_n|$ is a permutation. Let $\mathfrak{S}_n^\pm$ be the set of signed permutations of size n. For ease of notation put $\pi_0 = 0$. The descent set of a signed permutation π is a subset of $[n]$ defined as $\{i: \pi_{i-1} > \pi_i\}$. For $S \subseteq [n]$ let $\beta_n^\pm(S)$ denote the number of permutations in $\mathfrak{S}_n^\pm$ with descent set S.

An equivalent way to using quasisymmetric functions to encode the flag f-vector data of a poset is via the **ab**-index. Let **a** and **b** be two non-commutative variables. For $S \subseteq [n - 1]$ let u_S be the

monomial $u_1 u_2 \cdots u_{n-1}$ where $u_i = \mathbf{a}$ if $i \notin S$ and $u_i = \mathbf{b}$ if $i \in S$. The **ab**-*index* of a poset P of rank n is defined as the sum

$$\Psi(P) = \sum_S h_S \cdot u_S.$$

When the poset P is Eulerian then its **ab**-index can be written in terms of $\mathbf{c} = \mathbf{a} + \mathbf{b}$ and $\mathbf{d} = \mathbf{ab} + \mathbf{ba}$. This more compact form removes all linear redundancies among the flag vector entries [2]. The linear relations satisfied by the flag f-vectors of Eulerian posets are known as the generalized Dehn–Sommerville relations [1]. Similarly to quasisymmetric functions, the **ab**-index and **cd**-index also have an underlying coalgebra structure. For more details, see [11].

The poset associated to signed permutations is the cubical lattice C_n, that is, the face lattice of an n-dimensional cube. Observe that C_n has rank $n + 1$. We have

$$\Psi(C_n) = \sum_{S \subseteq [n]} \beta_n^{\pm}(S) \cdot u_S.$$

A more general setting for the **cd**-index of the cube is that of zonotopes. Recall that a *zonotope* is a Minkowski sum of line segments. Associated to every zonotope Z there is a central hyperplane arrangement $\mathcal{H}$. Let L be the intersection lattice of the arrangement $\mathcal{H}$. A result by Billera, Ehrenborg, and Readdy [3] shows how to compute the **cd**-index of the zonotope from the **ab**-index of the intersection lattice L. First, introduce the linear map ω from $\mathbb{Z}\langle \mathbf{a}, \mathbf{b} \rangle$ to $\mathbb{Z}\langle \mathbf{c}, \mathbf{d} \rangle$ defined on an **ab**-monomial as follows. Replace each occurrence of **ab** by 2**d** and then replace the remaining letters by **c**. The main result in [3] states that the **cd**-index of the zonotope Z is given by

$$\Psi(Z) = \omega\big(\mathbf{a} \cdot \Psi(L)\big). \tag{4.1}$$

In particular, for the cubical lattice we have

$$\Psi(C_n) = \omega\big(\mathbf{a} \cdot \Psi(B_n)\big), \tag{4.2}$$

since the associated hyperplane arrangement is the coordinate arrangement and its intersection lattice is the Boolean algebra.

Considering Eq. (4.1) modulo 2, we observe that $\Psi(Z) \equiv \mathbf{c}^n \bmod 2$ and hence we obtain the following result.

Lemma 4.1. *All the entries of the flag h-vector of a zonotope are odd. In particular, all the signed descent set statistics are odd.*

In order to understand the flag h-vector modulo 4, we need a few lemmas.

Lemma 4.2. *After expanding the* **cd**-*polynomial*

$$\sum_{i=0}^{n-2} \mathbf{c}^i \cdot \mathbf{d} \cdot \mathbf{c}^{n-i-2}$$

into an **ab**-*polynomial, exactly half of the coefficients are odd.*

Proof. Since $\mathbf{d} \equiv \mathbf{ab} - \mathbf{ba} \bmod 2$, it is sufficient to consider the identity

$$\sum_{i=0}^{n-2} \mathbf{c}^i \cdot (\mathbf{ab} - \mathbf{ba}) \cdot \mathbf{c}^{n-i-2} = \mathbf{a} \cdot (\mathbf{a} + \mathbf{b})^{n-2} \cdot \mathbf{b} - \mathbf{b} \cdot (\mathbf{a} + \mathbf{b})^{n-2} \cdot \mathbf{a}.$$

This identity holds since the coefficient of an **ab**-polynomial in the sum is the number of occurrences of **ab** minus the number of occurrences of **ba** in the monomial. This difference only depends on the first and last letter in the monomial and the identity follows. To complete the proof, observe that out of 2^n **ab**-monomials of degree n, exactly 2^{n-1} appear in the right-hand side of the identity. $\square$

Lemma 4.3. *Let z and w be two homogeneous polynomials in $\mathbb{Z}\langle \mathbf{a}, \mathbf{b} \rangle$ of degree m and n, respectively, each having exactly half of their coefficients odd. Then the two **ab**-polynomials*

$$\mathbf{c}^i \cdot z \cdot \mathbf{c}^j \quad and \quad z \cdot \mathbf{c}^n + \mathbf{c}^m \cdot w$$

also each have exactly half of their coefficients odd.

Proof. We only prove the second statement of the lemma. We omit the proof of the first, as it is similar and easier. Let u and v be two **ab**-monomials of degrees m and n, respectively. The coefficient of $u \cdot v$ in $z \cdot \mathbf{c}^n + \mathbf{c}^m \cdot w$ is given by the sum of the coefficients of u in z and of v in w. Hence the coefficient of $u \cdot v$ is even when the coefficients of u and v are both even ($2^{m-1} \cdot 2^{n-1}$ cases) or the coefficients of u and v are both odd ($2^{m-1} \cdot 2^{n-1}$ cases). $\quad\square$

Combining Lemmas 4.2 and 4.3, we have:

Proposition 4.4. *Let $\alpha_1, \ldots, \alpha_n$ be integers, not all of which are even. When the **cd**-polynomial*

$$\sum_{i=0}^{n-2} \alpha_i \cdot \mathbf{c}^i \cdot \mathbf{d} \cdot \mathbf{c}^{n-i-2}$$

*is expanded into an **ab**-polynomial, exactly half of the coefficients are odd.*

Theorem 4.5. *For a zonotope Z either* (i) *exactly half of the flag h-vector entries are congruent to 1 modulo 4, and the other half are congruent to 3 modulo 4; or* (ii) *all the flag h-vector entries are congruent to 1 modulo 4.*

Proof. Considering the identity (4.1), we observe that the only terms in the right-hand side with non-zero coefficients modulo 4 are $\mathbf{c}^n$ and those **cd**-monomials having exactly one $\mathbf{d}$, that is,

$$\Psi(Z) \equiv \mathbf{c}^n + 2 \cdot \left(\sum_{i=0}^{n-2} \alpha_i \cdot \mathbf{c}^i \cdot \mathbf{d} \cdot \mathbf{c}^{n-i-2} \right) \bmod 4.$$

If all the α_i's are even then the flag h-vector entries are congruent to 1 modulo 4. If at least one α_i is odd, then by Proposition 4.4 exactly half of the flag h-vector entries are congruent to 1 modulo 4 and the other half are congruent to 3 modulo 4. $\quad\square$

Now we consider the cubical lattice, that is, the signed descent set statistics modulo 4.

