The one-sided cycle shuffles in the symmetric group algebra

Darij Grinberg and Nadia Lafrenière

March 10, 2024

Abstract. We study an infinite family of shuffling operators on the symmetric group S_n, which includes the well-studied top-to-random shuffle. The general shuffling scheme consists of removing one card at a time from the deck (according to some probability distribution) and re-inserting it at a position chosen uniformly at random among the positions below. Rewritten in terms of the group algebra $\mathbb{R}[S_n]$, our shuffle corresponds to right multiplication by a linear combination of the elements

$$t_\ell := \mathrm{cyc}_\ell + \mathrm{cyc}_{\ell,\ell+1} + \mathrm{cyc}_{\ell,\ell+1,\ell+2} + \cdots + \mathrm{cyc}_{\ell,\ell+1,\ldots,n} \in \mathbb{R}[S_n]$$

for all $\ell \in \{1, 2, \ldots, n\}$ (where $\mathrm{cyc}_{i_1,i_2,\ldots,i_p}$ denotes the permutation in S_n that cycles through $i_1, i_2, \ldots, i_p$).

We compute the eigenvalues of these shuffling operators and of all their linear combinations. In particular, we show that the eigenvalues of right multiplication by a linear combination $\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n$ (with $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{R}$) are the numbers $\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}$, where I ranges over the *lacunar* subsets of $\{1, 2, \ldots, n-1\}$ (i.e., over the subsets that contain no two consecutive integers), and where $m_{I,\ell}$ denotes the distance from ℓ to the next-higher element of I (which element is understood to be ℓ itself if $\ell \in I$, and to be $n+1$ if $\ell > \max I$). We compute the multiplicities of these eigenvalues and show that if they are all distinct, the shuffling operator is diagonalizable. To this purpose, we show that the operators of right multiplication by $t_1, t_2, \ldots, t_n$ on $\mathbb{R}[S_n]$ are simultaneously triangularizable, and in fact there is a combinatorially defined basis (the "descent-destroying basis", as we call it) of $\mathbb{R}[S_n]$ in which they are represented by upper-triangular matrices. The results stated here over $\mathbb{R}$ for convenience are actually stated and proved over an arbitrary commutative ring $\mathbf{k}$.

We finish by describing a strong stationary time for the random-to-below shuffle, which is the shuffle in which the card that moves below is selected uniformly at random, and we give the waiting time for this event to happen.

Mathematics Subject Classifications: 05E99, 20C30, 60J10.

Keywords: symmetric group, permutations, card shuffling, top-to-random shuffle, group algebra, substitutional analysis, Fibonacci numbers, filtration, representation theory, Markov chain.

Contents

1. Introduction

Card shuffling operators have been studied both from algebraic and probabilistic point of views. The interest in an algebraic study of those operators bloomed with the discovery by Diaconis and Shahshahani that the eigenvalues of some matrices could be used to bound the mixing time of the shuffles [DiaSha81], which answers the question "how many times should we shuffle a deck of cards to get a well-shuffled deck?". We now know a combinatorial description of the eigenvalues of several shuffling operators, including the transposition shuffle [DiaSha81], the riffle shuffle [BayDia92], the top-to-random shuffle [Phatar91] and the random-to-random shuffle [DieSal18], among several others. An interesting research question is to characterize shuffles whose eigenvalues admit a combinatorial description.

We contribute to this project by describing a new family of shuffles that do so.

Given a probability distribution P on the set $\{1, 2, \ldots, n\}$, the *one-sided cycle shuffle* corresponding to P consists of picking the card at position i with probability $P(i)$, removing it, and reinserting it at a position weakly below position i, chosen uniformly at random. By varying the probability distribution, we obtain an infinite family of shuffling operators, whose eigenvalues can be written as linear combinations of certain combinatorial numbers with coefficients given by the probability distribution. Special cases of interest include the top-to-random shuffle, the random-to-below shuffle (where position i is selected uniformly at random), and the unweighted one-sided cycle shuffle (where position i is selected with probability $\dfrac{2(n+1-i)}{n(n+1)}$). A more explicit description of the shuffles can be found in Section 3.

Two of our main results – Corollary 12.2 and Theorem 13.2 – give the eigenvalues of all the one-sided cycle shuffles. These eigenvalues are indexed by what we call "lacunar sets", which are subsets of $\mathbb{Z}$ that do not contain consecutive integers (see Section 5 for details). As a consequence, all eigenvalues are real, positive and explicitly described.

Most studies of eigenvalues of Markov chains focus on reversible chains, which means that their transition matrix is symmetric. In that case, eigenvalues can be used alone for bounding the mixing time of the Markov chain. This is however not the case for the one-sided cycle shuffles.

Examples of non-reversible Markov chains whose eigenvalues have been studied include the riffle shuffle [BayDia92], the top-to-random and random-to-top shuffles [Phatar91], the pop shuffles and other 'BHR' shuffling operators [BiHaRo99], and the top-m-to-random shuffles [DiFiPi92]. All these admit a combinatorial description of their eigenvalues. It is surprising that non-symmetric matrices admit real eigenvalues, let alone eigenvalues that can be computed by simple formulas. It is these surprisingly elegant eigenvalues that have given the impetus for the present study.

To prove and explain our main results, we decompose the one-sided cycle shuffles into linear combinations of n operators $t_1, t_2, \ldots, t_n$, which we call the *somewhere-to-below shuffles*. Each somewhere-to-below shuffle t_ℓ moves the card at position ℓ to a position weakly below it, chosen uniformly at random. We show that the somewhere-to-below shuffles are simultaneously triangularizable by giving explicitly a basis in which they can be triangularized. This later gives us the eigenvalues. The triangularity, in fact, is an understatement; we actually find a filtration $0 = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}} = \mathbb{Z}[S_n]$ of the group ring of S_n that is preserved by all somewhere-to-below shuffles and has the additional property that each t_ℓ acts as a scalar on each quotient F_i / F_{i-1}. Here, perhaps unexpectedly, f_{n+1} is the $(n+1)$-st Fibonacci number. Thus, the number of distinct eigenvalues of a one-sided cycle shuffle is never larger than f_{n+1}.

A diversity of algebraic techniques for computing the spectrum of shuffling operators have appeared recently [ReSaWe14, DiPaRa14, DieSal18, Lafren19, BaCoMR21, Pang22, NesPen22]. This paper contributes new algebraic methods to this extensive toolkit.

We end the paper by establishing a strong stationary time for one shuffling operator in our family, the random-to-below shuffle, which happens in an expected time of at most $n(\log n + \log(\log n) + \log 2) + 1$. The arguments used here are similar to those used to get a stationary time for the top-to-random shuffle; see Section 15.

This is the arXiv version of the present paper; a somewhat terser writeup has been published in the *Algebraic Combinatorics* journal. See also the extended abstract [GriLaf24] for a brief summary of this and some related work.

Acknowledgements The authors would like to thank Eran Assaf, Sarah Brauner, Colin Defant, Persi Diaconis, Theo Douvropoulos, Maxim Kontsevich, Martin Lorenz, Oliver Matheau-Raven, Amy Pang, Karol Penson, Victor Reiner and Franco Saliola for inspiring discussions and insightful comments. This work was made possible thanks to [SageMath].

2. The algebraic setup

Card shuffling schemes are often understood by mathematicians as drawing, randomly, a permutation and applying it to a deck of cards. Therefore, our work takes place in the symmetric group algebra, which we define in this section.

2.1. Basic notations

Let $\mathbf{k}$ be any commutative ring. (In most applications, $\mathbf{k}$ is either $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$.)

Let $\mathbb{N} := \{0, 1, 2, \ldots\}$ be the set of all nonnegative integers.

For any integers a and b, we set $[a, b] := \{x \in \mathbb{Z} \mid a \leq x \leq b\} = \{a, a+1, \ldots, b\}$. This is an empty set if $a > b$.

For each $n \in \mathbb{Z}$, let $[n] := [1, n] = \{1, 2, \ldots, n\}$.

Fix an integer $n \in \mathbb{N}$. Let S_n be the n-th symmetric group, i.e., the group of all permutations of $[n]$. We multiply permutations in the "continental" way: that is, $(\pi\sigma)(i) = \pi(\sigma(i))$ for all $\pi, \sigma \in S_n$ and $i \in [n]$.

For any k distinct elements $i_1, i_2, \ldots, i_k$ of $[n]$, we let $\operatorname{cyc}_{i_1, i_2, \ldots, i_k}$ be the permutation in S_n that sends $i_1, i_2, \ldots, i_{k-1}, i_k$ to $i_2, i_3, \ldots, i_k, i_1$, respectively while leaving all remaining elements of $[n]$ unchanged. This permutation is known as a *cycle*. Note that $\operatorname{cyc}_i = \operatorname{id}$ for any single $i \in [n]$.

2.2. Some elements of $\mathbf{k}[S_n]$

Consider the group algebra $\mathbf{k}[S_n]$. In this algebra, define n elements $t_1, t_2, \ldots, t_n$ by setting

$$t_\ell := \mathrm{cyc}_\ell + \mathrm{cyc}_{\ell,\ell+1} + \mathrm{cyc}_{\ell,\ell+1,\ell+2} + \cdots + \mathrm{cyc}_{\ell,\ell+1,\ldots,n} \in \mathbf{k}[S_n] \tag{1}$$

for each $\ell \in [n]$. Thus, in particular, $t_n = \mathrm{cyc}_n = \mathrm{id} = 1$ (where 1 means the unity of $\mathbf{k}[S_n]$). We shall refer to the n elements $t_1, t_2, \ldots, t_n$ as the *somewhere-to-below shuffles*, due to a probabilistic significance that we will discuss soon.

The first somewhere-to-below shuffle t_1 is known as the *top-to-random shuffle*, and has been studied, for example, in [DiFiPi92].[1] It shares a lot of properties with its adjoint operator, the *random-to-top shuffle*, also widely studied (sometimes with other names, such as the Tsetlin Library or the move-to-front rule, as in [Hendri72, Donnel91, Phatar91, Fill96, BiHaRo99]), and described in Section 14 as t'_1.

We shall study not just the somewhere-to-below shuffles, but also their $\mathbf{k}$-linear combinations $\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n$ (with $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$), which we call the *one-sided cycle shuffles*.

2.3. The card-shuffling interpretation

For $\mathbf{k} = \mathbb{R}$, the elements $t_1, t_2, \ldots, t_n$ (and many other elements of $\mathbf{k}[S_n]$) have an interpretation in terms of card shuffling.

Namely, we consider a permutation $w \in S_n$ as a way to order a deck of n cards[2] such that the cards are $w(1), w(2), \ldots, w(n)$ from top to bottom (so the top card is $w(1)$, and the bottom card is $w(n)$). Shuffling the deck corresponds to permuting the cards: A permutation $\sigma \in S_n$ transforms a deck order $w \in S_n$ into the deck order $w\sigma$ (that is, the order in which the cards are $w(\sigma(1)), w(\sigma(2)), \ldots, w(\sigma(n))$ from top to bottom).

A probability distribution on the $n!$ possible orders of a deck of n cards can be identified with the element $\sum\limits_{w \in S_n} P(w)\, w$ of $\mathbb{R}[S_n]$, where $P(w)$ is the probability of the deck having order w. Likewise, a nonzero element $\sum\limits_{\sigma \in S_n} P(\sigma)\, \sigma$ of $\mathbb{R}[S_n]$ (with all $P(\sigma)$ being nonnegative reals) defines a Markov chain on the set of all these $n!$ orders, in which the transition probability from deck order w to deck order $w\tau$

---

[1] Our t_1 equals the B_1 defined in [DiFiPi92, (4.4)] (since the cycles $\mathrm{cyc}_1, \mathrm{cyc}_{1,2}, \ldots, \mathrm{cyc}_{1,2,\ldots,n}$ are the only permutations $\pi \in S_n$ satisfying $\pi^{-1}(n) > \pi^{-1}(n-1) > \cdots > \pi^{-1}(2)$).

The (German) diploma thesis [Palmes10] provides a detailed exposition of the results of [DiFiPi92, (4.4)] (in particular, [Palmes10, Satz 2.4.6] is [DiFiPi92, Theorem 4.2]).

See also [Grinbe18] for an exposition of the most basic algebraic properties of t_1 (which is denoted by $\mathbf{A}$ in [Grinbe18]). An unexpected application to machine learning has recently been given in [Reizen19, proof of Lemma 29].

[2] As is customary in card-shuffling combinatorics, the cards are bijectively numbered $1, 2, \ldots, n$; there are no suits, colors or jokers.

equals $\dfrac{P(\tau)}{\sum\limits_{\sigma\in S_n} P(\sigma)}$ for each $w, \tau \in S_n$. This is an instance of a *right random walk on a group*, as defined (e.g.) in [LePeWi09, Section 2.6].

From this point of view, the top-to-random shuffle t_1 describes the Markov chain in which a deck is transformed by picking the topmost card and moving it into the deck at a position chosen uniformly at random (which may well be its original, topmost position). This explains the name of t_1 (and its significance to probabilists). More generally, a somewhere-to-below shuffle t_ℓ transforms a deck by picking its ℓ-th card from the top and moving it to a weakly lower place (chosen uniformly at random). Finally, a one-sided cycle shuffle $\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n$ (with $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{R}_{\geq 0}$ being not all 0) picks a card at random – specifically, picking the ℓ-th card from the top with probability $\dfrac{(n-\ell+1)\lambda_\ell}{\sum\limits_{i=1}^{n}(n-i+1)\lambda_i}$ – and moves it to a weakly lower place (chosen uniformly at random).

