

Top to random and reverse: analysis of a new descent algebra shuffle

Darij Grinberg*, Jonathan Parlett†

Extended and corrected version of the second author’s honors thesis at Drexel University (2025).

August 9, 2025

1 Introduction

Consider the symmetric group S_n , consisting of permutations of the n -element set $[n] := \{1, 2, \dots, n\}$. The permutations $w \in S_n$ are often visualized as a shuffled deck of n cards that are labeled $1, 2, \dots, n$: Any permutation $w \in S_n$ corresponds to the state in which the cards are ordered $w(1), w(2), \dots, w(n)$. We may define a random state (i.e., a probability distribution on the set of states) to be a formal linear combination of permutations $\sum_{w \in S_n} a_w w \in \mathbb{R}[S_n]$ where the $a_w \in \mathbb{R}$ are non-negative and $\sum_{w \in S_n} a_w = 1$. Then a_w is the probability that the deck is in state w . We may drop the $\sum_{w \in S_n} a_w = 1$ condition as we may simply “normalize” our sum (divide by $\sum_{w \in S_n} a_w$) to obtain a random state. For example, the element $1 + \text{cyc}_{1,2,3}$ (where $\text{cyc}_{1,2,3}$ is the 3-cycle $1 \mapsto 2 \mapsto 3 \mapsto 1$) corresponds to the random state where the probability of the deck being ordered $1, 2, 3$ is $1/2$ and ordered $2, 3, 1$ is $1/2$.

A random shuffle can then be defined as a Markov chain on S_n , or, equivalently, a linear endomorphism of the \mathbb{R} -vector space $\mathbb{R}[S_n]$ that is given by a stochastic matrix. However, $\mathbb{R}[S_n]$ is itself an \mathbb{R} -algebra – the group algebra of the group S_n – and thus each of its elements gives rise to two endomorphisms, one by left and one by right multiplication. Hence, each element of $\mathbb{R}[S_n]$ with nonnegative coefficients gives rise to two random shuffles. For instance, left multiplication by $1 + \text{cyc}_{1,2}$ swaps the cards labelled 1 and 2 with probability $1/2$ and otherwise leaves the deck unchanged; whereas right multiplication by $1 + \text{cyc}_{1,2}$ swaps the top two cards (whatever their labels are) with probability $1/2$ and otherwise leaves the deck unchanged. This rests on the fact that the multiplication in $\mathbb{R}[S_n]$ is just extending by linearity the multiplication in the symmetric group S_n , which corresponds to composing permutations (performing one after the other).

*Drexel University, Philadelphia, PA. darijgrinberg@gmail.com

†University of Georgia, Athens, GA. jonathan.m.parlett@gmail.com

This algebraic viewpoint on card shuffling first rose to prominence when Diaconis and Shahshahani bounded the mixing time of some shuffles by computing the eigenvalues of the respective operators [7]; this answers the (admittedly open-ended) question “how many times should we shuffle a deck of cards to obtain a well-shuffled deck”. See [6, 5] for surveys of work done along these lines. Recent research efforts have focused on identifying shuffles whose eigenvalues admit a combinatorial description [12, 7, 18, 8]. We extend this line of research by studying a new shuffle derived from the well-known top-to-random shuffle.

Let \mathbf{T}_k be the element of the group algebra $\mathbb{R}[S_n]$ given by

$$\mathbf{T}_k = \sum_{\substack{w \in S_n; \\ w^{-1}(k+1) < \dots < w^{-1}(n)}} w \quad (\text{for each integer } 0 \leq k \leq n).$$

The element \mathbf{T}_k is known as the **k -top-to-random** shuffle and has been well studied in [18]. In particular it is known that \mathbf{T}_1 is diagonalizable with integer eigenvalues that admit a combinatorial description. That is, the **minimal polynomial** of \mathbf{T}_1 – meaning the lowest-degree monic polynomial that vanishes when applied to \mathbf{T}_1 – is a product of linear factors, namely

$$\prod_{k \in \{0, 1, \dots, n-2, n\}} (x - k) \in \mathbb{R}[x]$$

(note the conspicuous absence of the $x - (n - 1)$ factor). This entails that when acting on $\mathbb{R}[S_n]$ either by left or right multiplication, \mathbf{T}_1 is a diagonalizable endomorphism with eigenvalues $0, 1, \dots, n - 2, n$; their multiplicities too can be computed. This analysis can be extended to arbitrary base rings \mathbf{k} instead of \mathbb{R} (we are restricting ourselves to \mathbb{R} in this introduction for simplicity’s sake), and to all the \mathbf{T}_k ’s (in fact, each \mathbf{T}_k is a polynomial in \mathbf{T}_1 , thus inheriting the diagonalizability of the latter). See [10] (where \mathbf{T}_k is denoted \mathbf{B}_k) for details and further references. Informally, \mathbf{T}_k – acting as a random shuffle by right multiplication – corresponds to taking the top k cards of the deck and moving them to random positions.

The **antipode** of $\mathbf{k}[S_n]$ is the \mathbf{k} -linear map $S : \mathbf{k}[S_n] \rightarrow \mathbf{k}[S_n]$ that sends each permutation $w \in S_n$ to its inverse w^{-1} . This is a \mathbf{k} -algebra anti-isomorphism, and thus preserves the minimal polynomial. Hence, to determine the minimal polynomial of some element it suffices to study its antipode.

The antipodes of the elements \mathbf{T}_k are instances of a wider class of shuffle-like elements, which form a basis of the **descent algebra** of $\mathbf{k}[S_n]$. These are indexed by the **compositions** of n , that is, by the tuples of positive integers with sum n . Given a composition $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k)$ of n , we set

$$\mathbf{B}_\alpha = \sum w,$$

where the sum ranges over all permutations $w \in S_n$ that increase on the smallest α_1 elements of $[n]$, on the next-smallest α_2 elements of $[n]$, on the next-smallest α_3 elements of $[n]$, etc. (but can decrease between these blocks). Note that $S(\mathbf{T}_k) = \mathbf{B}_\alpha$ for $\alpha = (1, 1, \dots, 1, n - k)$ (with k many 1s). These elements \mathbf{B}_α are known as the “ α -shuffles” in the shuffling world, and are diagonalizable as well; their eigenvalues are known since

Bidigare’s pioneering work [1, §4.1.9]. Moreover, any linear combination of the \mathbf{B}_α with nonnegative real coefficients is still diagonalizable and its eigenvalues are known, by a result of Brown [23, Theorem 4.1].

In this work, we extend this analysis to a “mirror version” of the α -shuffles and their linear combinations. The “mirroring” refers to reversing the deck, which is modelled by an application of the **longest word** w_0 . Formally, w_0 is defined as the permutation in S_n with one-line notation $(n, n-1, \dots, 1)$. We shall study the shuffles $w_0\mathbf{B}_\alpha$ and $\mathbf{B}_\alpha w_0$, which are conjugate because $w_0^{-1} = w_0$.

We shall now overview our results in the simple-looking (but already highly nontrivial) case when $\alpha = (1, n-1)$, in which case $\mathbf{B}_\alpha = S(\mathbf{T}_1)$. The 1-top-to-random shuffle \mathbf{T}_1 is denoted by \mathbf{A} , and is known as the **top-to-random shuffle** or the **Tsetlin library**; it has appeared (among other places) in Lie algebra cohomology [26, Appendix] and machine learning [20, Lemma 29].

Informally, the shuffle $w_0\mathbf{T}_1$ corresponds to picking the top card, moving it to a random position, and reversing the order of all cards in the deck, while $\mathbf{T}_1 w_0$ corresponds to first reversing the deck, then moving the top card to a random position. We thus call $w_0\mathbf{T}_1$ and $\mathbf{T}_1 w_0$ the **reverse top-to-random shuffles**.

Our first main result for this case is saying that $w_0\mathbf{T}_1$ is diagonalizable with integer eigenvalues. To be more precise, we have the following theorem:

Theorem 1.1 (Theorem 9.5 further on). Let $n > 1$. The minimal polynomial of $w_0\mathbf{A}$ and $\mathbf{A}w_0$ over \mathbb{R} is

$$\prod_{k \in \{-n+2\} \cup \{-n+4, n-3\} \cup \{0\} \cup \{n\}} (x - k) \in \mathbb{R}[x] \quad (1)$$

(where $[a, b] := \{k \in \mathbb{Z} : a \leq k \leq b\}$). Thus, the elements $w_0\mathbf{A}$ and $\mathbf{A}w_0$ – acting either by left or by right multiplication on $\mathbb{R}[S_n]$ – are diagonalizable linear endomorphisms whose eigenvalues are 0, as well as $\pm k$ for $k \in \{1, 2, \dots, n-4\}$, as well as $n-3$ and $-n+2$ and n .

Our path to proving Theorem 1.1 begins with a tour of Solomon’s descent algebra $D(S_n)$, which we define in Section 3 (including its **B-basis** elements \mathbf{B}_α), and its connection to Bidigare’s face algebra $\mathbf{k}\mathcal{F}$, which we introduce in Section 4. In these two sections, we will prove various combinatorial and algebraic properties of these objects, including some classical results of Bidigare and Brown. The underlying combinatorial objects are **compositions** (i.e., tuples of positive integers) and **set compositions** (also known as “ordered set partitions”, i.e., tuples of disjoint nonempty sets with a given union). We will refer to set compositions as “**faces**”, as they are known to correspond to the faces of the (type- A) braid arrangement; however, we will not use any geometry in this paper. We let \mathcal{F} be the set of all set compositions of $[n]$; this set is equipped with a monoid structure (Definition 4.4).

In Section 4, we will also introduce the **knapsack numbers** $n_\alpha(F)$, which – roughly speaking – count the ways that the blocks of a given set composition F of $[n]$ can be “packed” into bags of sizes $\alpha_1, \alpha_2, \dots, \alpha_k$ (the entries of the composition α). The set of all these knapsack numbers is denoted $n_\alpha(\mathcal{F})$. These numbers (for α fixed and F ranging over all faces) turn out to be the eigenvalues of \mathbf{B}_α , as (implicitly) shown by Brown [23, Theorem 4.1].

One of our main results is a similar description of the eigenvalues of $w_0\mathbf{B}_\alpha$: We will show (Theorem 8.1) that these eigenvalues are the **signed knapsack numbers** $\tilde{n}_\alpha(F) = (-1)^{n-\ell(F)} n_\alpha(F)$ of all faces F , where $\ell(F)$ denotes the number of blocks of F . Again, the element $w_0\mathbf{B}_\alpha$ is diagonalizable (over \mathbb{Q}), so that its minimal polynomial is therefore

$$\prod_{k \in \tilde{n}_\alpha(\mathcal{F})} (x - k).$$

This will be proved in Section 8, after the necessary tools have been developed in Sections 5, 6 and 7.

In Section 9, we will apply our results to the particular case $\alpha = (1, n-1)$, proving Theorem 1.1 (restated as Theorem 9.5). The perhaps strange-looking set $\{-n+2\} \cup [-n+4, n-3] \cup \{0\} \cup \{n\}$ will be revealed there as the set $\tilde{n}_{(1, n-1)}(\mathcal{F})$ of signed knapsack numbers.

In Section 10, we will extend our analysis from a single element \mathbf{B}_α to an arbitrary linear combination $\mathbf{B}_\gamma := \sum_\alpha \gamma_\alpha \mathbf{B}_\alpha$ (where α ranges over the compositions of n) of such elements with nonnegative real coefficients $\gamma_\alpha \geq 0$. Just like Brown determined the minimal polynomial of any such combination \mathbf{B}_γ , we will compute it for any $w_0\mathbf{B}_\gamma$. The result (Theorem 10.5) is that any such $w_0\mathbf{B}_\gamma$ is again diagonalizable, and its eigenvalues are the respective linear combinations $\sum_\alpha \gamma_\alpha \tilde{n}_\alpha(F)$ of the signed knapsack numbers. The proof is rather similar to the case of a single \mathbf{B}_α , and so we will just outline the differences. Note that the nonnegativity of the coefficients γ_α is important for the diagonalizability, but not for the computation of the eigenvalues.

With the eigenvalues computed, an obvious question to ask is about their algebraic multiplicities. This question can be asked about any element of the descent algebra (nonnegative coefficients are irrelevant), and it comes in four versions: the element can act either by left or by right multiplication, and it can do so either on the descent algebra or on the whole $\mathbf{k}[S_n]$. These four questions have three different answers (not four, because left and right action on $\mathbf{k}[S_n]$ yield the same multiplicities). The answer in the $\mathbf{k}[S_n]$ case can be pieced together from the work of Bidigare [1, Sections 3.8 and 4.1] and Brown [3, Appendix B] (see [11, Theorem 1.2], [19, Proposition 4.2] and [1, Corollary 4.1.3] for the specific results needed); the descent algebra case appears to lead into the combinatorics of integer matrices (via Solomon's Mackey formula, [22, Corollary 2.4]). Thus, we will avoid this topic in the present paper, hoping to study it in the detail it deserves in future work.

As mentioned above, we used the base ring \mathbb{R} in this introduction for the sake of concreteness. In the rest of the paper, we shall work over an arbitrary commutative ring \mathbf{k} much of the time; occasionally, we will restrict ourselves to fields of characteristic 0 (when discussing diagonalizability and minimal polynomials). When \mathbf{k} is a field of positive characteristic, the polynomials that would normally be minimal still vanish at the respective elements, but are not necessarily minimal any more; sometimes diagonalizability is also lost. (For example, for $n = 4$ and $\mathbf{k} = \mathbb{F}_3$, the element $w_0\mathbf{A}$ has minimal polynomial $x(x-1)^2$.) We do not venture any guesses on what the minimal polynomials over finite fields shall be.

Acknowledgments

The first author would like to thank Sarah Brauner, Patricia Commins and Franco Saliola for many enlightening conversations about the descent algebra.

2 Notation

Let $\mathbb{N} = \{0, 1, 2, \dots\}$. For each $n \in \mathbb{Z}$, we let $[n]$ denote the set $\{1, 2, \dots, n\}$. (This is empty if $n \leq 0$.) More generally, if $a, b \in \mathbb{Z}$ are any two integers, then $[a, b]$ will denote the set $\{x \in \mathbb{Z} \mid a \leq x \leq b\} = \{a, a+1, a+2, \dots, b\}$. (Thus, $[n] = [1, n]$.) Note that $[a, b] = \emptyset$ if $a > b$.

We fix a nonnegative integer $n \in \mathbb{N}$.

The symmetric group on n letters is denoted S_n ; it is the set of all bijections from $[n]$ to $[n]$. Its multiplication is given by $(\alpha \circ \beta)(i) = \alpha(\beta(i))$.

The **one-line notation** of a permutation $\sigma \in S_n$ is the n -tuple $(\sigma(1), \sigma(2), \dots, \sigma(n)) \in [n]^n$. Usually, we enclose this n -tuple in square brackets instead of parentheses.

By abuse of notation, we sometimes identify a permutation σ with its one-line notation – e.g., we write “the permutation $[2, 1, 4, 3]$ ” for “the permutation with one-line notation $[2, 1, 4, 3]$ ”. We hope this will not be confused with the interval notation $[a, b]$.

Let w_0 denote the permutation in S_n with one-line notation $(n, n-1, \dots, 1)$. More explicitly, $w_0(i) = n - i + 1$ for each $i \in [n]$.

Fix a commutative ring \mathbf{k} . (The reader might take $\mathbf{k} = \mathbb{Z}$ without losing much generality.)

We let $\mathbf{k}[S_n]$ denote the group algebra of S_n over \mathbf{k} .

3 The Descent Algebra

3.1 Compositions, subsets and the bijections between them

Definition 3.1.

(a) A **composition** of an integer $n \in \mathbb{N}$ into k parts is a k -tuple $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k) \in [n]^k$ such that $\alpha_1 + \alpha_2 + \dots + \alpha_k = n$. A tuple α is called simply a composition of n if it is a composition of n into k parts for some $k \geq 0$. In this case we may write $\alpha \models n$.

(b) The **length** of a composition α , denoted $\ell(\alpha)$, is its number of parts: $\ell(\alpha_1, \alpha_2, \dots, \alpha_k) = k$.

Example 3.2. The distinct compositions of $n = 4$, grouped by their length, are

length	compositions of this length
1	(4);
2	(3, 1), (2, 2), (1, 3);
3	(2, 1, 1), (1, 2, 1), (1, 1, 2);
4	(1, 1, 1, 1).

Definition 3.3. Let $\mathcal{P}([n-1])$ denote the set of all subsets of $[n-1] = \{1, 2, \dots, n-1\}$, and $C(n) = \{\alpha \models n\}$ denote the set of compositions of n . We define the following maps:

(a) The map $\text{gaps} : \mathcal{P}([n-1]) \rightarrow C(n)$ is given by

$$\text{gaps}(J) = (j_1 - j_0, j_2 - j_1, \dots, j_m - j_{m-1}),$$

where $J = \{j_1, j_2, \dots, j_{m-1}\} \subseteq [n-1]$ with $j_i < j_{i+1}$ and where we set $j_0 = 0$ and $j_m = n$. Visually speaking, $\text{gaps}(J)$ is the composition whose entries are the distances between adjacent elements of $\{0\} \cup J \cup \{n\}$, that is, the lengths of the little intervals into which the set J splinters the interval $[n]$.

(b) The map $\text{rev} : C(n) \rightarrow C(n)$ is given by

$$\text{rev}(\alpha_1, \alpha_2, \dots, \alpha_k) = (\alpha_k, \alpha_{k-1}, \dots, \alpha_1).$$

The composition $\text{rev } \alpha$ is called the **reverse** of the composition α .

(c) The map $\text{sub} : \mathcal{P}([n-1]) \rightarrow \mathcal{P}([n-1])$ is given by

$$\text{sub}(J) = n - J = \{n - j : j \in J\}.$$

Visually speaking, $\text{sub}(J)$ is the reflection of J across the point $n/2$ on the number line.

Proposition 3.4. These three maps gaps , rev and sub are bijections. In particular, sub and rev are involutions, and we have

$$\text{sub} = \text{gaps}^{-1} \circ \text{rev} \circ \text{gaps}. \quad (2)$$

Proof. Visually, this is obvious:¹ Reflecting a set $J \subseteq [n-1]$ across the point $n/2$ causes the distances between adjacent elements of $\{0\} \cup J \cup \{n\}$ to get reversed (i.e., the same distances appear in opposite order), since 0 and n trade places; thus, the composition $\text{gaps } J$ is replaced by its reverse $\text{rev}(\text{gaps } J)$. \square

Definition 3.5 (Descents). Let $w \in S_n$ be a permutation.

(a) An element $i \in [n-1]$ is called a **descent** of w if $w(i) > w(i+1)$.

(b) The **descent set** of w is the set of the descents of w . It is denoted by $\text{Des } w$. That is,

$$\text{Des } w = \{i \in [n-1] : w(i) > w(i+1)\}.$$

Example 3.6. The permutation $w = [5, 2, 3, 4, 1] \in S_5$ has descents 1 (since $w(1) = 5 > w(2) = 2$) and 4, but not 2 or 3. Thus, $\text{Des } w = \{1, 4\}$.

¹A formalized proof can be found in [13, ancillary file comps-compiled.pdf, Theorem 3.8 (i), Corollary 3.10] (where (2) is stated in the equivalent form " $D(\text{rev } \alpha) = \text{rev}_n(D(\alpha))$ for any composition α of n ", using the notations D and rev_n for what we call gaps^{-1} and sub).

3.2 The descent algebra and its \mathbf{B} - and \mathbf{D} -bases

Definition 3.7.

(a) For any $I \subseteq [n-1]$, we define an element

$$\mathbf{B}_I := \sum_{\substack{w \in S_n; \\ \text{Des } w \subseteq I}} w \in \mathbf{k}[S_n].$$

(b) For any $I \subseteq [n-1]$, we define an element

$$\mathbf{D}_I := \sum_{\substack{w \in S_n; \\ \text{Des } w = I}} w \in \mathbf{k}[S_n].$$

(c) We may also index the elements \mathbf{B}_I by the composition of n that corresponds to the subset I under the map gaps . That is, for each $\alpha \models n$, we set

$$\mathbf{B}_\alpha := \mathbf{B}_{\text{gaps}^{-1}(\alpha)} = \sum_{\substack{w \in S_n; \\ \text{Des } w \subseteq \text{gaps}^{-1}(\alpha)}} w.$$

(d) The **descent algebra** $D(S_n)$ is defined as the \mathbf{k} -linear span of the elements \mathbf{B}_I for all $I \subseteq [n-1]$ inside $\mathbf{k}[S_n]$. It follows from (4) and (5) below that this span is also the span of the elements \mathbf{D}_I for all $I \subseteq [n-1]$. Both families $(\mathbf{B}_I)_{I \subseteq [n-1]}$ and $(\mathbf{D}_I)_{I \subseteq [n-1]}$ are known to be bases of the \mathbf{k} -module $D(S_n)$ (this is easy to see²); we call them the **B-basis** and the **D-basis**.

As the name suggests, the descent algebra $D(S_n)$ is actually a subalgebra of $\mathbf{k}[S_n]$. This is a celebrated result of Solomon [24, Theorem 1], which we will say more about later (Theorem 4.12); at the present moment we will not need it.

Example 3.8. For $n = 4$, we have

$$\begin{aligned} \mathbf{D}_{\{1,3\}} &= [2, 1, 4, 3] + [3, 1, 4, 2] + [3, 2, 4, 1] + [4, 1, 3, 2] + [4, 2, 3, 1], \\ \mathbf{D}_{\{1\}} &= [2, 1, 3, 4] + [3, 1, 2, 4] + [4, 1, 2, 3], \\ \mathbf{D}_{\{3\}} &= [2, 3, 4, 1] + [1, 3, 4, 2] + [1, 2, 4, 3], \\ \mathbf{D}_\emptyset &= [1, 2, 3, 4], \end{aligned}$$

²The family $(\mathbf{D}_I)_{I \subseteq [n-1]}$ is linearly independent, since its entries \mathbf{D}_I are sums of disjoint nonempty sets of permutations (nonempty because each $I \subseteq [n-1]$ is the descent set of at least one permutation $w \in S_n$). Thus, the family $(\mathbf{B}_I)_{I \subseteq [n-1]}$ is also linearly independent, since Proposition 3.10 establishes a triangular change-of-basis relationship between these two families. Therefore, this latter family $(\mathbf{B}_I)_{I \subseteq [n-1]}$ is a basis of its span, which is what we call $D(S_n)$. Thus, $(\mathbf{D}_I)_{I \subseteq [n-1]}$ is a basis of $D(S_n)$ as well, again because of Proposition 3.10.

and

$$\begin{aligned} \mathbf{B}_{\{1,3\}} &= \mathbf{D}_{\{1,3\}} + \mathbf{D}_{\{1\}} + \mathbf{D}_{\{3\}} + \mathbf{D}_{\emptyset} \\ &= [2, 1, 4, 3] + [3, 1, 4, 2] + [3, 2, 4, 1] + [4, 1, 3, 2] + [4, 2, 3, 1] \\ &\quad + [2, 1, 3, 4] + [3, 1, 2, 4] + [4, 1, 2, 3] + [2, 3, 4, 1] + [1, 3, 4, 2] + [1, 2, 4, 3] \\ &\quad + [1, 2, 3, 4]. \end{aligned}$$

Example 3.9. The element $\mathbf{B}_{[n-1]} \in \mathbf{k}[S_n]$ is defined as the sum of all permutations $w \in S_n$ satisfying $\text{Des } w \subseteq [n-1]$. Thus, it is simply the sum of all permutations $w \in S_n$ (since the condition $\text{Des } w \subseteq [n-1]$ is a tautology). In other words,

$$\mathbf{B}_{[n-1]} = \sum_{w \in S_n} w. \quad (3)$$

The following proposition gives change-of-basis formulas between the \mathbf{B} -basis and the \mathbf{D} -basis:

Proposition 3.10. For any $I \subseteq [n-1]$, we have

$$\mathbf{B}_I = \sum_{J \subseteq I} \mathbf{D}_J \quad (4)$$

and

$$\mathbf{D}_I = \sum_{J \subseteq I} (-1)^{|I \setminus J|} \mathbf{B}_J. \quad (5)$$

Proof. The first formula is obvious. The second follows from it by Möbius inversion on the Boolean lattice $(\mathcal{P}([n-1]), \subseteq)$ (see, e.g., [9, Theorem 6.2.10] or [25, the dual form of Theorem 2.1.1]).³ \square

Note that w_0 is the unique permutation in S_n having descent set $[n-1]$. Thus, $w_0 = \mathbf{D}_{[n-1]} \in D(S_n)$. Hence, the change-of-basis formula (5) yields the following corollary.

Corollary 3.11. Let $n \geq 1$. Then,

$$w_0 = \sum_{I \subseteq [n-1]} (-1)^{n-|I|-1} \mathbf{B}_I. \quad (6)$$

Proof. Applying (5) to $I = [n-1]$, we find

$$\mathbf{D}_{[n-1]} = \sum_{J \subseteq [n-1]} (-1)^{|[n-1] \setminus J|} \mathbf{B}_J = \sum_{I \subseteq [n-1]} (-1)^{|[n-1] \setminus I|} \mathbf{B}_I = \sum_{I \subseteq [n-1]} (-1)^{n-|I|-1} \mathbf{B}_I,$$

since each $I \subseteq [n-1]$ satisfies $|[n-1] \setminus I| = (n-1) - |I| = n - |I| - 1$. Since $w_0 = \mathbf{D}_{[n-1]}$, this is precisely the claim of the corollary. \square

³In more detail: Apply [9, Theorem 6.2.10] to $S = [n-1]$ and $A = \mathbf{k}[S_n]$ and $a_I = \mathbf{D}_I$ and $b_I = \mathbf{B}_I$. Then, the theorem shows that (5) follows from (4).

Note that w_0 is an involution: $w_0^2 = \text{id}$, thus $w_0^{-1} = w_0$. Hence, conjugation by w_0 takes any element a of $\mathbf{k}[S_n]$ to $w_0 a w_0$. On the descent algebra, this takes the following simple form:

Proposition 3.12. Let $I \subseteq [n - 1]$. Then we have

$$w_0 \mathbf{B}_I w_0 = \mathbf{B}_{\text{sub } I}.$$

In order to prove this, we show two simple combinatorial lemmas:

Lemma 3.13. Let $\sigma \in S_n$. Then, $\text{Des}(w_0 \sigma w_0) = \text{sub}(\text{Des } \sigma)$.