Theorem 4.6. *For an integer $n \geqslant 2$, exactly half of the signed descent set statistics are congruent to 1 modulo 4, and the other half are congruent to 3 modulo 4.*

Proof. Observe that there are 2^n atoms in the cubical lattice. Hence $h_{\{1\}} = 2^n - 1 \equiv 3 \bmod 4$. Thus the result follows from Theorem 4.5. $\quad\square$

5. Descent set statistics modulo $2p$

For a set S of integers and a non-zero integer q, define the two notions $q \cdot S$ and S/q by

$$q \cdot S = \{q \cdot s \colon s \in S\},$$

$$S/q = \{s/q \colon s \in S \text{ and } q \mid s\}.$$

Recall that $\alpha_n(S)$ (resp., $\beta_n(S)$) denotes the number of permutations in $\mathfrak{S}_n$ with descent set contained in (resp., equal to) S.

Proposition 5.1. *Let $q = p^t$, where p is a prime and t is a non-negative integer. Let $n = r \cdot q$, where r is a positive integer. Then the descent set statistics modulo p are given by*

$$\beta_n(S) \equiv (-1)^{|S - q \cdot [r-1]|} \cdot \beta_r(S/q) \text{ mod } p,$$

where $S \subseteq [n-1]$.

Proof. Observe that

$$M^r_{(1)} = F(B_r) = \sum_{S \subseteq [r-1]} \alpha_r(S) \cdot M_S.$$

In this quasisymmetric function identity make the substitution $w_i \longmapsto w_i^q$. We then obtain

$$\begin{aligned}
M^r_{(q)} &= \sum_{S \subseteq [r-1]} \alpha_r(S) \cdot M_{q \cdot S} \\
&= \sum_{S \subseteq [r-1]} \sum_{\substack{T \subseteq [n-1] \\ q \cdot S \subseteq T}} \alpha_r(S) \cdot (-1)^{|T - q \cdot S|} \cdot L_T \\
&= \sum_{T \subseteq [n-1]} \sum_{q \cdot S \subseteq T} \alpha_r(S) \cdot (-1)^{|T - q \cdot S|} \cdot L_T \\
&= \sum_{T \subseteq [n-1]} (-1)^{|T - q \cdot [r-1]|} \cdot \left(\sum_{S \subseteq T/q} \alpha_r(S) \cdot (-1)^{|T/q - S|} \right) \cdot L_T \\
&= \sum_{T \subseteq [n-1]} (-1)^{|T - q \cdot [r-1]|} \cdot \beta_r(T/q) \cdot L_T.
\end{aligned}$$

Since $M^q_{(1)} \equiv M_{(q)}$ mod p, we have $F(B_n) = (M^q_{(1)})^r \equiv M^r_{(q)}$ mod p. Now by reading off the coefficients of L_T, the result follows. □

Corollary 5.2. *Let $q = p^t$, where p is a prime and t is a non-negative integer. Then*

$$\beta_q(S) \equiv (-1)^{|S|} \text{ mod } p.$$

Proof. The claim can be deduced from Proposition 5.1 by setting $r = 1$. A direct argument proceeds as follows. Since $(a + b)^q \equiv a^q + b^q$ mod p, we have

$$\begin{aligned}
F(B_q) &= (w_1 + w_2 + \cdots)^q \\
&\equiv w_1^q + w_2^q + \cdots \\
&= M_{(q)} = \sum_S (-1)^{|S|} \cdot L_S \text{ mod } p.   \square
\end{aligned}$$

Corollary 5.3. *Let $q = p^t$, where p is a prime and t is a non-negative integer. Then*

$$\beta_{2q}(S) \equiv (-1)^{|S - \{q\}|} \text{ mod } p.$$

Proof. The result follows from Proposition 5.1 by setting $r = 2$ and noting that $\beta_2(\varnothing) = \beta_2(\{1\}) = 1$. □

For n having the binary expansion $n = 2^{j_1} + 2^{j_2} + \cdots + 2^{j_k}$, where $j_1 > j_2 > \cdots > j_k \geqslant 0$, recall that an element $j \in [n-1]$ is nonessential if j is not a sum of a subset of $\{2^{j_1}, 2^{j_2}, \ldots, 2^{j_k}\}$.

Theorem 5.4. *Let $q = p^t$ for p an odd prime and t a non-negative integer, and let $n = r \cdot q$, where r is a positive integer. Suppose that there is a nonessential element $j \in [n-1]$ that is not divisible by q. Furthermore, suppose*

that there exist integers a and b not divisible by p such that $a \equiv b$ mod 2, and $\beta_n(S)$ is congruent to either a or b modulo p for all $S \subseteq [n-1]$. Then

$$\left|\left\{S \subseteq [n-1]: \beta_n(S) \equiv a \text{ mod } 2p\right\}\right| = \left|\left\{S \subseteq [n-1]: \beta_n(S) \equiv b \text{ mod } 2p\right\}\right|,$$

$$\left|\left\{S \subseteq [n-1]: \beta_n(S) \equiv a + p \text{ mod } 2p\right\}\right| = \left|\left\{S \subseteq [n-1]: \beta_n(S) \equiv b + p \text{ mod } 2p\right\}\right|.$$

In the case when the proportion $\rho(n)$ is 1/2, the four cardinalities above are all equal to 2^{n-3}.

Proof. Consider the collection of sets $S \subseteq [n-1]$ such that $\beta_n(S) \equiv a \equiv b$ mod 2. For S in this collection such that $j \notin S$, we have $\beta_n(S) \equiv \beta_n(S \cup \{j\})$ mod 2. However, since q does not divide j, we have $\beta_n(S) \equiv -\beta_n(S \cup \{j\})$ mod p by Proposition 5.1, that is, $\beta_n(S) \not\equiv \beta_n(S \cup \{j\})$ mod p, as a (resp., b) is not congruent to $-a$ (resp., $-b$) modulo p. Hence this collection splits into two classes of equal size when divided according to the value of $\beta(S)$ modulo $2p$. The same argument holds for the sets S satisfying $\beta(S) \equiv a + p \equiv b + p$ mod 2. $\square$

By the Chinese remainder theorem, we have $\beta(S) \equiv \pm 1, p \pm 1$ mod $2p$. For non-Mersenne primes we can say more.