3. The one-sided cycle shuffles

In this section, we shall explore the probabilistic significance of one-sided cycle shuffles and several particular cases thereof. We begin by a reindexing of the one-sided cycle shuffles that is particularly convenient for probabilistic considerations. Note that, since transition matrices of Markov chains have their rows summing to 1, the operators, as we describe them in this section, are scaled to satisfy this property. However, throughout the paper, the coefficients can sum up to any numbers; multiplying the operators by the appropriate number would give the corresponding Markov chain.

For a given probability distribution P on the set $[n]$, we define the *one-sided cycle shuffle governed by* P to be the element

$$\mathrm{OSC}(P,n) := \frac{P(1)}{n}t_1 + \frac{P(2)}{n-1}t_2 + \frac{P(3)}{n-2}t_3 + \cdots + \frac{P(n)}{1}t_n \in \mathbb{R}[S_n].$$

This one-sided cycle shuffle gives rise to a Markov chain on the symmetric group S_n, which transforms a deck order by selecting a card at random according to the probability distribution P (more precisely, we pick the **position**, not the value of the card, using P), and then applying the corresponding somewhere-to-below shuffle. The transition probability of this Markov chain is thus given by

$$Q(\tau,\sigma) = \begin{cases} \sum\limits_{i=1}^{n} \frac{P(i)}{n+1-i}, & \text{if } \sigma = \tau; \\ \frac{P(i)}{n+1-i}, & \text{if } \sigma = \tau \cdot \mathrm{cyc}_{i,i+1,\ldots,j} \text{ for some } j > i; \\ 0, & \text{otherwise.} \end{cases}$$

The $n! \times n!$-matrix $\left(Q\left(\tau,\sigma\right)\right)_{\tau,\sigma\in S_n}$ is the transition matrix of this Markov chain; when we talk of the eigenvalues of the Markov chain, we refer to the eigenvalues of the corresponding transition matrix.

These Markov chains are not reversible, which means that their transition matrices are not symmetric.

3.1. Interesting one-sided cycle shuffles

Some probability distributions on $[n]$ lead to one-sided cycle shuffles that have an interesting meaning in terms of card shuffling. We shall next consider three such cases.

The top-to-random shuffle The top-to-random shuffle t_1 is the one-sided cycle shuffle that garnered the most interest. We obtain it by setting $P(1) = 1$, and $P(i) = 0$ for all $i \neq 1$.

The transition matrix for the top-to-random shuffle, with 3 cards $w_1 := w\left(1\right)$, $w_2 := w\left(2\right)$ and $w_3 := w\left(3\right)$, is

$$\mathrm{T2R}_3 = \begin{array}{cc} & \begin{array}{cccccc} w_1w_2w_3 & w_1w_3w_2 & w_2w_1w_3 & w_2w_3w_1 & w_3w_1w_2 & w_3w_2w_1 \end{array} \\ \begin{array}{c} w_1w_2w_3 \\ w_1w_3w_2 \\ w_2w_1w_3 \\ w_2w_3w_1 \\ w_3w_1w_2 \\ w_3w_2w_1 \end{array} & \begin{pmatrix} \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{3} \end{pmatrix} \end{array}$$

(where $w_iw_jw_k$ is shorthand for the permutation in S_3 that sends $1, 2, 3$ to w_i, w_j, w_k, respectively).

The eigenvalues of this matrix are known since [Phatar91] to be $0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-2}{n}, 1$, and the multiplicity of the eigenvalue $\frac{i}{n}$ is the number of permutations in S_n that have exactly i fixed points.[3] In other words, the eigenvalues of t_1 are $0, 1, 2, \ldots, n-2, n$ with multiplicities as just said. Other descriptions of the eigenvalues of the top-to-random shuffle are given in terms of set partitions [BiHaRo99] and in terms of standard Young tableaux [ReSaWe14].

The random-to-below shuffle The *random-to-below shuffle* consists of picking any card randomly (with uniform probability), and inserting it anywhere weakly below (with uniform probability). This is the one-sided cycle shuffle governed by the uniform distribution (i.e., by the probability distribution P with $P(i) = \dfrac{1}{n}$ for all

[3]Actually, [Phatar91] studies a more general kind of shuffling operators with further parameters $p_1, p_2, \ldots, p_n$, but these can no longer be seen as random walks on a group and do not appear to fit into a well-behaved "somewhere-to-below shuffle" family in the way t_1 does.

$i \in [n]$). Hence, the random-to-below operator is, in terms of the somewhere-to-below operators,

$$\mathrm{R2B}_n = \frac{1}{n^2} t_1 + \frac{1}{n(n-1)} t_2 + \frac{1}{n(n-2)} t_3 + \cdots + \frac{1}{n} t_n.$$

A sample transition matrix for the random-to-below shuffle is given here for a deck with 3 cards:

$$\mathrm{R2B}_3 = \begin{array}{c} \\ w_1w_2w_3 \\ w_1w_3w_2 \\ w_2w_1w_3 \\ w_2w_3w_1 \\ w_3w_1w_2 \\ w_3w_2w_1 \end{array} \begin{array}{c} \begin{array}{cccccc} w_1w_2w_3 & w_1w_3w_2 & w_2w_1w_3 & w_2w_3w_1 & w_3w_1w_2 & w_3w_2w_1 \end{array} \\ \left(\begin{array}{cccccc} \frac{11}{18} & \frac{1}{6} & \frac{1}{9} & \frac{1}{9} & 0 & 0 \\ \frac{1}{6} & \frac{11}{18} & 0 & 0 & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{9} & \frac{1}{9} & \frac{11}{18} & \frac{1}{6} & 0 & 0 \\ 0 & 0 & \frac{1}{6} & \frac{11}{18} & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{9} & \frac{1}{9} & 0 & 0 & \frac{11}{18} & \frac{1}{6} \\ 0 & 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{6} & \frac{11}{18} \end{array} \right) \end{array}.$$

A recently studied shuffle admits a similar description, namely the one-sided transposition shuffle [BaCoMR21], that picks a card uniformly at random and swaps it with a card chosen uniformly at random among the cards below. Despite its similar-sounding description, it is not a one-sided cycle shuffle (unless $n \leq 2$), and a striking difference between the two shuffles is that the matrix of the one-sided transposition shuffle is symmetric, unlike the one for random-to-below.

The unweighted one-sided cycle Consider a variation of the problem, in which we pick a somewhere-to-below move uniformly among the possible moves allowed. That is, we choose (with uniform probability) two integers i and j in $[n]$ satisfying $i \leq j$, and then we apply the cycle $\mathrm{cyc}_{i,i+1,\ldots,j}$. Thus, the probability of applying the cycle $\mathrm{cyc}_{i,i+1,\ldots,j}$ is $\dfrac{2}{n(n+1)}$ for all $i < j$, and the probability of applying the identity is $\dfrac{2}{n+1}$. This is the one-sided cycle shuffle governed by the probability distribution P with $P(i) = \dfrac{2(n-i+1)}{n(n+1)}$. For $n = 3$, its transition matrix is

$$\begin{array}{c} \\ w_1w_2w_3 \\ w_1w_3w_2 \\ w_2w_1w_3 \\ w_2w_3w_1 \\ w_3w_1w_2 \\ w_3w_2w_1 \end{array} \begin{array}{c} \begin{array}{cccccc} w_1w_2w_3 & w_1w_3w_2 & w_2w_1w_3 & w_2w_3w_1 & w_3w_1w_2 & w_3w_2w_1 \end{array} \\ \left(\begin{array}{cccccc} \frac{1}{2} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 0 & 0 \\ \frac{1}{6} & \frac{1}{2} & 0 & 0 & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{2} & \frac{1}{6} & 0 & 0 \\ 0 & 0 & \frac{1}{6} & \frac{1}{2} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & 0 & 0 & \frac{1}{2} & \frac{1}{6} \\ 0 & 0 & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{2} \end{array} \right) \end{array}.$$

3.2. Eigenvalues and mixing time results for one-sided cycle shuffles

Corollary 12.2 further below describes the eigenvalues for any one-sided cycle shuffle. For a deck of n cards, the eigenvalues are indexed by lacunar subsets of $[n-1]$, which are subsets of $[n-1]$ that do not contain consecutive integers. Given such a subset I, we define in Section 5 the nonnegative integers $m_{I,1}, m_{I,2}, \ldots, m_{I,n}$. Then, the eigenvalue of the one-sided cycle shuffle $\operatorname{OSC}(P, n)$ indexed by I is

$$\frac{P(1)}{n} m_{I,1} + \frac{P(2)}{n-1} m_{I,2} + \cdots + \frac{P(n)}{1} m_{I,n}.$$

A consequence of this description is that all the eigenvalues are nonnegative reals (and are rational if the $P(1), P(2), \ldots, P(n)$ are). This is a surprising result for a matrix that is not symmetric.

However, the fact that the matrices are not symmetric means that their eigenvalues cannot be used alone to bound the mixing time for the one-sided cycle shuffle. To palliate this, we describe a strong stationary time for the one-sided cycle shuffles in Section 15. In the specific case of the random-to-below shuffle, we give the waiting time to achieve it.

Eigenvalues of some interesting one-sided cycle shuffles The statement above can be used to find the eigenvalues of any one-sided cycle shuffle, including the top-to-random shuffle. In this case, the eigenvalues are given as $\frac{m_{I,1}}{n}$. It should become clear, after we define the numbers $m_{I,1}$ and lacunar sets in Section 5, that the values that $m_{I,1}$ can take are exactly the integers $0, 1, 2, \ldots, n-2, n$.

Similarly, Corollary 12.2 (as restated above) yields that the eigenvalues for the unweighted one-sided cycle shuffle are given by $\frac{2}{n(n+1)} (m_{I,1} + m_{I,2} + \ldots + m_{I,n})$, and are indexed by the lacunar subsets of $[n-1]$. As far as we can tell, there is no known simple combinatorial expression for the sum $m_{I,1} + m_{I,2} + \cdots + m_{I,n}$.

4. The operators in the symmetric group algebra

We now resume the algebraic study of general one-sided cycle shuffles (with arbitrary $\mathbf{k}$ and not necessarily governed by a probability distribution). We will find it more convenient to work with endomorphisms of the $\mathbf{k}$-module $\mathbf{k}[S_n]$ rather than with $n! \times n!$-matrices.

For each element $x \in \mathbf{k}[S_n]$, let $R(x)$ denote the $\mathbf{k}$-linear map

$$\begin{aligned} \mathbf{k}[S_n] &\to \mathbf{k}[S_n], \\ y &\mapsto yx. \end{aligned}$$

This map is known as "right multiplication by x", and is an endomorphism of the free $\mathbf{k}$-module $\mathbf{k}[S_n]$; thus, it makes sense to speak of eigenvalues, eigenvectors and triangularization.

One of our main results is the following:

Theorem 4.1. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Then, the $\mathbf{k}$-module endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ of $\mathbf{k}[S_n]$ can be triangularized – i.e., there exists a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$ such that this endomorphism is represented by an upper-triangular matrix with respect to this basis. Moreover, this basis does not depend on $\lambda_1, \lambda_2, \ldots, \lambda_n$.

We shall eventually describe both the basis and the eigenvalues of this endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ explicitly; indeed, both will follow from Theorem 11.1.

Remark 4.2. In general, the endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ cannot be diagonalized. For example:

- If we take $\mathbf{k} = \mathbb{C}$, $n = 4$ and $\lambda_i = 1$ for each $i \in [n]$ (which is the unweighted one-sided cycle shuffle), then the minimal polynomial of the endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is $(x-10)(x-6)(x-4)^2(x-2)$, so that this endomorphism is not diagonalizable.

- If we take $\mathbf{k} = \mathbb{C}$, $n = 3$ and $\lambda_i = \dfrac{6}{i}$ for each $i \in [n]$, then the minimal polynomial of the endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is $(x-8)^2(x-26)$, so that this endomorphism is not diagonalizable.

Consequently, there is (in general) no basis of $\mathbf{k}[S_n]$ such that all the endomorphisms $R(t_1), R(t_2), \ldots, R(t_n)$ are represented by diagonal matrices with respect to this basis. Triangular matrices are thus the best one might hope for; and Theorem 4.1 reveals that this hope indeed comes true. Eventually, we will see (Theorem 12.3) that the endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is diagonalizable (over a field) for a sufficiently generic choice of $\lambda_1, \lambda_2, \ldots, \lambda_n$.

5. Subset basics: Lacunarity, Enclosure and Non-Shadow

In order to concretize the claims of Theorem 4.1, we shall introduce some features of sets of integers and a rather famous integer sequence. The main role will be played by the *lacunar sets*, which will later index a certain filtration of $\mathbf{k}[S_n]$ on whose subquotients the endomorphisms $R(t_\ell)$ act by scalars. This is especially convenient since the number of lacunar sets is relatively small (a Fibonacci number).

Let $(f_0, f_1, f_2, \ldots)$ be the *Fibonacci sequence*. This is the sequence of integers defined recursively by

$$f_0 = 0, \qquad f_1 = 1, \qquad \text{and} \qquad f_m = f_{m-1} + f_{m-2} \text{ for all } m \geq 2.$$

We shall say that a set $I \subseteq \mathbb{Z}$ is *lacunar* if it contains no two consecutive integers (i.e., there exists no $i \in I$ such that $i + 1 \in I$). For instance, the set $\{1, 4, 6\}$ is lacunar, while the set $\{1, 4, 5\}$ is not. Lacunar sets are also known as "sparse sets" (in [AgNyOr06]) or as "Zeckendorf sets" (in [Chu19], at least when they are finite subsets of $\{1, 2, 3, \ldots\}$).