Proof. Let $i \in [n - 1]$. It suffices to show that $i \in \text{Des}(w_0 \sigma w_0)$ if and only if $i \in \text{sub}(\text{Des } \sigma)$.

The permutation w_0 sends each $k \in [n]$ to $n + 1 - k$. By the definition of $\text{Des } w$, we have the following chain of equivalences:⁴

$$\begin{aligned} & (i \in \text{Des}(w_0 \sigma w_0)) \\ \iff & (w_0 \sigma w_0 i > w_0 \sigma w_0 (i + 1)) \quad (\text{by the definition of a descent}) \\ \iff & (\sigma w_0 i < \sigma w_0 (i + 1)) \\ & \left(\begin{array}{l} \text{since } w_0 \text{ is strictly decreasing, so that} \\ \text{two elements } p, q \in [n] \text{ satisfy } w_0 p > w_0 q \text{ if and only if } p < q \end{array} \right) \\ \iff & (\sigma(n + 1 - i) < \sigma(n - i)) \\ & \quad (\text{since } w_0 i = n + 1 - i \text{ and } w_0(i + 1) = n - i) \\ \iff & (\sigma(n - i) > \sigma(n + 1 - i)) \\ \iff & (\sigma(n - i) > \sigma((n - i) + 1)) \\ \iff & (n - i \in \text{Des } \sigma) \quad (\text{by the definition of a descent}) \\ \iff & (i \in \text{sub}(\text{Des } \sigma)) \quad (\text{by the definition of the map sub}). \end{aligned}$$

This proves the desired equivalence. □

Lemma 3.14. Let $\sigma \in S_n$, and $I \subseteq [n - 1]$. Then, $\text{Des } \sigma \subseteq I$ if and only if $\text{Des}(w_0 \sigma w_0) \subseteq \text{sub } I$.

Proof. The map $\text{sub} : \mathcal{P}([n - 1]) \rightarrow \mathcal{P}([n - 1])$ clearly respects containment of sets: Two sets $U, V \in \mathcal{P}([n - 1])$ satisfy $U \subseteq V$ if and only if $\text{sub } U \subseteq \text{sub } V$. Hence, we have $\text{Des } \sigma \subseteq I$ if and only if $\text{sub}(\text{Des } \sigma) \subseteq \text{sub } I$. But Lemma 3.13 yields that $\text{sub}(\text{Des } \sigma) = \text{Des}(w_0 \sigma w_0)$, so this can be rewritten as “ $\text{Des } \sigma \subseteq I$ if and only if $\text{Des}(w_0 \sigma w_0) \subseteq \text{sub } I$ ”. This proves the lemma. □

⁴In the following computation, we will use the shorthand notation uk for the image $u(k)$ of an element $k \in [n]$ under a permutation $u \in S_n$. Thus, an expression of the form uvk with $u, v \in S_n$ and $k \in [n]$ can be read either as $(uv)k$ or as $u(vk)$. This ambiguity is harmless, since $(uv)k$ and $u(vk)$ are equal. Likewise, expressions like $uvwk$ can be made sense of.

Proof of Proposition 3.12. By the definition of \mathbf{B}_I , we have $\mathbf{B}_I = \sum_{\substack{\sigma \in S_n; \\ \text{Des } \sigma \subseteq I}} \sigma$. Thus,

$$\begin{aligned}
w_0 \mathbf{B}_I w_0 &= w_0 \sum_{\substack{\sigma \in S_n; \\ \text{Des } \sigma \subseteq I}} \sigma w_0 = \sum_{\substack{\sigma \in S_n; \\ \text{Des } \sigma \subseteq I}} w_0 \sigma w_0 \\
&= \sum_{\substack{\sigma \in S_n; \\ \text{Des}(w_0 \sigma w_0) \subseteq \text{sub } I}} w_0 \sigma w_0 \quad (\text{by Lemma 3.14}) \\
&= \sum_{\substack{\sigma \in S_n; \\ \text{Des } \sigma \subseteq \text{sub } I}} \sigma \quad (\text{here, we have substituted } \sigma \text{ for } w_0 \sigma w_0) \\
&= \mathbf{B}_{\text{sub } I} \quad (\text{by the definition of } \mathbf{B}_{\text{sub } I}),
\end{aligned}$$

as desired. \square

Translating from the set to the composition indexing of the \mathbf{B} -basis, we obtain the following corollary.

Corollary 3.15. Let $\alpha \models n$. Then,

$$w_0 \mathbf{B}_\alpha w_0 = \mathbf{B}_{\text{rev } \alpha}.$$

Proof. Let $I = \text{gaps}^{-1}(\alpha)$. Then, $\mathbf{B}_\alpha = \mathbf{B}_I$ by Definition 3.7 (c). Moreover, (2) yields

$$\text{sub } I = \left(\text{gaps}^{-1} \circ \text{rev} \circ \text{gaps} \right) (I) = \text{gaps}^{-1}(\text{rev}(\text{gaps } I)) = \text{gaps}^{-1}(\text{rev } \alpha)$$

(since the definition of I shows that $\text{gaps } I = \alpha$). Hence, $\mathbf{B}_{\text{sub } I} = \mathbf{B}_{\text{gaps}^{-1}(\text{rev } \alpha)} = \mathbf{B}_{\text{rev } \alpha}$ (again by Definition 3.7 (c)). But Proposition 3.12 yields $w_0 \mathbf{B}_I w_0 = \mathbf{B}_{\text{sub } I} = \mathbf{B}_{\text{rev } \alpha}$. In view of $\mathbf{B}_\alpha = \mathbf{B}_I$, this rewrites as $w_0 \mathbf{B}_\alpha w_0 = \mathbf{B}_{\text{rev } \alpha}$. This proves the corollary. \square

4 The Face Algebra

4.1 Faces and their algebra

We shall now introduce another combinatorial notion – that of *set compositions*. Realizing their relevance to the descent algebra was Bidigare’s main contribution [1].⁵ We will use them to describe the eigenvalues of our operators.

⁵Bidigare used them to reprove Solomon’s main results from [24] in simpler and more conceptual ways.

Recently, a similar approach was taken by Kenyon, Kontsevich, Ogievetsky, Pohoata, Sawin and Shlosman [15] in a more general setting: In fact, if their poset X is an antichain, their matrix M^X represents the left multiplication by a generic element $\sum_{\beta \models n} a_\beta \mathbf{D}_\beta$ of the descent algebra $D(S_n)$ on the symmetric group algebra $\mathbf{k}[S_n]$ (though they index the sum not by the compositions but by the “ ε functions”, i.e., bitstrings of length $n - 1$); and their main result [15, Theorem 1] is saying that the eigenvalues of this matrix M^X are \mathbb{Z} -linear combinations of the coefficients a_β . This is implicit in Bidigare’s thesis [1] and [23, Theorem 4.1], and explicit in [16, Proposition 3.12] (each of the sources describes the eigenvalues). Their proof of this fact proceeds by embedding the descent algebra in the face algebra $\mathbf{k}\mathcal{F}$, just as Bidigare did (their “filters” are in bijection with the set compositions of $[n]$), but subsequently they (implicitly) extend $\mathbf{k}\mathcal{F}$ to a larger space indexed by the *tournaments* on $[n]$. Thus, their approach is an interesting variation and new viewpoint on Bidigare’s.

Definition 4.1 (Set compositions).

(a) A **set composition** of $[n]$ – or, for short, a **face** of $[n]$ – means an (ordered) tuple $F = (F_1, F_2, \dots, F_k)$ of nonempty sets satisfying $\bigcup_{i=1}^k F_i = [n]$ and $F_i \cap F_j = \emptyset$ for each $i \neq j$. If F is a set composition of $[n]$, we may write $F \models [n]$.

(b) A **block** of a set composition $F = (F_1, F_2, \dots, F_k)$ is one of its entries F_i for $i \in [k]$.

(c) The **length** of a set composition is its number of blocks. We denote the length of F by $\ell(F)$. More formally, if $F = (F_1, F_2, \dots, F_k)$, then $\ell(F) = k$.

(d) We define the **type** of a set composition (F_1, F_2, \dots, F_k) of $[n]$ to be the composition

$$\text{type}(F_1, F_2, \dots, F_k) := (|F_1|, |F_2|, \dots, |F_k|) \models n.$$

(e) For an integer $n \in \mathbb{N}$, we denote the set of all set compositions of $[n]$ by \mathcal{F} or by $\mathcal{F}(n)$ when n is not clear from context.

Example 4.2. Let $n = 3$. Then, $(\{1, 2, 3\})$, $(\{1, 2\}, \{3\})$ and $(\{3\}, \{1, 2\})$ are three distinct set compositions / faces of the set $[3] = \{1, 2, 3\}$. When it is not confusing to do so, we will omit braces and commas when writing a face. With this convention, the above three faces are (123) , $(12, 3)$ and $(3, 12)$. The blocks of $(12, 3)$ are $\{1, 2\}$ and $\{3\}$. The faces $(12, 3)$ and $(3, 12)$ have length 2, while (123) has length 1. We have $\text{type}(12, 3) = (2, 1)$, $\text{type}(3, 12) = (1, 2)$ and $\text{type}(123) = (3)$.

Example 4.3. Here are all set compositions of $[3]$, grouped by type:

type	set compositions of this type
(3)	(3);
(2, 1)	(12, 3), (13, 2), (23, 1);
(1, 2)	(1, 23), (2, 13), (3, 12);
(1, 1, 1)	(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1).

The word “face” harkens back to the bijection between set compositions and the faces of the n -th braid arrangement (see [1, §4.1.4] or [22, §1.2.1]). We will not use this bijection – or any geometry for that matter – but we will still often use the word “face” for its brevity.

Definition 4.4 (Face monoid/algebra).

(a) If $H = (H_1, H_2, \dots, H_m)$ is a list of sets, then its **reduction** H^{red} means the list obtained by removing all the empty sets from H .

(b) Recall that \mathcal{F} is the set of set compositions of $[n]$. We define a multiplication on \mathcal{F} as follows: For $F = (F_1, F_2, \dots, F_k) \in \mathcal{F}$ and $G = (G_1, G_2, \dots, G_m) \in \mathcal{F}$, set

$$(F_1, F_2, \dots, F_k) \cdot (G_1, G_2, \dots, G_m) = (F_1 \cap G_1, \dots, F_1 \cap G_m, \dots, F_k \cap G_m)^{\text{red}},$$

where the list on the right hand side contains all the pairwise intersections $F_i \cap G_j$ in the order of lexicographically increasing (i, j) . In other words, FG is obtained from F by replacing each block F_i with its m intersections $F_i \cap G_1, F_i \cap G_2, \dots, F_i \cap G_m$ (in this order) and throwing away the empty intersections. By Lemma 4.6 below, this turns \mathcal{F} into a monoid.

(c) Let $\mathbf{k}\mathcal{F}$ be the monoid algebra of the monoid \mathcal{F} over \mathbf{k} . This is the free \mathbf{k} -module with basis \mathcal{F} , equipped with a multiplication that extends the multiplication of \mathcal{F} in the usual bilinear way.

Example 4.5. Consider the two faces $(12, 3), (3, 2, 1) \in \mathcal{F}(3)$. Then we have

$$\begin{aligned} (12, 3)(3, 2, 1) &= (12 \cap 3, 12 \cap 2, 12 \cap 1, 3 \cap 3, 3 \cap 2, 3 \cap 1)^{\text{red}} \\ &= (\emptyset, 2, 1, 3, \emptyset, \emptyset)^{\text{red}} = (2, 1, 3), \end{aligned}$$

while $(3, 2, 1)(12, 3) = (3, 2, 1)$. We also have

$$(12, 3)(123) = (12 \cap 123, 3 \cap 123) = (12, 3),$$

and more generally, the set composition $([n])$ is the unity of $\mathcal{F}(n)$. Let $\mathbf{k} = \mathbb{Z}$; then $3(12, 3)$ and $(123) - (3, 12)$ are elements of the algebra $\mathbb{Z}\mathcal{F}(3)$. Their product is

$$\begin{aligned} 3(12, 3)((123) - (3, 12)) &= 3((12, 3)(123) - (12, 3)(3, 12)) \\ &= 3\left((12, 3) - (12 \cap 3, 12 \cap 12, 3 \cap 3, 3 \cap 12)^{\text{red}}\right) \\ &= 3((12, 3) - (12, 3)) = 3 \cdot 0 = 0. \end{aligned}$$

Thus we see that $\mathbf{k}\mathcal{F}$ has zero divisors in general.

Note that the monoid \mathcal{F} (and thus the algebra $\mathbf{k}\mathcal{F}$) is not commutative in general: For two faces F and G , the products FG and GF have the same blocks, but usually appearing in different orders.

Lemma 4.6. The multiplication defined in Definition 4.4 (b) is associative and has neutral element $([n])$; thus, \mathcal{F} really is a monoid.

Proof. We define a **set decomposition** of $[n]$ in the same way as a set composition, but without requiring that its blocks be nonempty (so it is a tuple of disjoint sets whose union is $[n]$). Thus, each set decomposition $F = (F_1, F_2, \dots, F_k)$ gives rise to a set composition $F^{\text{red}} = (F_1, F_2, \dots, F_k)^{\text{red}}$. Of course, when F is itself a set composition, we just have $F^{\text{red}} = F$.

Now we shall show the following **auxiliary formula**:

Auxiliary formula: If (F_1, F_2, \dots, F_k) and (G_1, G_2, \dots, G_m) are two set decompositions of $[n]$, then the multiplication on \mathcal{F} satisfies

$$(F_1, F_2, \dots, F_k)^{\text{red}} \cdot (G_1, G_2, \dots, G_m)^{\text{red}} = (F_1 \cap G_1, \dots, F_1 \cap G_m, \dots, F_k \cap G_m)^{\text{red}}.$$

Indeed, if a block F_i is empty, then its intersections $F_i \cap G_j$ are empty for all j , and likewise an empty block G_j gives rise to empty intersections $F_i \cap G_j$. Hence, the right hand side of the auxiliary formula does not change if we remove an empty block from either (F_1, F_2, \dots, F_k) or (G_1, G_2, \dots, G_m) . Therefore, in particular, it does not change if we remove all the empty blocks, i.e., if we replace (F_1, F_2, \dots, F_k) and (G_1, G_2, \dots, G_m) by $(F_1, F_2, \dots, F_k)^{\text{red}}$ and $(G_1, G_2, \dots, G_m)^{\text{red}}$. But then the above auxiliary formula just boils down to the definition of the multiplication on \mathcal{F} . So the auxiliary formula is proved.

Now, if $E = (E_1, E_2, \dots, E_p)$, $F = (F_1, F_2, \dots, F_q)$ and $G = (G_1, G_2, \dots, G_r)$ are three set compositions of $[n]$, then we can use the above auxiliary formula to compute both products $(EF)G$ and $E(FG)$: Indeed, we get

$$FG = (F_1, F_2, \dots, F_q) (G_1, G_2, \dots, G_r) = (F_1 \cap G_1, \dots, F_1 \cap G_r, \dots, F_q \cap G_r)^{\text{red}}$$

and thus

$$\begin{aligned} E(FG) &= \underbrace{(E_1, E_2, \dots, E_p)}_{=(E_1, E_2, \dots, E_p)^{\text{red}}} \cdot (F_1 \cap G_1, \dots, F_1 \cap G_r, \dots, F_q \cap G_r)^{\text{red}} \\ &= (E_1, E_2, \dots, E_p)^{\text{red}} \cdot (F_1 \cap G_1, \dots, F_1 \cap G_r, \dots, F_q \cap G_r)^{\text{red}} \\ &= (E_1 \cap (F_1 \cap G_1), \dots, E_1 \cap (F_1 \cap G_r), \dots, E_1 \cap (F_q \cap G_r), \dots, E_p \cap (F_q \cap G_r))^{\text{red}} \\ &\quad \text{(by the auxiliary formula)} \\ &= (E_1 \cap F_1 \cap G_1, \dots, E_p \cap F_q \cap G_r)^{\text{red}}, \end{aligned}$$

where the triple intersections $E_i \cap F_j \cap G_k$ on the right hand side are listed in the order of lexicographically increasing $(i, (j, k))$, or, equivalently, of lexicographically increasing (i, j, k) . A similar computation yields the same expression for $(EF)G$. Hence, $E(FG) = (EF)G$, and thus associativity is proved.

It remains to show that $([n])$ is a neutral element for the multiplication on \mathcal{F} . But this is clear, since any block F_i of any face $F \in \mathcal{F}$ satisfies $[n] \cap F_i = F_i \cap [n] = F_i$. \square

Definition 4.7 (Actions of S_n on \mathcal{F} and $\mathbf{k}\mathcal{F}$; invariant subalgebra of $\mathbf{k}\mathcal{F}$). Consider the left action of the symmetric group S_n on the set \mathcal{F} that applies the permutation to each entry of each block of the set composition. That is, a permutation $w \in S_n$ acts on a set composition $(F_1, F_2, \dots, F_k) \in \mathcal{F}$ by

$$w(F_1, F_2, \dots, F_k) := (w(F_1), w(F_2), \dots, w(F_k)).$$

This action extends linearly to an action of S_n on $\mathbf{k}\mathcal{F}$. Then the invariant subalgebra $(\mathbf{k}\mathcal{F})^{S_n} \subseteq \mathbf{k}\mathcal{F}$ is defined by

$$(\mathbf{k}\mathcal{F})^{S_n} := \{\mathbf{F} \in \mathbf{k}\mathcal{F} : w(\mathbf{F}) = \mathbf{F} \text{ for all } w \in S_n\}.$$

Proposition 4.8 (Invariant subalgebra of $\mathbf{k}\mathcal{F}$). This invariant subalgebra $(\mathbf{k}\mathcal{F})^{S_n}$ is actually a \mathbf{k} -subalgebra of $\mathbf{k}\mathcal{F}$.

Proof. 1. The action of S_n on \mathcal{F} introduced in Definition 4.7 respects the multiplication on \mathcal{F} , meaning that any permutation $w \in S_n$ and any two set compositions $F, G \in \mathcal{F}$ satisfy $w(F \cdot G) = (wF) \cdot (wG)$. This is clear from the definitions, since $w(F_i \cap G_j) = w(F_i) \cap w(G_j)$ for any blocks F_i, G_j of F, G .

2. Thus, S_n acts on \mathcal{F} by monoid automorphisms, and hence (by linearity) acts on the monoid algebra $\mathbf{k}\mathcal{F}$ by \mathbf{k} -algebra automorphisms. Hence, the invariant subalgebra $(\mathbf{k}\mathcal{F})^{S_n}$ is a \mathbf{k} -subalgebra of $\mathbf{k}\mathcal{F}$ (since this holds for every action by \mathbf{k} -algebra automorphisms). \square

Definition 4.9. For each composition $\alpha \models n$, we define the element

$$\tilde{\mathbf{B}}_\alpha := \sum_{\substack{F \in \mathcal{F}; \\ \text{type } F = \alpha}} F \in \mathbf{k}\mathcal{F}.$$

Proposition 4.10 (The $\tilde{\mathbf{B}}_\alpha$ form a basis). The family of the elements $\tilde{\mathbf{B}}_\alpha$, where α ranges over all compositions of n , is a basis of $(\mathbf{k}\mathcal{F})^{S_n}$.

Proof. We must show that the elements $\tilde{\mathbf{B}}_\alpha$ actually belong to $(\mathbf{k}\mathcal{F})^{S_n}$ and form a basis of $(\mathbf{k}\mathcal{F})^{S_n}$.

The S_n -representation $\mathbf{k}\mathcal{F}$ is a permutation module: The action of S_n permutes the basis \mathcal{F} of $\mathbf{k}\mathcal{F}$. Thus, the invariant subspace $(\mathbf{k}\mathcal{F})^{S_n}$ has a basis (as a \mathbf{k} -module) consisting of the orbit sums (i.e., of the sums $\sum_{F \in \mathcal{O}} F$ for each orbit \mathcal{O} of the S_n -action on \mathcal{F}).

⁶ It remains to show that the elements $\tilde{\mathbf{B}}_\alpha$ are precisely these orbit sums.⁷

The S_n -action on \mathcal{F} preserves the type of a set composition: If $F \in \mathcal{F}$ and $w \in S_n$, then $\text{type}(wF) = \text{type } F$, since $|w(F_i)| = |F_i|$ for each block F_i of F . Hence, two set compositions F and G lying in the same S_n -orbit must have the same type. Conversely, if two set compositions F and G have the same type, then they lie in the same S_n -orbit (indeed, we can easily construct a permutation $w \in S_n$ that satisfies $wF = G$: just let it map the elements of each block of F to the elements of the corresponding block of G , in some arbitrarily chosen order). Summarizing, we see that two set compositions F and G in \mathcal{F} lie in the same S_n -orbit if and only if they have the same type.

Hence, each orbit \mathcal{O} of the S_n -action on \mathcal{F} is the set of all set compositions $F \in \mathcal{F}$ having a given type $\alpha \models n$. The orbit sum $\sum_{F \in \mathcal{O}} F$ of the former orbit can thus be written as $\sum_{\substack{F \in \mathcal{F}; \\ \text{type } F = \alpha}} F = \tilde{\mathbf{B}}_\alpha$. Moreover, the correspondence between the orbits \mathcal{O} and the types

$\alpha \models n$ is a bijection⁸. Therefore, the orbit sums $\sum_{F \in \mathcal{O}} F$ are precisely the elements $\tilde{\mathbf{B}}_\alpha$. This completes our proof. \square

⁶What we are using here is the following folklore fact: If a group G acts on a finite set X , then the invariant subspace $(\mathbf{k}X)^G := \{\mathbf{x} \in \mathbf{k}X : w\mathbf{x} = \mathbf{x} \text{ for all } w \in G\}$ of the permutation module $\mathbf{k}X$ has a basis consisting of the orbit sums (i.e., of the sums $\sum_{x \in \mathcal{O}} x$ for each orbit \mathcal{O} of the G -action on X). For a proof of this fact, see Proposition A.2 in the Appendix (Subsection A.4).

⁷We invite the reader to take another look at Example 4.3. The rows of the table in that example are precisely the orbits of the S_n -action on \mathcal{F} for $n = 3$.

⁸Injectivity is obvious (different orbits correspond to different types), and surjectivity is easy (for each composition $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k) \models n$, there is at least one set composition $F \in \mathcal{F}$ of type α , since we can certainly subdivide $[n]$ into subsets of sizes $\alpha_1, \alpha_2, \dots, \alpha_k$).

4.2 Bidigare's anti-isomorphism

As we know, the family $(\mathbf{B}_I)_{I \subseteq [n-1]}$ is a basis of the descent algebra $D(S_n)$ (as \mathbf{k} -module). Reindexing this family using compositions instead of subsets (see Definition 3.7 (c)), we conclude that the family $(\mathbf{B}_\alpha)_{\alpha \models n}$ is a basis of $D(S_n)$. This allows us to define the following crucial map (due to Bidigare [1, Theorem 3.8.1]):

Definition 4.11. Let $\rho : D(S_n) \rightarrow (\mathbf{k}\mathcal{F})^{S_n}$ be the \mathbf{k} -linear map defined by

$$\rho(\mathbf{B}_\alpha) = \tilde{\mathbf{B}}_\alpha \quad \text{for each } \alpha \models n \quad (7)$$

and extended linearly to all of $D(S_n)$.

(We have used the fact that the $\tilde{\mathbf{B}}_\alpha$ belong to $(\mathbf{k}\mathcal{F})^{S_n}$; this is part of Proposition 4.10.)

Theorem 4.12 (Bidigare). The set $D(S_n)$ is a \mathbf{k} -subalgebra of $\mathbf{k}[S_n]$. The map $\rho : D(S_n) \rightarrow (\mathbf{k}\mathcal{F})^{S_n}$ is a \mathbf{k} -algebra anti-isomorphism.

Proof. This is Bidigare's result [1, Theorem 3.8.1], and appears all across the literature. We give a self-contained proof in the Appendix (Subsection A.3). Here, however, let us outline how it can be obtained from more recent sources: Saliola, in [22, proof of Theorem 2.1], constructs a \mathbf{k} -algebra anti-morphism $\zeta : (\mathbf{k}\mathcal{F})^{S_n} \rightarrow \mathbf{k}[S_n]$ and shows that it satisfies $\zeta(\tilde{\mathbf{B}}_\alpha) = \mathbf{B}_\alpha$ for each composition $\alpha \models n$ (in his notations, this takes the form $\zeta(a_B) = x_J$, with B being a set composition of type α and J being the set $\text{gaps}^{-1}(\alpha)$). The same is also proved in [14, Theorem 1] (take $G = \{1\}$ and observe that $\sigma_\alpha = \tilde{\mathbf{B}}_\alpha$ and $X_\alpha = \mathbf{B}_\alpha$) and in [2, Appendix B, a few lines above Remark B.5] (their q is our α , so that $X^q = \tilde{\mathbf{B}}_\alpha$ and $\Xi^q = \mathbf{B}_\alpha$), as well as in [4, Theorem 7].