Theorem 5.5. *Let $q = p^t$ be an odd prime power which has k 1's in its binary expansion. Suppose that $q > 2^k - 1$, that is, q is not a Mersenne prime. Then*

$$\left|\left\{S \subseteq [q-1]: \beta_q(S) \equiv 1 \text{ mod } 2p\right\}\right| = \left|\left\{S \subseteq [q-1]: \beta_q(S) \equiv -1 \text{ mod } 2p\right\}\right|,$$

$$\left|\left\{S \subseteq [q-1]: \beta_q(S) \equiv p - 1 \text{ mod } 2p\right\}\right| = \left|\left\{S \subseteq [q-1]: \beta_q(S) \equiv p + 1 \text{ mod } 2p\right\}\right|.$$

In the case the proportion $\rho(q)$ is 1/2, the four cardinalities above are equal to 2^{q-3}.

Proof. Since $q > 2^k - 1$, as in the proof of Theorem 3.4 there exists a nonessential element $j \in [q-1]$. Thus Theorem 5.4 applies. $\square$

When $q = p$ is a prime and $k = 2$, Theorem 5.5 applies only to the Fermat primes which are greater than 3, that is, 5, 17, 257 and 65537. We also know that the proportion is 1/2 for the case $k = 3$, that is, primes whose binary expansion has three 1's. The first few such primes are $7, 11, 13, 19, 37, 41, 67, 73, 97$; see sequence A081091 in The On-Line Encyclopedia of Integer Sequences.

For prime powers of the form $q = p^t$ with $t \geqslant 2$, the only case with $k = 2$ we know is $q = 3^2$. Similarly, with $k = 3$ we know six cases: $5^2, 7^2, 3^4, 17^2, 23^2, 257^2$ and 65537^2. It is not surprising that the squares of the Fermat's primes and the square of 3^2 appear in this list. The two sporadic cases are 7^2 and 23^2.

The next theorem concerns permutations of size twice a prime power.

Theorem 5.6. *Let $q = p^t$ be an odd prime power which has k 1's in its binary expansion. Then*

$$\left|\left\{S \subseteq [2q-1]: \beta_{2q}(S) \equiv 1 \text{ mod } 2p\right\}\right| = \left|\left\{S \subseteq [2q-1]: \beta_{2q}(S) \equiv -1 \text{ mod } 2p\right\}\right|,$$

$$\left|\left\{S \subseteq [2q-1]: \beta_{2q}(S) \equiv p - 1 \text{ mod } 2p\right\}\right| = \left|\left\{S \subseteq [2q-1]: \beta_{2q}(S) \equiv p + 1 \text{ mod } 2p\right\}\right|.$$

In the case the proportion $\rho(q)$ is 1/2, the four cardinalities above are equal to 2^{2q-3}.

Proof. By Corollary 5.3, $\beta_{2q}(S) \equiv (-1)^{|S-\{q\}|}$ mod p. Furthermore, since $2q$ is even, the element 1 is nonessential, and Theorem 5.4 applies. $\square$

6. The descent set polynomial

A different approach to view the results from the previous sections is in terms of the *descent set polynomial*

$$Q_n(t) = \sum_{S \subseteq [n-1]} t^{\beta_n(S)}.$$

The degree of this polynomial is the nth Euler number E_n. For $n \geqslant 2$ the polynomial is divisible by $2t$. Theorems 2.1, 3.5, 5.5 and 5.6 can be reformulated as follows.

Theorem 6.1.

(i) *For a positive integer n we have $Q_n(-1) = 2^n \cdot (1/2 - \rho(n))$. In particular, when n has two or three 1's in its binary expansion, then -1 is a root of $Q_n(t)$.*

(ii) *For $n = 2^j \geqslant 4$ the imaginary unit i is a root of $Q_n(t)$.*

(iii) *Let $q = p^t$ be a prime power, where p is an odd prime. Suppose that q has k 1's in its binary expansion and satisfies $q > 2^k - 1$. Let ζ be a primitive $2p$th root of unity. Then*

$$Q_q(\zeta) = 2^q \cdot \text{Re}(\zeta) \cdot \left(\rho(q) - \frac{1}{2} \right),$$

where $\text{Re}(\zeta)$ denotes the real part of ζ.

(iv) *Let $q = p^t$ be a prime power, where p is an odd prime. Suppose that q has k 1's in its binary expansion. Let ζ be a primitive $2p$th root of unity. Then*

$$Q_{2q}(\zeta) = 2^{2q} \cdot \text{Re}(\zeta) \cdot \left(\rho(q) - \frac{1}{2} \right).$$

It is curious to observe that the polynomial $Q_n(t)$ quite often has zeroes occurring at roots of unity. An equivalent formulation is that $Q_n(t)$ often has cyclotomic polynomials $\Phi_k(t)$ as factors. (Recall that the *cyclotomic polynomial* $\Phi_k(t)$ is defined as the product $\prod_\zeta (t - \zeta)$, where ζ ranges over all primitive kth roots of unity.) See Table 2 for the cyclotomic factors of $Q_n(t)$ for $n \leqslant 23$.

Lemma 6.2. *Let q be an odd prime power. Then the cyclotomic polynomial Φ_q does not divide the descent set polynomial $Q_n(t)$.*

Proof. If q is a power of an odd prime p then $\Phi_q(1) = p$. Since $Q_n(1) = 2^{n-1}$ has no odd factors, the lemma follows. □

Lemma 6.3. *Let q be the odd prime power p^t. Then*

(i) *If $n = 2^j$ then the cyclotomic polynomial Φ_{2q} does not divide $Q_n(t)$.*

(ii) *If n has four 1's in its binary expansion and $p \geqslant 5$ then the cyclotomic polynomial Φ_{2q} does not divide $Q_n(t)$.*

(iii) *If n has five 1's in its binary expansion and $p \geqslant 11$ then the cyclotomic polynomial Φ_{2q} does not divide $Q_n(t)$.*

Proof. We have $\Phi_{2q}(-1) = p$. Since $Q_n(-1) = 2^n \cdot (1/2 - \rho(n))$ the result follows by consulting Table 1. □

7. Quadratic factors in the descent set polynomial

In order to study the double root behavior of the descent set polynomial $Q_n(t)$ or, equivalently, quadratic factors in $Q_n(t)$, we need to prove a few identities for the descent set statistics. We begin