It is known (see, e.g., [Grinbe20, Proposition 1.4.9]) that the number of lacunar subsets of $[n]$ is the Fibonacci number f_{n+2}. Applying this to $n - 1$ instead of n, we conclude that the number of lacunar subsets of $[n-1]$ is f_{n+1} whenever $n > 0$. A moment's thought reveals that this holds for $n = 0$ as well (since $[-1] = \varnothing$), and thus holds for each nonnegative integer n.

If I is any set of integers, then $I - 1$ will denote the set $\{i - 1 \mid i \in I\}$; this is again a set of integers. For instance, $\{2, 4, 5\} - 1 = \{1, 3, 4\}$. Note that a set I is lacunar if and only if $I \cap (I - 1) = \varnothing$.

For any subset I of $[n]$, we define the following:

- We let $\widehat{I}$ be the set $\{0\} \cup I \cup \{n + 1\}$. We shall refer to $\widehat{I}$ as the *enclosure* of I.

  For example, if $n = 5$, then $\widehat{\{2, 3\}} = \{0, 2, 3, 6\}$.

- For any $\ell \in [n]$, we let $m_{I,\ell}$ be the number

  $$\left(\text{smallest element of } \widehat{I} \text{ that is } \geq \ell\right) - \ell \in [0, n + 1 - \ell] \subseteq [0, n].$$

  Those numbers $m_{I,\ell}$ already appeared in Subsection 3.2, as they play a crucial role in the expression of the eigenvalues of the one-sided cycle shuffles.

  For example, if $n = 5$ and $I = \{2, 3\}$, then

  $$(m_{I,1},\ m_{I,2},\ m_{I,3},\ m_{I,4},\ m_{I,5}) = (1,\ 0,\ 0,\ 2,\ 1).$$

  We note that an $\ell \in [n]$ satisfies $m_{I,\ell} = 0$ if and only if $\ell \in \widehat{I}$ (or, equivalently, $\ell \in I$).

- We let I' be the set $[n-1] \setminus (I \cup (I - 1))$. This is the set of all $i \in [n-1]$ satisfying $i \notin I$ and $i + 1 \notin I$. We shall refer to I' as the *non-shadow* of I.

  For example, if $n = 5$, then $\{2, 3\}' = [4] \setminus \{1, 2, 3\} = \{4\}$.

6. The simple transpositions s_i

In this section, we will recall the basic properties of simple transpositions in the symmetric group S_n, and use them to rewrite the definition (1) of the somewhere-to-below shuffles.

For any $i \in [n-1]$, we let $s_i := \operatorname{cyc}_{i,i+1} \in S_n$. This permutation s_i is called a *simple transposition*. It is well-known that $s_1, s_2, \ldots, s_{n-1}$ generate the group S_n. Moreover, it is known that two simple transpositions s_i and s_j commute whenever $|i-j| > 1$. This latter fact is known as *reflection locality*.

It is furthermore easy to see that

$$\operatorname{cyc}_{\ell,\ell+1,\ldots,k} = s_\ell s_{\ell+1} \cdots s_{k-1} \tag{2}$$

for each $\ell \leq k$ in $[n]$. Thus, (1) rewrites as follows:

$$\begin{aligned} t_\ell &= 1 + s_\ell + s_\ell s_{\ell+1} + \cdots + s_\ell s_{\ell+1} \cdots s_{n-1} \\ &= \sum_{j=\ell}^{n} s_\ell s_{\ell+1} \cdots s_{j-1} \end{aligned} \tag{3}$$

for each $\ell \in [n]$.

The following relationship between simple transpositions will later be used in proving the triangularizability of the somewhere-to-below shuffles:

Lemma 6.1. Let $\ell \in [n]$ and $j \in [n]$. Let $i \in [\ell, j-2]$. Then,

$$s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i = s_{i+1} \cdot s_\ell s_{\ell+1} \cdots s_{j-1}.$$

Proof of Lemma 6.1. From $i \in [\ell, j-2]$, we obtain $i \in [\ell, j-1]$ and $i+1 \in [\ell, j-1]$ and $\ell \leq i \leq j-2 < j$.

It is well-known that

$$\sigma \operatorname{cyc}_{p_1,p_2,\ldots,p_k} \sigma^{-1} = \operatorname{cyc}_{\sigma(p_1),\sigma(p_2),\ldots,\sigma(p_k)} \tag{4}$$

for any $\sigma \in S_n$ and any k distinct elements $p_1, p_2, \ldots, p_k$ of $[n]$.

Let $\sigma = \operatorname{cyc}_{\ell,\ell+1,\ldots,j}$. Then, $\sigma(i) = i+1$ (since $i \in [\ell, j-1]$) and $\sigma(i+1) = i+2$ (since $i+1 \in [\ell, j-1]$). However, (4) yields

$$\sigma \operatorname{cyc}_{i,i+1} \sigma^{-1} = \operatorname{cyc}_{\sigma(i),\sigma(i+1)} = \operatorname{cyc}_{i+1,i+2}$$

(since $\sigma(i) = i+1$ and $\sigma(i+1) = i+2$). In view of $s_i = \operatorname{cyc}_{i,i+1}$ and $s_{i+1} = \operatorname{cyc}_{i+1,i+2}$, this rewrites as $\sigma s_i \sigma^{-1} = s_{i+1}$. In other words, $\sigma s_i = s_{i+1} \sigma$. In view of $\sigma = \operatorname{cyc}_{\ell,\ell+1,\ldots,j} = s_\ell s_{\ell+1} \cdots s_{j-1}$, we can rewrite this as $s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i = s_{i+1} \cdot s_\ell s_{\ell+1} \cdots s_{j-1}$. This proves Lemma 6.1. $\square$

7. The invariant spaces $F(I)$

Recall that our goal is to prove Theorem 4.1, which claims that the one-sided cycle shuffles are triangularizable. To that end, we will construct a $\mathbf{k}$-submodule filtration of $\mathbf{k}[S_n]$ that is preserved by all the somewhere-to-below shuffles. In this section, we define a first family of submodules $F(I)$ of $\mathbf{k}[S_n]$, which will later serve as building blocks for this filtration.

7.1. Definition

For any subset I of $[n]$, we define the following:

- We let $\operatorname{sum} I$ denote the sum of all elements of I. This is an integer with $0 \leq \operatorname{sum} I \leq n(n+1)/2$.

- We let
$$F(I) := \left\{ q \in \mathbf{k}[S_n] \mid qs_i = q \text{ for all } i \in I' \right\}.$$
This is a $\mathbf{k}$-submodule of $\mathbf{k}[S_n]$. Intuitively, it can be understood as follows: Writing each permutation $\pi \in S_n$ as the n-tuple $(\pi(1), \pi(2), \ldots, \pi(n))$ (this is called *one-line notation*), we can view an element $q \in \mathbf{k}[S_n]$ as a $\mathbf{k}$-linear combination of such n-tuples. The group S_n acts on such n-tuples from the right by permuting positions, and thus acts on their linear combinations by linearity. An element $q \in \mathbf{k}[S_n]$ belongs to $F(I)$ if and only if it is invariant under permuting any two adjacent positions i and $i+1$ that both lie outside of I. We thus call $F(I)$ an *invariant space*.

  In terms of shuffling operators, one can think of $F(I)$ as the set of all random decks (i.e., probability distributions on the $n!$ orderings of a deck) that are *fully shuffled* within each contiguous interval of $[n] \backslash I$. This is to be understood as follows: Let $q \in F(I)$, and let $\sigma \in S_n$ be a term appearing in q with coefficient c. Let $[i, j]$ be an interval of $[n]$ containing no element of I. Then, for any permutation $\tau \in S_n$ that fixes each element of $[n] \backslash [i, j]$, the coefficient of $\sigma\tau$ in q is also c. Moreover, this property characterizes the elements q of $F(I)$.

  Note that the set $F(I)$ depends only on n and I', but not on I. We nevertheless find it better to index it by I.

Note that $F([n]) = \mathbf{k}[S_n]$, since $[n]' = \varnothing$. (Also, many other subsets I of $[n]$ satisfy $F(I) = \mathbf{k}[S_n]$. For example, this holds for $I = \{2, 4, 6, 8, \ldots\} \cap [n]$ and for $I = \{1, 3, 5, 7, \ldots\} \cap [n]$ and for $I = [n-1]$. Indeed, all of these sets I satisfy $I' = \varnothing$.)

Here are some more examples of the sets $F(I)$:

Example 7.1. Let $n = 3$. Then, there are $2^3 = 8$ many subsets I of $[n] = [3]$. We shall compute the non-shadow I' and the invariant space $F(I)$ for each of them:

- We have $\varnothing' = [2]$ and thus
$$\begin{aligned} F(\varnothing) &= \{ q \in \mathbf{k}[S_n] \mid qs_i = q \text{ for all } i \in [2] \} \\ &= \operatorname{span}([123] + [132] + [213] + [231] + [312] + [321]). \end{aligned}$$
Here, the notation "span" means a $\mathbf{k}$-linear span, whereas the notation $[ijk]$ means the permutation $\sigma \in S_3$ that sends $1, 2, 3$ to i, j, k, respectively. (In our case, we are taking the span of a single vector, but soon we will see some more complicated spans.)

- We have $\{1\}' = \{2\}$ and thus

$$\begin{aligned} F(\{1\}) &= \{q \in \mathbf{k}[S_n] \mid qs_2 = q\} \\ &= \operatorname{span}([123]+[132],\ \ [213]+[231],\ \ [312]+[321]). \end{aligned}$$

- We have $\{3\}' = \{1\}$ and thus

$$\begin{aligned} F(\{3\}) &= \{q \in \mathbf{k}[S_n] \mid qs_1 = q\} \\ &= \operatorname{span}([123]+[213],\ \ [132]+[312],\ \ [231]+[321]). \end{aligned}$$

- If I is any of the sets $\{2\}$, $\{1,2\}$, $\{1,3\}$, $\{2,3\}$ and $\{1,2,3\}$, then $I' = \varnothing$ and thus

$$\begin{aligned} F(I) &= \{q \in \mathbf{k}[S_n]\} = \mathbf{k}[S_n] \\ &= \operatorname{span}([123],\ \ [132],\ \ [213],\ \ [231],\ \ [312],\ \ [321]). \end{aligned}$$

Example 7.2. Let $n = 4$. Then, $\{1\}' = \{2,3\}$ and thus

$$\begin{aligned} F(\{1\}) &= \{q \in \mathbf{k}[S_n] \mid qs_i = q \text{ for all } i \in \{2,3\}\} \\ &= \operatorname{span}([1234]+[1243]+[1324]+[1342]+[1423]+[1432], \\ &\qquad [2134]+[2143]+[2314]+[2341]+[2413]+[2431], \\ &\qquad [3124]+[3142]+[3214]+[3241]+[3412]+[3421], \\ &\qquad [4123]+[4132]+[4213]+[4231]+[4312]+[4321]). \end{aligned}$$

Here, $[ijk\ell]$ means the permutation $\sigma \in S_4$ that sends $1,2,3,4$ to i,j,k,ℓ, respectively.

In Section 8, we shall define a filtration of $\mathbf{k}[S_n]$ that requires sorting subsets according to the sum of their elements. Hence, for each $k \in \mathbb{N}$, we set

$$F(<k) := \sum_{\substack{J \subseteq [n]; \\ \operatorname{sum} J < k}} F(J).$$

7.2. Right multiplication by $t_\ell - m_{I,\ell}$ moves us down the $F(I)$-grid

We now claim the following theorem, which will play a crucial role in our proof of Theorem 4.1:

Theorem 7.3. Let $I \subseteq [n]$ and $\ell \in [n]$. Then,

$$F(I) \cdot (t_\ell - m_{I,\ell}) \subseteq F(< \operatorname{sum} I).$$

In other words, for each $q \in F(I)$, we have $q \cdot (t_\ell - m_{I,\ell}) \in F(< \operatorname{sum} I)$.

This theorem is essential to establishing the triangularization stated in Theorem 4.1, which requires sorting the submodules $F(I)$ according to the sum of elements in I.

Proof of Theorem 7.3. Fix $q \in F(I)$. We must prove that $q \cdot (t_\ell - m_{I,\ell}) \in F(< \operatorname{sum} I)$. There are three main parts to our proof. In the first part, we express $q \cdot (t_\ell - m_{I,\ell})$ as a sum of products of q with simple transpositions (Equation (7)). In the second part, we will break this sum up into smaller sums (Equation (8)). In the third and last part, we will show that each of these smaller sums is in $F(K)$ for some $K \subseteq [n]$ satisfying $\operatorname{sum} K < \operatorname{sum} I$ (and therefore in $F(< \operatorname{sum} I)$). This will complete the proof.

Write the set I in the form $I = \{i_1 < i_2 < \cdots < i_p\}$, and furthermore set $i_0 := 0$ and $i_{p+1} := n+1$. Then, the enclosure of I is

$$\widehat{I} = \{0 = i_0 < i_1 < i_2 < \cdots < i_p < i_{p+1} = n+1\}.$$

Let i_k be the smallest element of $\widehat{I}$ that is greater than or equal to ℓ. Thus, $m_{I,\ell} = i_k - \ell$ (by the definition of $m_{I,\ell}$) and

$$i_0 < i_1 < \cdots < i_{k-1} < \ell \leq i_k < i_{k+1} < \cdots < i_{p+1}. \tag{5}$$

Note that $k \geq 1$ (since $k = 0$ would entail $\ell \leq i_k = i_0 = 0$, which is absurd), so that $i_k \geq 1$.