Either way, we now know that the \mathbf{k} -algebra anti-morphism $\zeta : (\mathbf{k}\mathcal{F})^{S_n} \rightarrow \mathbf{k}[S_n]$ satisfies $\zeta(\tilde{\mathbf{B}}_\alpha) = \mathbf{B}_\alpha$ for each composition $\alpha \models n$. Since the $\tilde{\mathbf{B}}_\alpha$ form a basis of $(\mathbf{k}\mathcal{F})^{S_n}$ (by Proposition 4.10), this shows that the image of ζ is the span of the \mathbf{B}_α 's for $\alpha \models n$, which of course is the descent algebra $D(S_n)$. Hence, $D(S_n)$ is a \mathbf{k} -subalgebra of $\mathbf{k}[S_n]$ (since the image of a \mathbf{k} -algebra anti-morphism is always a \mathbf{k} -subalgebra of its target). Moreover, the \mathbf{k} -algebra anti-morphism ζ is clearly injective (since the \mathbf{B}_α 's are \mathbf{k} -linearly independent), and thus is a \mathbf{k} -algebra anti-isomorphism from $(\mathbf{k}\mathcal{F})^{S_n}$ to its image $D(S_n)$. Thus, we have found an anti-isomorphism from $(\mathbf{k}\mathcal{F})^{S_n}$ to $D(S_n)$ that sends each $\tilde{\mathbf{B}}_\alpha$ to \mathbf{B}_α . Its inverse must obviously be our map ρ . This shows that ρ is a \mathbf{k} -algebra anti-isomorphism. \square

Using this anti-isomorphism ρ we can transport our identities from the descent algebra to the face algebra and back. Let us set

$$\tilde{w}_0 := \rho(w_0) \quad (8)$$

(this is allowed, since $w_0 \in D(S_n)$). Applying ρ to Proposition 3.12, we obtain the following corollary:

Corollary 4.13. For any $\alpha \models n$, we have

$$\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \tilde{w}_0 = \tilde{\mathbf{B}}_{\text{rev } \alpha} \quad (9)$$

and

$$\left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \right)^2 = \tilde{\mathbf{B}}_{\text{rev } \alpha} \tilde{\mathbf{B}}_\alpha. \quad (10)$$

Proof. Let $\alpha \models n$. Then, Corollary 3.15 yields $w_0 \mathbf{B}_\alpha w_0 = \mathbf{B}_{\text{rev } \alpha}$. Applying the algebra anti-morphism ρ to this equality, we obtain precisely (9) (since ρ sends w_0 to \tilde{w}_0 and sends each \mathbf{B}_β to $\tilde{\mathbf{B}}_\beta$).

To prove (10), we multiply the equality (9) by $\tilde{\mathbf{B}}_\alpha$ from the right, obtaining

$$\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \tilde{w}_0 \tilde{\mathbf{B}}_\alpha = \tilde{\mathbf{B}}_{\text{rev } \alpha} \tilde{\mathbf{B}}_\alpha.$$

This proves (10), since the left hand side here is $\left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \right)^2$. \square

To make this more explicit, we give an explicit formula for $\tilde{w}_0 = \rho(w_0)$:

Proposition 4.14. We have

$$\tilde{w}_0 = \sum_{F \in \mathcal{F}} (-1)^{n-\ell(F)} F. \quad (11)$$

Proof. We assume that $n \geq 1$, since the $n = 0$ case is trivial. Applying the \mathbf{k} -linear map ρ to both sides of (6), we find

$$\begin{aligned} \rho(w_0) &= \sum_{I \subseteq [n-1]} \underbrace{(-1)^{n-|I|-1}}_{=(-1)^{n-\ell(\text{gaps } I)} \text{ (since } \ell(\text{gaps } I) = |I| + 1)} \underbrace{\rho(\mathbf{B}_I)}_{=\rho(\mathbf{B}_{\text{gaps } I}) \text{ (since } \mathbf{B}_I = \mathbf{B}_{\text{gaps } I} \text{ by Definition 3.7 (c))}} = \sum_{I \subseteq [n-1]} (-1)^{n-\ell(\text{gaps } I)} \rho(\mathbf{B}_{\text{gaps } I}). \end{aligned}$$

Since $\text{gaps} : \mathcal{P}([n-1]) \rightarrow C(n)$ is a bijection, we can now substitute α for $\text{gaps } I$ on the right hand side, and this becomes

$$\begin{aligned} \rho(w_0) &= \sum_{\alpha \models n} (-1)^{n-\ell(\alpha)} \rho(\mathbf{B}_\alpha) \\ &= \sum_{\alpha \models n} (-1)^{n-\ell(\alpha)} \tilde{\mathbf{B}}_\alpha \quad (\text{by (7)}) \\ &= \sum_{\alpha \models n} (-1)^{n-\ell(\alpha)} \sum_{\substack{F \in \mathcal{F}; \\ \text{type } F = \alpha}} F \quad (\text{by the definition of } \tilde{\mathbf{B}}_\alpha) \\ &= \sum_{\alpha \models n} \sum_{\substack{F \in \mathcal{F}; \\ \text{type } F = \alpha}} (-1)^{n-\ell(\alpha)} F = \sum_{F \in \mathcal{F}} (-1)^{n-\ell(F)} F \end{aligned}$$

(since each set composition F has a unique type α and satisfies $\ell(\alpha) = \ell(F)$). Since the left hand side is \tilde{w}_0 , we have thus proved the proposition. \square

Thanks to the anti-isomorphism ρ , we can use the element $\tilde{w}_0 \tilde{\mathbf{B}}_\alpha$ of $(\mathbf{k}\mathcal{F})^{S_n}$ as a stand-in for the elements $\mathbf{B}_\alpha w_0$ and $w_0 \mathbf{B}_\alpha$ of $D(S_n)$. The precise way this works is formalized in the following lemma:

Lemma 4.15. Let $f(x) \in \mathbf{k}[x]$ be a polynomial. Let $\alpha \models n$. Then, we have the equivalences

$$(f(\mathbf{B}_\alpha w_0) = 0) \iff (f(w_0 \mathbf{B}_\alpha) = 0) \iff (f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha) = 0).$$

Proof. The map ρ is a \mathbf{k} -algebra anti-isomorphism (by Theorem 4.12). Thus,

$$\rho(\mathbf{B}_\alpha w_0) = \rho(w_0) \rho(\mathbf{B}_\alpha) = \tilde{w}_0 \tilde{\mathbf{B}}_\alpha \quad (12)$$

(since $\rho(w_0) = \tilde{w}_0$ and $\rho(\mathbf{B}_\alpha) = \tilde{\mathbf{B}}_\alpha$).

Let ω be the map $D(S_n) \rightarrow D(S_n)$, $a \mapsto w_0 a w_0^{-1}$. This map ω is simply conjugation by w_0 in the \mathbf{k} -algebra $D(S_n)$. Thus, it is a \mathbf{k} -algebra isomorphism, and sends $\mathbf{B}_\alpha w_0$ to

$$\omega(\mathbf{B}_\alpha w_0) = w_0 (\mathbf{B}_\alpha w_0) w_0^{-1} = w_0 \mathbf{B}_\alpha. \quad (13)$$

However, polynomials are known to commute with algebra morphisms and anti-morphisms: That is, if A and B are any two \mathbf{k} -algebras, if $\phi : A \rightarrow B$ is a \mathbf{k} -algebra morphism or anti-morphism, and if $g(x) \in \mathbf{k}[x]$ is any polynomial, then

$$\phi(g(a)) = g(\phi(a)) \quad \text{for any } a \in A. \quad (14)$$

Applying this fact to $A = D(S_n)$ and $B = (\mathbf{k}\mathcal{F})^{S_n}$ and $\phi = \rho$ (a \mathbf{k} -algebra anti-morphism) and $g(x) = f(x)$ and $a = \mathbf{B}_\alpha w_0$, we obtain $\rho(f(\mathbf{B}_\alpha w_0)) = f(\rho(\mathbf{B}_\alpha w_0)) = f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha)$ (by (12)).

Applying (14) to $A = D(S_n)$ and $B = D(S_n)$ and $\phi = \omega$ (a \mathbf{k} -algebra morphism) and $g(x) = f(x)$ and $a = \mathbf{B}_\alpha w_0$, we obtain $\omega(f(\mathbf{B}_\alpha w_0)) = f(\omega(\mathbf{B}_\alpha w_0)) = f(w_0 \mathbf{B}_\alpha)$ (by (13)).

Now, the map ρ is a \mathbf{k} -module isomorphism (being a \mathbf{k} -algebra anti-isomorphism). Hence, we have the equivalences

$$(f(\mathbf{B}_\alpha w_0) = 0) \iff (\rho(f(\mathbf{B}_\alpha w_0)) = 0) \iff (f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha) = 0)$$

(since $\rho(f(\mathbf{B}_\alpha w_0)) = f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha)$). Furthermore, the map ω is a \mathbf{k} -algebra isomorphism. Hence, we have the equivalences

$$(f(\mathbf{B}_\alpha w_0) = 0) \iff (\omega(f(\mathbf{B}_\alpha w_0)) = 0) \iff (f(w_0 \mathbf{B}_\alpha) = 0)$$

(since $\omega(f(\mathbf{B}_\alpha w_0)) = f(w_0 \mathbf{B}_\alpha)$). These two equivalences prove the lemma. \square

A similar (but simpler) argument shows the following:

Lemma 4.16. Let $f(x) \in \mathbf{k}[x]$ be a polynomial. Let $\alpha \models n$. Then, we have the equivalence

$$(f(\mathbf{B}_\alpha) = 0) \iff (f(\tilde{\mathbf{B}}_\alpha) = 0).$$

Proof. Left to the reader. \square

4.3 The containment relation

We return to the combinatorics of set compositions.

Definition 4.17. Let $F = (F_1, F_2, \dots, F_k)$ and $G = (G_1, G_2, \dots, G_m)$ be two faces in \mathcal{F} . We say F is **contained** in G – and we write $F \rightarrow G$ – if every block of F is a subset of a block of G . (More formally: if for each $i \in [k]$, there is a $j \in [m]$ such that $F_i \subseteq G_j$.)

Example 4.18. If $G = (45, 123)$ (we omit the commas and the set braces, so for example 45 means $\{4, 5\}$), then the faces $(5, 4, 123)$, $(123, 4, 5)$, $(45, 2, 13)$, $(5, 1, 2, 4, 3)$ (and several others) are contained in G , while $(5, 134, 2)$ is not (as are many others).

Clearly, the relation \rightarrow is transitive and reflexive. It is not antisymmetric, because reordering the blocks of a face F yields a new face G that satisfies $F \rightarrow G \rightarrow F$. More generally, the relation $F \rightarrow G$ depends only on the **set** of blocks of F and the **set** of blocks of G , not on their respective orders. Thus, the relation \rightarrow is better understood as a relation between set partitions (known as the **refinement order** of set partitions), not set compositions. However, we will find it useful on set compositions.

If a face F is contained in a face G , then G can be obtained from F by merging and reordering its blocks. What blocks are merged and where they are placed can be encoded by a set composition of $[\ell(F)]$, which is obtained from F by renaming the blocks of F as $1, 2, \dots, \ell(F)$ from left to right. For example, for $F = (123, 4, 5)$ and $G = (45, 123)$, we can obtain G from F by merging the last two blocks and swapping the result with the first block; this is encoded by the set composition $(23, 1)$ of $[\ell(F)] = [3]$. In full generality, the encoding is described by the following proposition:

Proposition 4.19. Let $F = (F_1, F_2, \dots, F_m) \in \mathcal{F}$ be a face (i.e., a set composition of $[n]$). Then, the map

$$f : \{G \in \mathcal{F} : F \rightarrow G\} \rightarrow \{H : H \models [m]\},$$

$$(G_1, G_2, \dots, G_k) \mapsto (H_1, H_2, \dots, H_k) \text{ where } H_i = \{j \in [m] : F_j \subseteq G_i\}$$

is a bijection. This bijection is furthermore length-preserving:

$$\ell(f(G)) = \ell(G).$$

The proof of this proposition is a standard argument in combinatorics (see, e.g., [25, Example 3.10.4] for the analogue for unordered set partitions); we give it in the Appendix (Subsection A.1).

The following simple properties of the containment are also easy to prove:

Proposition 4.20. Let F and G be two faces in \mathcal{F} . Then:

- (a) If F is contained in G , then $\ell(F) \geq \ell(G)$.
- (b) The product FG is contained in both F and G .
- (c) We have $FG = F$ if and only if F is contained in G .
- (d) We have $\ell(FG) \geq \ell(F)$. Equality holds if and only if F is contained in G .
- (e) We have $\ell(FG) \geq \ell(G)$.

We again refer to the Appendix (Subsection A.2) for the proof of Proposition 4.20.

4.4 The knapsack numbers $n_\alpha(F)$

The following definition will be crucial to the study of \mathbf{B}_α and related elements:

Definition 4.21. Let $\alpha \models n$ be a composition.

- (a) Given a face $F \in \mathcal{F}$, we define the finite set $N_\alpha(F)$ by

$$N_\alpha(F) = \{G \in \mathcal{F} : F \twoheadrightarrow G \text{ and } \text{type } G = \alpha\},$$

and we define the nonnegative integer $n_\alpha(F)$ by

$$n_\alpha(F) = |N_\alpha(F)|.$$

Thus, $n_\alpha(F)$ is the number of faces $G \in \mathcal{F}$ satisfying $F \twoheadrightarrow G$ and $\text{type } G = \alpha$. We refer to $n_\alpha(F)$ as the **knapsack number** of F with respect to α .

- (b) We will furthermore write $n_\alpha(\mathcal{F})$ for the set $\{n_\alpha(F) : F \in \mathcal{F}\}$, which consists of the knapsack numbers of all faces. This is the image of \mathcal{F} under the map n_α . It is obviously a finite set of nonnegative integers.

Example 4.22. Let $n = 4$ and $\alpha = (2, 2)$. Then:

1. If $F = (4, 23, 1)$, then

$$N_\alpha(F) = \{(14, 23), (23, 14)\}, \quad \text{and thus } n_\alpha(F) = 2.$$

2. If $F = (123, 4)$, then $N_\alpha(F) = \emptyset$ and thus $n_\alpha(F) = 0$.

3. If $F = (3, 2, 1, 4)$, then $N_\alpha(F)$ consists of all six faces of type $\alpha = (2, 2)$, and thus $n_\alpha(F) = 6$.

4. Systematically computing $n_\alpha(F)$ for all faces $F \in \mathcal{F}$ shows that $n_\alpha(\mathcal{F}) = \{0, 2, 6\}$.

Example 4.23. Let $n \geq 1$ and $\alpha = (n)$. Then, the only face $G \in \mathcal{F}$ of type α is $([n])$. Each face $F \in \mathcal{F}$ satisfies $F \twoheadrightarrow ([n])$ and thus

$$N_{(n)}(F) = \{G \in \mathcal{F} : F \twoheadrightarrow G \text{ and } \text{type } G = (n)\} = \{([n])\},$$

so that

$$n_{(n)}(F) = |\{([n])\}| = 1. \tag{15}$$

The word “knapsack number” refers to the knapsack problem in combinatorial optimization. Indeed, given a composition $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k) \models n$ and a face $F \in \mathcal{F}$, we can view the knapsack number $n_\alpha(F)$ as the number of ways to distribute the blocks of F into k (labeled) bags such that the total size of the blocks in the i -th bag is α_i for each i . (In fact, such a distribution corresponds to a face $G \in N_\alpha(F)$, namely the face $G = (G_1, G_2, \dots, G_k)$ whose i -th block G_i is the union of the blocks of F in the i -th bag.)

We shall now show some simple properties of knapsack numbers.

Proposition 4.24. Let $\alpha \models n$. Let $F, G \in \mathcal{F}$ be such that $F \twoheadrightarrow G$. Then, we have $n_\alpha(F) \geq n_\alpha(G)$.

Proof. Recall that $n_\alpha(F) = |N_\alpha(F)|$ and likewise $n_\alpha(G) = |N_\alpha(G)|$. However, for each $H \in N_\alpha(G)$, we have $G \twoheadrightarrow H$ and $\text{type } H = \alpha$ (by the definition of $N_\alpha(G)$), so that $F \twoheadrightarrow G \twoheadrightarrow H$ (since the containment relation is transitive), and thus $H \in N_\alpha(F)$ (since $F \twoheadrightarrow H$ and $\text{type } H = \alpha$). Thus, we have shown that

$$N_\alpha(G) \subseteq N_\alpha(F).$$

Hence, $|N_\alpha(G)| \leq |N_\alpha(F)|$. In other words, $n_\alpha(G) \leq n_\alpha(F)$ (since $n_\alpha(F) = |N_\alpha(F)|$ and likewise $n_\alpha(G) = |N_\alpha(G)|$). This yields the proposition. \square

Proposition 4.25. Let $\alpha \models n$. Let $F, G \in \mathcal{F}$. Then, we have $n_\alpha(FG) \geq n_\alpha(F)$ and $n_\alpha(FG) \geq n_\alpha(G)$.

Proof. Proposition 4.20 (b) yields $FG \twoheadrightarrow F$ and $FG \twoheadrightarrow G$. Hence, by Proposition 4.24, we conclude that $n_\alpha(FG) \geq n_\alpha(F)$ and $n_\alpha(FG) \geq n_\alpha(G)$. \square

Proposition 4.26. Let $\alpha \models n$. Let $F, G \in \mathcal{F}$ be such that $\text{type } G = \alpha$ and $F \not\twoheadrightarrow G$. Then, we have $n_\alpha(FG) > n_\alpha(F)$.

Proof. Recall that $n_\alpha(F) = |N_\alpha(F)|$ and likewise $n_\alpha(FG) = |N_\alpha(FG)|$. Hence, in order to prove that $n_\alpha(FG) > n_\alpha(F)$, it suffices to show that $N_\alpha(F)$ is a proper subset of $N_\alpha(FG)$.

It is easy to see that $N_\alpha(F)$ is a subset of $N_\alpha(FG)$: In fact, any $H \in N_\alpha(F)$ satisfies $F \twoheadrightarrow H$ and thus (by Proposition 4.20 (b)) also $FG \twoheadrightarrow F \twoheadrightarrow H$, so that $H \in N_\alpha(FG)$.

It remains to show that the subset $N_\alpha(F)$ of $N_\alpha(FG)$ is proper. For this, we must find an element that belongs to $N_\alpha(FG)$ but not to $N_\alpha(F)$. But G is such an element: Indeed, $G \in N_\alpha(FG)$ (because Proposition 4.20 (b) shows that $FG \twoheadrightarrow G$ and $\text{type } G = \alpha$) and $G \notin N_\alpha(F)$ (since $F \not\twoheadrightarrow G$). Thus, the proof is finished. \square

Proposition 4.27. Let $\alpha \models n$ and $F \in \mathcal{F}$. Then, $n_\alpha(F) = n_{\text{rev } \alpha}(F)$.

Proof. If F is contained in some face G , then F will still be contained in any face obtained by reordering the blocks of G . Thus, in particular, F is contained in a face $G = (G_1, G_2, \dots, G_k)$ if and only if it is contained in its reverse $\text{rev } G := (G_k, G_{k-1}, \dots, G_1)$. Furthermore, a face G satisfies $\text{type } G = \alpha$ if and only if $\text{type}(\text{rev } G) = \text{rev}(\alpha)$, since we always have $\text{type}(\text{rev } G) = \text{rev}(\text{type } G)$. Thus, the map

$$\begin{aligned} N_\alpha(F) &\rightarrow N_{\text{rev } \alpha}(F), \\ G &\mapsto \text{rev } G \end{aligned}$$

is well-defined. This map is furthermore a bijection, since an inverse map can be defined in the exact same way (note that $\text{rev}(\text{rev } \alpha) = \alpha$). By the bijection principle, we thus obtain $|N_\alpha(F)| = |N_{\text{rev } \alpha}(F)|$. In other words, $n_\alpha(F) = n_{\text{rev } \alpha}(F)$. \square

Remark. Let $\alpha \models n$ and $F \in \mathcal{F}$. In our above proof, we essentially showed that $n_\alpha(F)$ does not change if we permute the entries of the composition α . But there are further symmetries: $n_\alpha(F)$ also remains unchanged if we permute the blocks of F or apply a permutation $w \in S_n$ to F . Hence, $n_\alpha(F)$ depends on the **unordered** type of F (that is, of the partition of n obtained from the composition $\text{type } F$ by sorting the entries in decreasing order) rather than on F itself. In particular, the size of the set $n_\alpha(\mathcal{F})$ is at most the number $p(n)$ of partitions of n .

5 The knapsack filtration and the first annihilating polynomials

From now on, we fix a composition α of n .

Our goal in this section is to establish polynomials that annihilate⁹ \mathbf{B}_α and $w_0\mathbf{B}_\alpha$ (Theorem 5.1 and Theorem 5.7, respectively). The former polynomial is well-known, and the latter is suboptimal (i.e., has higher degree than necessary); however, these polynomials make natural stepping stones on the way to our main result (Theorem 7.2), allowing us to introduce the relevant ideas one at a time.

5.1 A polynomial annihilating \mathbf{B}_α

The following theorem (a particular case of [16, Proposition 3.12] and of [23, Theorem 4.1]) gives a polynomial that annihilates \mathbf{B}_α :

Theorem 5.1. The element $\mathbf{B}_\alpha \in D(S_n)$ satisfies

$$\prod_{k \in n_\alpha(\mathcal{F})} (\mathbf{B}_\alpha - k) = 0. \quad (16)$$

(This product ranges over all **distinct** elements $k \in n_\alpha(\mathcal{F})$. Thus, even if several different faces F have the same knapsack number k , there is only one $\mathbf{B}_\alpha - k$ factor in the product.)

To prove this theorem, we need some preparations. We begin with a definition, which will be equally important in further proofs later on:

Definition 5.2 (The knapsack filtration of $\mathbf{k}\mathcal{F}$).

(a) For each $k \in \mathbb{N} \cup \{\infty\}$, we define $\mathcal{F}_k := \{F \in \mathcal{F} : n_\alpha(F) \geq k\}$. (Thus, $\mathcal{F}_\infty = \emptyset$.)

We furthermore let $\mathbf{k}\mathcal{F}_k$ denote the \mathbf{k} -linear span of \mathcal{F}_k inside $\mathbf{k}\mathcal{F}$.

(b) Write the set $n_\alpha(\mathcal{F})$ as $\{k_0 < k_1 < k_2 < \dots < k_m\}$. Set $k_{m+1} = \infty$. Then the \mathcal{F}_{k_i} form a filtration of \mathcal{F} :

$$\mathcal{F} = \mathcal{F}_{k_0} \supseteq \mathcal{F}_{k_1} \supseteq \dots \supseteq \mathcal{F}_{k_m} \supseteq \mathcal{F}_{k_{m+1}} = \emptyset.$$

Therefore their \mathbf{k} -linear spans form a filtration of $\mathbf{k}\mathcal{F}$:

$$\mathbf{k}\mathcal{F} = \mathbf{k}\mathcal{F}_{k_0} \supseteq \mathbf{k}\mathcal{F}_{k_1} \supseteq \dots \supseteq \mathbf{k}\mathcal{F}_{k_m} \supseteq \mathbf{k}\mathcal{F}_{k_{m+1}} = 0.$$

We shall call this the **knapsack filtration** of $\mathbf{k}\mathcal{F}$.

To illustrate Definition 5.2, we compute the smallest element k_0 of $n_\alpha(\mathcal{F})$:

Proposition 5.3. (a) If $\alpha \neq (n)$, then $k_0 = 0$.

(b) If $\alpha = (n)$, then $k_0 = 1$ and $m = 0$.

⁹We say that a polynomial $f \in \mathbf{k}[x]$ **annihilates** an element a of a \mathbf{k} -algebra if $f(a) = 0$.

Proof. (a) Assume that $\alpha \neq (n)$. Thus,

$$N_\alpha([n]) = \{G \in \mathcal{F} : ([n]) \twoheadrightarrow G \text{ and } \text{type } G = \alpha\} = \emptyset,$$

since the face $([n])$ is contained only in itself and is of type $(n) \neq \alpha$ by assumption. Therefore, $n_\alpha([n]) = 0$, so that $0 = n_\alpha([n]) \in n_\alpha(\mathcal{F})$. Since $n_\alpha(\mathcal{F})$ is a set of nonnegative integers, this shows that 0 is its smallest element; that is, $k_0 = 0$.

(b) Assume that $\alpha = (n)$. For every face $F \in \mathcal{F}$, we have $n_{(n)}(F) = 1$ by (15). Consequently $n_{(n)}(\mathcal{F}) = \{1\}$, and thus $k_m = k_0 = 1$ and $m = 0$, as desired. \square

The following simple fact will be used without mention:

Proposition 5.4. Let $k \in \mathbb{N} \cup \{\infty\}$. Then, $\mathbf{k}\mathcal{F}_k$ is a (two-sided) ideal of $\mathbf{k}\mathcal{F}$.

Proof. The set $\mathbf{k}\mathcal{F}_k$ is defined as a \mathbf{k} -linear span, and thus is closed under addition and contains zero. It remains to prove that it satisfies the absorption axiom – i.e., that if one of two elements $\mathbf{F}, \mathbf{G} \in \mathbf{k}\mathcal{F}$ belongs to $\mathbf{k}\mathcal{F}_k$, then $\mathbf{F}\mathbf{G} \in \mathbf{k}\mathcal{F}_k$ as well. By linearity, it suffices to show that if one of two faces $F, G \in \mathcal{F}$ belongs to \mathcal{F}_k , then $FG \in \mathcal{F}_k$ as well (since $\mathbf{k}\mathcal{F}_k$ and $\mathbf{k}\mathcal{F}$ are the spans of \mathcal{F}_k and \mathcal{F}).

But this is easy: Let $F, G \in \mathcal{F}$ be two faces. Assume that one of them belongs to \mathcal{F}_k . That is, one of the knapsack numbers $n_\alpha(F)$ and $n_\alpha(G)$ is $\geq k$. Hence, we have $\max\{n_\alpha(F), n_\alpha(G)\} \geq k$. But Proposition 4.25 shows that $n_\alpha(FG) \geq n_\alpha(F)$ and $n_\alpha(FG) \geq n_\alpha(G)$, so that $n_\alpha(FG) \geq \max\{n_\alpha(F), n_\alpha(G)\} \geq k$. In other words, $FG \in \mathcal{F}_k$. This is just what we needed to prove. \square

This shows that the knapsack filtration of $\mathbf{k}\mathcal{F}$ is a filtration by ideals (i.e., by $(\mathbf{k}\mathcal{F}, \mathbf{k}\mathcal{F})$ -bimodules). Hence, the subquotients $\mathbf{k}\mathcal{F}_{k_i}/\mathbf{k}\mathcal{F}_{k_{i+1}}$ of this filtration are $\mathbf{k}\mathcal{F}$ - $\mathbf{k}\mathcal{F}$ -bimodules. The following lemma says that right multiplication by $\tilde{\mathbf{B}}_\alpha$ acts on these subquotients as scaling by k_i :

Lemma 5.5. Let $F \in \mathcal{F}$. Let $i \in [0, m]$ be such that $n_\alpha(F) = k_i$. Then we have

$$F\tilde{\mathbf{B}}_\alpha \equiv k_i F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}.$$

Proof. The definition of $\tilde{\mathbf{B}}_\alpha$ yields $\tilde{\mathbf{B}}_\alpha = \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha}} G$. Hence,

$$\begin{aligned} F\tilde{\mathbf{B}}_\alpha &= \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha}} FG = \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \twoheadrightarrow G}} \underbrace{FG}_{=F} + \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \not\twoheadrightarrow G}} FG \\ &= \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \twoheadrightarrow G}} F + \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \not\twoheadrightarrow G}} FG. \end{aligned} \tag{17}$$

But the sum $\sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \twoheadrightarrow G}} F$ can be rewritten as $\sum_{G \in N_\alpha(F)} F$ (by the definition of $N_\alpha(F)$).