Table 2
Cyclotomic factors of $Q_n(t)$

n	Degree	Cyclotomic factors of $Q_n(t)$
3	2	Φ_2
4	5	Φ_4^2
5	16	$\Phi_2^2 \cdot \Phi_{10}$
6	61	$\Phi_2^2 \cdot \Phi_6^2 \cdot \Phi_{10}$
7	272	Φ_2
8	1385	$\Phi_4^2 \cdot \Phi_{28}$
9	7936	$\Phi_2^2 \cdot \Phi_6 \cdot \Phi_{18}$
10	50521	$\Phi_2^2 \cdot \Phi_6 \cdot \Phi_{10}^2 \cdot \Phi_{18} \cdot \Phi_{30}$
11	353792	$\Phi_2 \cdot \Phi_6 \cdot \Phi_{22}$
12	2702765	$\Phi_2^2 \cdot \Phi_6 \cdot \Phi_{10} \cdot \Phi_{18} \cdot \Phi_{22}^2 \cdot \Phi_{66} \cdot \Phi_{110} \cdot \Phi_{198}$
13	22368256	$\Phi_2 \cdot \Phi_{26}$
14	$1.993 \cdot 10^8$	$\Phi_2 \cdot \Phi_2 \cdot \Phi_4 \cdot \Phi_{14} \cdot \Phi_{14} \cdot \Phi_{26} \cdot \Phi_{28} \cdot \Phi_{182}$
15	$1.904 \cdot 10^9$	–
16	$1.939 \cdot 10^{10}$	$\Phi_4^2 \cdot \Phi_{12} \cdot \Phi_{20} \cdot \Phi_{44} \cdot \Phi_{52} \cdot \Phi_{60} \cdot \Phi_{156} \cdot \Phi_{220} \cdot \Phi_{260} \cdot \Phi_{572}$
17	$2.099 \cdot 10^{11}$	$\Phi_2^2 \cdot \Phi_{34}$
18	$2.405 \cdot 10^{12}$	$\Phi_2^2 \cdot \Phi_6^2 \cdot \Phi_{18} \cdot \Phi_{34} \cdot \Phi_{102} \cdot \Phi_{306}$
19	$2.909 \cdot 10^{13}$	$\Phi_2 \cdot \Phi_{38}$
20	$3.704 \cdot 10^{14}$	$\Phi_2^2 \cdot \Phi_6 \cdot \Phi_{10} \cdot \Phi_{30} \cdot \Phi_{34} \cdot \Phi_{38}^2 \cdot \Phi_{102} \cdot \Phi_{114} \cdot \Phi_{170}$ $\cdot \Phi_{190} \cdot \Phi_{510} \cdot \Phi_{570} \cdot \Phi_{646} \cdot \Phi_{1938} \cdot \Phi_{3230} \cdot \Phi_{9690}$
21	$4.951 \cdot 10^{15}$	$\Phi_2 \cdot \Phi_6 \cdot \Phi_{14} \cdot \Phi_{42}$
22	$6.935 \cdot 10^{16}$	$\Phi_2 \cdot \Phi_2 \cdot \Phi_{14} \cdot \Phi_{22} \cdot \Phi_{22} \cdot \Phi_{154}$
23	$1.015 \cdot 10^{18}$	–

by introducing the multivariate **ab**- and **cd**-indexes. Let $\mathbf{a}_1, \mathbf{a}_2, \ldots$ and $\mathbf{b}_1, \mathbf{b}_2, \ldots$ be non-commutative variables. For $S \subseteq [n-1]$ let u_S be the monomial $u_1 u_2 \cdots u_{n-1}$ where $u_i = \mathbf{a}_i$ if $i \notin S$ and $u_i = \mathbf{b}_i$ if $i \in S$. The *multivariate* **ab**-*index* of a poset P of rank n is defined as the sum

$$\Psi(P) = \sum_S h_S \cdot u_S,$$

where S ranges over all subsets of $[n-1]$.

Lemma 7.1. *For an Eulerian poset P the multivariate **ab**-index can be written in terms of the non-commutative variables $\mathbf{c}_i = \mathbf{a}_i + \mathbf{b}_i$ and $\mathbf{d}_{i,i+1} = \mathbf{a}_i \mathbf{b}_{i+1} + \mathbf{b}_i \mathbf{a}_{i+1}$.*

Proof. Observe that by adding the index i to the ith letter in an **ab**-monomial of degree $n-1$, we obtain a natural bijection between the regular and the multivariate **ab**-indices of the same poset P. Thus the statement of the lemma is equivalent to the statement that the regular **ab**-index of P can be expressed in terms of the variables $\mathbf{c} = \mathbf{a} + \mathbf{b}$ and $\mathbf{d} = \mathbf{ab} + \mathbf{ba}$. ◻

In this case, we call the resulting polynomial the *multivariate* **cd**-*index*. Observe that for a rank n Eulerian poset each of the indices 1 through n appears in each monomial of the multivariate **cd**-index.

Proposition 7.2. *Let h_S be the flag h-vector of an Eulerian poset P of rank n, or more generally, h_S belongs to the generalized Dehn–Sommerville subspace. Let $T \subseteq [n-1]$ such that T contains an interval $[s,t] = \{s, s+1, \ldots, t\}$ of odd cardinality with $s-1, t+1 \notin T$. Then*

$$\sum_{S \subseteq [n-1]} (-1)^{|S \cap T|} \cdot h_S = 0.$$

Proof. The sum is obtained from the multivariate **ab**-index of the poset P by setting $\mathbf{a}_i = 1$ and

$$\mathbf{b}_i = \begin{cases} -1 & \text{if } i \in T, \\ 1 & \text{otherwise.} \end{cases}$$

Notice that $\mathbf{c}_i = 0$ for $i \in [s,t]$ and that $\mathbf{d}_{s-1,s} = \mathbf{d}_{t,t+1} = 0$. If $s = 1$ we set $\mathbf{d}_{0,1} = 0$, and if $t = n-1$ we set $\mathbf{d}_{n-1,n} = 0$. Since P is Eulerian, the multivariate **ab**-index can be written in terms of multivariate **cd**-monomials (Lemma 7.1). A multivariate **cd**-monomial that contains $\mathbf{d}_{s-1,s}$ or $\mathbf{d}_{t,t+1}$ evaluates to zero. Since the interval $[s,t]$ has odd size, a multivariate **cd**-monomial not containing $\mathbf{d}_{s-1,s}$ and $\mathbf{d}_{t,t+1}$ must contain at least one variable $\mathbf{c}_i$ with $i \in [s,t]$. Hence this monomial also evaluates to zero. $\quad\square$

Observe that the identity in Proposition 7.2 is a part of the generalized Dehn–Sommerville relations; see [1].