From $i_{p+1} = n+1$, we obtain $n = i_{p+1} - 1$. Now, multiplying the equality (3) by q, we obtain

$$\begin{aligned}
qt_\ell &= q \sum_{j=\ell}^{n} s_\ell s_{\ell+1} \cdots s_{j-1} = \sum_{j=\ell}^{n} q s_\ell s_{\ell+1} \cdots s_{j-1} \\
&= \sum_{j=\ell}^{i_{p+1}-1} q s_\ell s_{\ell+1} \cdots s_{j-1} \qquad \left(\text{since } n = i_{p+1} - 1\right) \\
&= \sum_{j=\ell}^{i_k - 1} q s_\ell s_{\ell+1} \cdots s_{j-1} + \sum_{j=i_k}^{i_{p+1}-1} q s_\ell s_{\ell+1} \cdots s_{j-1}
\end{aligned} \tag{6}$$

(since $\ell \leq i_k \leq i_{p+1}$).

Now, from (5), it is easy to see that each $u \in [\ell, i_k - 2]$ belongs to the non-shadow I' (since neither u nor $u+1$ belongs to I). Thus, each $u \in [\ell, i_k - 2]$ satisfies

$qs_u = q$ (since $q \in F(I)$). By applying this observation multiple times, we see that $qs_\ell s_{\ell+1} \cdots s_{j-1} = q$ for each $j \in [\ell, i_k - 1]$. Thus,

$$\sum_{j=\ell}^{i_k-1} \underbrace{qs_\ell s_{\ell+1} \cdots s_{j-1}}_{=q} = \sum_{j=\ell}^{i_k-1} q = \underbrace{(i_k - \ell)}_{=m_{I,\ell}} q = m_{I,\ell} q.$$

Hence, we can rewrite (6) as

$$qt_\ell = m_{I,\ell} q + \sum_{j=i_k}^{i_{p+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}.$$

In other words,

$$qt_\ell - m_{I,\ell} q = \sum_{j=i_k}^{i_{p+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}.$$

Since $qt_\ell - m_{I,\ell} q = q \cdot (t_\ell - m_{I,\ell})$, we can rewrite this further as

$$q \cdot (t_\ell - m_{I,\ell}) = \sum_{j=i_k}^{i_{p+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}. \tag{7}$$

Next, recall that $i_k < i_{k+1} < \cdots < i_{p+1}$. Hence, the interval $[i_k, i_{p+1} - 1]$ can be written as the disjoint union

$$[i_k, i_{k+1} - 1] \sqcup [i_{k+1}, i_{k+2} - 1] \sqcup \cdots \sqcup [i_p, i_{p+1} - 1].$$

Thus, the sum on the right hand side of (7) can be split up as follows:

$$\sum_{j=i_k}^{i_{p+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1} = \sum_{r=k}^{p} \sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}.$$

Therefore, (7) can be rewritten as

$$q \cdot (t_\ell - m_{I,\ell}) = \sum_{r=k}^{p} \sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}. \tag{8}$$

Recall that our goal is to prove that $q \cdot (t_\ell - m_{I,\ell}) \in F(< \operatorname{sum} I)$. In order to do so, we only need to show that

$$\sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1} \in F(< \operatorname{sum} I) \qquad \text{for each } r \in [k, p]$$

(because once this is proved, the equality (8) will become

$$q \cdot (t_\ell - m_{I,\ell}) = \sum_{r=k}^{p} \underbrace{\sum_{j=i_r}^{i_{r+1}-1} q s_\ell s_{\ell+1} \cdots s_{j-1}}_{\in F(<\operatorname{sum} I)} \in \sum_{r=k}^{p} F\left(<\operatorname{sum} I\right) \subseteq F\left(<\operatorname{sum} I\right),$$

and we will have achieved our goal).

This is what we shall now do. So let us fix some $r \in [k, p]$. We set

$$q' := \sum_{j=i_r}^{i_{r+1}-1} q s_\ell s_{\ell+1} \cdots s_{j-1}. \tag{9}$$

We must show that $q' \in F\left(<\operatorname{sum} I\right)$.

To do so, we make extensive use of the facts stated in Section 6 about simple transpositions, and the rest of the proof is obtained by dealing with several cases.

From $r \in [k, p]$, we obtain $k \leq r \leq p$. From $k \leq p$ and $k \geq 1$, we obtain $k \in [p]$, so that $i_k \in \left\{i_1, i_2, \ldots, i_p\right\} = I \subseteq [n]$. Therefore, $i_k \leq n$.

Also, from $r \leq p$ and $r \geq k \geq 1$, we obtain $r \in [p]$, so that $i_r \in \left\{i_1, i_2, \ldots, i_p\right\} = I \subseteq [n]$. Therefore, $i_r \leq n$.

Furthermore, from $k \leq r \leq p$, we obtain $i_k \leq i_r \leq i_p$ (since $i_1 < i_2 < \cdots < i_p$).

Moreover, from $i_r \in [n]$, we obtain $i_r \geq 1$. From $i_0 < i_1 < i_2 < \cdots < i_p < i_{p+1} = n+1$, we obtain $i_{r+1} \leq n+1$, so that $i_{r+1} - 1 \leq n$. Combining this with $i_r \geq 1$, we conclude that $[i_r, i_{r+1} - 1] \subseteq [n]$.

We define a set

$$K := \left(\left(I \setminus \{i_k, i_{k+1}, \ldots, i_r\}\right) \cup \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\}\right) \cap [n].$$

Thus, K is obtained from I by replacing the elements $i_k, i_{k+1}, \ldots, i_r$ by $i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1$ (and intersecting the resulting set with $[n]$, which has the effect of removing 0 if we have replaced 1 by 0). Therefore, K is a subset of $[n]$ and satisfies $\operatorname{sum} K \leq \operatorname{sum} I - (r - k + 1)$ (since $i_k, i_{k+1}, \ldots, i_r$ are $r - k + 1$ distinct elements of I, and we subtracted 1 from each of them[4]). Hence, $\operatorname{sum} K \leq \operatorname{sum} I - (r - k + 1) < \operatorname{sum} I$ (because $r \geq k$). Thus, $F(K) \subseteq F\left(<\operatorname{sum} I\right)$. Hence, in order to prove that $q' \in F\left(<\operatorname{sum} I\right)$, it will suffice to show the more precise statement that

$$q' \in F(K).$$

We shall thus focus on proving this.

In order to prove this, it will clearly suffice to show that $q' s_i = q'$ for each $i \in K'$, because of the definition of $F(K)$. So let us fix $i \in K'$. We must prove that $q' s_i = q'$. The rest of the proof is dedicated to that goal.

[4]Note that the inequality $\operatorname{sum} K \leq \operatorname{sum} I - (r - k + 1)$ is not necessarily an equality, since some of $i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1$ might already belong to $I \setminus \{i_k, i_{k+1}, \ldots, i_r\}$.

We have $i \in K' = [n-1] \setminus (K \cup (K-1))$ (by the definition of K', the non-shadow of K). Thus, $i \in [n-1]$ and $i \notin K \cup (K-1)$. From the latter fact, we conclude that $i \notin K$ and $i+1 \notin K$. From $i \in [n-1]$, we obtain $i+1 \in [n]$.

It is easy to see that

$$i + 1 \notin I \tag{10}$$

[5]. Thus, it is also easy to see that

$$i \in I' \text{ if } i \notin [i_k, i_r] \tag{11}$$

[6]. Similarly, we can show that

$$i + 1 \in I' \text{ if } i \in [\ell, i_r - 1] \tag{12}$$

[7].

---

[5]*Proof of (10):* Assume the contrary. Thus, $i + 1 \in I = \{i_1 < i_2 < \cdots < i_p\}$. In other words, $i + 1 = i_s$ for some $s \in [p]$. Consider this s. From $i + 1 = i_s$, we obtain $i = i_s - 1$.

If we had $s \in [k, r]$, then we would have

$$\begin{aligned} i = i_s - 1 &\in \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\} \qquad (\text{since } s \in [k, r]) \\ &\subseteq (I \setminus \{i_k, i_{k+1}, \ldots, i_r\}) \cup \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\} \end{aligned}$$

and therefore

$$i \in ((I \setminus \{i_k, i_{k+1}, \ldots, i_r\}) \cup \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\}) \cap [n]$$

(since $i \in [n-1] \subseteq [n]$). This would contradict the fact that

$$i \notin K = ((I \setminus \{i_k, i_{k+1}, \ldots, i_r\}) \cup \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\}) \cap [n].$$

Hence, we cannot have $s \in [k, r]$. Thus, we have either $s < k$ or $s > r$. Therefore, we have $i_s \notin \{i_k, i_{k+1}, \ldots, i_r\}$ (because of $i_1 < i_2 < \cdots < i_p$). In other words, $i + 1 \notin \{i_k, i_{k+1}, \ldots, i_r\}$ (since $i + 1 = i_s$). Combining $i + 1 \in I$ with $i + 1 \notin \{i_k, i_{k+1}, \ldots, i_r\}$, we obtain

$$i + 1 \in I \setminus \{i_k, i_{k+1}, \ldots, i_r\} \subseteq (I \setminus \{i_k, i_{k+1}, \ldots, i_r\}) \cup \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\}$$

and therefore

$$\begin{aligned} i + 1 &\in ((I \setminus \{i_k, i_{k+1}, \ldots, i_r\}) \cup \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\}) \cap [n] \qquad (\text{since } i + 1 \in [n]) \\ &= K. \end{aligned}$$

This contradicts $i + 1 \notin K$. This contradiction shows that our assumption was false, and thus (10) is proved.

[6]*Proof of (11):* Assume that $i \notin [i_k, i_r]$. We must show that $i \in I'$.

Indeed, assume the contrary. Thus, $i \notin I' = [n-1] \setminus (I \cup (I-1))$ (by the definition of I'). Since $i \in [n-1]$, this entails that $i \in I \cup (I-1)$. In other words, $i \in I$ or $i + 1 \in I$. Since (10) yields $i + 1 \notin I$, we thus must have $i \in I$. Hence, $i \in I \setminus K$ (since $i \in I$ but $i \notin K$).

The definition of K shows that $I \setminus K \subseteq \{i_k, i_{k+1}, \ldots, i_r\}$ (although this inclusion is not necessarily an equality). Therefore, each element of $I \setminus K$ must belong to $\{i_k, i_{k+1}, \ldots, i_r\}$ and therefore to the interval $[i_k, i_r]$ as well (since $i_0 < i_1 < i_2 < \cdots < i_p < i_{p+1}$ entails $\{i_k, i_{k+1}, \ldots, i_r\} \subseteq [i_k, i_r]$). Hence, from $i \in I \setminus K$, we obtain $i \in [i_k, i_r]$. But this contradicts $i \notin [i_k, i_r]$. This contradiction shows that our assumption was false. Thus, (11) is proved.

[7]*Proof of (12):* Assume that $i \in [\ell, i_r - 1]$. We must show that $i + 1 \in I'$.

From (5) and $r \geq k$, we obtain $\ell \leq i_r < i_{r+1}$. Hence, we are in one of the following five cases:

Case 1: We have $i < \ell - 1$.

Case 2: We have $i = \ell - 1$.

Case 3: We have $\ell \leq i < i_r$.

Case 4: We have $i_r \leq i < i_{r+1}$.

Case 5: We have $i \geq i_{r+1}$.

For each of these cases, we need to prove that $q' s_i = q'$.

Let us first consider Case 1. In this case, we have $i < \ell - 1$. Thus, $i < \ell - 1 < \ell \leq i_k$, so that $i \notin [i_k, i_r]$. Hence, from (11), we obtain $i \in I'$. Thus, $q s_i = q$ (since $q \in F(I)$). Furthermore, from $i < \ell - 1$, we see that s_i commutes with all the permutations $s_\ell, s_{\ell+1}, \ldots, s_{i_{r+1}-2}$ that appear on the right hand side of (9) (by reflection locality). Hence, multiplying the equality (9) by s_i, we find

$$q' s_i = \sum_{j=i_r}^{i_{r+1}-1} q \underbrace{s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i}_{\substack{= s_i \cdot s_\ell s_{\ell+1} \cdots s_{j-1} \\ \text{(since } s_i \text{ commutes with all of } s_\ell, s_{\ell+1}, \ldots, s_{j-1})}} = \sum_{j=i_r}^{i_{r+1}-1} \underbrace{q s_i}_{=q} \cdot s_\ell s_{\ell+1} \cdots s_{j-1}$$
$$= \sum_{j=i_r}^{i_{r+1}-1} q s_\ell s_{\ell+1} \cdots s_{j-1} = q'.$$

We have thus proved $q' s_i = q'$ in Case 1.

Indeed, assume the contrary. Thus, $i + 1 \notin I' = [n-1] \setminus (I \cup (I - 1))$ (by the definition of I').

From $i \in [\ell, i_r - 1]$, we obtain $i \geq \ell$ and $i \leq i_r - 1$. The latter inequality yields $i + 1 \leq i_r$. However, (10) yields $i + 1 \notin I$. Thus, $i + 1 \neq i_r$ (because if we had $i + 1 = i_r$, then $i + 1 = i_r \in I$ would contradict $i + 1 \notin I$). Combining this with $i + 1 \leq i_r$, we obtain $i + 1 < i_r \leq n$. Hence, $i + 1 \leq n - 1$, so that $i + 1 \in [n-1]$.