Hence,

$$\sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \twoheadrightarrow G}} F = \sum_{G \in N_\alpha(F)} F = \underbrace{|N_\alpha(F)|}_{=n_\alpha(F)=k_i} F = k_i F. \tag{18}$$

On the other hand, if $G \in \mathcal{F}$ satisfies type $G = \alpha$ and $F \not\rightsquigarrow G$, then Proposition 4.26 yields $n_\alpha(FG) > n_\alpha(F) = k_i$ and thus $n_\alpha(FG) \geq k_{i+1}$ (since $n_\alpha(FG)$ belongs to the set $n_\alpha(\mathcal{F}) = \{k_0 < k_1 < k_2 < \dots < k_m\}$, and thus cannot be $> k_i$ without being $\geq k_{i+1}$), so that $FG \in \mathcal{F}_{k_{i+1}} \subseteq \mathbf{k}\mathcal{F}_{k_{i+1}}$ and therefore

$$FG \equiv 0 \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}. \quad (19)$$

Thus, (17) becomes

$$F\tilde{\mathbf{B}}_\alpha = \underbrace{\sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \rightarrow G}} F}_{=k_i F \text{ (by (18))}} + \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \not\rightsquigarrow G}} FG \equiv 0 \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}} \quad \underbrace{FG}_{\equiv 0 \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}} \text{ (by (19))}} \equiv k_i F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}.$$

□

Lemma 5.6. Let $i \in [0, m]$. If $\mathbf{F} \in \mathbf{k}\mathcal{F}_{k_i}$, then

$$\mathbf{F} \left(\tilde{\mathbf{B}}_\alpha - k_i \right) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

Proof. By linearity, it suffices to prove that the lemma holds when \mathbf{F} is a single face $F \in \mathcal{F}_{k_i}$. Thus, let us assume that this is the case; thus, $n_\alpha(F) \geq k_i$. Thus, we have either $n_\alpha(F) > k_i$ or $n_\alpha(F) = k_i$. If $n_\alpha(F) > k_i$, then $n_\alpha(F)$ must be at least k_{i+1} (since $n_\alpha(F) \in n_\alpha(\mathcal{F}) = \{k_0 < k_1 < k_2 < \dots < k_m\}$), so that $F \in \mathcal{F}_{k_{i+1}}$. In this case, we thus conclude that $\mathbf{F} = F \in \mathcal{F}_{k_{i+1}} \subseteq \mathbf{k}\mathcal{F}_{k_{i+1}}$ and therefore $\mathbf{F} \left(\tilde{\mathbf{B}}_\alpha - k_i \right) \in \mathbf{k}\mathcal{F}_{k_{i+1}}$ as well (since $\mathbf{k}\mathcal{F}_{k_{i+1}}$ is an ideal of $\mathbf{k}\mathcal{F}$). So Lemma 5.6 is proved in this case.

Hence, we WLOG assume that $n_\alpha(F) = k_i$. Thus, Lemma 5.5 yields $F\tilde{\mathbf{B}}_\alpha \equiv k_i F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}$. In other words, $F\tilde{\mathbf{B}}_\alpha - k_i F \in \mathbf{k}\mathcal{F}_{k_{i+1}}$. But $\mathbf{F} = F$, so that

$$\mathbf{F} \left(\tilde{\mathbf{B}}_\alpha - k_i \right) = F \left(\tilde{\mathbf{B}}_\alpha - k_i \right) = F\tilde{\mathbf{B}}_\alpha - k_i F \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

This proves Lemma 5.6. □

Proof of Theorem 5.1. Define the polynomial

$$f(x) := \prod_{k \in n_\alpha(\mathcal{F})} (x - k) \in \mathbf{k}[x].$$

Thus, our goal is to prove that $f(\mathbf{B}_\alpha) = 0$. This is equivalent to proving that $f(\tilde{\mathbf{B}}_\alpha) = 0$, because of Lemma 4.16. So this is what we need to do.

In other words, we need to prove the equality

$$\prod_{k \in n_\alpha(\mathcal{F})} \left(\tilde{\mathbf{B}}_\alpha - k \right) = 0$$

(by the definition of f). Using the notations of Definition 5.2, we can rewrite this as

$$\prod_{j=0}^m (\tilde{\mathbf{B}}_\alpha - k_j) = 0 \quad (20)$$

(since k_0, k_1, \dots, k_m are the elements of $n_\alpha(\mathcal{F})$ in increasing order).

We will obtain this equality as a particular case ($i = m$) of the equality

$$\prod_{j=0}^i (\tilde{\mathbf{B}}_\alpha - k_j) \in \mathbf{k}\mathcal{F}_{k_{i+1}}, \quad (21)$$

which we claim to hold for each $i \in [-1, m]$. This latter equality (21) will be proved by induction on i :

The *base case* ($i = -1$) is saying that the empty product belongs to $\mathbf{k}\mathcal{F}_{k_0}$. But this is clear, since $\mathbf{k}\mathcal{F}_{k_0} = \mathbf{k}\mathcal{F}$.

The *induction step* (from $i - 1$ to i) follows from Lemma 5.6, because

$$\begin{aligned} \prod_{j=0}^i (\tilde{\mathbf{B}}_\alpha - k_j) &= \underbrace{\left(\prod_{j=0}^{i-1} (\tilde{\mathbf{B}}_\alpha - k_j) \right)}_{\in \mathbf{k}\mathcal{F}_{k_i} \text{ (by the induction hypothesis)}} (\tilde{\mathbf{B}}_\alpha - k_i) \\ &\in \mathbf{k}\mathcal{F}_{k_i} (\tilde{\mathbf{B}}_\alpha - k_i) \subseteq \mathbf{k}\mathcal{F}_{k_{i+1}} \quad \text{by Lemma 5.6.} \end{aligned}$$

Thus, (21) is proved. Applying (21) to $i = m$, we find $\prod_{j=0}^m (\tilde{\mathbf{B}}_\alpha - k_j) \in \mathbf{k}\mathcal{F}_{k_{m+1}} = 0$, so that (20) follows. As explained above, this completes the proof of Theorem 5.1. \square

5.2 A polynomial annihilating $w_0\mathbf{B}_\alpha$

We now present a polynomial that annihilates $w_0\mathbf{B}_\alpha$:

Theorem 5.7. The element $w_0\mathbf{B}_\alpha \in D(S_n)$ satisfies

$$w_0\mathbf{B}_\alpha \prod_{\substack{k \in n_\alpha(\mathcal{F}); \\ k \neq 0}} (w_0\mathbf{B}_\alpha + k) (w_0\mathbf{B}_\alpha - k) = 0. \quad (22)$$

The proof will rely on the following two lemmas:

Lemma 5.8. Let $F \in \mathcal{F}$. Let $i \in [0, m]$ be such that $n_\alpha(F) = k_i$. Then

$$F\tilde{\mathbf{B}}_{\text{rev } \alpha} \tilde{\mathbf{B}}_\alpha \equiv k_i^2 F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}.$$

Proof. By Proposition 4.27, we have $n_{\text{rev } \alpha}(F) = n_\alpha(F) = k_i$. But Lemma 5.5 yields $F\tilde{\mathbf{B}}_\alpha \equiv k_i F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}$. Likewise, Lemma 5.5 (applied to $\text{rev } \alpha$ instead of α) yields $F\tilde{\mathbf{B}}_{\text{rev } \alpha} \equiv k_i F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}$ (since $n_{\text{rev } \alpha}(F) = k_i$, and since Proposition 4.27 shows that

$n_{\text{rev } \alpha}(\mathcal{F}) = n_\alpha(\mathcal{F}) = \{k_0 < k_1 < k_2 < \cdots < k_m\}$). Since $\mathbf{k}\mathcal{F}_{k_{i+1}}$ is a right ideal, we can multiply this congruence by $\tilde{\mathbf{B}}_\alpha$, thus obtaining

$$\begin{aligned} F\tilde{\mathbf{B}}_{\text{rev } \alpha}\tilde{\mathbf{B}}_\alpha &\equiv k_i F\tilde{\mathbf{B}}_\alpha \equiv k_i k_i F && \left(\text{since } F\tilde{\mathbf{B}}_\alpha \equiv k_i F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}} \right) \\ &= k_i^2 F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}, \end{aligned}$$

as desired. \square

Lemma 5.9. Let $i \in [0, m]$. If $\mathbf{F} \in \mathbf{k}\mathcal{F}_{k_i}$, then

$$\mathbf{F} \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_i \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_i \right) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

Proof. It suffices to show that the lemma holds when \mathbf{F} is a single face $F \in \mathcal{F}_{k_i}$, so let us assume this is the case; thus, $n_\alpha(F) \geq k_i$. The case when $n_\alpha(F) > k_i$ can be handled just as in the proof of Lemma 5.6 above¹⁰. Hence, we WLOG assume that $n_\alpha(F) = k_i$. Then, Lemma 5.8 yields $F\tilde{\mathbf{B}}_{\text{rev } \alpha}\tilde{\mathbf{B}}_\alpha \equiv k_i^2 F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}$. In other words,

$$F\tilde{\mathbf{B}}_{\text{rev } \alpha}\tilde{\mathbf{B}}_\alpha - k_i^2 F \in \mathbf{k}\mathcal{F}_{k_{i+1}}. \quad (23)$$

Now,

$$\left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_i \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_i \right) = \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \right)^2 - k_i^2 = \tilde{\mathbf{B}}_{\text{rev } \alpha} \tilde{\mathbf{B}}_\alpha - k_i^2 \quad (\text{by (10)}),$$

so that

$$\begin{aligned} \mathbf{F} \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_i \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_i \right) &= \mathbf{F} \left(\tilde{\mathbf{B}}_{\text{rev } \alpha} \tilde{\mathbf{B}}_\alpha - k_i^2 \right) = F \left(\tilde{\mathbf{B}}_{\text{rev } \alpha} \tilde{\mathbf{B}}_\alpha - k_i^2 \right) \quad (\text{since } \mathbf{F} = F) \\ &= F\tilde{\mathbf{B}}_{\text{rev } \alpha}\tilde{\mathbf{B}}_\alpha - k_i^2 F \in \mathbf{k}\mathcal{F}_{k_{i+1}} \quad (\text{by (23)}). \quad \square \end{aligned}$$

Proof of Theorem 5.7. Define the polynomial

$$f(x) := x \prod_{\substack{k \in n_\alpha(\mathcal{F}); \\ k \neq 0}} (x+k)(x-k) \in \mathbf{k}[x].$$

Thus, our goal is to prove that $f(w_0 \mathbf{B}_\alpha) = 0$. According to Lemma 4.15, this is equivalent to proving that $f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha) = 0$. So this is what we need to do.

In other words, we need to prove the equality

$$\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \prod_{\substack{k \in n_\alpha(\mathcal{F}); \\ k \neq 0}} \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k \right) = 0$$

¹⁰If $n_\alpha(F) > k_i$, then $n_\alpha(F)$ must be at least k_{i+1} , so that $F \in \mathcal{F}_{k_{i+1}}$, thus $\mathbf{F} = F \in \mathcal{F}_{k_{i+1}} \subseteq \mathbf{k}\mathcal{F}_{k_{i+1}}$. Then, since $\mathbf{k}\mathcal{F}_{k_{i+1}}$ is an ideal of $\mathbf{k}\mathcal{F}$, we must have $\mathbf{F} \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_i \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_i \right) \in \mathbf{k}\mathcal{F}_{k_{i+1}}$ as well.

(by the definition of f). Using the notations of Definition 5.2, we can rewrite this as

$$\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \prod_{j=p}^m \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_j \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_j \right) = 0, \quad (24)$$

where p is the smallest element of $[0, m]$ satisfying $k_p > 0$ (clearly, p is either 0 or 1, depending on whether k_0 is positive or 0).

We will obtain this equality as a particular case ($i = m$) of the equality

$$\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \prod_{j=p}^i \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_j \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_j \right) \in \mathbf{k}\mathcal{F}_{k_{i+1}}, \quad (25)$$

which we claim to hold for each $i \in [p-1, m]$. This latter equality (25) will be proved by induction on i :

The *base case* ($i = p-1$) is saying that $\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \in \mathbf{k}\mathcal{F}_{k_p}$. To prove this, it suffices to show that $\tilde{\mathbf{B}}_\alpha \in \mathbf{k}\mathcal{F}_{k_p}$ (since $\mathbf{k}\mathcal{F}_{k_p}$ is an ideal). But this is easy: Any face $F \in \mathcal{F}$ that satisfies type $F = \alpha$ must satisfy $N_\alpha(F) \neq \emptyset$ (indeed, F itself is a $G \in \mathcal{F}$ satisfying $F \rightarrow G$ and type $G = \alpha$; thus, the set $N_\alpha(F)$ contains at least F as an element) and thus $n_\alpha(F) > 0$ and therefore $n_\alpha(F) \geq k_p$ (since the definition of p shows that k_p is the smallest positive element of $n_\alpha(\mathcal{F})$), so that $F \in \mathcal{F}_{k_p} \subseteq \mathbf{k}\mathcal{F}_{k_p}$. Thus, $\tilde{\mathbf{B}}_\alpha$ (being a sum of such F 's) belongs to $\mathbf{k}\mathcal{F}_{k_p}$ as well. This completes the base case.

The *induction step* (from $i-1$ to i) follows from Lemma 5.9, because

$$\begin{aligned} & \tilde{w}_0 \tilde{\mathbf{B}}_\alpha \prod_{j=p}^i \left(\left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_j \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_j \right) \right) \\ &= \underbrace{\left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha \prod_{j=p}^{i-1} \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_j \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_j \right) \right)}_{\substack{\in \mathbf{k}\mathcal{F}_{k_i} \\ \text{(by the induction hypothesis)}}} \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_i \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_i \right) \\ &\in \mathbf{k}\mathcal{F}_{k_i} \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_i \right) \left(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_i \right) \subseteq \mathbf{k}\mathcal{F}_{k_{i+1}} \quad \text{by Lemma 5.9.} \end{aligned}$$

Thus, (25) is proved. Applying (25) to $i = m$ and recalling that $\mathbf{k}\mathcal{F}_{k_{m+1}} = 0$, we obtain (24), and Theorem 5.7 follows. \square

6 Alternating sum identities for set compositions

To improve on the polynomial in Theorem 5.7, we need two combinatorial identities regarding set compositions:

Lemma 6.1. We have

$$\sum_{G \in \mathcal{F}} (-1)^{\ell(G)} = (-1)^n.$$

Proof. This is essentially [21, Theorem 2.2.2] (see the first paragraph in the proof of [21, Theorem 2.2.2] for an explanation). However, let us give a new proof here, using the tools of this paper.

Consider the composition $(1, 1, \dots, 1)$ of n (with n many 1's). The definition of $\tilde{\mathbf{B}}_{(1,1,\dots,1)}$ yields

$$\tilde{\mathbf{B}}_{(1,1,\dots,1)} = \sum_{\substack{F \in \mathcal{F}; \\ \text{type } F = (1,1,\dots,1)}} F = \sum_{\substack{A \in \mathcal{F}; \\ \text{type } A = (1,1,\dots,1)}} A. \quad (26)$$

One of the addends in this sum is the face $(\{1\}, \{2\}, \dots, \{n\}) \in \mathcal{F}$. Hence, the coefficient of this face in $\tilde{\mathbf{B}}_{(1,1,\dots,1)}$ is 1.

Set

$$\lambda := \sum_{F \in \mathcal{F}} (-1)^{n-\ell(F)} \in \mathbb{Z}. \quad (27)$$

Let $A \in \mathcal{F}$ be a face of type $(1, 1, \dots, 1) \models n$. (Note that there are $n!$ such faces, each of them having the form $(\{\sigma(1)\}, \{\sigma(2)\}, \dots, \{\sigma(n)\})$ for some permutation $\sigma \in S_n$.) Then, the blocks of A have size 1, and therefore cannot be subdivided any further by intersecting them with the blocks of another face $F \in \mathcal{F}$. Hence,

$$AF = A \quad \text{for each } F \in \mathcal{F}. \quad (28)$$

But Proposition 4.14 yields

$$A\tilde{w}_0 = A \sum_{F \in \mathcal{F}} (-1)^{n-\ell(F)} F = \sum_{F \in \mathcal{F}} (-1)^{n-\ell(F)} \underbrace{AF}_{\substack{=A \\ \text{(by (28))}}} = \sum_{F \in \mathcal{F}} \underbrace{(-1)^{n-\ell(F)}}_{= \lambda} A = \lambda A.$$

Forget that we fixed A . We thus have proved the equality $A\tilde{w}_0 = \lambda A$ for each face $A \in \mathcal{F}$ of type $(1, 1, \dots, 1) \models n$. Summing this equality over all such faces A , we obtain

$$\sum_{\substack{A \in \mathcal{F}; \\ \text{type } A = (1,1,\dots,1)}} A\tilde{w}_0 = \lambda \sum_{\substack{A \in \mathcal{F}; \\ \text{type } A = (1,1,\dots,1)}} A. \quad (29)$$

Using (26), we can rewrite this as

$$\tilde{\mathbf{B}}_{(1,1,\dots,1)}\tilde{w}_0 = \lambda \tilde{\mathbf{B}}_{(1,1,\dots,1)}.$$

On the other hand, $(1, 1, \dots, 1) = \text{gaps}([n-1])$, so that

$$\mathbf{B}_{(1,1,\dots,1)} = \mathbf{B}_{[n-1]} = \sum_{w \in S_n} w$$

(by (3)), and therefore

$$w_0 \mathbf{B}_{(1,1,\dots,1)} = w_0 \sum_{w \in S_n} w = \sum_{w \in S_n} w_0 w = \sum_{w \in S_n} w$$

(here, we have substituted w for w_0w in the sum). Comparing these two equalities, we obtain $w_0\mathbf{B}_{(1,1,\dots,1)} = \mathbf{B}_{(1,1,\dots,1)}$. Applying the map ρ to this equality, we find

$$\rho\left(w_0\mathbf{B}_{(1,1,\dots,1)}\right) = \rho\left(\mathbf{B}_{(1,1,\dots,1)}\right) = \tilde{\mathbf{B}}_{(1,1,\dots,1)} \quad (\text{by the definition of } \rho),$$

so that

$$\begin{aligned} \tilde{\mathbf{B}}_{(1,1,\dots,1)} &= \rho\left(w_0\mathbf{B}_{(1,1,\dots,1)}\right) \\ &= \underbrace{\rho\left(\mathbf{B}_{(1,1,\dots,1)}\right)}_{=\tilde{\mathbf{B}}_{(1,1,\dots,1)}} \underbrace{\rho(w_0)}_{=\tilde{w}_0} \quad (\text{since } \rho \text{ is a } \mathbf{k}\text{-algebra anti-morphism}) \\ &= \tilde{\mathbf{B}}_{(1,1,\dots,1)}\tilde{w}_0 = \lambda\tilde{\mathbf{B}}_{(1,1,\dots,1)}. \end{aligned}$$

Comparing coefficients in front of the face $(\{1\}, \{2\}, \dots, \{n\}) \in \mathcal{F}$ in this equality, we obtain $1 = \lambda$ (since the coefficient of this face in $\tilde{\mathbf{B}}_{(1,1,\dots,1)}$ is 1). Thus, $1 = \lambda = \sum_{F \in \mathcal{F}} (-1)^{n-\ell(F)}$ (by the definition of λ). Dividing this equality by $(-1)^n$, we find $(-1)^n = \sum_{F \in \mathcal{F}} (-1)^{\ell(F)} = \sum_{G \in \mathcal{F}} (-1)^{\ell(G)}$, qed. \square

Lemma 6.2. Let $F \in \mathcal{F}$ be a face. Then,

$$\sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} (-1)^{n-\ell(G)} = (-1)^{n-\ell(F)}.$$

Proof. Write the set composition F as $F = (F_1, F_2, \dots, F_m)$, so that $\ell(F) = m$. Then, Proposition 4.19 shows that there is a length-preserving bijection

$$\begin{aligned} f : \{G \in \mathcal{F} : F \rightarrow G\} &\rightarrow \{H : H \models [m]\}, \\ (G_1, G_2, \dots, G_k) &\mapsto (H_1, H_2, \dots, H_k) \text{ where } H_i = \{j \in [m] : F_j \subseteq G_i\}. \end{aligned}$$

Using this bijection, we can reindex the sum $\sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} (-1)^{n-\ell(G)}$ as follows:

$$\sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} (-1)^{n-\ell(G)} = \sum_{H \models [m]} (-1)^{n-\ell(H)} = \sum_{G \models [m]} (-1)^{n-\ell(G)} = (-1)^n \sum_{G \models [m]} (-1)^{\ell(G)}.$$

However, applying Lemma 6.1 to m instead of n , we find

$$\sum_{G \models [m]} (-1)^{\ell(G)} = (-1)^m.$$

In light of this, the previous equality simplifies to

$$\sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} (-1)^{n-\ell(G)} = (-1)^n (-1)^m = (-1)^{n-m} = (-1)^{n-\ell(F)}$$

(since $m = \ell(F)$), as desired. \square

7 The optimal polynomial for $w_0\mathbf{B}_\alpha$

Recall that α is a fixed composition of n .

As we mentioned above, the equality (22) provides a polynomial that annihilates $w_0\mathbf{B}_\alpha$, but this polynomial is not optimal: Some of the factors can be removed from the product without turning it nonzero. In this section, we shall find an optimal polynomial that annihilates $w_0\mathbf{B}_\alpha$ (meaning that – at least when \mathbf{k} is a field of characteristic 0 – it is the minimal polynomial of $w_0\mathbf{B}_\alpha$, as we will see in Theorem 8.1).

First, we need some more notations.

Definition 7.1.

(a) The **signed knapsack number** $\tilde{n}_\alpha(F)$ of a face $F \in \mathcal{F}$ is the integer defined by

$$\tilde{n}_\alpha(F) = (-1)^{n-\ell(F)} n_\alpha(F). \quad (30)$$

(b) We will furthermore write $\tilde{n}_\alpha(\mathcal{F})$ for the set $\{\tilde{n}_\alpha(F) : F \in \mathcal{F}\}$, which consists of the signed knapsack numbers of all faces. This is the image of \mathcal{F} under the map \tilde{n}_α . It is obviously a finite set of integers.

Note that each face $F \in \mathcal{F}$ satisfies

$$|\tilde{n}_\alpha(F)| = n_\alpha(F) \quad (31)$$

(by (30), since $n_\alpha(F)$ is nonnegative). Hence, each signed knapsack number $k \in \tilde{n}_\alpha(\mathcal{F})$ satisfies

$$|k| \in n_\alpha(\mathcal{F}) = \{k_0 < k_1 < \dots < k_m\}$$

(see Definition 5.2 (b) for the latter equality).

Our main result takes the following form (recall that α is a fixed composition of n):

Theorem 7.2. The elements $w_0\mathbf{B}_\alpha$ and $\mathbf{B}_\alpha w_0$ of $D(S_n)$ satisfy

$$\prod_{k \in \tilde{n}_\alpha(\mathcal{F})} (w_0\mathbf{B}_\alpha - k) = 0 \quad (32)$$

and

$$\prod_{k \in \tilde{n}_\alpha(\mathcal{F})} (\mathbf{B}_\alpha w_0 - k) = 0. \quad (33)$$

(Each of these products ranges over all **distinct** elements $k \in \tilde{n}_\alpha(\mathcal{F})$. Thus, even if several different faces F have the same signed knapsack number k , there is only one $w_0\mathbf{B}_\alpha - k$ (resp. $\mathbf{B}_\alpha w_0 - k$) factor in each product.)

The proof of this will rely on a counterpart to Lemma 5.9:

Lemma 7.3. Let $k \in \tilde{n}_\alpha(\mathcal{F})$. Let $i \in [0, m]$ be such that $|k| = k_i$. Let $\mathbf{F} \in \mathbf{k}\mathcal{F}_{k_i}$. Then:

(a) If $-k \notin \tilde{n}_\alpha(\mathcal{F})$, then

$$\mathbf{F}(\tilde{w}_0 - \text{sign } k) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

Here, $\text{sign } k$ means the sign of k (that is, 1 if $k > 0$ and -1 if $k < 0$).

(b) We have

$$\mathbf{F}(\tilde{\mathbf{B}}_\alpha - |k|) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

(c) If $\tilde{n}_\alpha(\mathcal{F}) \cap \{k, -k\} = \{k\}$ (that is, if $-k = k$ or $-k \notin \tilde{n}_\alpha(\mathcal{F})$), then

$$\mathbf{F}(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

Proof. (a) Assume that $-k \notin \tilde{n}_\alpha(\mathcal{F})$. Then, $-k \neq k$ (since $k \in \tilde{n}_\alpha(\mathcal{F})$), so that $k \neq 0$. Thus, $\text{sign } k$ is well-defined.

We must prove that $\mathbf{F}(\tilde{w}_0 - \text{sign } k) \in \mathbf{k}\mathcal{F}_{k_{i+1}}$. By linearity, we WLOG assume that \mathbf{F} is a single face $F = (F_1, F_2, \dots, F_p) \in \mathcal{F}_{k_i}$. Thus, $n_\alpha(F) \geq k_i$, so that $n_\alpha(F) > k_i$ or $n_\alpha(F) = k_i$. If $n_\alpha(F) > k_i$, then $n_\alpha(F) \geq k_{i+1}$ (since $n_\alpha(F)$ belongs to the set $n_\alpha(\mathcal{F}) = \{k_0 < k_1 < k_2 < \dots < k_m\}$, and thus cannot be $> k_i$ without being $\geq k_{i+1}$), so that $\mathbf{F} = F \in \mathcal{F}_{k_{i+1}} \subseteq \mathbf{k}\mathcal{F}_{k_{i+1}}$, and so the claim follows because $\mathbf{k}\mathcal{F}_{k_{i+1}}$ is an ideal of $\mathbf{k}\mathcal{F}$. Hence, we WLOG assume that $n_\alpha(F) = k_i$.