Theorem 7.3. *If the binary expansion of n has two 1's and n > 3, then Φ_2^2 divides $Q_n(t)$.*

Proof. Suppose that $n = m_1 + m_2$, where $m_1 = 2^{j_1}$, $m_2 = 2^{j_2}$, and $j_1 > j_2$. From the proof of Theorem 3.4 we have

$$\beta_n(S) \equiv \begin{cases} 1 \mod 2 & \text{if } |S \cap \{m_1, m_2\}| = 0, 2, \\ 0 \mod 2 & \text{if } |S \cap \{m_1, m_2\}| = 1. \end{cases}$$

Hence

$$Q_n'(-1) = \sum_{S \subseteq [n-1]} \beta_n(S) \cdot (-1)^{\beta_n(S)-1} = \sum_{S \subseteq [n-1]} (-1)^{|S \cap \{m_1, m_2\}|} \cdot \beta_n(S),$$

which is zero by Proposition 7.2. $\quad\square$

Theorem 7.4. *If $n = 2^j \geqslant 4$ then Φ_4^2 divides $Q_n(t)$.*

Proof. Let $m = n/2$. The proof of Theorem 3.5 states that $\beta(S) \equiv (-1)^{|S-\{m\}|} \mod 4$. Let i be the imaginary unit, so that $i^2 = -1$. Observe that $i^{(-1)^k-1} = (-1)^k$. We have

$$Q_n'(i) = \sum_{S \subseteq [n-1]} \beta_n(S) \cdot i^{\beta_n(S)-1} = \sum_{S \subseteq [n-1]} (-1)^{|S-\{m\}|} \cdot \beta_n(S).$$

By Proposition 7.2, $Q_n'(i) = 0$ since $S - \{m\} = S \cap \{1, \ldots, m-1, m+1, \ldots, n-1\}$ and $m-1$ is odd. $\quad\square$

The next result applies to prime powers that have two 1's in their binary expansion. The only cases known so far are the five known Fermat primes $3, 5, 17, 257, 65537$ and the prime power 3^2.

Theorem 7.5. *Let $q = p^t$ be a prime power, where p is an odd prime and assume that q has two 1's in its binary expansion. Then the cyclotomic polynomial Φ_{2p}^2 divides $Q_{2q}(t)$.*

Proof. In this case $n = 2q = m + 2$, where $m = 2^j$. From the proof of Theorem 3.4 we have

$$\beta_{2q}(S) \equiv \begin{cases} 1 \mod 2 & \text{if } |S \cap \{2, m\}| = 0, 2, \\ 0 \mod 2 & \text{if } |S \cap \{2, m\}| = 1. \end{cases}$$

Hence combining it with the proof of Corollary 5.3, we have

$$\beta_{2q}(S) \equiv \begin{cases} (-1)^{|S-\{q\}|} \mod 2p & \text{if } |S \cap \{2, m\}| = 0, 2, \\ p + (-1)^{|S-\{q\}|} \mod 2p & \text{if } |S \cap \{2, m\}| = 1. \end{cases}$$

Thus for $\zeta = \mathrm{Re}(\zeta) + \mathrm{Im}(\zeta) \cdot \mathrm{i}$ a $2p$th primitive root of unity, we have that

$$\zeta^{\beta_{2q}(S)} = (-1)^{|S \cap \{2,m\}|} \cdot \zeta^{(-1)^{|S-\{q\}|}}$$
$$= (-1)^{|S \cap \{2,m\}|} \cdot \left(\mathrm{Re}(\zeta) + (-1)^{|S-\{q\}|} \cdot \mathrm{Im}(\zeta) \cdot \mathrm{i}\right).$$

Evaluating the sum and using the fact that

$$\left|S \cap \{2,m\}\right| + \left|S - \{q\}\right| \equiv \left|S \cap \{2,q,m\}\right| \bmod 2$$

we have

$$\zeta \cdot Q'_{2q}(\zeta) = \sum_{S \subseteq [2q-1]} \beta_{2q}(S) \cdot \zeta^{\beta_{2q}(S)}$$
$$= \mathrm{Re}(\zeta) \cdot \sum_{S \subseteq [2q-1]} (-1)^{|S \cap \{2,m\}|} \cdot \beta_{2q}(S) + \mathrm{Im}(\zeta) \cdot \mathrm{i} \cdot \sum_{S \subseteq [2q-1]} (-1)^{|S \cap \{2,q,m\}|} \cdot \beta_{2q}(S),$$

where both sums vanish by Proposition 7.2. □

8. The signed descent set polynomial

Similarly to the descent set polynomial we can define the *signed descent set polynomial:*

$$Q_n^{\pm}(t) = \sum_{S \subseteq [n]} t^{\beta_n^{\pm}(S)};$$

see Section 4 for definitions relevant to signed permutations. The degree of this polynomial is the nth signed Euler number $E_n^{\pm}$, which is the number of alternating signed permutations of size n. Yet again, for $n \geqslant 1$ this polynomial is divisible by $2t$. Theorem 4.6 can now be stated as follows.

Theorem 8.1. *For $n \geqslant 2$ the signed descent set polynomial $Q_n^{\pm}(t)$ has the cyclotomic factor Φ_4.*

The space of quasisymmetric functions of type B is defined as $\mathrm{BQSym} = \mathbb{Z}[s] \otimes \mathrm{QSym}$. Quasisymmetric functions of type B were first defined by Chow [5]. We will view them to be functions in the variables $s, w_1, w_2, \ldots$, that are quasisymmetric in $w_1, w_2, \ldots$. For a composition $(\gamma_0, \ldots, \gamma_m)$ define the monomial quasisymmetric function of type B by

$$M^B_{(\gamma_0, \gamma_1, \ldots, \gamma_m)} = s^{\gamma_0 - 1} \cdot M_{(\gamma_1, \ldots, \gamma_m)}.$$

A third method to encode the flag vector data of a poset P of rank at least 1 is the *quasisymmetric function of type B*

$$F_B(P) = \sum_c M^B_{\rho(c)}, \tag{8.1}$$

where the sum is over all chains $c = \{\hat{0} = x_0 < x_1 < \cdots < x_m = \hat{1}\}$ in the poset P; see [12]. A different way to write Eq. (8.1) is

$$F_B(P) = \sum_{\hat{0} < x \leqslant \hat{1}} s^{\rho(x)-1} \cdot F\left([x, \hat{1}]\right). \tag{8.2}$$

The diamond product of two posets P and Q is

$$P \diamond Q = \left(P - \{\hat{0}\}\right) \times \left(Q - \{\hat{0}\}\right) \cup \{\hat{0}\}.$$

Using identity (8.2) one can show that the type B quasisymmetric function of a poset is multiplicative with respect to the diamond product of posets, that is, $F_B(P \diamond Q) = F_B(P) \cdot F_B(Q)$. Applying the bijection D between compositions and subsets, we have

$$F_B(P) = \sum_{S \subseteq [n-1]} f_S \cdot M^B_S,$$

where we write M_S^B instead of $M_{D(S)}^B$, and the poset P has rank n. The *fundamental quasisymmetric function of type B*, denoted by L_T^B, is given by

$$L_T^B = \sum_{T \subseteq S} M_S^B.$$

Then the flag h-vector appears as the coefficients in the decomposition

$$F_B(P) = \sum_{S \subseteq [n-1]} h_S \cdot L_S^B,$$

where the poset P has rank n.