Therefore, from $i + 1 \notin [n-1] \setminus (I \cup (I - 1))$, we obtain $i + 1 \in I \cup (I - 1)$. In other words, $i + 1 \in I$ or $i + 1 \in I - 1$. Since $i + 1 \notin I$, we thus conclude that $i + 1 \in I - 1$. Thus, $i + 2 \in I = \{i_1 < i_2 < \cdots < i_p\}$. In other words, there exists some $s \in [p]$ such that $i + 2 = i_s$. Consider this s.

From $i + 1 < i_r$, we obtain $i + 1 \leq i_r - 1$, so that $i + 2 \leq i_r$. Combining this with $i + 2 > i \geq \ell$, we find that $i + 2 \in [\ell, i_r]$. Thus, $i_s = i + 2 \in [\ell, i_r]$. However, the only numbers of the form i_t (with $t \in [0, p+1]$) that belong to the interval $[\ell, i_r]$ are $i_k, i_{k+1}, \ldots, i_r$ (because of (5)). Hence, from $i_s \in [\ell, i_r]$, we obtain $s \in [k, r]$. Therefore,

$$\begin{aligned} i + 1 &= i_s - 1 \qquad (\text{since } i + 2 = i_s) \\ &\in \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\} \qquad (\text{since } s \in [k, r]) \\ &\subseteq (I \setminus \{i_k, i_{k+1}, \ldots, i_r\}) \cup \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\}. \end{aligned}$$

Combined with $i + 1 \in [n]$, this results in

$$i + 1 \in ((I \setminus \{i_k, i_{k+1}, \ldots, i_r\}) \cup \{i_k - 1,\ i_{k+1} - 1,\ \ldots,\ i_r - 1\}) \cap [n] = K.$$

But this contradicts $i + 1 \notin K$. This contradiction shows that our assumption was false. Thus, (12) is proved.

Let us next consider Case 2. In this case, we have $i = \ell - 1$. Thus, $i = \ell - 1 < \ell \leq i_k$, so that $i \notin [i_k, i_r]$. Hence, from (11), we obtain $i \in I'$. Thus, $qs_i = q$ (since $q \in F(I)$). We must prove that $q's_i = q'$. This easily follows in the case when $\ell = n$ [8]. Hence, for the rest of Case 2, we WLOG assume that $\ell \neq n$. Therefore, $\ell \in [n-1]$. Moreover, $\ell = i + 1$ (since $i = \ell - 1$). Now, it is easy to see that $\ell \in I'$ [9]. Hence, $qs_\ell = q$ (since $q \in F(I)$). From $\ell \in I' = [n-1] \setminus (I \cup (I-1))$, we furthermore obtain $\ell \notin I \cup (I-1)$, so that $\ell \notin I$ and thus $\ell \neq i_r$ (because $i_r \in I$). Hence, $\ell < i_r$ (since $\ell \leq i_k \leq i_r$). Now, (9) rewrites as

$$q' = \sum_{j=i_r}^{i_{r+1}-1} \underbrace{qs_\ell s_{\ell+1} \cdots s_{j-1}}_{\substack{=(qs_\ell)\cdot s_{\ell+1}s_{\ell+2}\cdots s_{j-1} \\ \text{(since } \ell < i_r \leq j)}} = \sum_{j=i_r}^{i_{r+1}-1} \underbrace{(qs_\ell)}_{=q} \cdot s_{\ell+1}s_{\ell+2}\cdots s_{j-1}$$
$$= \sum_{j=i_r}^{i_{r+1}-1} qs_{\ell+1}s_{\ell+2}\cdots s_{j-1}. \tag{13}$$

From $i = \ell - 1 < \ell$, we see that s_i commutes with all the permutations $s_{\ell+1}, s_{\ell+2}, \ldots, s_{i_{r+1}-2}$ that appear on the right hand side of (13) (by reflection locality). Hence, multiplying the equality (13) by s_i, we find

$$q's_i = \sum_{j=i_r}^{i_{r+1}-1} q \underbrace{s_{\ell+1}s_{\ell+2}\cdots s_{j-1} \cdot s_i}_{\substack{=s_i \cdot s_{\ell+1}s_{\ell+2}\cdots s_{j-1} \\ \text{(since } s_i \text{ commutes with all of } s_{\ell+1}, s_{\ell+2}, \ldots, s_{j-1})}} = \sum_{j=i_r}^{i_{r+1}-1} \underbrace{qs_i}_{=q} \cdot s_{\ell+1}s_{\ell+2}\cdots s_{j-1}$$
$$= \sum_{j=i_r}^{i_{r+1}-1} qs_{\ell+1}s_{\ell+2}\cdots s_{j-1} = q' \qquad \text{(by (13))}.$$

We have thus proved $q's_i = q'$ in Case 2.

Let us now consider Case 3. In this case, we have $\ell \leq i < i_r$. It is easy to see that $i < i_r - 1$ [10]. Hence, $i + 1 < i_r \leq n$, so that $i + 1 \in [n-1]$. Also, $i \in [\ell, i_r - 1]$ (since $\ell \leq i < i_r$). Thus, (12) yields $i + 1 \in I'$. Hence, $qs_{i+1} = q$ (since $q \in F(I)$).

[8] *Proof.* Assume that $\ell = n$. Then, it is easy to see that the sum on the right hand side of (9) simplifies to q (since none of the $s_\ell, s_{\ell+1}, \ldots, s_{n-1}$ factors actually exist). Hence, (9) rewrites as $q' = q$. Thus, $q's_i = q'$ follows from $qs_i = q$, qed.

[9] *Proof.* Assume the contrary. Thus, $\ell \notin I' = [n-1] \setminus (I \cup (I-1))$ (by the definition of I'). Hence, $\ell \in I \cup (I-1)$ (since $\ell \in [n-1]$). In other words, $\ell \in I$ or $\ell + 1 \in I$. Since $\ell - 1 = i \in I' = [n-1] \setminus (I \cup (I-1))$, we have $\ell - 1 \notin I \cup (I-1)$, so that $\ell - 1 \notin I$ and $\ell \notin I$. In particular, $\ell \notin I$. Hence, $\ell + 1 \in I$ (since we just showed that $\ell \in I$ or $\ell + 1 \in I$). Combining $\ell \notin I$ and $\ell + 1 \in I$, we obtain $i_k = \ell + 1$ (by the definition of i_k). In other words, $i_k - 1 = \ell$. However, $i_k - 1 \in K$ (by the definition of K). In other words, $\ell \in K$ (since $i_k - 1 = \ell$). But this contradicts $\ell = i + 1 \notin K$. This contradiction shows that our assumption was false, qed.

[10] *Proof.* The construction of K yields $i_r - 1 \in K$ (unless $i_r - 1 = 0$). Hence, we cannot have $i = i_r - 1$ (since this would imply $i = i_r - 1 \in K$, which would contradict $i \notin K$). However, from $i < i_r$, we obtain $i \leq i_r - 1$. Thus, $i < i_r - 1$ (since we cannot have $i = i_r - 1$).

Let $j \in [i_r, i_{r+1} - 1]$. Then, $i_r \leq j \leq i_{r+1} - 1$, so that $i < \underbrace{i_r}_{\leq j} - 1 \leq j - 1$. Hence, $i \in [\ell, j - 2]$ (since $\ell \leq i$). Also, $j \in [i_r, i_{r+1} - 1] \subseteq [n]$. Therefore,

$$\begin{aligned} q \underbrace{s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i}_{\substack{= s_{i+1} \cdot s_\ell s_{\ell+1} \cdots s_{j-1} \\ \text{(by Lemma 6.1)}}} &= \underbrace{q s_{i+1}}_{=q} \cdot s_\ell s_{\ell+1} \cdots s_{j-1} \\ &= q s_\ell s_{\ell+1} \cdots s_{j-1}. \end{aligned} \tag{14}$$

Forget that we fixed j. We thus have proved (14) for each $j \in [i_r, i_{r+1} - 1]$. Now, multiplying the equality (9) by s_i, we find

$$q' s_i = \sum_{j=i_r}^{i_{r+1}-1} \underbrace{q s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i}_{\substack{= q s_\ell s_{\ell+1} \cdots s_{j-1} \\ \text{(by (14))}}} = \sum_{j=i_r}^{i_{r+1}-1} q s_\ell s_{\ell+1} \cdots s_{j-1} = q'.$$

We have thus proved $q' s_i = q'$ in Case 3.

Next, let us consider Case 4. In this case, we have $i_r \leq i < i_{r+1}$. It is easy to see that the latter inequality can be strengthened to $i < i_{r+1} - 1$ [11]. In other words, $i + 1 \leq i_{r+1} - 1$. Thus, both i and $i + 1$ belong to the interval $[i_r, i_{r+1} - 1]$ (since $i_r \leq i < i + 1$).

Now, we make the following three claims:

- *Claim 1:* For any $j \in [i_r, i_{r+1} - 1] \setminus \{i, i+1\}$, we have
$$q s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i = q s_\ell s_{\ell+1} \cdots s_{j-1}.$$
- *Claim 2:* We have
$$q s_\ell s_{\ell+1} \cdots s_{i-1} \cdot s_i = q s_\ell s_{\ell+1} \cdots s_i.$$
- *Claim 3:* We have
$$q s_\ell s_{\ell+1} \cdots s_i \cdot s_i = q s_\ell s_{\ell+1} \cdots s_{i-1}.$$

Note that Claim 2 is trivial, while Claim 3 follows from $s_i^2 = \mathrm{id}$. Let us now prove Claim 1:

[*Proof of Claim 1:* Fix some $j \in [i_r, i_{r+1} - 1] \setminus \{i, i+1\}$. Thus, $j \in [i_r, i_{r+1} - 1]$ and $j \notin \{i, i+1\}$. The latter fact reveals that either $j < i$ or $j > i + 1$. This means that we are in one of two subcases, which we consider separately:

[11] *Proof.* We have $i \in [n-1]$ and thus $i < n$. If $r + 1 = p + 1$, then $i_{r+1} = i_{p+1} = n + 1$ and thus $i_{r+1} - 1 = n$, whence $i < n = i_{r+1} - 1$. Thus, for the rest of this proof, we WLOG assume that we don't have $r + 1 = p + 1$. Hence, $r + 1 \in [p]$. Thus, $i_{r+1} \in \{i_1 < i_2 < \cdots < i_p\} = I$. If we had $i + 1 = i_{r+1}$, then we would thus have $i + 1 = i_{r+1} \in I$, which would contradict (10). Hence, we cannot have $i + 1 = i_{r+1}$. Thus, we have $i + 1 \neq i_{r+1}$, so that $i \neq i_{r+1} - 1$. However, $i \leq i_{r+1} - 1$ (since $i < i_{r+1}$). Combining these two facts, we obtain $i < i_{r+1} - 1$.

- Let us first consider the subcase when $j < i$. In this subcase, s_i commutes with each of $s_\ell, s_{\ell+1}, \ldots, s_{j-1}$ (by reflection locality). Thus, $s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i = s_i \cdot s_\ell s_{\ell+1} \cdots s_{j-1}$. Also, $j < i$ entails $i > j \geq i_r$ (since $j \in [i_r, i_{r+1} - 1]$). Hence, $i \notin [i_k, i_r]$. Therefore, (11) yields $i \in I'$. Thus, $qs_i = q$ (since $q \in F(I)$). Now,

$$q \underbrace{s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i}_{= s_i \cdot s_\ell s_{\ell+1} \cdots s_{j-1}} = \underbrace{qs_i}_{=q} \cdot s_\ell s_{\ell+1} \cdots s_{j-1} = qs_\ell s_{\ell+1} \cdots s_{j-1}.$$

  We have thus proved Claim 1 in the subcase when $j < i$.

- Let us now consider the subcase when $j > i + 1$. In this subcase, we have $i < j - 1$ and thus $i \leq j - 2$. Combining this with $\ell \leq i_r \leq i$, we obtain $i \in [\ell, j - 2]$. Hence, Lemma 6.1 yields $s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i = s_{i+1} \cdot s_\ell s_{\ell+1} \cdots s_{j-1}$ (since $j \in [i_r, i_{r+1} - 1] \subseteq [n]$). Moreover, from $j \in [i_r, i_{r+1} - 1] \subseteq [n]$, we obtain $j \leq n$, so that $n \geq j > i + 1$. Hence, $i + 1 < n$, so that $i + 1 \in [n - 1]$.

  Furthermore, $i_r \leq i < i + 1$. On the other hand, from $j > i + 1$, we obtain $i + 1 < j \leq i_{r+1} - 1$ (since $j \in [i_r, i_{r+1} - 1]$), so that $i + 2 < i_{r+1}$. Hence, $i_r < i + 1 < i + 2 < i_{r+1}$. This chain of inequalities shows that both numbers $i + 1$ and $i + 2$ lie strictly between the two numbers i_r and i_{r+1}, which are two adjacent elements of the enclosure $\widehat{I}$ (in the sense that there are no further elements of $\widehat{I}$ between them). Hence, neither $i + 1$ nor $i + 2$ can belong to $\widehat{I}$. Thus, neither $i + 1$ nor $i + 2$ can belong to I (since $I \subseteq \widehat{I}$). In other words, $i + 1 \notin I \cup (I - 1)$. Since $i + 1 \in [n - 1]$, we thus obtain $i + 1 \in [n - 1] \setminus (I \cup (I - 1)) = I'$ (by the definition of I'). Thus, $qs_{i+1} = q$ (since $q \in F(I)$). Now,

$$q \underbrace{s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i}_{= s_{i+1} \cdot s_\ell s_{\ell+1} \cdots s_{j-1}} = \underbrace{qs_{i+1}}_{=q} \cdot s_\ell s_{\ell+1} \cdots s_{j-1} = qs_\ell s_{\ell+1} \cdots s_{j-1}.$$

  We have thus proved Claim 1 in the subcase when $j > i + 1$.