Therefore, (31) yields $|\tilde{n}_\alpha(F)| = n_\alpha(F) = k_i = |k|$. In other words, $\tilde{n}_\alpha(F) = \pm k$. But $\tilde{n}_\alpha(F)$ cannot be $-k$, since $-k \notin \tilde{n}_\alpha(\mathcal{F})$. Hence, we conclude that $\tilde{n}_\alpha(F) = k$. Hence, $k = \tilde{n}_\alpha(F) = (-1)^{n-\ell(F)} n_\alpha(F)$, so that

$$\text{sign } k = (-1)^{n-\ell(F)} \tag{34}$$

(since $n_\alpha(F) \geq 0$ and $k \neq 0$).

Next, we claim that if $G \in \mathcal{F}$ is any face such that $F \not\rightarrow G$, then

$$FG \in \mathcal{F}_{k_{i+1}}. \tag{35}$$

[*Proof of (35):* Let $G \in \mathcal{F}$ be any face such that $F \not\rightarrow G$. Then, there exists some block F_u of F that is not a subset of any block of G . Consider this block F_u . Thus, F_u intersects at least two distinct blocks of G . Let G_v be one of the blocks of G that F_u intersects. Then, the sets $F_u \cap G_v$ and $F_u \setminus G_v$ are both nonempty and disjoint, and their union is F_u . Hence, replacing the block F_u of F by the two nonempty blocks $F_u \cap G_v$ and $F_u \setminus G_v$, we obtain a new set composition

$$H := (F_1, F_2, \dots, F_{u-1}, F_u \cap G_v, F_u \setminus G_v, F_{u+1}, F_{u+2}, \dots, F_p),$$

which has length $p + 1 = \ell(F) + 1$ (since $p = \ell(F)$) and satisfies $FG \rightarrow H \rightarrow F$. Thus, Proposition 4.24 yields $n_\alpha(FG) \geq n_\alpha(H) \geq n_\alpha(F)$.

Recall that $\tilde{n}_\alpha(F) = k$. Thus, $-\tilde{n}_\alpha(F) = -k \notin \tilde{n}_\alpha(\mathcal{F})$. Hence, in particular, $-\tilde{n}_\alpha(F) \neq \tilde{n}_\alpha(H)$. However, if we had $n_\alpha(H) = n_\alpha(F)$, then we would have $\tilde{n}_\alpha(H) = -\tilde{n}_\alpha(F)$ (since $\ell(H) = \ell(F) + 1$ shows that the signs $(-1)^{n-\ell(H)}$ and $(-1)^{n-\ell(F)}$ in the definitions of $\tilde{n}_\alpha(H)$ and $\tilde{n}_\alpha(F)$ are opposite), which would contradict $-\tilde{n}_\alpha(F) \neq \tilde{n}_\alpha(H)$. Thus,

we cannot have $n_\alpha(H) = n_\alpha(F)$. Therefore, $n_\alpha(H) > n_\alpha(F)$ (since $n_\alpha(H) \geq n_\alpha(F)$). Altogether, $n_\alpha(FG) \geq n_\alpha(H) > n_\alpha(F) = k_i$. Hence, $n_\alpha(FG) \geq k_{i+1}$ (again since $n_\alpha(FG)$ belongs to the set $n_\alpha(\mathcal{F}) = \{k_0 < k_1 < k_2 < \dots < k_m\}$) and therefore $FG \in \mathcal{F}_{k_{i+1}}$. This proves (35).]

Now, multiplying the equalities $\mathbf{F} = F$ and (11), we obtain

$$\begin{aligned}
\mathbf{F}\tilde{w}_0 &= F \sum_{G \in \mathcal{F}} (-1)^{n-\ell(G)} G = \sum_{G \in \mathcal{F}} (-1)^{n-\ell(G)} FG \\
&= \sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} (-1)^{n-\ell(G)} FG + \sum_{\substack{G \in \mathcal{F}; \\ F \not\rightarrow G}} (-1)^{n-\ell(G)} \underbrace{FG}_{\substack{\in \mathcal{F}_{k_{i+1}} \\ \text{(by (35))}}} \\
&\equiv \sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} (-1)^{n-\ell(G)} \underbrace{FG}_{\substack{=F \\ \text{(by Proposition 4.20 (c))}}} \\
&= \underbrace{\sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} (-1)^{n-\ell(G)}}_{\substack{= (-1)^{n-\ell(F)} \\ \text{(by Lemma 6.2)}}} F = \underbrace{(-1)^{n-\ell(F)}}_{\substack{= \text{sign } k \\ \text{(by (34))}}} \underbrace{F}_{=F} = \text{sign } k \cdot \mathbf{F} \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}.
\end{aligned}$$

In other words,

$$\mathbf{F}\tilde{w}_0 - \text{sign } k \cdot \mathbf{F} \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

Equivalently,

$$\mathbf{F}(\tilde{w}_0 - \text{sign } k) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

Thus, Lemma 7.3 (a) is proved.

(b) Lemma 5.6 yields

$$\mathbf{F}(\tilde{\mathbf{B}}_\alpha - k_i) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

Since $|k| = k_i$, we can rewrite this as $\mathbf{F}(\tilde{\mathbf{B}}_\alpha - |k|) \in \mathbf{k}\mathcal{F}_{k_{i+1}}$. This proves Lemma 7.3 (b).

(c) Recall that $\mathbf{k}\mathcal{F}_{k_{i+1}}$ is an ideal of $\mathbf{k}\mathcal{F}$, so we can compute modulo it as with integers.

Now, assume that $\tilde{n}_\alpha(\mathcal{F}) \cap \{k, -k\} = \{k\}$ (that is, that $-k = k$ or $-k \notin \tilde{n}_\alpha(\mathcal{F})$). Thus, we are in one of the following two cases:

Case 1: We have $-k = k$.

Case 2: We have $-k \notin \tilde{n}_\alpha(\mathcal{F})$.

We begin by handling Case 1. In this case, $-k = k$. Hence, $k = 0$, so that our goal is to prove that $\mathbf{F}\tilde{w}_0\tilde{\mathbf{B}}_\alpha \in \mathbf{k}\mathcal{F}_{k_{i+1}}$. But $\mathbf{F} \in \mathbf{k}\mathcal{F}_{k_i}$ and thus $\mathbf{F}\tilde{w}_0 \in \mathbf{k}\mathcal{F}_{k_i}$ (since $\mathbf{k}\mathcal{F}_{k_i}$ is an ideal). Hence, part (b) (applied to $\mathbf{F}\tilde{w}_0$ instead of \mathbf{F}) yields $\mathbf{F}\tilde{w}_0(\tilde{\mathbf{B}}_\alpha - |k|) \in \mathbf{k}\mathcal{F}_{k_{i+1}}$. In view of $k = 0$, this simplifies to $\mathbf{F}\tilde{w}_0\tilde{\mathbf{B}}_\alpha \in \mathbf{k}\mathcal{F}_{k_{i+1}}$, which is what we desired to prove. Thus, Lemma 7.3 (c) is proved in Case 1.

Now let us consider Case 2. In this case, $-k \notin \tilde{n}_\alpha(\mathcal{F})$. Hence, part (a) yields $\mathbf{F}(\tilde{w}_0 - \text{sign } k) \in \mathbf{k}\mathcal{F}_{k_{i+1}}$. In other words,

$$\mathbf{F}\tilde{w}_0 \equiv \text{sign } k \cdot \mathbf{F} \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}. \quad (36)$$

But part **(b)** yields $\mathbf{F}(\tilde{\mathbf{B}}_\alpha - |k|) \in \mathbf{k}\mathcal{F}_{k_{i+1}}$. That is,

$$\mathbf{F}\tilde{\mathbf{B}}_\alpha \equiv |k|\mathbf{F} \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}.$$

Multiplying the congruence (36) with $\tilde{\mathbf{B}}_\alpha$ from the right, we find

$$\mathbf{F}\tilde{w}_0\tilde{\mathbf{B}}_\alpha \equiv \text{sign } k \cdot \underbrace{\mathbf{F}\tilde{\mathbf{B}}_\alpha}_{\equiv |k|\mathbf{F} \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}} \equiv \underbrace{\text{sign } k \cdot |k|}_{=k} \mathbf{F} = k\mathbf{F} \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}.$$

In other words,

$$\mathbf{F}(\tilde{w}_0\tilde{\mathbf{B}}_\alpha - k) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

Thus, Lemma 7.3 **(c)** is proved in Case 2. Hence, the proof of Lemma 7.3 **(c)** is complete in both cases. \square

We combine Lemmas 5.9 and 7.3 into one:

Lemma 7.4. Let $i \in [0, m]$ and $\mathbf{F} \in \mathbf{k}\mathcal{F}_{k_i}$. Then,

$$\mathbf{F} \prod_{\substack{h \in \tilde{n}_\alpha(\mathcal{F}); \\ |h|=k_i}} (\tilde{w}_0\tilde{\mathbf{B}}_\alpha - h) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

Proof. We have $n_\alpha(\mathcal{F}) = \{k_0 < k_1 < \dots < k_m\}$ and thus $k_i \in n_\alpha(\mathcal{F})$. Hence, there exists a face $F \in \mathcal{F}$ such that $n_\alpha(F) = k_i$. Consider this face F . Its signed knapsack number $\tilde{n}_\alpha(F)$ must then be either k_i or $-k_i$ (since it is defined to be $\underbrace{(-1)^{n-\ell(F)}}_{=\pm 1} \underbrace{n_\alpha(F)}_{=k_i} = \pm k_i$).

Therefore, at least one of k_i and $-k_i$ equals $\tilde{n}_\alpha(F)$ and thus belongs to $\tilde{n}_\alpha(\mathcal{F})$. In other words, there exists an element $k \in \{k_i, -k_i\}$ that belongs to $\tilde{n}_\alpha(\mathcal{F})$. We are thus in one of the following two cases:

Case 1: There exists exactly one element $k \in \{k_i, -k_i\}$ that belongs to $\tilde{n}_\alpha(\mathcal{F})$. (That is, either $k_i = -k_i$, or exactly one of the two numbers k_i and $-k_i$ belongs to $\tilde{n}_\alpha(\mathcal{F})$.)

Case 2: There are two elements $k \in \{k_i, -k_i\}$ that belong to $\tilde{n}_\alpha(\mathcal{F})$. (That is, k_i and $-k_i$ are distinct, and both belong to $\tilde{n}_\alpha(\mathcal{F})$.)

Let us consider Case 1. In this case, there exists exactly one element $k \in \{k_i, -k_i\}$ that belongs to $\tilde{n}_\alpha(\mathcal{F})$. Consider this k . Then, $k = \pm k_i$, so that $|k| = |k_i| = k_i$ (since $k_i = n_\alpha(F) \geq 0$). This also yields $\{k, -k\} = \{k_i, -k_i\}$. But k is the only element of $\{k_i, -k_i\}$ that belongs to $\tilde{n}_\alpha(\mathcal{F})$. In other words, k is the only element of $\{k, -k\}$ that belongs to $\tilde{n}_\alpha(\mathcal{F})$ (since $\{k, -k\} = \{k_i, -k_i\}$). That is, $\tilde{n}_\alpha(\mathcal{F}) \cap \{k, -k\} = \{k\}$. Hence, Lemma 7.3 **(c)** shows that

$$\mathbf{F}(\tilde{w}_0\tilde{\mathbf{B}}_\alpha - k) \in \mathbf{k}\mathcal{F}_{k_{i+1}} \quad (\text{since } |k| = k_i).$$

However, the only $h \in \tilde{n}_\alpha(\mathcal{F})$ satisfying $|h| = k_i$ is k (since the condition $|h| = k_i$ is equivalent to $h \in \{k_i, -k_i\}$, but we know that k is the only element of $\{k_i, -k_i\}$ that

belongs to $\tilde{n}_\alpha(\mathcal{F})$). Thus,

$$\prod_{\substack{h \in \tilde{n}_\alpha(\mathcal{F}); \\ |h|=k_i}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - h) = \tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k.$$

Hence,

$$\mathbf{F} \prod_{\substack{h \in \tilde{n}_\alpha(\mathcal{F}); \\ |h|=k_i}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - h) = \mathbf{F} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k) \in \mathbf{k}\mathcal{F}_{k_{i+1}}.$$

This proves Lemma 7.4 in Case 1.

Let us next consider Case 2. In this case, there are two elements $k \in \{k_i, -k_i\}$ that belong to $\tilde{n}_\alpha(\mathcal{F})$. Thus, both numbers k_i and $-k_i$ belong to $\tilde{n}_\alpha(\mathcal{F})$ (and are distinct). Hence, the elements $h \in \tilde{n}_\alpha(\mathcal{F})$ satisfying $|h| = k_i$ are k_i and $-k_i$ (and these two values are distinct). Therefore,

$$\prod_{\substack{h \in \tilde{n}_\alpha(\mathcal{F}); \\ |h|=k_i}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - h) = (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - (-k_i)) (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_i) = (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_i) (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_i).$$

Multiplying this by \mathbf{F} from the left, we find

$$\mathbf{F} \prod_{\substack{h \in \tilde{n}_\alpha(\mathcal{F}); \\ |h|=k_i}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - h) = \mathbf{F} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha + k_i) (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k_i) \in \mathbf{k}\mathcal{F}_{k_{i+1}}$$

by Lemma 5.9. Thus, Lemma 7.4 is proved in Case 2. \square

We are now ready to prove Theorem 7.2:

Proof of Theorem 7.2. Define the polynomial

$$f(x) := \prod_{k \in \tilde{n}_\alpha(\mathcal{F})} (x - k) \in \mathbf{k}[x].$$

Thus, our goal is to prove that $f(w_0 \mathbf{B}_\alpha) = 0$ and $f(\mathbf{B}_\alpha w_0) = 0$. According to Lemma 4.15, both of these equalities will follow if we can show that $f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha) = 0$. So this is what we shall now do.

First, we shall prove that each $i \in [0, m+1]$ satisfies

$$\prod_{\substack{k \in \tilde{n}_\alpha(\mathcal{F}); \\ |k| < k_i}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k) \in \mathbf{k}\mathcal{F}_{k_i}. \quad (37)$$

Once this is proved, we will easily obtain $f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha) = 0$ by applying (37) to $i = m+1$.

We shall prove (37) by induction on i :

Base case: The validity of (37) for $i = 0$ is obvious, since the left hand side is an empty product (thus equals 1), while the right hand side $\mathbf{k}\mathcal{F}_{k_0}$ is the whole algebra $\mathbf{k}\mathcal{F}$.

Induction step: Fix $i \in [0, m]$. Assume that (37) holds for this i . We must prove that (37) holds for $i + 1$ instead of i as well.

We note that any $k \in \tilde{n}_\alpha(\mathcal{F})$ that satisfies $|k| < k_{i+1}$ must satisfy $|k| \leq k_i$ (since each $k \in \tilde{n}_\alpha(\mathcal{F})$ satisfies $|k| \in n_\alpha(\mathcal{F}) = \{k_0 < k_1 < \dots < k_m\}$), and thus must satisfy either $|k| < k_i$ or $|k| = k_i$. Hence,

$$\begin{aligned} \prod_{\substack{k \in \tilde{n}_\alpha(\mathcal{F}); \\ |k| < k_{i+1}}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k) &= \underbrace{\prod_{\substack{k \in \tilde{n}_\alpha(\mathcal{F}); \\ |k| < k_i}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k)}_{\in \mathbf{k}\mathcal{F}_{k_i}} \cdot \underbrace{\prod_{\substack{k \in \tilde{n}_\alpha(\mathcal{F}); \\ |k| = k_i}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k)}_{= \prod_{\substack{h \in \tilde{n}_\alpha(\mathcal{F}); \\ |h| = k_i}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - h)} \\ &\in \mathbf{k}\mathcal{F}_{k_i} \cdot \prod_{\substack{h \in \tilde{n}_\alpha(\mathcal{F}); \\ |h| = k_i}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - h) \subseteq \mathbf{k}\mathcal{F}_{k_{i+1}} \end{aligned}$$

(by our induction hypothesis, which says that (37) holds for i)

(by Lemma 7.4). This shows that (37) holds for $i + 1$ instead of i . Thus, the induction is complete, so that (37) is proved.

Now, applying (37) to $i = m + 1$, we obtain

$$\prod_{\substack{k \in \tilde{n}_\alpha(\mathcal{F}); \\ |k| < k_{m+1}}} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k) \in \mathbf{k}\mathcal{F}_{k_{m+1}}.$$

Since each $k \in \tilde{n}_\alpha(\mathcal{F})$ satisfies $|k| < k_{m+1}$ (because $k_{m+1} = \infty$), and since $\mathcal{F}_{k_{m+1}} = \emptyset$, we can rewrite this as

$$\prod_{k \in \tilde{n}_\alpha(\mathcal{F})} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k) \in \mathbf{k}\emptyset = 0.$$

In other words,

$$\prod_{k \in \tilde{n}_\alpha(\mathcal{F})} (\tilde{w}_0 \tilde{\mathbf{B}}_\alpha - k) = 0. \tag{38}$$

Since the left hand side of this equality is $f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha)$ (by the definition of $f(x)$), we can rewrite this as $f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha) = 0$. As we explained above, this proves Theorem 7.2. \square

8 Identifying the minimal polynomial

Recall that if \mathbf{k} is a field, and if a is an element of a \mathbf{k} -algebra A , then the **minimal polynomial** of a (over \mathbf{k}) means the smallest-degree monic polynomial $p \in \mathbf{k}[x]$ satisfying $p(a) = 0$. This always exists when A is finite-dimensional over \mathbf{k} . In particular, if A is a matrix ring $\mathbf{k}^{r \times r}$, then this is just the minimal polynomial of a matrix.

In this section, **we shall assume that \mathbf{k} is a field of characteristic 0**. Note that the minimal polynomial of an element a of a \mathbf{k} -algebra A does not change if we replace A

by a larger algebra that contains A as a subalgebra. Thus, we shall denote this minimal polynomial by $\mu(a)$ without explicitly specifying A .

If two elements of a \mathbf{k} -algebra are conjugate, then they have the same minimal polynomials. Thus,

$$\mu(\mathbf{B}_\alpha w_0) = \mu(w_0 \mathbf{B}_\alpha),$$

since the two elements $\mathbf{B}_\alpha w_0$ and $w_0 \mathbf{B}_\alpha$ of $\mathbf{k}[S_n]$ are conjugate (indeed, conjugating $\mathbf{B}_\alpha w_0$ by w_0 yields $w_0(\mathbf{B}_\alpha w_0)w_0^{-1} = w_0 \mathbf{B}_\alpha$). This minimal polynomial $\mu(\mathbf{B}_\alpha w_0) = \mu(w_0 \mathbf{B}_\alpha)$ will be the focus of our study in this section.

Injective \mathbf{k} -algebra morphisms preserve minimal polynomials: That is, if $f : A \rightarrow B$ is an injective \mathbf{k} -algebra morphism, and if $a \in A$ has a minimal polynomial, then $f(a)$ has the same minimal polynomial as a (that is, $\mu(f(a)) = \mu(a)$). This is because each polynomial $p \in \mathbf{k}[x]$ satisfies $p(f(a)) = f(p(a))$, but the injectivity of f ensures that $f(p(a)) = 0$ if and only if $p(a) = 0$. The same reasoning works when f is an injective \mathbf{k} -algebra anti-morphism instead of a \mathbf{k} -algebra morphism; thus, we conclude that

$$\mu(f(a)) = \mu(a) \tag{39}$$

holds in this case as well. In particular, we can apply this to f being the \mathbf{k} -algebra anti-isomorphism $\rho : D(S_n) \rightarrow (\mathbf{k}\mathcal{F})^{S_n}$, and conclude that

$$\mu(\rho(a)) = \mu(a) \quad \text{for each } a \in D(S_n).$$

Applying this to $a = \mathbf{B}_\alpha w_0$, we obtain $\mu(\rho(\mathbf{B}_\alpha w_0)) = \mu(\mathbf{B}_\alpha w_0)$. In view of (12), we can rewrite this as

$$\mu(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha) = \mu(\mathbf{B}_\alpha w_0) = \mu(w_0 \mathbf{B}_\alpha) \tag{40}$$

(as we saw above). We shall use this to compute $\mu(w_0 \mathbf{B}_\alpha)$.

Theorem 8.1. Assume that \mathbf{k} is a field of characteristic 0. Let $\alpha \models n$. Then, the minimal polynomial of the element $w_0 \mathbf{B}_\alpha$ of $\mathbf{k}[S_n]$ is

$$\mu(w_0 \mathbf{B}_\alpha) = \prod_{k \in \tilde{n}_\alpha(\mathcal{F})} (x - k). \tag{41}$$

This will follow from a description of the eigenvalues of the “right multiplication by $\tilde{w}_0 \tilde{\mathbf{B}}_\alpha$ ” operator on $\mathbf{k}\mathcal{F}$:

Theorem 8.2. Assume that \mathbf{k} is a field of characteristic 0. Let $\alpha \models n$. Then, the \mathbf{k} -linear operator

$$\begin{aligned} \mathbf{k}\mathcal{F} &\rightarrow \mathbf{k}\mathcal{F}, \\ \mathbf{F} &\mapsto \mathbf{F} \tilde{w}_0 \tilde{\mathbf{B}}_\alpha \end{aligned}$$

is diagonalizable, and its eigenvalues are the signed knapsack numbers $\tilde{n}_\alpha(F)$ of the faces $F \in \mathcal{F}$. (The algebraic multiplicity of each eigenvalue λ is the number of the faces F whose signed knapsack number is λ .)

To prove this, we will need the following two lemmas:

Lemma 8.3 (More blocks lemma). Let $F \in \mathcal{F}$ and $\alpha \models n$. Then we have

$$F \cdot \tilde{w}_0 \tilde{\mathbf{B}}_\alpha = \tilde{n}_\alpha(F) F + \sum_{\substack{G \in \mathcal{F}; \\ \ell(G) > \ell(F)}} c_G G \quad \text{for some scalars } c_G \in \mathbf{k}.$$

Proof. Let I be the set of all faces $G \in \mathcal{F}$ satisfying $\ell(G) > \ell(F)$. Let $\mathbf{k}I$ be the \mathbf{k} -linear span of this set I in $\mathbf{k}\mathcal{F}$. This span $\mathbf{k}I$ is an ideal of $\mathbf{k}\mathcal{F}$ (by an argument analogous to the proof of Proposition 5.4, but now using Proposition 4.20 (d) and (e) instead of Proposition 4.25). Our goal is to show that $F \cdot \tilde{w}_0 \tilde{\mathbf{B}}_\alpha \equiv \tilde{n}_\alpha(F) F \pmod{\mathbf{k}I}$.

But Definition 4.9 yields

$$\begin{aligned} F \cdot \tilde{\mathbf{B}}_\alpha &= F \cdot \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha}} G = \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha}} FG \\ &= \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \rightarrow G}} \underbrace{FG}_{=F} \quad + \quad \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \not\rightarrow G}} \underbrace{FG}_{\equiv 0 \pmod{\mathbf{k}I}} \\ &\quad \text{(by Proposition 4.20 (c))} \quad \text{(since Proposition 4.20 (d) yields } \ell(FG) > \ell(F), \text{ so that } FG \in I) \\ &\equiv \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha; \\ F \rightarrow G}} F = n_\alpha(F) F \pmod{\mathbf{k}I} \end{aligned} \tag{42}$$

(since the sum consists of $n_\alpha(F)$ equal addends, by Definition 4.21). Furthermore, (11) yields

$$\begin{aligned} F \cdot \tilde{w}_0 &= F \cdot \sum_{G \in \mathcal{F}} (-1)^{n-\ell(G)} G = \sum_{G \in \mathcal{F}} (-1)^{n-\ell(G)} FG \\ &= \sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} (-1)^{n-\ell(G)} \underbrace{FG}_{=F} \quad + \quad \sum_{\substack{G \in \mathcal{F}; \\ F \not\rightarrow G}} (-1)^{n-\ell(G)} \underbrace{FG}_{\equiv 0 \pmod{\mathbf{k}I}} \\ &\quad \text{(by Proposition 4.20 (c))} \quad \text{(since Proposition 4.20 (d) yields } \ell(FG) > \ell(F), \text{ so that } FG \in I) \\ &\equiv \underbrace{\sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} (-1)^{n-\ell(G)} F}_{=(-1)^{n-\ell(F)} \text{ (by Lemma 6.2)}} = (-1)^{n-\ell(F)} F \pmod{\mathbf{k}I}. \end{aligned}$$

Since $\mathbf{k}I$ is an ideal, we can multiply the latter congruence by $\tilde{\mathbf{B}}_\alpha$ from the right, obtaining

$$\begin{aligned} F \cdot \tilde{w}_0 \tilde{\mathbf{B}}_\alpha &\equiv (-1)^{n-\ell(F)} F \cdot \tilde{\mathbf{B}}_\alpha \equiv \underbrace{(-1)^{n-\ell(F)} n_\alpha(F) F}_{=\tilde{n}_\alpha(F)} \quad \text{(by (42))} \\ &= \tilde{n}_\alpha(F) F \pmod{\mathbf{k}I}. \end{aligned}$$

Recalling how I was defined, we see that this is the claim of the lemma. \square

Lemma 8.4. Let \mathbf{k} be a field. Let A be a \mathbf{k} -algebra. Let $a \in A$ be an element that has a minimal polynomial. Let

$$\begin{aligned} R_a : A &\rightarrow A, \\ x &\mapsto xa \end{aligned}$$

be the map known as “right multiplication by a ”. This R_a is a \mathbf{k} -linear map, i.e., belongs to the endomorphism ring $\text{End } A$. Then,

$$\mu(R_a) = \mu(a).$$

Proof. Forget that we fixed a . We thus have defined an endomorphism $R_a \in \text{End } A$ for each $a \in A$. The map $f : A \rightarrow \text{End } A$ that sends each $a \in A$ to this endomorphism R_a is easily seen to be an injective \mathbf{k} -algebra anti-morphism (injective because $R_a(1) = 1a = a$; anti-morphism because $R_b(R_a(x)) = (xa)b = x(ab) = R_{ab}(x)$). Thus, (39) yields $\mu(f(a)) = \mu(a)$ for each $a \in A$. In other words, $\mu(R_a) = \mu(a)$ for each $a \in A$ (since $f(a) = R_a$). This proves the lemma. \square

Proof of Theorem 8.2. Let us denote this operator by Φ . Define a polynomial

$$f(x) := \prod_{k \in \tilde{n}_\alpha(\mathcal{F})} (x - k) \in \mathbf{k}[x].$$

This polynomial factors into distinct monic linear factors (distinct because \mathbf{k} has characteristic 0). Clearly, (38) says that $f(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha) = 0$. Thus, the minimal polynomial $\mu(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha)$ must divide f (since the minimal polynomial $\mu(a)$ of an element a of a \mathbf{k} -algebra always divides any polynomial that annihilates a).