The cubical lattice C_n has rank $n + 1$ and can be obtained as a diamond power of the Boolean algebra B_2, that is, $C_n = B_2^{\diamond n}$. Therefore we have the following result.

Lemma 8.2. *The type B quasisymmetric function of the cubical lattice is given by*

$$F_B(C_n) = (s + 2 \cdot M_{(1)})^n.$$

Theorem 8.3. *For p an odd prime the cyclotomic polynomial Φ_{4p} divides the signed descent set polynomial $Q_p^{\pm}(t)$.*

Proof. Observe that modulo 4 we have

$$\begin{aligned}
F_B(C_p) &\equiv (s + 2 \cdot M_{(1)})^p \\
&\equiv s^p + 2 \cdot p \cdot s^{p-1} \cdot M_{(1)} \\
&\equiv M_{(p+1)}^B + 2 \cdot p \cdot M_{(p,1)}^B \\
&\equiv M_{\varnothing}^B + 2 \cdot M_{\{p\}}^B \\
&\equiv \sum_{S \subseteq [p]} (-1)^{|S|} \cdot L_S^B + 2 \cdot \sum_{p \in S} (-1)^{|S|-1} \cdot L_S^B \\
&\equiv \sum_{p \notin S} (-1)^{|S|} \cdot L_S^B + \sum_{p \in S} (-1)^{|S|-1} \cdot L_S^B \bmod 4.
\end{aligned}$$

Hence the signed descent set statistics satisfy $\beta_p^{\pm}(S) \equiv (-1)^{|S-\{p\}|} \bmod 4$ for $S \subseteq [p]$. Now modulo p we have

$$\begin{aligned}
F_B(C_p) &\equiv (s + 2 \cdot M_{(1)})^p \\
&\equiv s^p + 2 \cdot M_{(p)} \\
&\equiv M_{(p+1)}^B + 2 \cdot M_{(1,p)}^B \\
&\equiv M_{\varnothing}^B + 2 \cdot M_{\{1\}}^B \bmod p.
\end{aligned}$$

This directly implies that $\beta_p^{\pm}(S) \equiv (-1)^{|S-\{1\}|} \bmod p$. Combining these two statements we obtain

$$\beta_p^{\pm}(S) \equiv \begin{cases} (-1)^{|S|} & \bmod 4p \text{ if } 1, p \notin S, \\ (-1)^{|S|-1} & \bmod 4p \text{ if } 1, p \in S, \\ 2 \cdot p + (-1)^{|S|} & \bmod 4p \text{ if } 1 \notin S, p \in S, \\ 2 \cdot p + (-1)^{|S|-1} & \bmod 4p \text{ if } 1 \in S, p \notin S. \end{cases} \tag{8.3}$$

Observe that for $p \notin S$ we have $\beta_p^{\pm}(S) \equiv \beta_p^{\pm}(S \cup \{p\}) + 2 \cdot p \bmod 4p$, implying that $\zeta^{\beta_p^{\pm}(S)} = -\zeta^{\beta_p^{\pm}(S \cup \{p\})}$ for ζ a $4p$th primitive root of unity. Now sum over all subsets of $[p]$, and the result follows. □

Theorem 8.4. *For p an odd prime, Φ_{4p}^2 does not divide the signed descent set polynomial $Q_p^{\pm}(t)$. In fact, evaluating the derivative of the signed descent set polynomial $Q_p^{\pm}(t)$ at ζ, where ζ is a $4p$th primitive root of unity, gives*

$$\zeta \cdot Q_p^{\pm\prime}(\zeta) = \mathrm{Im}(\zeta) \cdot \mathrm{i} \cdot (-1)^{(p-1)/2} \cdot 2^p \cdot p \cdot E_{p-1}.$$

Proof. From (8.3) we have:

$$\begin{aligned}
\zeta \cdot Q_p^{\pm\prime}(\zeta) &= \sum_{S \subseteq [p]} \beta_p^{\pm}(S) \cdot \zeta^{\beta_p^{\pm}(S)} \\
&= \sum_{S \subseteq [p]} \beta_p^{\pm}(S) \cdot (-1)^{|S \cap \{1,p\}|} \cdot \zeta^{(-1)^{|S-\{1\}|}} \\
&= \mathrm{Re}(\zeta) \cdot \sum_{S \subseteq [p]} \beta_p^{\pm}(S) \cdot (-1)^{|S \cap \{1,p\}|} + \mathrm{Im}(\zeta) \cdot \mathrm{i} \cdot \sum_{S \subseteq [p]} \beta_p^{\pm}(S) \cdot (-1)^{|S \cap \{1,p\}|} \cdot (-1)^{|S-\{1\}|}.
\end{aligned}$$

The first sum is zero by Proposition 7.2. The second sum simplifies to

$$\mathrm{Im}(\zeta) \cdot \mathrm{i} \cdot \sum_{S \subseteq [p]} \beta_p^{\pm}(S) \cdot (-1)^{|S \cap [1,p-1]|}.$$

This sum can evaluated by setting $\mathbf{a}_j = 1$, $\mathbf{b}_1 = \cdots = \mathbf{b}_{p-1} = -1$ and $\mathbf{b}_p = 1$ in the multivariate **ab**-index of the cubical lattice C_p. Observe that $\mathbf{c}_1 = \cdots = \mathbf{c}_{p-1} = 0$ and $\mathbf{d}_{p-1,p} = 0$. Hence the only surviving **cd**-monomial is $\mathbf{d}_{1,2} \cdots \mathbf{d}_{p-2,p-1}\mathbf{c}_p$. The coefficient of this monomial is computed as follows:

$$\begin{aligned}
\left[\mathbf{d}^{(p-1)/2}\mathbf{c}\right]\Psi(C_p) &= 2^{(p-1)/2} \cdot \left[(2\mathbf{d})^{(p-1)/2}\mathbf{c}\right]\Psi(C_p) \\
&= 2^{(p-1)/2} \cdot \left(\left[(\mathbf{ab})^{(p-1)/2}\mathbf{a}\right]\mathbf{a} \cdot \Psi(B_p) + \left[(\mathbf{ab})^{(p-1)/2}\mathbf{b}\right]\mathbf{a} \cdot \Psi(B_p)\right) \\
&= 2^{(p-1)/2} \cdot p \cdot \left[\mathbf{b}(\mathbf{ab})^{(p-3)/2}\right]\Psi(B_{p-1}) \\
&= 2^{(p-1)/2} \cdot p \cdot E_{p-1}.
\end{aligned}$$