We have now covered both possible subcases. Hence, Claim 1 is proved.]

We have now proved all three Claims 1, 2 and 3. Now, consider the sum $\sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}$. This sum contains both an addend for $j = i$ and an addend for $j = i + 1$ (since both i and $i + 1$ belong to the interval $[i_r, i_{r+1} - 1]$). When we multiply this sum by s_i on the right (i.e., when we replace it by $\sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i$), the addend for $j = i$ becomes $qs_\ell s_{\ell+1} \cdots s_{i-1} \cdot s_i = qs_\ell s_{\ell+1} \cdots s_i$ (by Claim 2), whereas the addend for $j = i + 1$ becomes $qs_\ell s_{\ell+1} \cdots s_i \cdot s_i = qs_\ell s_{\ell+1} \cdots s_{i-1}$ (by Claim 3), and all remaining addends stay unchanged (by Claim 1). Hence, multiplying the sum $\sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}$ by s_i on the right merely permutes its addends (specifically, the addend for $j = i$ is swapped with the addend for $j = i + 1$, while all other addends stay unchanged) and therefore does not change the sum. In other words, we have

$$\sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i = \sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}.$$

Since $q' = \sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}$, this rewrites as $q's_i = q'$. Thus, we have proved $q's_i = q'$ in Case 4.

Finally, let us consider Case 5. In this case, we have $i \geq i_{r+1}$. Thus, $i \geq i_{r+1} > i_r$ (since $i_0 < i_1 < i_2 < \cdots < i_p < i_{p+1}$), so that $i \notin [i_k, i_r]$. Hence, from (11), we obtain $i \in I'$. Thus, $qs_i = q$ (since $q \in F(I)$). Furthermore, from $i \geq i_{r+1}$, we see that s_i commutes with all the permutations $s_\ell, s_{\ell+1}, \ldots, s_{i_{r+1}-2}$ that appear on the right hand side of (9) (by reflection locality). Hence, multiplying the equality (9) by s_i, we find

$$\begin{aligned} q's_i &= \sum_{j=i_r}^{i_{r+1}-1} q \underbrace{s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i}_{\substack{= s_i \cdot s_\ell s_{\ell+1} \cdots s_{j-1} \\ \text{(since } s_i \text{ commutes with all of } s_\ell, s_{\ell+1}, \ldots, s_{j-1})}} = \sum_{j=i_r}^{i_{r+1}-1} \underbrace{qs_i}_{=q} \cdot s_\ell s_{\ell+1} \cdots s_{j-1} \\ &= \sum_{j=i_r}^{i_{r+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1} = q'. \end{aligned}$$

We have thus proved $q's_i = q'$ in Case 5.

We have now proved $q's_i = q'$ in all five cases. Thus, $q's_i = q'$ always holds. As explained above, this completes the proof of $q' \in F(K)$. Therefore, $q' \in F(K) \subseteq F(< \operatorname{sum} I)$. But this is precisely what we needed to prove. Thus, Theorem 7.3 is proven. □

8. The Fibonacci filtration

In this section, we shall build a filtration of $\mathbf{k}[S_n]$ by $\mathbf{k}$-submodules that are invariant under the somewhere-to-below shuffles $R(t_\ell)$, which furthermore has the property that the latter shuffles act as scalars on the subquotients of the filtration. This filtration will be built up from the submodules $F(I)$ defined in the previous section, and its properties will rely on Theorem 7.3.

8.1. Definition and examples

Recall from Section 5 that the number of lacunar subsets of $[n-1]$ is f_{n+1}. Let $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ be all these f_{n+1} lacunar subsets of $[n-1]$, listed in an order that satisfies

$$\operatorname{sum}(Q_1) \leq \operatorname{sum}(Q_2) \leq \cdots \leq \operatorname{sum}\left(Q_{f_{n+1}}\right). \tag{15}$$

Then, define a $\mathbf{k}$-submodule

$$F_i := F(Q_1) + F(Q_2) + \cdots + F(Q_i) \qquad \text{of } \mathbf{k}[S_n]$$

for each $i \in [0, f_{n+1}]$ (so that $F_0 = 0$). We claim the following:

Theorem 8.1.

(a) We have
$$0 = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}} = \mathbf{k}[S_n].$$
In other words, the $\mathbf{k}$-submodules $F_0, F_1, \ldots, F_{f_{n+1}}$ form a $\mathbf{k}$-module filtration of $\mathbf{k}[S_n]$.

(b) We have $F_i \cdot t_\ell \subseteq F_i$ for each $i \in [0, f_{n+1}]$ and $\ell \in [n]$.

(c) For each $i \in [f_{n+1}]$ and $\ell \in [n]$, we have
$$F_i \cdot \left(t_\ell - m_{Q_i,\ell}\right) \subseteq F_{i-1}.$$

We will eventually prove this theorem; we will also show that each F_i is a free $\mathbf{k}$-module, so that its dimension $\dim F_i$ (also known as its rank) is well-defined whenever $\mathbf{k} \neq 0$. First, let us tabulate the dimensions of the $F_0, F_1, \ldots, F_{f_{n+1}}$ for some small values of n:

Example 8.2. Let $n = 3$. Then, the lacunar subsets of $[n-1]$ are $Q_1 = \varnothing$ and $Q_2 = \{1\}$ and $Q_3 = \{2\}$ (this is the only possible ordering that satisfies (15), because no two lacunar subsets of $[n-1]$ have the same sum). The corresponding $F(I)$'s have already been computed in Example 7.1. Here are some properties of the corresponding F_i's:

i	1	2	3
Q_i	$\varnothing$	$\{1\}$	$\{2\}$
Q_i'	$\{1,2\}$	$\{2\}$	$\varnothing$
$\dim F_i$	1	3	6
$\dim F_i - \dim F_{i-1}$	1	2	3

Of course, $F_0 = 0$, so we are not showing an $i = 0$ column.

Example 8.3. Let $n = 4$. Then, the lacunar subsets of $[n-1]$ are $Q_1 = \varnothing$ and $Q_2 = \{1\}$ and $Q_3 = \{2\}$ and $Q_4 = \{3\}$ and $Q_5 = \{1,3\}$ (again, there is no other ordering). Here are some properties of the corresponding F_i's:

i	1	2	3	4	5
Q_i	$\varnothing$	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,3\}$
Q'_i	$\{1,2,3\}$	$\{2,3\}$	$\{3\}$	$\{1\}$	$\varnothing$
$\dim F_i$	1	4	12	18	24
$\dim F_i - \dim F_{i-1}$	1	3	8	6	6

Example 8.4. Let $n = 5$. Then, the lacunar subsets of $[n-1]$ are $Q_1 = \varnothing$ and $Q_2 = \{1\}$ and $Q_3 = \{2\}$ and $Q_4 = \{3\}$ and $Q_5 = \{4\}$ and $Q_6 = \{1,3\}$ and $Q_7 = \{1,4\}$ and $Q_8 = \{2,4\}$ (this is one of two possible orderings; another can be obtained by swapping Q_5 with Q_6). Here are some properties of the corresponding F_i's:

i	1	2	3	4	5	6	7	8
Q_i	$\varnothing$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{1,3\}$	$\{1,4\}$	$\{2,4\}$
Q'_i	$\{1,2,3,4\}$	$\{2,3,4\}$	$\{3,4\}$	$\{1,4\}$	$\{1,2\}$	$\{4\}$	$\{2\}$	$\varnothing$
$\dim F_i$	1	5	20	40	50	70	90	120
$\dim F_i - \dim F_{i-1}$	1	4	15	20	10	20	20	30

.

Example 8.5. Let $n = 6$. Then, the lacunar subsets of $[n-1]$ (in one of several orderings) can be found in the following table:

i	1	2	3	4	5	6	7	8	9	10	11	12	13
Q_i	$\varnothing$	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{1,3\}$	$\{5\}$	$\{1,4\}$	$\{1,5\}$	$\{2,4\}$	$\{2,5\}$	$\{3,5\}$	$\{1,3,5\}$
d_i	1	6	30	75	115	160	175	255	300	420	540	630	720
δ_i	1	5	24	45	40	45	15	80	45	120	120	90	90

,

where we set $d_i := \dim F_i$ and $\delta_i := \dim F_i - \dim F_{i-1}$ for brevity. (We have not listed the sets Q'_i to avoid stretching the table too much.)

When $\mathbf{k}$ is a field, Theorem 8.1 entails that the endomorphisms $R(t_1), R(t_2), \ldots, R(t_n)$ on $\mathbf{k}[S_n]$ can be simultaneously triangularized (as endomorphisms of the $\mathbf{k}$-module $\mathbf{k}[S_n]$). Thus, in particular, any $\mathbf{k}$-linear combination $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ of $R(t_1), R(t_2), \ldots, R(t_n)$ has all its eigenvalues in $\mathbf{k}$. However, we will later prove this more generally, without assuming that $\mathbf{k}$ is a field, by explicitly constructing a basis of $\mathbf{k}[S_n]$ that triangularizes $R(t_1), R(t_2), \ldots, R(t_n)$.

8.2. Properties of non-shadows

So far, it may seem mysterious that the definition of our filtration $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}}$ relies only on the $F(I)$ for the lacunar subsets I of $[n-1]$, rather than using the $F(I)$ for all subsets I of $[n]$. The reason for this is the observation (Corollary 8.8 further below) that the lacunar subsets I of $[n-1]$ are "enough" (i.e., the $F(I)$ for which I is not a lacunar subset of $[n-1]$ "contribute nothing new" to the filtration). More precisely, each $F(I)$ (for any $I \subseteq [n]$) is contained in the sum of the $F(J)$ where $J \subseteq [n-1]$ is lacunar and satisfies $\operatorname{sum} J \leq \operatorname{sum} I$.

Before we can prove this, we shall show a few combinatorial properties of non-shadows.

Proposition 8.6. Let I be a subset of $[n]$. Let $j \in I$. Set $K := (I \setminus \{j\}) \cup \{j-1\}$ if $j > 1$, and otherwise set $K := I \setminus \{j\}$. Then:

(a) We have $K' \subseteq I' \cup \{j\}$.

(b) If $j+1 \in I$, then $K' \subseteq I'$.

Proof. **(a)** Let $g \in K' \setminus \{j\}$. We shall show that $g \in I'$.

Indeed, we have $g \in K' \setminus \{j\}$. In other words, $g \in K'$ and $g \neq j$. Now, $g \in K' = [n-1] \setminus (K \cup (K-1))$ (by the definition of K'). In other words, $g \in [n-1]$ and $g \notin K \cup (K-1)$. From $g \notin K \cup (K-1)$, we obtain $g \notin K$ and $g+1 \notin K$.

However, the construction of K yields $I \setminus \{j\} \subseteq K$.

If we had $g \in I$, then we would have $g \in I \setminus \{j\}$ (since $g \in I$ and $g \neq j$), which would entail $g \in I \setminus \{j\} \subseteq K$, contradicting $g \notin K$. Hence, we cannot have $g \in I$. Thus, we have $g \notin I$.

We shall now show that $g+1 \notin I$. Indeed, let us assume the contrary. Then, $g+1 \in I$. If we had $g+1 \neq j$, then we would have $g+1 \in I \setminus \{j\}$ (since $g+1 \in I$ and $g+1 \neq j$), which would entail $g+1 \in I \setminus \{j\} \subseteq K$, contradicting $g+1 \notin K$. Hence, we cannot have $g+1 \neq j$. Thus, we must have $g+1 = j$, so that $g = j-1$ and thus $j-1 = g \in [n-1]$. Hence, $j-1 \geq 1$, so that $j \geq 2$. Thus, the definition of K yields $K = (I \setminus \{j\}) \cup \{j-1\}$. Consequently, $j-1 \in K$. But this contradicts $j-1 = g \notin K$. This contradiction shows that our assumption was false. Hence, $g+1 \notin I$ is proved.

Now, we know that $g \in [n-1]$ satisfies $g \notin I$ and $g+1 \notin I$. In other words, $g \in I'$ (by the definition of I').

Forget that we fixed g. We thus have shown that $g \in I'$ for each $g \in K' \setminus \{j\}$. In other words, $K' \setminus \{j\} \subseteq I'$. Hence,

$$K' \subseteq \underbrace{(K' \setminus \{j\})}_{\subseteq I'} \cup \{j\} \subseteq I' \cup \{j\}.$$

This proves Proposition 8.6 **(a)**.

(b) Assume that $j+1 \in I$. Thus, $j+1 \in I \setminus \{j\}$ (since $j+1 \neq j$). However, the definition of K yields $K \supseteq I \setminus \{j\}$. Thus, $j+1 \in I \setminus \{j\} \subseteq K$. Hence, $j \in K-1 \subseteq K \cup (K-1)$, so that $j \notin [n-1] \setminus (K \cup (K-1))$. In other words, $j \notin K'$ (since $K' = [n-1] \setminus (K \cup (K-1))$). Hence, $K' \setminus \{j\} = K'$ and therefore

$$K' = \underbrace{K'}_{\substack{\subseteq I' \cup \{j\} \\ \text{(by Proposition 8.6 (a))}}} \setminus \{j\} \subseteq \left(I' \cup \{j\}\right) \setminus \{j\} \subseteq I'.$$

This proves Proposition 8.6 **(b)**. □

Proposition 8.7. Let $I \subseteq [n]$. Assume that I is not a lacunar subset of $[n-1]$. Then, there exists a subset K of $[n]$ such that $\operatorname{sum} K < \operatorname{sum} I$ and $K' \subseteq I'$.