As we recall, the operator Φ sends each element $F \in \mathbf{k}\mathcal{F}$ to $F\tilde{w}_0 \tilde{\mathbf{B}}_\alpha$. In other words, this operator Φ is right multiplication by $\tilde{w}_0 \tilde{\mathbf{B}}_\alpha$. Hence, Lemma 8.4 (applied to $A = \mathbf{k}\mathcal{F}$ and $a = \tilde{w}_0 \tilde{\mathbf{B}}_\alpha$ and $R_a = \Phi$) shows that $\mu(\Phi) = \mu(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha)$. Hence, the polynomial $\mu(\Phi)$ divides f (since the polynomial $\mu(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha)$ divides f).

Therefore, this polynomial $\mu(\Phi)$ factors into distinct monic linear factors (because the same is true of f). Hence, the operator Φ is diagonalizable (because $\mathbf{k}\mathcal{F}$ is a finite-dimensional \mathbf{k} -vector space, and thus any endomorphism of $\mathbf{k}\mathcal{F}$ whose minimal polynomial factors into distinct monic linear factors must be diagonalizable).

It remains to determine its eigenvalues. The faces in \mathcal{F} form a basis of the \mathbf{k} -vector space $\mathbf{k}\mathcal{F}$. Let us order this basis by increasing length of the face (breaking ties arbitrarily). Then, the operator Φ is represented by a lower-triangular matrix with respect to this ordered basis, because Lemma 8.3 gives an expansion of $\Phi(F) = F \cdot \tilde{w}_0 \tilde{\mathbf{B}}_\alpha$ as a linear combination of F and longer (thus later) faces. But the eigenvalues of a lower-triangular matrix are its diagonal entries (and their algebraic multiplicities are how often they appear on the diagonal). In our case, the diagonal entries of the matrix that represents Φ are the numbers $\tilde{n}_\alpha(F)$, again according to Lemma 8.3. Hence, the eigenvalues of Φ are these numbers $\tilde{n}_\alpha(F)$. This completes the proof of Theorem 8.2. \square

Proof of Theorem 8.1. Let $\Phi : \mathbf{k}\mathcal{F} \rightarrow \mathbf{k}\mathcal{F}$ be the operator defined in Theorem 8.2. As shown in that theorem, the eigenvalues of this operator Φ are the signed knapsack numbers $\tilde{n}_\alpha(F)$ of the faces $F \in \mathcal{F}$. Thus, the set of all eigenvalues of Φ is $\tilde{n}_\alpha(\mathcal{F})$. Since Φ is furthermore diagonalizable (again by Theorem 8.2), this shows that the minimal polynomial $\mu(\Phi)$ of Φ is the polynomial

$$f(x) := \prod_{k \in \tilde{n}_\alpha(\mathcal{F})} (x - k) \in \mathbf{k}[x]$$

(since the minimal polynomial of a diagonalizable endomorphism is the product of $x - \lambda$ over the distinct eigenvalues λ of the endomorphism).

However, Φ is just the right multiplication by $\tilde{w}_0 \tilde{\mathbf{B}}_\alpha$. Hence, Lemma 8.4 (applied to $A = \mathbf{k}\mathcal{F}$ and $a = \tilde{w}_0 \tilde{\mathbf{B}}_\alpha$ and $R_a = \Phi$) shows that $\mu(\Phi) = \mu(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha)$. Thus, $\mu(\tilde{w}_0 \tilde{\mathbf{B}}_\alpha) = \mu(\Phi) = f(x)$, as we just saw.

Comparing this with (40), we obtain $\mu(w_0 \mathbf{B}_\alpha) = f(x)$. Upon recalling the definition of $f(x)$, this proves Theorem 8.1. \square

9 Application to top-to-random-and-reverse

In this section, we shall focus on the case when α is the composition $(1, n-1)$ (for $n > 1$). In this case, $\mathbf{B}_\alpha = \mathbf{B}_{(1, n-1)}$ is the image of the **top-to-random shuffle** under the **antipode** map of the symmetric group algebra $\mathbf{k}[S_n]$. We recall their definitions:

Definition 9.1. The **top-to-random shuffle** is the element

$$\mathbf{A} := \sum_{i=1}^n \text{cyc}_{1,2,\dots,i} \in \mathbf{k}[S_n], \quad (43)$$

where $\text{cyc}_{k_1, k_2, \dots, k_m}$ denotes the m -cycle in S_n that sends $k_1 \mapsto k_2 \mapsto \dots \mapsto k_m \mapsto k_1$.

Definition 9.2. The **antipode** of the symmetric group algebra $\mathbf{k}[S_n]$ is the \mathbf{k} -linear map $S : \mathbf{k}[S_n] \rightarrow \mathbf{k}[S_n]$ that sends each basis vector (permutation) $w \in S_n$ to w^{-1} . It is well-known that S is a \mathbf{k} -algebra anti-isomorphism.

Now, our above claim about $\mathbf{B}_{(1, n-1)}$ can be stated as follows:

Proposition 9.3. We have

$$S(\mathbf{A}) = \mathbf{B}_{(1, n-1)}.$$

Proof. This is well-known, but we give a proof for completeness. By definition of \mathbf{B}_α , we have

$$\begin{aligned} \mathbf{B}_{(1, n-1)} &= \mathbf{B}_{\text{gaps}^{-1}(1, n-1)} = \mathbf{B}_{\{1\}} && \left(\text{since } \text{gaps}^{-1}(1, n-1) = \{1\} \right) \\ &= \sum_{\substack{w \in S_n \\ \text{Des } w \subseteq \{1\}}} w. && (44) \end{aligned}$$

But the permutations $w \in S_n$ that satisfy $\text{Des } w \subseteq \{1\}$ are precisely those permutations that satisfy $w(2) < w(3) < \dots < w(n)$; in other words, they consist of an arbitrary element $i \in [n]$ in their first position, followed by the remaining elements of $[n]$ in increasing order. Such permutations can be written as cycles $\text{cyc}_{i,i-1,\dots,2,1}$. Hence, we can rewrite (44) as

$$\mathbf{B}_{(1,n-1)} = \sum_{i=1}^n \text{cyc}_{i,i-1,\dots,2,1}.$$

On the other hand, the definition of \mathbf{A} yields

$$S(\mathbf{A}) = S\left(\sum_{i=1}^n \text{cyc}_{1,2,\dots,i}\right) = \sum_{i=1}^n \text{cyc}_{1,2,\dots,i}^{-1},$$

since the antipode S sends each permutation to its inverse. The right hand sides of these two equalities are equal, since $\text{cyc}_{i,i-1,\dots,2,1} = \text{cyc}_{1,2,\dots,i}^{-1}$ for each i . Therefore, the left hand sides are equal as well. In other words, $\mathbf{B}_{(1,n-1)} = S(\mathbf{A})$. \square

Since the antipode S is a \mathbf{k} -algebra anti-morphism, we have

$$S(\mathbf{A}w_0) = S(w_0)S(\mathbf{A}) = w_0\mathbf{B}_{(1,n-1)} \quad (45)$$

(since $S(w_0) = w_0^{-1} = w_0$ and $S(\mathbf{A}) = \mathbf{B}_{(1,n-1)}$ by Proposition 9.3). Thus, if \mathbf{k} is a field of characteristic 0, then the element $w_0\mathbf{B}_{(1,n-1)} = S(\mathbf{A}w_0)$ has the same minimal polynomial as $\mathbf{A}w_0$ (by (39), since $S : \mathbf{k}[S_n] \rightarrow \mathbf{k}[S_n]$ is an algebra anti-isomorphism). From Theorem 8.1, this minimal polynomial is

$$\mu\left(w_0\mathbf{B}_{(1,n-1)}\right) = \prod_{k \in \tilde{n}_{(1,n-1)}(\mathcal{F})} (x - k).$$

To make this concrete, we will determine the set $\tilde{n}_{(1,n-1)}(\mathcal{F})$ indexing this product.

Proposition 9.4. Assume that $n > 1$. Then, the set $\tilde{n}_{(1,n-1)}(\mathcal{F})$ is the set

$$L(n) := \{-n+2\} \cup [-n+4, n-3] \cup \{0\} \cup \{n\}.$$

Once this proposition is proved, we will be able to conclude:

Theorem 9.5. Assume that \mathbf{k} is a field of characteristic 0, and that $n > 1$. Then, the elements $w_0\mathbf{A}$ and $\mathbf{A}w_0$ of $\mathbf{k}[S_n]$ have minimal polynomial

$$\mu(w_0\mathbf{A}) = \mu(\mathbf{A}w_0) = \prod_{k \in L(n)} (x - k).$$

Proof. The elements $w_0\mathbf{A}$ and $\mathbf{A}w_0$ are conjugate (via conjugation by w_0), and thus have the same minimal polynomial. That is, $\mu(w_0\mathbf{A}) = \mu(\mathbf{A}w_0)$. Furthermore, $S : \mathbf{k}[S_n] \rightarrow \mathbf{k}[S_n]$ is a \mathbf{k} -algebra anti-isomorphism. Hence, (39) yields $\mu(S(\mathbf{A}w_0)) = \mu(\mathbf{A}w_0)$. By

(45), this rewrites as $\mu(w_0 \mathbf{B}_{(1,n-1)}) = \mu(\mathbf{A}w_0)$. But by Theorem 8.1, the minimal polynomial of $w_0 \mathbf{B}_{(1,n-1)}$ is

$$\mu(w_0 \mathbf{B}_{(1,n-1)}) = \prod_{k \in \tilde{n}_{(1,n-1)}(\mathcal{F})} (x - k) = \prod_{k \in L(n)} (x - k) \quad (\text{by Proposition 9.4}).$$

Comparing these two equalities, we find $\mu(\mathbf{A}w_0) = \prod_{k \in L(n)} (x - k)$. Together with $\mu(w_0 \mathbf{A}) = \mu(\mathbf{A}w_0)$, this completes our proof. \square

It remains to prove Proposition 9.4. We begin with a definition.

Definition 9.6 (Singleton blocks). For each face $F = (F_1, F_2, \dots, F_k) \in \mathcal{F}$, we set

$$\begin{aligned} \text{Sin } F &:= \{F_i : |F_i| = 1\} = \{\text{all blocks of } F \text{ that have size } 1\} & \text{and} \\ \text{sin } F &:= |\text{Sin } F|. \end{aligned}$$

Thus, $\text{sin } F$ is the number of all size-1 blocks (“singleton blocks”) of F .

Example 9.7. The set composition $(4, 25, 1, 7, 36)$ of $[7]$ has singleton blocks $\{4\}, \{1\}, \{7\}$, so we have $\text{Sin}(4, 25, 1, 7, 36) = \{\{4\}, \{1\}, \{7\}\}$ and $\text{sin}(4, 25, 1, 7, 36) = 3$.

Lemma 9.8. Consider the composition $(1, n - 1)$ of $n > 1$. For each $F \in \mathcal{F}$, we have

$$n_{(1,n-1)}(F) = \text{sin } F \quad \text{and} \quad (46)$$

$$\tilde{n}_{(1,n-1)}(F) = (-1)^{n-\ell(F)} \text{sin } F. \quad (47)$$

Proof. Let $\alpha = (1, n - 1)$. Fix $F \in \mathcal{F}$.

The faces $G \in \mathcal{F}$ having type $\alpha = (1, n - 1)$ are precisely the n faces of the form

$$(\{k\}, [n] \setminus \{k\}) \quad \text{for some } k \in [n].$$

Hence, in particular, all the faces $G \in N_\alpha(F)$ have this form.

Moreover, if a face $G \in N_\alpha(F)$ is written as $(\{k\}, [n] \setminus \{k\})$, then $\{k\}$ is a block of F (indeed, $G \in N_\alpha(F)$ entails $F \twoheadrightarrow G$, so that each block of F is a subset of a block of G ; in other words, each block of F is either a subset of $\{k\}$ or a subset of $[n] \setminus \{k\}$; but the only way this is possible is when $\{k\}$ is a block of F). Thus, it must satisfy $\{k\} \in \text{Sin } F$. Hence, we can define a map

$$\begin{aligned} N_\alpha(F) &\rightarrow \text{Sin } F, \\ (\{k\}, [n] \setminus \{k\}) &\mapsto \{k\}. \end{aligned}$$

This map is injective (obviously) and surjective (since each singleton block $\{k\}$ of F does satisfy $F \twoheadrightarrow (\{k\}, [n] \setminus \{k\})$ and therefore $(\{k\}, [n] \setminus \{k\}) \in N_\alpha(F)$). Hence, it is bijective. Thus, $|N_\alpha(F)| = |\text{Sin } F| = \text{sin } F$, so that

$$n_\alpha(F) = |N_\alpha(F)| = \text{sin } F. \quad (48)$$

This proves (46) (since $\alpha = (1, n - 1)$). Moreover, the definition of $\tilde{n}_\alpha(F)$ shows that

$$\tilde{n}_\alpha(F) = (-1)^{n-\ell(F)} n_\alpha(F) = (-1)^{n-\ell(F)} \text{sin } F \quad (49)$$

(by (48)). This proves (47), and thus completes the proof. \square

Proof of Proposition 9.4. We assume that $n > 3$; the other cases ($n = 2$ and $n = 3$) are left to the reader.

Let $\alpha = (1, n - 1)$. Thus, we must prove that $\tilde{n}_\alpha(\mathcal{F}) = L(n)$. In other words, we must prove that each $r \in L(n)$ belongs to $\tilde{n}_\alpha(\mathcal{F})$, and conversely, that each $k \in \tilde{n}_\alpha(\mathcal{F})$ belongs to $L(n)$.

In order to prove that each $r \in L(n)$ belongs to $\tilde{n}_\alpha(\mathcal{F})$, we need to construct a face $F \in \mathcal{F}$ satisfying $\tilde{n}_\alpha(F) = r$. We do this case by case:

1. If $r = \pm s$ for some $s \in [0, n - 4]$, then we set

$$\begin{aligned} \text{either } F &= (\{1\}, \{2\}, \dots, \{s\}, [s + 1, n]) \\ \text{or } F &= (\{1\}, \{2\}, \dots, \{s\}, \{s + 1, s + 2\}, [s + 3, n]). \end{aligned}$$

Both of these faces satisfy $\sin F = s$ (here we are using $s \leq n - 4$, which ensures that the last block $[s + 3, n]$ of the second F has size > 1), but their lengths are $s + 1$ and $s + 2$ respectively, so that the corresponding $(-1)^{n-\ell(F)}$ factors are 1 and -1 in some order. Thus, by (47), we conclude that the signed knapsack numbers $\tilde{n}_\alpha(F) = \tilde{n}_{(1, n-1)}(F)$ of these two faces F are s and $-s$ in some order; in particular, one of them is r (since $r = \pm s$). This shows that r is the signed knapsack number of a face. In other words, $r \in \tilde{n}_\alpha(\mathcal{F})$.

2. If $r = n - 3$, then we set $F = (\{1\}, \{2\}, \dots, \{n - 3\}, [n - 2, n])$. This face satisfies $\sin F = n - 3$ and $\ell(F) = n - 2$, so that (47) yields $\tilde{n}_\alpha(F) = (-1)^{n-(n-2)}(n - 3) = n - 3 = r$. Therefore, r is the signed knapsack number of a face. That is, $r \in \tilde{n}_\alpha(\mathcal{F})$.
3. If $r = -n + 2$, then we set $F = (\{1\}, \{2\}, \dots, \{n - 2\}, [n - 1, n])$. This face satisfies $\sin F = n - 2$ and $\ell(F) = n - 1$, so that (47) yields $\tilde{n}_\alpha(F) = (-1)^{n-(n-1)}(n - 2) = -n + 2 = r$. Therefore, r is the signed knapsack number of a face. In other words, $r \in \tilde{n}_\alpha(\mathcal{F})$.
4. If $r = n$, then we set $F = (\{1\}, \{2\}, \dots, \{n\})$, which satisfies $\tilde{n}_\alpha(F) = n = r$. Thus, $r = \tilde{n}_\alpha(F) \in \tilde{n}_\alpha(\mathcal{F})$.

This shows that each $r \in L(n)$ belongs to $\tilde{n}_\alpha(\mathcal{F})$.

It remains to prove that conversely, each $k \in \tilde{n}_\alpha(\mathcal{F})$ belongs to $L(n)$. So we fix a $k \in \tilde{n}_\alpha(\mathcal{F})$. Then, $k = \tilde{n}_\alpha(F)$ for some face $F \in \mathcal{F}$. Consider this F . Recall that $\alpha = (1, n - 1)$. Hence, by (47), we have $\tilde{n}_\alpha(F) = (-1)^{n-\ell(F)} \sin F = \pm \sin F$. But $\sin F$ is clearly an element of $[0, n]$, and cannot be $n - 1$ (because if F contains $n - 1$ singleton blocks, then the last remaining block must also be a singleton block, so F actually has n singleton blocks). Thus, $\sin F \in [0, n] \setminus \{n - 1\}$, so that

$$k = \tilde{n}_\alpha(F) = \pm \underbrace{\sin F}_{\in [0, n] \setminus \{n-1\}} \in [-n, n] \setminus \{-n + 1, n - 1\}.$$

This is almost enough to show that $k \in L(n)$; we only need to prove that k cannot be $-n$ or $-n + 3$ or $n - 2$. This can be done fairly easily:

1. If k was $-n$, then $\sin F$ would be n (since $k = \pm \sin F$), which would mean that F has n singleton blocks; thus, F would have the form $(\{\sigma(1)\}, \{\sigma(2)\}, \dots, \{\sigma(n)\})$ for some $\sigma \in S_n$. But such faces F have signed knapsack number $\tilde{n}_\alpha(F) = (-1)^{n-\ell(F)} \sin F = (-1)^{n-n} n = n$, not $-n$.
2. If k was $-n + 3$, then $\sin F$ would be $n - 3$ (since $k = \pm \sin F$), which would mean that F has $n - 3$ singleton blocks, which account for all but three elements of $[n]$; the remaining three elements would then be all in one single block (as there is no way to break them into more than one block without creating singleton blocks). Thus, F would have $n - 2$ blocks in total, and therefore the signed knapsack number $\tilde{n}_\alpha(F)$ would be $(-1)^{n-(n-2)} (n - 3) = n - 3$, not $-n + 3$.
3. If k was $n - 2$, then a similar argument would show that $\tilde{n}_\alpha(F)$ is $-n + 2$, not $n - 2$.

Hence, k cannot be $-n$ or $-n + 3$ or $n - 2$. This shows that $k \in L(n)$. In other words, k belongs to $L(n)$. This completes the proof of Proposition 9.4. \square

10 Positive linear combinations

Our above results can be generalized with fairly little effort, from single elements \mathbf{B}_α to their linear combinations $\sum_{\alpha \models n} \gamma_\alpha \mathbf{B}_\alpha \in D(S_n)$. However, since the proofs use inequalities between the knapsack numbers $n_\alpha(F)$ (such as Proposition 4.26), we cannot let the coefficients γ_α be arbitrary. It turns out that requiring them to be nonnegative reals is sufficient. This idea goes back to Brown [4, Theorem 5] and was stated explicitly for the \mathbf{B}_α by Schocker [23, Theorem 4.1], but we shall now extend it to $w_0 \mathbf{B}_\alpha$ and prove it anew.

Instead of fixing a composition $\alpha \models n$, **we now fix a family $\gamma = (\gamma_\alpha)_{\alpha \models n}$ of nonnegative real numbers $\gamma_\alpha \geq 0$ indexed by the compositions α of n** . We assume that the ring \mathbf{k} is ordered and contains these numbers γ_α (for instance, $\mathbf{k} = \mathbb{R}$, or $\mathbf{k} = \mathbb{Q}$ if these numbers are rational).

We define the element

$$\mathbf{B}_\gamma := \sum_{\alpha \models n} \gamma_\alpha \mathbf{B}_\alpha \in D(S_n).$$

For each face $F \in \mathcal{F}$, we define the **γ -weighted knapsack number of F** to be the number

$$n_\gamma(F) := \sum_{\alpha \models n} \gamma_\alpha n_\alpha(F) \in \mathbf{k},$$

and we define the **γ -weighted signed knapsack number of F** to be the number

$$\tilde{n}_\gamma(F) := \sum_{\alpha \models n} \gamma_\alpha \tilde{n}_\alpha(F) \in \mathbf{k}.$$

We set $n_\gamma(\mathcal{F}) = \{n_\gamma(F) \mid F \in \mathcal{F}\}$ and $\tilde{n}_\gamma(\mathcal{F}) = \{\tilde{n}_\gamma(F) \mid F \in \mathcal{F}\}$.

Now, we claim the following generalizations of Theorem 5.1 and Theorem 7.2:

Theorem 10.1. The element $\mathbf{B}_\gamma \in D(S_n)$ satisfies

$$\prod_{k \in n_\gamma(\mathcal{F})} (\mathbf{B}_\gamma - k) = 0. \quad (50)$$

Theorem 10.2. The elements $w_0\mathbf{B}_\gamma$ and $\mathbf{B}_\gamma w_0$ of $D(S_n)$ satisfy

$$\prod_{k \in \tilde{n}_\gamma(\mathcal{F})} (w_0\mathbf{B}_\gamma - k) = 0 \quad (51)$$

and

$$\prod_{k \in \tilde{n}_\gamma(\mathcal{F})} (\mathbf{B}_\gamma w_0 - k) = 0. \quad (52)$$

The proofs of Theorem 10.1 and Theorem 10.2 proceed mostly analogously to the proofs of Theorem 5.1 and Theorem 7.2; we just need to replace every object O_α that depends on a composition α by the corresponding linear combination $\sum_{\alpha \models n} \gamma_\alpha O_\alpha$ of such objects. In particular, we need to

- replace \mathbf{B}_α by \mathbf{B}_γ ,
- replace $\tilde{\mathbf{B}}_\alpha$ by $\tilde{\mathbf{B}}_\gamma := \sum_{\alpha \models n} \gamma_\alpha \tilde{\mathbf{B}}_\alpha \in (\mathbf{k}\mathcal{F})^{S_n}$ (noting that $\rho(\mathbf{B}_\gamma) = \tilde{\mathbf{B}}_\gamma$ follows from (7) by linearity),
- replace $\tilde{\mathbf{B}}_{\text{rev } \alpha}$ by $\tilde{\mathbf{B}}_{\text{rev } \gamma} := \sum_{\alpha \models n} \gamma_\alpha \tilde{\mathbf{B}}_{\text{rev } \alpha}$,
- replace $n_\alpha(F)$ by $n_\gamma(F)$,
- replace $n_{\text{rev } \alpha}(F)$ by $n_{\text{rev } \gamma}(F) := \sum_{\alpha \models n} \gamma_\alpha n_{\text{rev } \alpha}(F)$,
- replace $\tilde{n}_\alpha(F)$ by $\tilde{n}_\gamma(F)$ (which equals $(-1)^{n-\ell(F)} n_\gamma(F)$),
- etc. (beware: $\tilde{\mathbf{B}}_{\text{rev } \alpha} \tilde{\mathbf{B}}_\alpha$ must be replaced by $\tilde{\mathbf{B}}_{\text{rev } \gamma} \tilde{\mathbf{B}}_\gamma$, not by $\sum_{\alpha \models n} \gamma_\alpha \tilde{\mathbf{B}}_{\text{rev } \alpha} \tilde{\mathbf{B}}_\alpha$).

The reader can easily make the necessary changes to almost all relevant results in Sections 4, 5 and 7, including the lemmas.¹¹ Some of the modified lemmas can be derived from the original unmodified ones, whereas others can be proved analogously. For instance:

- Corollary 4.13 must be replaced by the statement that $\tilde{w}_0 \tilde{\mathbf{B}}_\gamma \tilde{w}_0 = \tilde{\mathbf{B}}_{\text{rev } \gamma}$ and $(\tilde{w}_0 \tilde{\mathbf{B}}_\gamma)^2 = \tilde{\mathbf{B}}_{\text{rev } \gamma} \tilde{\mathbf{B}}_\gamma$. The first of these equalities follows by applying (9) to each composition α of n , multiplying it by γ_α and summing the resulting equalities. The second equality follows from the first in the same way as (10) was derived from (9).
- Proposition 4.27 must be replaced by the statement that each $F \in \mathcal{F}$ satisfies $n_\gamma(F) = n_{\text{rev } \gamma}(F)$. This follows from applying Proposition 4.27 to each $\alpha \models n$, multiplying the result by γ_α and summing over all α 's.

¹¹Do not bother changing Proposition 5.3 and Theorem 5.7, as these are not needed anyway. No changes are needed in Section 6.

- Lemma 5.8 must be replaced by the statement that every $F \in \mathcal{F}$ and every $i \in [0, m]$ satisfying $n_\gamma(F) = k_i$ satisfy $F\tilde{\mathbf{B}}_{\text{rev } \gamma} \tilde{\mathbf{B}}_\gamma \equiv k_i^2 F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}$, where we are now writing the set $n_\gamma(\mathcal{F})$ (not $n_\alpha(\mathcal{F})$) as $\{k_0 < k_1 < k_2 < \cdots < k_m\}$. The proof of this is analogous to the above proof of Lemma 5.8, of course using the generalized versions of Proposition 4.27 and Lemma 5.5.