The third step is MacMahon's "Multiplication Theorem"; see [13, Article 159]. It can be stated in terms of the **ab**-indices as follows:

$$[u\mathbf{a}v]\Psi(B_{m+n}) + [u\mathbf{b}v]\Psi(B_{m+n}) = \binom{m+n}{m} \cdot [u]\Psi(B_m) + [v]\Psi(B_n),$$

where u and v have degrees $m-1$ and $n-1$, respectively. The monomial itself evaluates to $(-2)^{(p-1)/2} \cdot 2$, since $\mathbf{d}_{1,2} = \cdots = \mathbf{d}_{p-2,p-1} = -2$ and $\mathbf{c}_p = 2$. Combining all the factors, the evaluation at ζ follows. $\square$

9. Concluding remarks

Is there a reason why $\rho(n) - 1/2$ factors so nicely? See Table 1.

The two main results for unsigned permutations in Section 2, Theorems 2.1 and 3.4, can also be proved using the **ab**-index and the mixing operator; see [7]. We have omitted this approach since Kummer's theorem and the quasisymmetric functions are more succinct in this case.

Tables 2 and 3 contain cyclotomic factors of polynomials $Q_n(t)$ and $Q_n^{\pm}(t)$ for small n. Those factors whose presence is explained in this paper are highlighted in boldface. Here are several observations about the data in Table 2:

  (i) All the indices k of cyclotomic factors Φ_k of the polynomials $Q_n(t)$ are even.
 (ii) Any prime factor p that occurs in an index of a cyclotomic factor of $Q_n(t)$ is less than or equal to n.
(iii) If Φ_{k_1} and Φ_{k_2} are factors of $Q_n(t)$, so is $\Phi_{\gcd(k_1,k_2)}$. That is, the set of indices is closed under the meet operation in the divisor lattice.

Table 3
Cyclotomic factors of $Q_n^{\pm}(t)$

n	Degree	Cyclotomic factors of $Q_n^{\pm}(t)$
2	3	Φ_4
3	11	$\Phi_4 \cdot \Phi_8 \cdot \Phi_{12}$
4	57	$\Phi_4 \cdot \Phi_{16} \cdot \Phi_{32}$
5	361	$\Phi_4 \cdot \Phi_{16} \cdot \Phi_{20} \cdot \Phi_{32} \cdot \Phi_{80}$
6	2763	$\Phi_4 \cdot \Phi_8 \cdot \Phi_{24} \cdot \Phi_{32} \cdot \Phi_{40} \cdot \Phi_{96} \cdot \Phi_{120} \cdot \Phi_{160}$
7	24611	$\Phi_4 \cdot \Phi_8 \cdot \Phi_{24} \cdot \Phi_{28} \cdot \Phi_{32} \cdot \Phi_{56} \cdot \Phi_{168} \cdot \Phi_{224}$
8	250737	$\Phi_4 \cdot \Phi_{32} \cdot \Phi_{64} \cdot \Phi_{224} \cdot \Phi_{448} \cdot \Phi_{512}$
9	2873041	$\Phi_4 \cdot \Phi_{12} \cdot \Phi_{32} \cdot \Phi_{36} \cdot \Phi_{64} \cdot \Phi_{96} \cdot \Phi_{192} \cdot \Phi_{288} \cdot \Phi_{448}$ $\cdot \Phi_{512}^2 \cdot \Phi_{576} \cdot \Phi_{1344} \cdot \Phi_{1536} \cdot \Phi_{4032} \cdot \Phi_{4608}$
10	36581523	$\Phi_4 \cdot \Phi_8 \cdot \Phi_{24} \cdot \Phi_{40} \cdot \Phi_{64} \cdot \Phi_{72} \cdot \Phi_{120} \cdot \Phi_{192} \cdot \Phi_{320} \cdot \Phi_{360}$ $\cdot \Phi_{448} \cdot \Phi_{512} \cdot \Phi_{960} \cdot \Phi_{1344} \cdot \Phi_{1536} \cdot \Phi_{2240} \cdot \Phi_{2560} \cdot \Phi_{6720} \cdot \Phi_{7680}$
11	$5.123 \cdot 10^8$	$\Phi_4 \cdot \Phi_8 \cdot \Phi_{40} \cdot \Phi_{44} \cdot \Phi_{64} \cdot \Phi_{88} \cdot \Phi_{192} \cdot \Phi_{320} \cdot \Phi_{440}$ $\cdot \Phi_{512} \cdot \Phi_{704} \cdot \Phi_{960} \cdot \Phi_{2112} \cdot \Phi_{2560} \cdot \Phi_{3520} \cdot \Phi_{5632}$
12	$7.828 \cdot 10^9$	$\Phi_4 \cdot \Phi_{16} \cdot \Phi_{32} \cdot \Phi_{48} \cdot \Phi_{96} \cdot \Phi_{160} \cdot \Phi_{176} \cdot \Phi_{288} \cdot \Phi_{352}$ $\cdot \Phi_{480} \cdot \Phi_{512} \cdot \Phi_{528} \cdot \Phi_{1056} \cdot \Phi_{1440} \cdot \Phi_{1536} \cdot \Phi_{1760} \cdot \Phi_{2560}$ $\cdot \Phi_{3168} \cdot \Phi_{4608} \cdot \Phi_{5280} \cdot \Phi_{5632}$
13	$1.296 \cdot 10^{11}$	$\Phi_4 \cdot \Phi_{16} \cdot \Phi_{32} \cdot \Phi_{48} \cdot \Phi_{52} \cdot \Phi_{160} \cdot \Phi_{208} \cdot \Phi_{352} \cdot \Phi_{416}$ $\cdot \Phi_{512}^2 \cdot \Phi_{624} \cdot \Phi_{1536} \cdot \Phi_{1760} \cdot \Phi_{2080} \cdot \Phi_{4576} \cdot \Phi_{5632} \cdot \Phi_{6656}$
14	$2.310 \cdot 10^{12}$	$\Phi_4 \cdot \Phi_8 \cdot \Phi_{32} \cdot \Phi_{56} \cdot \Phi_{104} \cdot \Phi_{224} \cdot \Phi_{352} \cdot \Phi_{416} \cdot \Phi_{512}$ $\cdot \Phi_{728} \cdot \Phi_{1536} \cdot \Phi_{2464} \cdot \Phi_{2912} \cdot \Phi_{3584} \cdot \Phi_{4576} \cdot \Phi_{5632} \cdot \Phi_{6656}$
15	$4.411 \cdot 10^{13}$	$\Phi_4 \cdot \Phi_8 \cdot \Phi_{12} \cdot \Phi_{20} \cdot \Phi_{24} \cdot \Phi_{32} \cdot \Phi_{40} \cdot \Phi_{56} \cdot \Phi_{60}$ $\cdot \Phi_{96} \cdot \Phi_{120} \cdot \Phi_{160} \cdot \Phi_{168} \cdot \Phi_{224} \cdot \Phi_{280} \cdot \Phi_{416} \cdot \Phi_{480} \cdot \Phi_{512}$ $\cdot \Phi_{672} \cdot \Phi_{840} \cdot \Phi_{1120} \cdot \Phi_{1248} \cdot \Phi_{1536} \cdot \Phi_{2080} \cdot \Phi_{2560} \cdot \Phi_{2912} \cdot \Phi_{3360}$ $\cdot \Phi_{5632} \cdot \Phi_{6240} \cdot \Phi_{6656} \cdot \Phi_{7680} \cdot \Phi_{8736}$
16	$8.986 \cdot 10^{14}$	$\Phi_4 \cdot \Phi_{64} \cdot \Phi_{128} \cdot \Phi_{192} \cdot \Phi_{320} \cdot \Phi_{640} \cdot \Phi_{896} \cdot \Phi_{960}$ $\cdot \Phi_{1024} \cdot \Phi_{1664} \cdot \Phi_{3072} \cdot \Phi_{4480} \cdot \Phi_{5120} \cdot \Phi_{8320}$
17	$1.945 \cdot 10^{16}$	$\Phi_4 \cdot \Phi_{64} \cdot \Phi_{68} \cdot \Phi_{128} \cdot \Phi_{640} \cdot \Phi_{896}$ $\cdot \Phi_{1024}^2 \cdot \Phi_{1088} \cdot \Phi_{2176} \cdot \Phi_{4480} \cdot \Phi_{5120}$
18	$4.458 \cdot 10^{17}$	$\Phi_4 \cdot \Phi_8 \cdot \Phi_{24} \cdot \Phi_{72} \cdot \Phi_{128} \cdot \Phi_{136} \cdot \Phi_{384} \cdot \Phi_{408} \cdot \Phi_{640}$ $\cdot \Phi_{1024} \cdot \Phi_{1152} \cdot \Phi_{1224} \cdot \Phi_{1920} \cdot \Phi_{2176} \cdot \Phi_{3072} \cdot \Phi_{5760} \cdot \Phi_{6528} \cdot \Phi_{9216}$