Proof. We have assumed that I is not a lacunar subset of $[n-1]$. Thus, we are in one of the following two cases:

Case 1: The set I is not a subset of $[n-1]$.

Case 2: The set I is not lacunar.

Let us first consider Case 1. In this case, the set I is not a subset of $[n-1]$. Hence, we have $n \in I$ (since $I \subseteq [n]$). Let $K := (I \setminus \{n\}) \cup \{n-1\}$ (or just $K := I \setminus \{n\}$ in the case when $n \leq 1$). Then,

$$\begin{aligned} \operatorname{sum} K &\leq \operatorname{sum} I - n + (n-1) \\ &\qquad \text{(since } n \in I \text{, but } n-1 \text{ may or may not belong to } I\text{)} \\ &= \operatorname{sum} I - 1 < \operatorname{sum} I. \end{aligned}$$

However, Proposition 8.6 **(a)** (applied to $j = n$) yields $K' \subseteq I' \cup \{n\}$ (since $n \in I$). From this, we easily obtain $K' \subseteq I'$ [12]. Hence, Proposition 8.7 is proved in Case 1.

Let us now consider Case 2. In this case, the set I is not lacunar. In other words, I contains two consecutive integers $q-1$ and q. Consider these $q-1$ and q. Let $K := (I \setminus \{q-1\}) \cup \{q-2\}$ (or just $K := I \setminus \{q-1\}$ in the case when $q-2 = 0$). Then, $\operatorname{sum} K < \operatorname{sum} I$ (similarly to Case 1). However, Proposition 8.6 **(b)** (applied to $j = q-1$) yields $K' \subseteq I'$ (since $q-1 \in I$ and $(q-1)+1 = q \in I$). Hence, Proposition 8.7 is proved in Case 2.

We now have proved Proposition 8.7 in both Cases 1 and 2. □

Roughly speaking, Proposition 8.7 tells us that if a subset I of $[n]$ is not a lacunar subset of $[n-1]$, then we can replace it by a subset K that has a smaller sum (i.e.,

[12] *Proof:* The definition of K' yields $K' = [n-1] \setminus (K \cup (K-1)) \subseteq [n-1]$. Combining this with $K' \subseteq I' \cup \{n\}$, we obtain

$$K' \subseteq [n-1] \cap \left(I' \cup \{n\}\right) = \underbrace{([n-1] \cap I')}_{\subseteq I'} \cup \underbrace{([n-1] \cap \{n\})}_{=\varnothing} \subseteq I'.$$

satisfies $\operatorname{sum} K < \operatorname{sum} I$) and a non-shadow that is contained in that of I. The latter subset K may or may not be a lacunar subset of $[n-1]$. If it is not, then we can apply Proposition 8.7 to it again. Repeatedly applying Proposition 8.7 like this, we obtain the following corollary:

Corollary 8.8. Let $I \subseteq [n]$. Then, there exists a lacunar subset J of $[n-1]$ such that $\operatorname{sum} J \leq \operatorname{sum} I$ and $J' \subseteq I'$.

Proof. We proceed by strong induction on $\operatorname{sum} I$. Thus, we fix some $I \subseteq [n]$. We must prove that there exists a lacunar subset J of $[n-1]$ satisfying $\operatorname{sum} J \leq \operatorname{sum} I$ and $J' \subseteq I'$.

If I itself is a lacunar subset of $[n-1]$, then taking $J = I$ suffices. Thus, assume that I is not. Hence, Proposition 8.7 yields that there exists a subset K of $[n]$ such that $\operatorname{sum} K < \operatorname{sum} I$ and $K' \subseteq I'$. Consider this K. Because of $\operatorname{sum} K < \operatorname{sum} I$, we can apply the induction hypothesis to K instead of I. We thus conclude that there exists a lacunar subset J of $[n-1]$ such that $\operatorname{sum} J \leq \operatorname{sum} K$ and $J' \subseteq K'$. This lacunar subset J satisfies $\operatorname{sum} J \leq \operatorname{sum} I$ (since $\operatorname{sum} J \leq \operatorname{sum} K < \operatorname{sum} I$) and $J' \subseteq I'$ (since $J' \subseteq K' \subseteq I'$). Hence, it is precisely the kind of subset that we were looking for. This completes the induction step, and therefore Corollary 8.8 is proved. $\square$

Corollary 8.8 is largely responsible for the fact that the filtration in Theorem 8.1 uses only the lacunar subsets of $[n-1]$ (rather than all subsets of $[n]$).

Next, we observe an essentially obvious fact: If A and B are two subsets of $[n]$ satisfying $B' \subseteq A'$, then

$$F(A) \subseteq F(B). \tag{16}$$

(This follows directly from the definition of $F(I)$ in terms of I', given at the beginning of Section 7.)

Corollary 8.9. Let $k \in \mathbb{N}$. Then,

$$F(<k) = \sum_{\substack{J \subseteq [n-1] \text{ is lacunar;} \\ \operatorname{sum} J < k}} F(J).$$

Proof. The definition of $F(<k)$ yields

$$F(<k) = \sum_{\substack{J \subseteq [n]; \\ \operatorname{sum} J < k}} F(J) = \sum_{\substack{I \subseteq [n]; \\ \operatorname{sum} I < k}} F(I).$$

Now, we shall show the following claim:

> *Claim 1:* For each $I \subseteq [n]$ satisfying $\operatorname{sum} I < k$, there exists some lacunar $J \subseteq [n-1]$ satisfying $\operatorname{sum} J < k$ and $F(I) \subseteq F(J)$.

[*Proof of Claim 1:* Let $I \subseteq [n]$ satisfy $\operatorname{sum} I < k$. Then, Corollary 8.8 yields that there exists a lacunar subset J of $[n-1]$ such that $\operatorname{sum} J \leq \operatorname{sum} I$ and $J' \subseteq I'$. This lacunar subset J then clearly satisfies $\operatorname{sum} J \leq \operatorname{sum} I < k$ and $F(I) \subseteq F(J)$ (by (16), applied to $A = I$ and $B = J$). Thus, Claim 1 follows.]

Claim 1 shows that each addend of the sum $\sum\limits_{\substack{I \subseteq [n]; \\ \operatorname{sum} I < k}} F(I)$ is a subset of some addend of the sum $\sum\limits_{\substack{J \subseteq [n-1] \text{ is lacunar}; \\ \operatorname{sum} J < k}} F(J)$. Hence, we have

$$\sum_{\substack{I \subseteq [n]; \\ \operatorname{sum} I < k}} F(I) \subseteq \sum_{\substack{J \subseteq [n-1] \text{ is lacunar}; \\ \operatorname{sum} J < k}} F(J).$$

Combining this inclusion with the reverse inclusion

$$\sum_{\substack{J \subseteq [n-1] \text{ is lacunar}; \\ \operatorname{sum} J < k}} F(J) \subseteq \sum_{\substack{I \subseteq [n]; \\ \operatorname{sum} I < k}} F(I)$$

(which is obvious, since the left hand side is a sub-sum of the right hand side), we obtain

$$\sum_{\substack{I \subseteq [n]; \\ \operatorname{sum} I < k}} F(I) = \sum_{\substack{J \subseteq [n-1] \text{ is lacunar}; \\ \operatorname{sum} J < k}} F(J).$$

Thus,

$$F(<k) = \sum_{\substack{I \subseteq [n]; \\ \operatorname{sum} I < k}} F(I) = \sum_{\substack{J \subseteq [n-1] \text{ is lacunar}; \\ \operatorname{sum} J < k}} F(J).$$

This proves Corollary 8.9. □

We now have the tools to restrict our study of the $\mathbf{k}$-submodules $F(I)$ to the sets I that are lacunar subsets of $[n-1]$.

8.3. Proof of the filtration

Using the properties of non-shadows that we just established, we can prove Theorem 8.1, which gives a filtration of $\mathbf{k}[S_n]$ preserved by the somewhere-to-below shuffles.

Proof of Theorem 8.1. We must establish the following three claims:

Claim 1: We have $0 = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}} = \mathbf{k}[S_n]$.

Claim 2: We have $F_i \cdot t_\ell \subseteq F_i$ for each $i \in [0, f_{n+1}]$ and $\ell \in [n]$.

Claim 3: For each $i \in [f_{n+1}]$ and $\ell \in [n]$, we have

$$F_i \cdot \left(t_\ell - m_{Q_i,\ell}\right) \subseteq F_{i-1}.$$

First of all, let us show an auxiliary claim:

Claim 0: Let $k \in \mathbb{N}$. Let i_k be the largest $i \in [f_{n+1}]$ satisfying $\operatorname{sum}(Q_i) < k$ (or 0 if no such i exists). Then, $F(<k) = F_{i_k}$.

[*Proof of Claim 0:* Recall that $\operatorname{sum}(Q_1) \leq \operatorname{sum}(Q_2) \leq \cdots \leq \operatorname{sum}\left(Q_{f_{n+1}}\right)$. Thus, the inequality $\operatorname{sum}(Q_i) < k$ holds for each $i \leq i_k$ but does not hold for any other i (because i_k is the largest $i \in [f_{n+1}]$ satisfying $\operatorname{sum}(Q_i) < k$). Therefore, the lacunar subsets J of $[n-1]$ satisfying $\operatorname{sum} J < k$ are precisely $Q_1, Q_2, \ldots, Q_{i_k}$ (since $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are all the lacunar subsets of $[n-1]$). Hence,

$$\sum_{\substack{J \subseteq [n-1] \text{ is lacunar;} \\ \operatorname{sum} J < k}} F(J) = F(Q_1) + F(Q_2) + \cdots + F\left(Q_{i_k}\right) = F_{i_k}$$

(by the definition of F_{i_k}). However, Corollary 8.9 yields

$$F(<k) = \sum_{\substack{J \subseteq [n-1] \text{ is lacunar;} \\ \operatorname{sum} J < k}} F(J) = F_{i_k}.$$

Thus, Claim 0 is proved.]

We can now easily prove Claims 1, 3 and 2 in this order:

[*Proof of Claim 1:* From the construction of the modules F_i, it is clear that $0 = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}}$. We thus only need to prove $F_{f_{n+1}} = \mathbf{k}[S_n]$.

Let $k = \dbinom{n}{2} + 1$. Then, $\operatorname{sum}[n] = \dbinom{n}{2} < k$, so that $F([n]) \subseteq F(<k)$ (by the definition of $F(<k)$). Let i_k be the largest $i \in [f_{n+1}]$ satisfying $\operatorname{sum}(Q_i) < k$. Hence, Claim 0 yields $F(<k) = F_{i_k}$. Consider this i_k. However, $F([n]) = \mathbf{k}[S_n]$ because the non-shadow $[n]' = \varnothing$. Thus, $\mathbf{k}[S_n] = F([n]) \subseteq F(<k) = F_{i_k} \subseteq F_{f_{n+1}}$ (because $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}}$). Thus, $F_{f_{n+1}} = \mathbf{k}[S_n]$ (since $F_{f_{n+1}} \subseteq \mathbf{k}[S_n]$). The proof of Claim 1 is thus finished.]

[*Proof of Claim 3:* Let $i \in [f_{n+1}]$ and $\ell \in [n]$. We must prove that $F_i \cdot \left(t_\ell - m_{Q_i,\ell}\right) \subseteq F_{i-1}$.

The definition of F_{i-1} yields $F_{i-1} = F(Q_1) + F(Q_2) + \cdots + F(Q_{i-1})$. Now, it is easy to see that

$$F(<\operatorname{sum}(Q_k)) \subseteq F_{i-1} \tag{17}$$

for each $k \in [i]$ [13].

The definition of F_i yields $F_i = F(Q_1) + F(Q_2) + \cdots + F(Q_i) = \sum_{k=1}^{i} F(Q_k)$. Thus,

$$\begin{aligned}
F_i \cdot (t_\ell - m_{Q_i,\ell}) &= \sum_{k=1}^{i} F(Q_k) \cdot \underbrace{(t_\ell - m_{Q_i,\ell})}_{=(t_\ell - m_{Q_k,\ell}) + (m_{Q_k,\ell} - m_{Q_i,\ell})} \\
&= \sum_{k=1}^{i} \underbrace{F(Q_k) \cdot ((t_\ell - m_{Q_k,\ell}) + (m_{Q_k,\ell} - m_{Q_i,\ell}))}_{\subseteq F(Q_k) \cdot (t_\ell - m_{Q_k,\ell}) + F(Q_k) \cdot (m_{Q_k,\ell} - m_{Q_i,\ell})} \\
&\subseteq \sum_{k=1}^{i} \left(F(Q_k) \cdot (t_\ell - m_{Q_k,\ell}) + F(Q_k) \cdot (m_{Q_k,\ell} - m_{Q_i,\ell}) \right) \\
&= \sum_{k=1}^{i} F(Q_k) \cdot (t_\ell - m_{Q_k,\ell}) + \underbrace{\sum_{k=1}^{i} F(Q_k) \cdot (m_{Q_k,\ell} - m_{Q_i,\ell})}_{\substack{= \sum_{k=1}^{i-1} F(Q_k) \cdot (m_{Q_k,\ell} - m_{Q_i,\ell}) \\ \text{(here, we have removed the addend} \\ \text{for } k=i\text{, since this addend is 0)}}} \\
&= \sum_{k=1}^{i} \underbrace{F(Q_k) \cdot (t_\ell - m_{Q_k,\ell})}_{\substack{\subseteq F(<\operatorname{sum}(Q_k)) \\ \text{(by Theorem 7.3,} \\ \text{applied to } I=Q_k)}} + \sum_{k=1}^{i-1} \underbrace{F(Q_k) \cdot (m_{Q_k,\ell} - m_{Q_i,\ell})}_{\substack{\subseteq F(Q_k) \\ \text{(since } m_{Q_k,\ell} - m_{Q_i,\ell} \text{ is just a scalar)}}} \\
&\subseteq \sum_{k=1}^{i} \underbrace{F(< \operatorname{sum}(Q_k))}_{\substack{\subseteq F_{i-1} \\ \text{(by (17))}}} + \underbrace{\sum_{k=1}^{i-1} F(Q_k)}_{\substack{= F(Q_1) + F(Q_2) + \cdots + F(Q_{i-1}) \\ = F_{i-1} \\ \text{(by the definition of } F_{i-1})}} \\
&\subseteq \sum_{k=1}^{i} F_{i-1} + F_{i-1} \subseteq F_{i-1}.
\end{aligned}$$

This proves Claim 3.]