More substantial changes are needed to the proof of Proposition 4.26 and to the proof of Lemma 5.5; thus we shall dwell on them now. Proposition 4.26 must be replaced by the following:

Proposition 10.3. Let $F, G \in \mathcal{F}$ be such that $\gamma_{\text{type } G} > 0$ and $F \not\rightarrow G$. Then, we have $n_\gamma(FG) > n_\gamma(F)$.

Proof. Proposition 4.25 shows that $n_\alpha(FG) \geq n_\alpha(F)$ for each composition α . Multiplying this inequality by the nonnegative scalar γ_α and summing over all α , we obtain

$$\sum_{\alpha \models n} \gamma_\alpha n_\alpha(FG) \geq \sum_{\alpha \models n} \gamma_\alpha n_\alpha(F).$$

In other words, $n_\gamma(FG) \geq n_\gamma(F)$. It remains to prove that this inequality is strict (that is, $>$ rather than $=$). For this purpose, we need to ensure that at least one of the inequalities $\gamma_\alpha n_\alpha(FG) \geq \gamma_\alpha n_\alpha(F)$ that were summed is strict. In other words, we need to find a composition $\alpha \models n$ satisfying $\gamma_\alpha > 0$ and $n_\alpha(FG) > n_\alpha(F)$. But type G is such a composition α , since $\gamma_{\text{type } G} > 0$ (by assumption) and $n_{\text{type } G}(FG) > n_{\text{type } G}(F)$ (by Proposition 4.26). \square

We now come to the generalized Lemma 5.5. The changes to the lemma itself are pretty obvious, but the proof requires some adapting:

Lemma 10.4. Let $F \in \mathcal{F}$. Let $i \in [0, m]$ be such that $n_\gamma(F) = k_i$. Then we have

$$F\tilde{\mathbf{B}}_\gamma \equiv k_i F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}.$$

(Note that $\{k_0 < k_1 < k_2 < \cdots < k_m\}$ now stands for $n_\gamma(\mathcal{F})$, not for $n_\alpha(\mathcal{F})$.)

Proof. The definition of $\tilde{\mathbf{B}}_\gamma$ yields

$$\tilde{\mathbf{B}}_\gamma = \sum_{\alpha \models n} \gamma_\alpha \tilde{\mathbf{B}}_\alpha = \sum_{\alpha \models n} \gamma_\alpha \sum_{\substack{G \in \mathcal{F}; \\ \text{type } G = \alpha}} G = \sum_{G \in \mathcal{F}} \gamma_{\text{type } G} G.$$

Multiplying this by F from the left, we find

$$\begin{aligned} F\tilde{\mathbf{B}}_\gamma &= \sum_{G \in \mathcal{F}} \gamma_{\text{type } G} FG = \sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} \gamma_{\text{type } G} \underbrace{FG}_{=F} + \sum_{\substack{G \in \mathcal{F}; \\ F \not\rightarrow G}} \gamma_{\text{type } G} FG \\ &= \sum_{\substack{G \in \mathcal{F}; \\ F \rightarrow G}} \gamma_{\text{type } G} F + \sum_{\substack{G \in \mathcal{F}; \\ F \not\rightarrow G}} \gamma_{\text{type } G} FG. \end{aligned} \tag{53}$$

But

$$\begin{aligned}
\sum_{\substack{G \in \mathcal{F}; \\ F \twoheadrightarrow G}} \gamma_{\text{type } G} &= \sum_{\alpha \models n} \underbrace{\sum_{\substack{G \in \mathcal{F}; \\ F \twoheadrightarrow G; \\ \text{type } G = \alpha}} \gamma_\alpha}_{= |N_\alpha(F)| \gamma_{\alpha = n_\alpha(F)} \gamma_\alpha} = \sum_{\alpha \models n} n_\alpha(F) \gamma_\alpha = \sum_{\alpha \models n} \gamma_\alpha n_\alpha(F) = n_\gamma(F) \\
&= k_i.
\end{aligned} \tag{54}$$

On the other hand, if $G \in \mathcal{F}$ satisfies $\gamma_{\text{type } G} > 0$ and $F \not\twoheadrightarrow G$, then Proposition 10.3 yields $n_\gamma(FG) > n_\gamma(F) = k_i$ and thus $n_\gamma(FG) \geq k_{i+1}$ (by the standard argument), so that $FG \in \mathcal{F}_{k_{i+1}} \subseteq \mathbf{k}\mathcal{F}_{k_{i+1}}$ and therefore

$$\gamma_{\text{type } G} FG \equiv 0 \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}.$$
 \tag{55}

The same conclusion can be reached if $\gamma_{\text{type } G} = 0$, albeit for the trivial reason that the left hand side of this congruence is 0 then. Hence, (55) holds for each $G \in \mathcal{F}$ satisfying $F \not\twoheadrightarrow G$. Thus, (53) becomes

$$\begin{aligned}
\widetilde{\mathbf{F}}\mathbf{B}_\gamma &= \underbrace{\sum_{\substack{G \in \mathcal{F}; \\ F \twoheadrightarrow G}} \gamma_{\text{type } G} F}_{= k_i \text{ (by (54))}} + \sum_{\substack{G \in \mathcal{F}; \\ F \not\twoheadrightarrow G}} \underbrace{\gamma_{\text{type } G} FG}_{\equiv 0 \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}} \text{ (by (55))}} \equiv k_i F \pmod{\mathbf{k}\mathcal{F}_{k_{i+1}}}.
\end{aligned}$$

□

By making similar changes to the results in Section 8, we obtain the following generalizations of Theorem 8.1 and Theorem 8.2:

Theorem 10.5. Assume that \mathbf{k} is a field of characteristic 0. Then, the minimal polynomial of the element $w_0 \mathbf{B}_\gamma$ of $\mathbf{k}[S_n]$ is

$$\mu(w_0 \mathbf{B}_\gamma) = \prod_{k \in \tilde{n}_\gamma(\mathcal{F})} (x - k).$$

Theorem 10.6. Assume that \mathbf{k} is a field of characteristic 0. Then, the \mathbf{k} -linear operator

$$\begin{aligned}
\mathbf{k}\mathcal{F} &\rightarrow \mathbf{k}\mathcal{F}, \\
\mathbf{F} &\mapsto \mathbf{F} \widetilde{w}_0 \widetilde{\mathbf{B}}_\gamma
\end{aligned}$$

is diagonalizable, and its eigenvalues are the γ -weighted signed knapsack numbers $\tilde{n}_\gamma(F)$ of the faces $F \in \mathcal{F}$. (The algebraic multiplicity of each eigenvalue λ is the number of faces F whose γ -weighted signed knapsack number is λ .)

Actually, the claim about eigenvalues and their algebraic multiplicities in Theorem 10.6 holds even if \mathbf{k} is just a field (not necessarily ordered, not necessarily of characteristic 0) and the γ_α are arbitrary scalars (not necessarily ≥ 0). However, the operator is not always diagonalizable in this generality. Similarly, if we drop all assumptions on the field \mathbf{k} and the scalars γ_α in Theorem 10.5, then the minimal polynomial $\mu(w_0 \mathbf{B}_\gamma)$ is still a product of factors of the form $x - k$ with $k \in \tilde{n}_\gamma(\mathcal{F})$, but some of these factors can appear multiple times.

A Omitted proofs

A.1 Proof of Proposition 4.19

Proof of Proposition 4.19. Let $A = \{G \in \mathcal{F} : F \twoheadrightarrow G\}$, and $B = \{H : H \models [m]\}$. Define the maps $f : A \rightarrow B$ and $g : B \rightarrow A$ by

$$f(G_1, G_2, \dots, G_k) := (H_1, H_2, \dots, H_k) \text{ where } H_i = \{j \in [m] : F_j \subseteq G_i\}$$

and

$$g(H_1, H_2, \dots, H_k) := (G_1, G_2, \dots, G_k) \text{ where } G_i = \bigcup_{j \in H_i} F_j.$$

We first show these maps are well-defined:

1. To see that f is well-defined, we let $G = (G_1, G_2, \dots, G_k) \in A$. Define the set $H_i = \{j \in [m] : F_j \subseteq G_i\}$ for each $i \in [k]$. We must show that $(H_1, H_2, \dots, H_k) \in B$, that is, $(H_1, H_2, \dots, H_k) \models [m]$.

From $G = (G_1, G_2, \dots, G_k) \in A$, we see that $G = (G_1, G_2, \dots, G_k) \models [n]$ and $F \twoheadrightarrow G$. Thus, each block F_j of F is a subset of some G_i (since $F \twoheadrightarrow G$) and therefore satisfies $j \in H_i$ for this i , so that $j \in \bigcup_{i \in [k]} H_i$. Hence, $\bigcup_{i \in [k]} H_i = [m]$.

To see that the sets H_i are disjoint, note that if $j \in H_i \cap H_{i'}$ for two distinct indices i and i' , then $F_j \subseteq G_i$ and $F_j \subseteq G_{i'}$, so that $F_j \subseteq G_i \cap G_{i'} = \emptyset$ (since the blocks of G are disjoint), which contradicts the nonemptiness of F_j .

Finally, we claim that the sets H_i are nonempty. Indeed, let $i \in [k]$. Then, the block G_i is nonempty, so there exists some $x \in G_i$. Pick this x , and let F_j be the block of F that contains x . From $F \twoheadrightarrow G$, we see that F_j is a subset of **some** G_p . This G_p must then satisfy $x \in F_j \subseteq G_p$ and thus $x \in G_p \cap G_i$ (since $x \in G_i$), so that $G_p \cap G_i \neq \emptyset$, which is impossible unless $p = i$ (since different blocks of G are disjoint). Hence, $p = i$, so that $F_j \subseteq G_p = G_i$. Therefore, $j \in H_i$, and thus H_i is nonempty.

Thus we have shown that the sets H_i are disjoint and nonempty and satisfy $\bigcup_{i \in [k]} H_i = [m]$. In other words, $(H_1, H_2, \dots, H_k) \models [m]$. This shows that f is well-defined.

2. To see that g is well-defined, we let $H = (H_1, H_2, \dots, H_k) \in B$, that is, $(H_1, H_2, \dots, H_k) \models [m]$. We define the set $G_i = \bigcup_{j \in H_i} F_j$ for each $i \in [k]$. We must show that $(G_1, G_2, \dots, G_k) \in A$, that is, we must show that $(G_1, G_2, \dots, G_k) \in \mathcal{F}$ and $F \twoheadrightarrow (G_1, G_2, \dots, G_k)$.

Each of the sets G_i is nonempty, since it is a nonempty union of nonempty sets (as each H_i and each F_j are nonempty). Furthermore, their definition shows that $\bigcup_{i \in [k]} G_i = \bigcup_{i \in [k]} \bigcup_{j \in H_i} F_j = \bigcup_{j \in [m]} F_j = [n]$, where the second equality sign is a consequence of the fact that each $j \in [m]$ belongs to some H_i . Finally, the sets G_i are disjoint, since each element of $[n]$ belongs to exactly one F_j , and since the corresponding j belongs to exactly one H_i . These three facts together show that $(G_1, G_2, \dots, G_k) \models [n]$, that is, $(G_1, G_2, \dots, G_k) \in \mathcal{F}$.

It remains to show that $F \twoheadrightarrow (G_1, G_2, \dots, G_k)$. This is again clear: Each block F_j of F is a subset of a block of G (namely, of G_i , where i is such that $j \in H_i$; this i exists because H is a set composition of $[m]$).

Altogether, we have thus shown that $(G_1, G_2, \dots, G_k) \in A$. The map g is therefore well-defined.

Now we show that these maps f and g are mutually inverse:

1. To show that $g \circ f = \text{id}$, we must prove that $g(f(G)) = G$ for each set composition $G = (G_1, G_2, \dots, G_k) \in A$. So let us fix such set composition G . Let $i \in [k]$. Then, the i -th block of $f(G)$ is $f(G)_i = \{j \in [m] : F_j \subseteq G_i\}$ (by the definition of f). Hence, the i -th block of $g(f(G))$ is in turn

$$g(f(G))_i = \bigcup_{j \in f(G)_i} F_j = \bigcup_{j \in [m] \text{ satisfies } F_j \subseteq G_i} \underbrace{F_j}_{\subseteq G_i} \subseteq G_i.$$

Now, let us prove the reverse inclusion $G_i \subseteq g(f(G))_i$. Indeed, let $x \in G_i$. Since $g(f(G))$ is a set composition of $[n]$, we have $[n] = \bigcup_{s \in [k]} g(f(G))_s$. Hence, $x \in G_i \subseteq [n] = \bigcup_{s \in [k]} g(f(G))_s$. In other words, $x \in g(f(G))_s$ for some $s \in [k]$. Consider this s . Just as we showed $g(f(G))_i \subseteq G_i$, we see that $g(f(G))_s \subseteq G_s$. Hence, $x \in g(f(G))_s \subseteq G_s$. Combined with $x \in G_i$, this leads to $x \in G_i \cap G_s$, so that $G_i \cap G_s \neq \emptyset$. But this is only possible if $i = s$, since otherwise the blocks G_i and G_s would be disjoint. Hence, we have $i = s$. Thus, from $x \in g(f(G))_s$, we obtain $x \in g(f(G))_i$. Since we have proved this for each $x \in G_i$, we thus conclude that $G_i \subseteq g(f(G))_i$. Combined with $g(f(G))_i \subseteq G_i$, this shows that $g(f(G))_i = G_i$.

So we have shown that $g(f(G))_i = G_i$ for each $i \in [k]$. In other words, $g(f(G)) = G$. Hence, $g \circ f = \text{id}$ is proved.

2. Next, we show that $f \circ g = \text{id}$. Indeed, let $H = (H_1, H_2, \dots, H_k) \models [m]$. Then, for each $i \in [k]$, we have (using the definitions of f and g as before)

$$\begin{aligned} f(g(H))_i &= \{j \in [m] : F_j \subseteq g(H)_i\} = \{p \in [m] : F_p \subseteq g(H)_i\} \\ &= \left\{ p \in [m] : F_p \subseteq \bigcup_{j \in H_i} F_j \right\} = H_i \end{aligned}$$

(since the blocks F_j of F are disjoint and nonempty, so that the only blocks F_p that are subsets of the union $\bigcup_{j \in H_i} F_j$ are the very addends of this union). That is, $f(g(H)) = H$. This shows that $f \circ g = \text{id}$.

Thus, f and g are mutually inverse, and hence are bijections. These bijections f and g are obviously length-preserving. In particular, f is a length-preserving bijection. This proves Proposition 4.19, since our f is precisely the f defined in the proposition. \square

A.2 Proof of Proposition 4.20

Proof of Proposition 4.20. Write the faces F and G in the forms $F = (F_1, F_2, \dots, F_k)$ and $G = (G_1, G_2, \dots, G_m)$. Thus, of course, $\ell(F) = k$ and $\ell(G) = m$.

(b) Each block of FG is of the form $F_i \cap G_j$ for some $i \in [k]$ and $j \in [m]$ (by the definition of FG). Hence, it is a subset of a block of F (namely, of F_i) and a subset of a block of G (namely, of G_j). Thus, $FG \twoheadrightarrow F$ and $FG \twoheadrightarrow G$, as desired.

(c) “If”: Assume that F is contained in G . Then, each block F_i of F is a subset of some block $G_{j(i)}$ of G , and therefore disjoint from all the other blocks of G (since the blocks of G are disjoint); therefore, the intersection $F_i \cap G_{j(i)}$ is nonempty (and equals F_i), whereas all other intersections $F_i \cap G_r$ with $r \neq j(i)$ are empty. But the definition of FG yields

$$FG = (F_1 \cap G_1, \dots, F_1 \cap G_m, \dots, F_k \cap G_m)^{\text{red}} = (F_1 \cap G_{j(1)}, F_2 \cap G_{j(2)}, \dots, F_k \cap G_{j(k)}),$$

since the reduction operation removes all the empty intersections $F_i \cap G_r$ and leaves only the nonempty intersections $F_i \cap G_{j(i)}$ around. But since the latter nonempty intersections $F_i \cap G_{j(i)}$ are just the blocks F_i (because $F_i \subseteq G_{j(i)}$), we can rewrite this as

$$FG = (F_1, F_2, \dots, F_k) = F.$$

This proves the “if” direction.

“Only if”: Assume that $FG = F$. But part **(b)** shows that FG is contained in G . Hence, F is contained in G (since $FG = F$). This proves the “only if” direction.

(d) The blocks of FG are the nonempty intersections of the form $F_i \cap G_j$ (by the definition of FG). Each block F_i of F gives rise to at least one such nonempty intersection $F_i \cap G_j$ (since $\bigcup_j (F_i \cap G_j) = F_i \cap \underbrace{\bigcup_j G_j}_{=[n]} = F_i \cap [n] = F_i$ is nonempty). Consequently, there are at

least k nonempty intersections of the form $F_i \cap G_j$ (since there are k blocks F_i of F). In other words, FG has at least k blocks. In other words, $\ell(FG) \geq k = \ell(F)$.

It remains to show that this inequality becomes an equality if and only if F is contained in G .

“If”: Assume that F is contained in G . Then, part **(c)** shows that $FG = F$. Hence, $\ell(FG) = \ell(F)$. Thus, equality holds.

“Only if”: Now assume that F is not contained in G . Then, there is a block of F – say, F_{i_0} – that is not a subset of any block of G . Hence, F_{i_0} has nonempty intersection with more than one block of G . But the blocks of FG are the nonempty intersections of the form $F_i \cap G_j$. Each block F_i of F gives rise to at least one such nonempty intersection $F_i \cap G_j$ (as we already saw above), but the block F_{i_0} gives rise to more than one such nonempty intersection (since F_{i_0} has nonempty intersection with more than one block of G). Consequently, the total number of nonempty intersections of the form $F_i \cap G_j$ is larger than the number of blocks F_i of F . In other words, $\ell(FG) > \ell(F)$. Hence, equality does not hold in $\ell(FG) \geq \ell(F)$. The proof of part **(d)** is thus complete.

(e) This is similar to the proof of $\ell(FG) \geq \ell(F)$ in part (d). (This time, we have to argue that each block G_j of G gives rise to at least one nonempty intersection of the form $F_i \cap G_j$.) Alternatively, we can apply part (d) with the roles of F and G interchanged, and then observe that $\ell(FG) = \ell(GF)$ because the set compositions FG and GF differ only in the order of their blocks.

(a) Assume that F is contained in G . Then, $FG = F$ by part (c). But part (e) yields $\ell(FG) \geq \ell(G)$. Since $FG = F$, we can rewrite this as $\ell(F) \geq \ell(G)$. \square

A.3 Proof of Theorem 4.12

We shall now give a self-contained proof of Theorem 4.12. This is essentially just Bidigare's proof ([1, Theorem 3.8.1], [22, proof of Theorem 2.1], [14, Theorem 1], etc.), restated in our language for the sake of consistency.

We begin with a lemma that is so simple that its usefulness is hard to believe. It is implicit in most expositions of Theorem 4.12, but in our view it is worth isolating, as it makes the rest of the proof more transparent.

Lemma A.1. Let B and C be two monoids (written multiplicatively). Let $f : B \rightarrow C$ be any map.

Let S be a set on which both monoids B and C act from the left. Let $s \in S$ be an element that generates a free C -orbit – i.e., that has the property that

$$\text{if } c_1, c_2 \in C \text{ satisfy } c_1 s = c_2 s, \text{ then } c_1 = c_2. \quad (56)$$

Assume furthermore that

$$b(cs) = c(bs) \quad \text{for all } b \in B \text{ and } c \in C. \quad (57)$$

Assume moreover that

$$bs = f(b)s \quad \text{for each } b \in B. \quad (58)$$

Then, f is a monoid anti-morphism, i.e., it satisfies

$$f(ab) = f(b)f(a) \quad \text{for all } a, b \in B$$

and $f(1_B) = 1_C$.

Proof. From (58), we have $1_B s = f(1_B)s$, so that $f(1_B)s = 1_B s = s = 1_C s$. Thus, (56) (applied to $c_1 = f(1_B)$ and $c_2 = 1_C$) yields $f(1_B) = 1_C$.

It thus remains to show that $f(ab) = f(b)f(a)$ for all $a, b \in B$.

To prove this, we fix any $a, b \in B$. Then, (58) (applied to ab instead of b) shows that $abs = f(ab)s$. However, (58) also yields $bs = f(b)s$ and $as = f(a)s$.

On the other hand, (57) (applied to a and $f(b)$ instead of b and c) shows that $a(f(b)s) = f(b)(as)$. In view of $bs = f(b)s$, we can rewrite this as $a(bs) = f(b)(\underbrace{as}_{=f(a)s}) =$

$f(b)f(a)s$. Comparing this with $a(bs) = abs = f(ab)s$, we find $f(ab)s = f(b)f(a)s$. Therefore, (56) (applied to $c_1 = f(ab)$ and $c_2 = f(b)f(a)$) yields $f(ab) = f(b)f(a)$. This completes our proof of Lemma A.1. \square

Proof of Theorem 4.12. Recall the left action of S_n on \mathcal{F} introduced in Definition 4.7. We shall need one more piece of notation:

For any permutation $w \in S_n$, we let P_w be the face

$$P_w := (\{w(1)\}, \{w(2)\}, \dots, \{w(n)\}) \in \mathcal{F}.$$

In particular, $P_{\text{id}} = (\{1\}, \{2\}, \dots, \{n\})$. It is easy to see that each permutation $w \in S_n$ satisfies

$$P_w = wP_{\text{id}}, \tag{59}$$

where the action of S_n on \mathcal{F} is the one from Definition 4.7. Note that the \mathbf{k} -module $\mathbf{k}\mathcal{F}$ has a linear left S_n -action (as we know from Definition 4.7), and thus is a left $\mathbf{k}[S_n]$ -module. Furthermore, the \mathbf{k} -module $\mathbf{k}\mathcal{F}$ is a left $(\mathbf{k}\mathcal{F})^{S_n}$ -module (by left multiplication, since $(\mathbf{k}\mathcal{F})^{S_n}$ is a subalgebra of $\mathbf{k}\mathcal{F}$). We shall use both of these module structures on $\mathbf{k}\mathcal{F}$ in what follows.

Now, we recall that the family $(\tilde{\mathbf{B}}_\alpha)_{\alpha \models n}$ is a basis of the \mathbf{k} -module $(\mathbf{k}\mathcal{F})^{S_n}$ (by Proposition 4.10). The \mathbf{k} -linear map $\rho : D(S_n) \rightarrow (\mathbf{k}\mathcal{F})^{S_n}$ (defined in Definition 4.11) sends the basis $(\mathbf{B}_\alpha)_{\alpha \models n}$ of $D(S_n)$ to the basis $(\tilde{\mathbf{B}}_\alpha)_{\alpha \models n}$ of $(\mathbf{k}\mathcal{F})^{S_n}$ (by its definition), and thus is a \mathbf{k} -module isomorphism (like any \mathbf{k} -linear map that sends a basis to a basis). Hence, it has a \mathbf{k} -linear inverse $\rho^{-1} : (\mathbf{k}\mathcal{F})^{S_n} \rightarrow D(S_n)$. We shall view ρ^{-1} as a \mathbf{k} -linear map $(\mathbf{k}\mathcal{F})^{S_n} \rightarrow \mathbf{k}[S_n]$ (since $D(S_n)$ is a \mathbf{k} -submodule of $\mathbf{k}[S_n]$).

We shall now attempt to apply Lemma A.1 to $B = (\mathbf{k}\mathcal{F})^{S_n}$ and $C = \mathbf{k}[S_n]$ (both viewed as monoids with respect to multiplication) and $f = \rho^{-1}$ and $S = \mathbf{k}\mathcal{F}$ (where the monoids B and C act on S since $S = \mathbf{k}\mathcal{F}$ is both a left $(\mathbf{k}\mathcal{F})^{S_n}$ -module and a left $\mathbf{k}[S_n]$ -module) and $s = P_{\text{id}} \in \mathbf{k}\mathcal{F}$. If we can show that all the conditions of Lemma A.1 are satisfied for these inputs, then Lemma A.1 will yield that ρ^{-1} is a monoid anti-morphism (with respect to multiplication), and this will quickly finish our proof of Theorem 4.12 (see below for the details).

We shall now show that the conditions of Lemma A.1 are satisfied:

1. We claim that (56) is satisfied. In other words, we claim that

$$\text{if } c_1, c_2 \in \mathbf{k}[S_n] \text{ satisfy } c_1 P_{\text{id}} = c_2 P_{\text{id}}, \text{ then } c_1 = c_2.$$

Proof: In other words, we must show that the map $\mathbf{k}[S_n] \rightarrow \mathbf{k}\mathcal{F}$, $c \mapsto cP_{\text{id}}$ is injective. But this map is \mathbf{k} -linear, and it sends the basis vectors $w \in S_n$ of the \mathbf{k} -module $\mathbf{k}[S_n]$ to the elements $wP_{\text{id}} = P_w$ (by (59)), which are distinct basis vectors of $\mathbf{k}\mathcal{F}$ (since all the faces P_w for $w \in S_n$ are distinct) and therefore are \mathbf{k} -linearly independent. Thus, this map must be injective (since a \mathbf{k} -linear map that sends a basis of its domain to a \mathbf{k} -linearly independent family in its target must always be injective). This proves that (56) is satisfied.