(iv) If k_1 divides k_2, k_2 divides k_3 and Φ_{k_1} and Φ_{k_3} occur as factors in $Q_n(t)$, then so does Φ_{k_2}. This is convexity in the divisor lattice.

(v) If both Φ_{k_1} and Φ_{k_2} divide $Q_n(t)$, where k_1 divides k_2, then the multiplicity of Φ_{k_1} is greater than or equal to the multiplicity of Φ_{k_2}.

(vi) If p is not a Mersenne prime then the largest cyclotomic factor occurring in $Q_p(t)$ is Φ_{2p}.

(vii) When $\rho(n) \neq 1/2$ then there are no cyclotomic factors in the descent set polynomial $Q_n(t)$.

(viii) For all primes p we conjecture that Φ_{2p}^2 divides Q_{2p}.

Moreover for the signed descent set polynomial we observe that:

(ix) For $n \geqslant 3$ the cyclotomic polynomial Φ_{4n} divides the signed descent set polynomial $Q_n^{\pm}(t)$.

(x) For $n \geqslant 5$ the cyclotomic polynomial $\Phi_{4n(n-1)}$ divides the signed descent set polynomial $Q_n^{\pm}(t)$.

Can these phenomena be explained?

For what pairs of an integer n and a prime number p does the descent set statistic $\beta_n(S)$ only take two values modulo p?

Finally, we end with two number-theoretic questions. Are there infinitely many primes whose binary expansion has three 1's? The only reference for these primes we found is The On-Line En-

cyclopedia of Integer Sequences, sequence A081091. Are there any more prime powers with two or three ones in its binary expansion?

Acknowledgments

References

[1] M. Bayer, L. Billera, Generalized Dehn–Sommerville relations for polytopes, spheres and Eulerian partially ordered sets, Invent. Math. 79 (1985) 143–157.
[2] M. Bayer, A. Klapper, A new index for polytopes, Discrete Comput. Geom. 6 (1991) 33–47.
[3] L.J. Billera, R. Ehrenborg, M. Readdy, The **c**-2**d**-index of oriented matroids, J. Combin. Theory Ser. A 80 (1997) 79–105.
[4] N.G. de Bruijn, Permutations with given ups and downs, Nieuw Arch. Wiskd. (3) 18 (1970) 61–65.
[5] C.-O. Chow, Noncommutative symmetric functions of type B, Doctoral dissertation, Massachusetts Institute of Technology, 2001.
[6] R. Ehrenborg, On posets and Hopf algebras, Adv. Math. 119 (1996) 1–25.
[7] R. Ehrenborg, H. Fox, Inequalities for **cd**-indices of joins and products of polytopes, Combinatorica 23 (2003) 427–452.
[8] R. Ehrenborg, M. Levin, M. Readdy, A probabilistic approach to the descent statistic, J. Combin. Theory Ser. A 98 (2002) 150–162.
[9] R. Ehrenborg, S. Mahajan, Maximizing the descent statistic, Ann. Comb. 2 (1998) 111–129.
[10] R. Ehrenborg, M. Readdy, The r-cubical lattice and a generalization of the cd-index, European J. Combin. 17 (1996) 709–725.
[11] R. Ehrenborg, M. Readdy, Coproducts and the **cd**-index, J. Algebraic Combin. 8 (1998) 273–299.
[12] R. Ehrenborg, M. Readdy, The Tchebyshev transforms of the first and second kind, Ann. Comb., in press.
[13] P.A. MacMahon, Combinatory Analysis, vol. I, Chelsea Publishing Company, New York, 1960.
[14] I. Niven, A combinatorial problem of finite sequences, Nieuw Arch. Wiskd. (3) 16 (1968) 116–123.
[15] M. Readdy, Extremal problems for the Möbius function in the face lattice of the n-octahedron, Discrete Math. 139 (1995) 361–380, Special issue on Algebraic Combinatorics.
[16] B. Sagan, Y.N. Yeh, G. Ziegler, Maximizing Möbius functions on subsets of Boolean algebras, Discrete Math. 126 (1994) 293–311.
[17] R.P. Stanley, Enumerative Combinatorics, vol. I, Wadsworth and Brooks/Cole, Pacific Grove, 1986.