2. We claim that (57) is satisfied. In other words, we claim that

$$b(cP_{\text{id}}) = c(bP_{\text{id}}) \quad \text{for all } b \in (\mathbf{k}\mathcal{F})^{S_n} \text{ and } c \in \mathbf{k}[S_n].$$

Proof: Let $b \in (\mathbf{k}\mathcal{F})^{S_n}$ and $c \in \mathbf{k}[S_n]$. We must prove the equality $b(cP_{\text{id}}) = c(bP_{\text{id}})$. Note that this equality depends \mathbf{k} -linearly on c . Hence, by linearity, we can WLOG assume that c is a permutation $w \in S_n$. Assume this, and consider this w . Recall that S_n acts on the monoid algebra $\mathbf{k}\mathcal{F}$ by \mathbf{k} -algebra automorphisms (see the proof of Proposition 4.8); thus,

$$w(pq) = (wp)(wq) \quad \text{for all } p, q \in \mathbf{k}\mathcal{F}.$$

Applying this to $p = b$ and $q = P_{\text{id}}$, we obtain $w(bP_{\text{id}}) = (wb)(wP_{\text{id}})$. But $b \in (\mathbf{k}\mathcal{F})^{S_n}$ and thus $wb = b$ (by the definition of $(\mathbf{k}\mathcal{F})^{S_n}$). Hence, $w(bP_{\text{id}}) = \underbrace{(wb)}_{=b}(wP_{\text{id}}) = b(wP_{\text{id}})$. Since $c = w$, we can rewrite this as $c(bP_{\text{id}}) = b(cP_{\text{id}})$. In other words, $b(cP_{\text{id}}) = c(bP_{\text{id}})$. This proves that (57) is satisfied.

3. We claim that (58) is satisfied. In other words, we claim that

$$bP_{\text{id}} = \rho^{-1}(b)P_{\text{id}} \quad \text{for each } b \in (\mathbf{k}\mathcal{F})^{S_n}.$$

Proof: Let $b \in (\mathbf{k}\mathcal{F})^{S_n}$. We must show that $bP_{\text{id}} = \rho^{-1}(b)P_{\text{id}}$.

Since this equality depends \mathbf{k} -linearly on b , we can WLOG assume that $b = \tilde{\mathbf{B}}_\alpha$ for some composition α of n (since we know from Proposition 4.10 that the family $(\tilde{\mathbf{B}}_\alpha)_{\alpha \models n}$ is a basis of $(\mathbf{k}\mathcal{F})^{S_n}$). Assume this, and consider this α . Thus, $b = \tilde{\mathbf{B}}_\alpha$. But the definition of ρ yields $\rho(\mathbf{B}_\alpha) = \tilde{\mathbf{B}}_\alpha$. Hence, $b = \tilde{\mathbf{B}}_\alpha = \rho(\mathbf{B}_\alpha)$, so that

$$\rho^{-1}(b) = \mathbf{B}_\alpha = \sum_{\substack{w \in S_n; \\ \text{Des } w \subseteq \text{gaps}^{-1}(\alpha)}} w \quad (\text{by the definition of } \mathbf{B}_\alpha).$$

Hence,

$$\begin{aligned} \rho^{-1}(b)P_{\text{id}} &= \left(\sum_{\substack{w \in S_n; \\ \text{Des } w \subseteq \text{gaps}^{-1}(\alpha)}} w \right) P_{\text{id}} = \sum_{\substack{w \in S_n; \\ \text{Des } w \subseteq \text{gaps}^{-1}(\alpha)}} \underbrace{wP_{\text{id}}}_{=P_w} \quad (\text{by (59)}) \\ &= \sum_{\substack{w \in S_n; \\ \text{Des } w \subseteq \text{gaps}^{-1}(\alpha)}} P_w. \end{aligned} \tag{60}$$

On the other hand, from $b = \tilde{\mathbf{B}}_\alpha = \sum_{\substack{F \in \mathcal{F}; \\ \text{type } F = \alpha}} F$, we obtain

$$bP_{\text{id}} = \left(\sum_{\substack{F \in \mathcal{F}; \\ \text{type } F = \alpha}} F \right) P_{\text{id}} = \sum_{\substack{F \in \mathcal{F}; \\ \text{type } F = \alpha}} FP_{\text{id}}. \tag{61}$$

Let us now prove that the right hand sides of (60) and of (61) are the same.

Indeed, write the composition α as $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k)$. Let $(I_1, I_2, \dots, I_k) \in \mathcal{F}$ be the unique set composition of $[n]$ that has type α and whose blocks I_1, I_2, \dots, I_k are intervals of $[n]$ arranged from left to right. That is, the block I_1 consists of the α_1 smallest elements of $[n]$ (that is, $I_1 = [1, \alpha_1]$); the next block I_2 consists of the α_2 next-smallest elements of $[n]$ (that is, $I_2 = [\alpha_1 + 1, \alpha_1 + \alpha_2]$); the next block I_3 consists of the α_3 next-smallest elements of $[n]$; and so on. Explicitly, these blocks I_j are given by

$$I_j = [\alpha_1 + \alpha_2 + \dots + \alpha_{j-1} + 1, \alpha_1 + \alpha_2 + \dots + \alpha_j] \quad \text{for all } j \in [k].$$

For example, if $n = 8$ and $\alpha = (2, 3, 1, 2)$, then

$$(I_1, I_2, \dots, I_k) = (\{1, 2\}, \{3, 4, 5\}, \{6\}, \{7, 8\}).$$

Note that the set $\text{gaps}^{-1}(\alpha)$ consists precisely of the numbers $\alpha_1 + \alpha_2 + \dots + \alpha_j$ for all $j \in [k-1]$; these numbers are the maxima of the intervals I_1, I_2, \dots, I_{k-1} (whereas the maximum of I_k is n). Thus, the permutations $w \in S_n$ that satisfy $\text{Des } w \subseteq \text{gaps}^{-1}(\alpha)$ are exactly those permutations $w \in S_n$ that have no descents except at the maxima of the intervals I_1, I_2, \dots, I_{k-1} (and possibly not even at those maxima); in other words, they are exactly those permutations $w \in S_n$ that are increasing on each of the intervals I_1, I_2, \dots, I_k . Obviously, such a permutation w is uniquely determined by the sets $w(I_1), w(I_2), \dots, w(I_k)$ (since w must send the elements of each I_j to the elements of $w(I_j)$ in increasing order), and these sets have respective sizes $\alpha_1, \alpha_2, \dots, \alpha_k$ (since $|w(I_j)| = |I_j| = \alpha_j$ for each $j \in [k]$) and thus form a set composition $(w(I_1), w(I_2), \dots, w(I_k)) \in \mathcal{F}$ of type α . Thus, we can define an injective map

$$\begin{aligned} \Omega_\alpha : \{w \in S_n \mid \text{Des } w \subseteq \text{gaps}^{-1}(\alpha)\} &\rightarrow \{F \in \mathcal{F} \mid \text{type } F = \alpha\}, \\ w &\mapsto (w(I_1), w(I_2), \dots, w(I_k)), \end{aligned}$$

which sends each w to the k -tuple formed of these sets $w(I_1), w(I_2), \dots, w(I_k)$. This map Ω_α is a bijection, since any set composition $F = (F_1, F_2, \dots, F_k) \in \mathcal{F}$ of type α can be written as $(w(I_1), w(I_2), \dots, w(I_k))$ for a unique permutation $w \in S_n$ that satisfies $\text{Des } w \subseteq \text{gaps}^{-1}(\alpha)$ (namely, the permutation w whose values on each interval I_j are the elements of F_j in increasing order). For example, if $n = 8$ and $\alpha = (2, 3, 1, 2)$ and if $w = [3, 5, 1, 4, 8, 2, 6, 7]$, then $\Omega_\alpha(w) = (35, 148, 2, 67)$.

Next, we claim that the bijection Ω_α has the following property: For any permutation $w \in S_n$ satisfying $\text{Des } w \subseteq \text{gaps}^{-1}(\alpha)$, we have

$$\Omega_\alpha(w) P_{\text{id}} = P_w. \tag{62}$$

[Proof of (62): Let $w \in S_n$ be a permutation satisfying $\text{Des } w \subseteq \text{gaps}^{-1}(\alpha)$. Then, from $\Omega_\alpha(w) = (w(I_1), w(I_2), \dots, w(I_k))$ (which follows from the definition of

Ω_α) and $P_{\text{id}} = (\{1\}, \{2\}, \dots, \{n\})$, we obtain

$$\begin{aligned}\Omega_\alpha(w) P_{\text{id}} &= (w(I_1), w(I_2), \dots, w(I_k)) (\{1\}, \{2\}, \dots, \{n\}) \\ &= (w(I_1) \cap \{1\}, \dots, w(I_1) \cap \{n\}, \dots, w(I_k) \cap \{n\})^{\text{red}}\end{aligned}$$

(by the definition of the product on \mathcal{F}). In other words, $\Omega_\alpha(w) P_{\text{id}}$ is the set composition whose blocks are the nonempty intersections of the form $w(I_j) \cap \{p\}$ for all $j \in [k]$ and $p \in [n]$, in the order of lexicographically increasing (j, p) . Thus, each block of the set composition $\Omega_\alpha(w) P_{\text{id}}$ has size 1 (since it has the form $w(I_j) \cap \{p\}$ for some $j \in [k]$ and $p \in [n]$, and thus is a subset of the 1-element set $\{p\}$; but this shows that it has size 0 or 1, and of course it cannot have size 0 when it is nonempty, so that it must then have size 1).

So we have shown that $\Omega_\alpha(w) P_{\text{id}}$ is a set composition of $[n]$ whose each block has size 1. Therefore, the blocks of this set composition $\Omega_\alpha(w) P_{\text{id}}$ are $\{1\}, \{2\}, \dots, \{n\}$ in some order. We are now going to identify this order. Namely, we shall show that the order in which these blocks appear in $\Omega_\alpha(w) P_{\text{id}}$ is $\{w(1)\}, \{w(2)\}, \dots, \{w(n)\}$. Once this is proved, it will follow that

$$\Omega_\alpha(w) P_{\text{id}} = (\{w(1)\}, \{w(2)\}, \dots, \{w(n)\}) = P_w,$$

and thus (62) will be proved.

So it remains to show that the order in which the blocks $\{1\}, \{2\}, \dots, \{n\}$ appear in $\Omega_\alpha(w) P_{\text{id}}$ is $\{w(1)\}, \{w(2)\}, \dots, \{w(n)\}$. Clearly, it suffices to show that if $a, b \in [n]$ are such that $a < b$, then the block $\{w(a)\}$ appears before¹² $\{w(b)\}$ in $\Omega_\alpha(w) P_{\text{id}}$. So we shall show this.

Fix two elements $a, b \in [n]$ such that $a < b$. We must show that

$$\{w(a)\} \text{ appears before } \{w(b)\} \text{ in } \Omega_\alpha(w) P_{\text{id}}. \quad (63)$$

Recall that $\text{Des } w \subseteq \text{gaps}^{-1}(\alpha)$; thus, the permutation w is increasing on each of the intervals I_1, I_2, \dots, I_k (as we have seen above). We distinguish between two cases:

Case 1: The elements a and b belong to the same interval I_i for some $i \in [k]$.

Case 2: The elements a and b belong to two different intervals I_i . In other words, $a \in I_{i_1}$ and $b \in I_{i_2}$ for some $i_1 \neq i_2$ in $[k]$.

Consider Case 1 first. In this case, $a, b \in I_i$ for some $i \in [k]$. Consider this i . Then, the permutation w is increasing on I_i (since w is increasing on each of the intervals I_1, I_2, \dots, I_k). Thus, from $a, b \in I_i$ and $a < b$, we obtain $w(a) < w(b)$. Furthermore, from $a \in I_i$, we obtain $w(a) \in w(I_i)$, so that $w(I_i) \cap \{w(a)\} = \{w(a)\}$. Likewise, $w(I_i) \cap \{w(b)\} = \{w(b)\}$.

Now, recall that $\Omega_\alpha(w) P_{\text{id}}$ is the set composition whose blocks are the nonempty intersections of the form $w(I_j) \cap \{p\}$ for all $j \in [k]$ and $p \in [n]$, in the order

¹²The word ‘‘before’’ means ‘‘someplace before’’, not ‘‘immediately before’’.

of lexicographically increasing (j, p) . Hence, the intersection $w(I_i) \cap \{w(a)\}$ appears before $w(I_i) \cap \{w(b)\}$ in this set composition (since $w(a) < w(b)$ and thus $(i, w(a)) < (i, w(b))$ in the lexicographic order). In other words, the block $\{w(a)\}$ appears before $\{w(b)\}$ in this set composition (since $w(I_i) \cap \{w(a)\} = \{w(a)\}$ and $w(I_i) \cap \{w(b)\} = \{w(b)\}$). This proves (63) in Case 1.

Let us now consider Case 2. In this case, $a \in I_{i_1}$ and $b \in I_{i_2}$ for some $i_1 \neq i_2$ in $[k]$. Consider these $i_1 \neq i_2$. If we had $i_1 > i_2$, then we would have $a > b$ (since the intervals I_1, I_2, \dots, I_k are arranged from left to right, so that any element of I_{i_1} would be larger than any element of I_{i_2}), which would contradict $a < b$. Hence, $i_1 \leq i_2$, so that $i_1 < i_2$ (since $i_1 \neq i_2$). Furthermore, from $a \in I_{i_1}$, we obtain $w(a) \in w(I_{i_1})$, so that $w(I_{i_1}) \cap \{w(a)\} = \{w(a)\}$. Likewise, $w(I_{i_2}) \cap \{w(b)\} = \{w(b)\}$.

Now, recall that $\Omega_\alpha(w) P_{\text{id}}$ is the set composition whose blocks are the nonempty intersections of the form $w(I_j) \cap \{p\}$ for all $j \in [k]$ and $p \in [n]$, in the order of lexicographically increasing (j, p) . Hence, the intersection $w(I_{i_1}) \cap \{w(a)\}$ appears before $w(I_{i_2}) \cap \{w(b)\}$ in this set composition (since $i_1 < i_2$ and thus $(i_1, w(a)) < (i_2, w(b))$ in the lexicographic order). In other words, the block $\{w(a)\}$ appears before $\{w(b)\}$ in this set composition. This proves (63) in Case 2.

We have now proved (63) in both cases; thus, (63) always holds. As we explained above, this concludes the proof of (62).]

Now, (61) becomes

$$bP_{\text{id}} = \sum_{\substack{F \in \mathcal{F}; \\ \text{type } F = \alpha}} FP_{\text{id}} = \sum_{\substack{w \in S_n; \\ \text{Des } w \subseteq \text{gaps}^{-1}(\alpha)}} \Omega_\alpha(w) P_{\text{id}}$$

(here, we have substituted $\Omega_\alpha(w)$ for F in the sum, since the map Ω_α is a bijection). Hence,

$$bP_{\text{id}} = \sum_{\substack{w \in S_n; \\ \text{Des } w \subseteq \text{gaps}^{-1}(\alpha)}} \underbrace{\Omega_\alpha(w) P_{\text{id}}}_{= P_w \text{ (by (62))}} = \sum_{\substack{w \in S_n; \\ \text{Des } w \subseteq \text{gaps}^{-1}(\alpha)}} P_w.$$

Comparing this with (60), we obtain $bP_{\text{id}} = \rho^{-1}(b) P_{\text{id}}$. This proves that (58) is satisfied.

Thus, all conditions of Lemma A.1 are satisfied. Hence, Lemma A.1 shows that ρ^{-1} (viewed as a map $(\mathbf{k}\mathcal{F})^{S_n} \rightarrow \mathbf{k}[S_n]$, where both $(\mathbf{k}\mathcal{F})^{S_n}$ and $\mathbf{k}[S_n]$ are regarded as monoids with respect to multiplication) is a monoid anti-morphism. Hence, ρ^{-1} is a \mathbf{k} -algebra anti-morphism (since ρ^{-1} is \mathbf{k} -linear). Thus, its image $\text{Im } \rho^{-1}$ is a \mathbf{k} -subalgebra of $\mathbf{k}[S_n]$ (since the image of a \mathbf{k} -algebra anti-morphism is always a \mathbf{k} -subalgebra of the target). Since $\text{Im } \rho^{-1} = D(S_n)$ (because ρ^{-1} was defined as the inverse of the map $\rho : D(S_n) \rightarrow (\mathbf{k}\mathcal{F})^{S_n}$), we thus have shown that $D(S_n)$ is a \mathbf{k} -subalgebra of $\mathbf{k}[S_n]$. Furthermore, the map ρ is the inverse of the \mathbf{k} -algebra anti-morphism ρ^{-1} , and thus is a \mathbf{k} -algebra anti-isomorphism itself. This completes the proof of Theorem 4.12. \square

A.4 The fixed points of a permutation module

Let us prove the following general fact ([17, §3.3.1, “Invariants of Permutation Representations”]) about permutation modules (which we have used in the proof of Proposition 4.10):

Proposition A.2. Let G be a group, and let X be a finite left G -set. Consider the invariant subspace $(\mathbf{k}X)^G := \{\mathbf{x} \in \mathbf{k}X : w\mathbf{x} = \mathbf{x} \text{ for all } w \in G\}$ of the permutation module $\mathbf{k}X$.

For each orbit \mathcal{O} of the G -action on X , let $\sum_{x \in \mathcal{O}} x$ be the sum of all elements of this orbit in $\mathbf{k}X$. This sum is called an **orbit sum**.

Then, the invariant subspace $(\mathbf{k}X)^G$ (as a \mathbf{k} -module) has a basis consisting of the orbit sums (i.e., of the sums $\sum_{x \in \mathcal{O}} x$ for each orbit \mathcal{O} of the G -action on X).

Proof. This fact is proved by combining three simple observations:

1. Each orbit sum $\sum_{x \in \mathcal{O}} x$ belongs to $(\mathbf{k}X)^G$, because the action of a $w \in G$ on this sum merely permutes its addends: $w \sum_{x \in \mathcal{O}} x = \sum_{x \in \mathcal{O}} wx = \sum_{x \in w\mathcal{O}} x = \sum_{x \in \mathcal{O}} x$ because $w\mathcal{O} = \mathcal{O}$.
2. If an element $\mathbf{x} = \sum_{x \in X} \lambda_x x \in \mathbf{k}X$ (with coefficients $\lambda_x \in \mathbf{k}$) belongs to $(\mathbf{k}X)^G$, then every two elements $x, y \in X$ that lie in the same G -orbit have the same coefficient (i.e., satisfy $\lambda_x = \lambda_y$), because the action of an appropriately chosen $w \in G$ puts λ_x in the position of λ_y . Thus, given such an element $\mathbf{x} \in (\mathbf{k}X)^G$, we can rename its coefficients λ_x as λ_{Gx} , where Gx (as usual) denotes the G -orbit containing x . Hence, we can rewrite $\mathbf{x} = \sum_{x \in X} \lambda_x x$ as $\mathbf{x} = \sum_{x \in X} \lambda_{Gx} x = \sum_{\mathcal{O} \text{ is a } G\text{-orbit}} \lambda_{\mathcal{O}} (\sum_{x \in \mathcal{O}} x)$, which shows that \mathbf{x} is a linear combination of orbit sums. Hence, the orbit sums span $(\mathbf{k}X)^G$.
3. The orbit sums $\sum_{x \in \mathcal{O}} x$ are \mathbf{k} -linearly independent, since any \mathbf{k} -linear combination $\sum_{\mathcal{O} \text{ is a } G\text{-orbit}} \lambda_{\mathcal{O}} (\sum_{x \in \mathcal{O}} x)$ can be rewritten as $\sum_{x \in X} \lambda_{Gx} x$ and thus cannot be 0 unless all the λ_{Gx} are 0, that is, unless all the $\lambda_{\mathcal{O}}$ are 0.

Thus, the orbit sums form a basis of $(\mathbf{k}X)^G$. □

References

- [1] Patrick Bidigare. “Hyperplane arrangement face algebras and their associated Markov chains”. PhD thesis. Univ. Michigan, 1997.
- [2] Dieter Blessenohl and Manfred Schocker. *Noncommutative character theory of the symmetric group*. River Edge, NJ: World Scientific, 2005. ISBN: 1-86094-511-2.
- [3] Kenneth S. Brown. “Semigroup and ring theoretical methods in probability”. In: *Representations of finite dimensional algebras and related topics in Lie theory and geometry. Proceedings from the 10th international conference on algebras and related topics, ICRA X, Toronto, Canada, July 15–August 10, 2002*. Providence, RI: American Mathematical Society (AMS), 2004, pp. 3–26. ISBN: 0-8218-3416-9.

- [4] Kenneth S. Brown. “Semigroups, rings, and Markov chains”. In: *J. Theor. Probab.* 13.3 (2000), pp. 871–938. ISSN: 0894-9840. DOI: [10.1023/A:1007822931408](https://doi.org/10.1023/A:1007822931408).
- [5] Persi Diaconis. “Mathematical developments from the analysis of riffle shuffling”. English. In: *Groups, combinatorics and geometry. Proceedings of the L. M. S. Durham symposium, Durham, UK, July 16–26, 2001*. <https://diaconis.ckirby.su.domains/papers.html>. River Edge, NJ: World Scientific, 2003, pp. 73–97. ISBN: 981-238-312-3.
- [6] Persi Diaconis and Jason Fulman. *The mathematics of shuffling cards*. English. Providence, RI: American Mathematical Society (AMS), 2023. ISBN: 978-1-4704-6303-8; 978-1-4704-7290-0. DOI: [10.1090/mbk/146](https://doi.org/10.1090/mbk/146).
- [7] Persi Diaconis and Mehrdad Shahshahani. “Generating a random permutation with random transpositions”. In: *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete* 57.2 (1981), pp. 159–179.
- [8] Antonius B Dieker and Franco V Saliola. “Spectral analysis of random-to-random Markov chains”. In: *Advances in Mathematics* 323 (2018), pp. 427–485. DOI: [10.1016/j.aim.2017.10.034](https://doi.org/10.1016/j.aim.2017.10.034).
- [9] Darij Grinberg. *An Introduction to Algebraic Combinatorics*. 2025. arXiv: [2506.00738v1](https://arxiv.org/abs/2506.00738v1) [math.CO]. URL: <https://arxiv.org/abs/2506.00738v1>.
- [10] Darij Grinberg. *Is this sum of cycles invertible in QS_n ?* MathOverflow. version: 2025-05-05. eprint: <https://mathoverflow.net/q/308600>. URL: <https://mathoverflow.net/q/308600>.
- [11] Darij Grinberg. *The one-sided cycle shuffles, and other mysteries and wonders of the symmetric group algebra [talk slides]*. 2025. URL: <https://www.cip.ifi.lmu.de/~grinberg/algebra/dc2023.pdf>.
- [12] Darij Grinberg and Nadia Lafrenière. “The one-sided cycle shuffles in the symmetric group algebra”. In: *arXiv preprint arXiv:2212.06274* (2022). URL: <https://arxiv.org/abs/2212.06274>.
- [13] Darij Grinberg and Ekaterina A. Vassilieva. *The enriched q -monomial basis of the quasi-symmetric functions*. 2024. arXiv: [2309.01118v3](https://arxiv.org/abs/2309.01118v3) [math.CO]. URL: <https://arxiv.org/abs/2309.01118v3>.
- [14] Samuel K. Hsiao. “A semigroup approach to wreath-product extensions of Solomon’s descent algebras”. In: *Electron. J. Comb.* 16.1 (2009), research paper r21, 9. ISSN: 1077-8926. URL: <https://eudml.org/doc/117303>.
- [15] Richard Kenyon et al. “The miracle of integer eigenvalues”. English. In: *Funct. Anal. Appl.* 58.2 (2024), pp. 182–194. ISSN: 0016-2663. DOI: [10.1134/S0016266324020072](https://doi.org/10.1134/S0016266324020072).
- [16] Daniel Krob, Bernard Leclerc, and Jean-Yves Thibon. “Noncommutative symmetric functions. II: Transformations of alphabets”. In: *Int. J. Algebra Comput.* 7.2 (1997), pp. 181–264. ISSN: 0218-1967. DOI: [10.1142/S0218196797000113](https://doi.org/10.1142/S0218196797000113).
- [17] Martin Lorenz. *A tour of representation theory*. English. Vol. 193. Grad. Stud. Math. Providence, RI: American Mathematical Society (AMS), 2018. ISBN: 978-1-4704-3680-3; 978-1-4704-4905-6. DOI: [10.1090/gsm/193](https://doi.org/10.1090/gsm/193).

- [18] Ravindra M. Phatarfod. “On the matrix occurring in a linear search problem”. In: *Journal of Applied Probability* 28.2 (1991), pp. 336–346. ISSN: 0021-9002. DOI: [10.1017/s0021900200039723](https://doi.org/10.1017/s0021900200039723).
- [19] Victor Reiner, Franco Saliola, and Volkmar Welker. “Spectra of symmetrized shuffling operators”. In: *Memoirs of the American Mathematical Society* 228.1072 (2014). Preprint available at [arXiv:1102.2460v2](https://arxiv.org/abs/1102.2460v2), pp. vi+109. ISSN: 0065-9266.
- [20] Jeremy Francis Reizenstein. “Iterated-Integral Signatures in Machine Learning”. PhD thesis. University of Warwick, 2019, pp. ix+107. URL: <http://wrap.warwick.ac.uk/131162/>.
- [21] Bruce E. Sagan. *Combinatorics: The Art of Counting*. Vol. 210. Graduate studies in mathematics. American Mathematical Society, 2020.
- [22] Franco Saliola. *Hyperplane arrangements and descent algebras*. corrections at <https://www.cip.ifi.lmu.de/~grinberg/algebra/saliola-errata.pdf>. URL: <https://saliola.github.io/maths/publications/LectureNotes/DesAlgLectureNotes.pdf>.
- [23] Manfred Schocker. “The descent algebra of the symmetric group”. In: *Representations of finite dimensional algebras and related topics in Lie theory and geometry. Proceedings from the 10th international conference on algebras and related topics, ICRA X, Toronto, Canada, July 15–August 10, 2002*. Providence, RI: American Mathematical Society (AMS), 2004, pp. 145–161. ISBN: 0-8218-3416-9.
- [24] Louis Solomon. “A Mackey formula in the group ring of a Coxeter group”. In: *Journal of Algebra* 41 (1976), pp. 255–264.
- [25] Richard P. Stanley. *Enumerative combinatorics*. 2nd ed. Vol. 1. Cambridge University Press, 2011.
- [26] Nolan R. Wallach. *Lie algebra cohomology and holomorphic continuation of generalized Jacquet integrals*. Representations of Lie groups: analysis on homogeneous spaces and representations of Lie groups, Proc. Symp., Kyoto/Jap. and Hiroshima/Jap. 1986, Adv. Stud. Pure Math. 14, 123-151 (1988). 1988. DOI: [10.2969/aspm/01410123](https://doi.org/10.2969/aspm/01410123).