[13] *Proof:* Let $k \in [i]$. Let $j = \operatorname{sum}(Q_k)$. Let i_j be the largest $\mathfrak{i} \in [f_{n+1}]$ satisfying $\operatorname{sum}(Q_\mathfrak{i}) < j$ (or 0 if no such $\mathfrak{i}$ exists). Then, Claim 0 (applied to j instead of k) yields $F(<j) = F_{i_j}$. In view of $j = \operatorname{sum}(Q_k)$, this rewrites as $F(< \operatorname{sum}(Q_k)) = F_{i_j}$.

However, recall that i_j is the largest $\mathfrak{i} \in [f_{n+1}]$ satisfying $\operatorname{sum}(Q_\mathfrak{i}) < j$. Thus, $\operatorname{sum}(Q_\mathfrak{i}) < j$ for each $\mathfrak{i} \leq i_j$ (because $\operatorname{sum}(Q_1) \leq \operatorname{sum}(Q_2) \leq \cdots \leq \operatorname{sum}(Q_{f_{n+1}})$). Since we **don't** have $\operatorname{sum}(Q_k) < j$ (because $j = \operatorname{sum}(Q_k)$), we thus cannot have $k \leq i_j$. Hence, we have $i_j < k$, so that $i_j \leq k-1 \leq i-1$ (because $k \leq i$). Hence, $F_{i_j} \subseteq F_{i-1}$. Now, $F(< \operatorname{sum}(Q_k)) = F_{i_j} \subseteq F_{i-1}$. This proves (17).

[*Proof of Claim 2:* Let $i \in [0, f_{n+1}]$ and $\ell \in [n]$. We must prove that $F_i \cdot t_\ell \subseteq F_i$. If $i = 0$, then this is clearly true (since $F_0 = 0$). Thus, we WLOG assume that $i \neq 0$. Hence, $i \in [f_{n+1}]$. Thus, Claim 3 yields $F_i \cdot (t_\ell - m_{Q_i,\ell}) \subseteq F_{i-1}$. Now,

$$\begin{aligned} F_i \cdot \underbrace{t_\ell}_{=(t_\ell - m_{Q_i,\ell}) + m_{Q_i,\ell}} &= F_i \cdot \left((t_\ell - m_{Q_i,\ell}) + m_{Q_i,\ell} \right) \\ &\subseteq \underbrace{F_i \cdot (t_\ell - m_{Q_i,\ell})}_{\subseteq F_{i-1} \subseteq F_i} + \underbrace{F_i \cdot m_{Q_i,\ell}}_{\substack{\subseteq F_i \\ \text{(since } m_{Q_i,\ell} \text{ is a scalar)}}} \\ &\subseteq F_i + F_i \subseteq F_i. \end{aligned}$$

This proves Claim 2.]

We have now proved all Claims 1, 2 and 3. This proves Theorem 7.3. □

9. The descent-destroying basis of $\mathbf{k}[S_n]$

We will now analyze the filtration $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}}$ from Theorem 8.1 further. We shall show that each of the $\mathbf{k}$-modules $F_0, F_1, \ldots, F_{f_{n+1}}$ in this filtration is free, and even better, that there exists a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$ such that each F_i is spanned by an appropriate subfamily of this basis.

9.1. Definition

To construct this basis, we need the following definitions (some of which are commonplace in the combinatorics of the symmetric group):

- The *descent set* of a permutation $w \in S_n$ is defined to be the set of all $i \in [n-1]$ such that $w(i) > w(i+1)$. This set is denoted by $\operatorname{Des} w$.

  For example, the permutation in S_4 that sends $1, 2, 3, 4$ to $3, 2, 4, 1$ has descent set $\{1, 3\}$.

- We define a total order $<$ on the set S_n as follows: If u and v are two distinct permutations in S_n, then we say that $u < v$ if and only if the smallest $i \in [n]$ satisfying $u(i) \neq v(i)$ satisfies $u(i) < v(i)$. This relation $<$ is a total order on the set S_n, and is known as the *lexicographic order* on S_n. (If we identify each permutation $w \in S_n$ with the n-tuple $(w(1), w(2), \ldots, w(n))$, then this order is precisely the lexicographic order on n-tuples of integers; this is why it has the same name.)

  For example, the smallest permutation in S_n with respect to the total order $<$ is the identity permutation id, whereas the largest permutation is the one that sends each $i \in [n]$ to $n + 1 - i$.

- For each $I \subseteq [n-1]$, we let $G(I)$ be the subgroup of S_n generated by the subset $\{s_i \mid i \in I\}$.

  For instance, if $n = 5$ and $I = \{2, 4\}$, then $G(I) = \langle s_2, s_4 \rangle \leq S_5$.

- For each $w \in S_n$, we set
$$a_w := \sum_{\sigma \in G(\operatorname{Des} w)} w\sigma \in \mathbf{k}[S_n]. \qquad (18)$$

Example 9.1. For this example, let $n = 3$. We write each permutation $w \in S_3$ as the list $[w(1)\ w(2)\ w(3)]$ (written without commas for brevity, and using square brackets to distinguish it from a parenthesized integer). Then,

$$\begin{aligned}
a_{[123]} &= [123]; \\
a_{[132]} &= [132] + [123]; \\
a_{[213]} &= [213] + [123]; \\
a_{[231]} &= [231] + [213]; \\
a_{[312]} &= [312] + [132]; \\
a_{[321]} &= [321] + [312] + [231] + [213] + [132] + [123].
\end{aligned}$$

The quickest way to compute a_w for a given permutation $w \in S_n$ is as follows:

- Break the n-tuple $(w(1), w(2), \ldots, w(n))$ into decreasing blocks by placing a vertical bar between $w(i)$ and $w(i+1)$ whenever $w(i) < w(i+1)$. (For example, if $(w(1), w(2), \ldots, w(n)) = (3, 5, 1, 2, 7, 6, 4)$, then the result of this break-up is $(3 \mid 5, 1 \mid 2 \mid 7, 6, 4)$.)

- Within each decreasing block, we permute the entries arbitrarily.

- All resulting n-tuples are again interpreted as permutations $v \in S_n$. The a_w is the sum of these permutations v.

9.2. The lexicographic property

As Example 9.1 demonstrates, it seems that an element a_w is a sum of w and several permutations that are smaller than w in the lexicographic order. This is indeed always the case, and will follow from the following proposition:

Proposition 9.2. Let $w \in S_n$. Let $\sigma \in G(\operatorname{Des} w)$ satisfy $\sigma \neq \mathrm{id}$. Then, $w\sigma < w$ (with respect to the lexicographic order).

Proposition 9.2 is easy to prove with a bit of handwaving, but trickier to prove formally. We shall thus give a quick informal proof first, and then a longer, formal proof.

Informal proof of Proposition 9.2. Let $i_1, i_2, \ldots, i_p$ be the elements of the set $[n-1] \setminus \operatorname{Des} w$ in increasing order. Furthermore, let $i_0 = 0$ and $i_{p+1} = n$, so that $0 = i_0 < i_1 < i_2 < \cdots < i_p < i_{p+1} = n$. Define an interval

$$J_k := [i_{k-1} + 1,\ i_k] \qquad \text{for each } k \in [p+1].$$

Then, the $p+1$ intervals $J_1, J_2, \ldots, J_{p+1}$ form a set partition of the interval $[n]$. The permutation w is decreasing on each of these $p+1$ intervals, and these $p+1$ intervals are actually the inclusion-maximal intervals with this property.

Now, $\sigma \in G(\operatorname{Des} w)$ means that the permutation σ preserves each of the $p+1$ intervals $J_1, J_2, \ldots, J_{p+1}$ (that is, we have $\sigma(J_k) = J_k$ for each $k \in [p+1]$). [14] Hence, the permutation $w\sigma$ is obtained from w by separately permuting the values on each of the $p+1$ intervals $J_1, J_2, \ldots, J_{p+1}$. However, recall that w is decreasing on each of these $p+1$ intervals; thus, if we permute the values of w on each of these $p+1$ intervals separately, then the permutation w can only become smaller in the lexicographic order. Hence, $w\sigma \leq w$. Combining this with $w\sigma \neq w$ (which follows from $\sigma \neq \operatorname{id}$), we obtain $w\sigma < w$. This proves Proposition 9.2 (if you believe this handwaving). $\square$

Next, we shall give a more formal proof of Proposition 9.2 for the skeptical reader. This proof will require a further definition and two lemmas (which might be of independent interest). We begin with the definition:

- If $w \in S_n$, then an *inversion* of w means a pair $(i, j) \in [n] \times [n]$ satisfying $i < j$ and $w(i) > w(j)$. We denote the set of all inversions of a given permutation $w \in S_n$ by $\operatorname{Inv} w$.

Now, we can state our two lemmas:

Lemma 9.3. Let $w \in S_n$. Let $\sigma \in G(\operatorname{Des} w)$. Then, $\operatorname{Inv}\left((w\sigma)^{-1}\right) \subseteq \operatorname{Inv}\left(w^{-1}\right)$.

Lemma 9.4. Let $u \in S_n$ and $v \in S_n$ satisfy $\operatorname{Inv}\left(u^{-1}\right) \subseteq \operatorname{Inv}\left(v^{-1}\right)$. Then, $u \leq v$ (with respect to the lexicographic order).

Proof of Lemma 9.3. Let $(i, j) \in \operatorname{Inv}\left((w\sigma)^{-1}\right)$.

We have $(i, j) \in \operatorname{Inv}\left((w\sigma)^{-1}\right)$. In other words, (i, j) is an inversion of $(w\sigma)^{-1}$. By the definition of an inversion, this means that $(i, j) \in [n] \times [n]$ and $i < j$ and $(w\sigma)^{-1}(i) > (w\sigma)^{-1}(j)$.

Set $a := w^{-1}(i)$ and $b := w^{-1}(j)$. We shall now show that $a > b$.

Indeed, assume the contrary. Thus, $a \leq b$. Since $a \neq b$ [15], we thus obtain $a < b$.

[14] Indeed, $\operatorname{Des} w = [n-1] \setminus \{i_1, i_2, \ldots, i_p\}$. Hence, the group $G(\operatorname{Des} w)$ is generated by the simple transpositions s_i with $i \in [n-1] \setminus \{i_1, i_2, \ldots, i_p\}$. Thus, $\sigma \in G(\operatorname{Des} w)$ shows that σ is a product of such simple transpositions. However, each such simple transposition preserves each of the $p+1$ intervals $J_1, J_2, \ldots, J_{p+1}$. Thus, so does σ.

[15] *Proof.* We have $i < j$, thus $i \neq j$ and therefore $w^{-1}(i) \neq w^{-1}(j)$. In other words, $a \neq b$ (since $a = w^{-1}(i)$ and $b = w^{-1}(j)$).

From $a = w^{-1}(i)$ and $b = w^{-1}(j)$, we obtain $w(a) = i$ and $w(b) = j$. Thus, $w(a) = i < j = w(b)$. Hence, there exists some $k \in [a, b-1] \setminus \operatorname{Des} w$ [16]. Consider this k.

From $k \in [a, b-1] \setminus \operatorname{Des} w \subseteq [a, b-1]$, we obtain $a \leq k \leq b-1 < b$. Therefore, $a \in [k]$ but $b \notin [k]$. Moreover, from $k \in [a, b-1] \setminus \operatorname{Des} w$, we obtain $k \notin \operatorname{Des} w$.

Let $I = \operatorname{Des} w$. Thus, $k \notin \operatorname{Des} w = I$. Hence, s_k is not among the generators of the group $G(I)$.

Therefore, it is easy to see that

$$\tau([k]) = [k] \qquad \text{for each } \tau \in G(I) \tag{19}$$

[17]. Applying this to $\tau = \sigma$, we obtain $\sigma([k]) = [k]$ (since $\sigma \in G\left(\underbrace{\operatorname{Des} w}_{=I}\right) = G(I)$). Thus, $\sigma^{-1}([k]) = [k]$ (since σ is a bijection). However,

$$(w\sigma)^{-1}(i) = \sigma^{-1}\left(\underbrace{w^{-1}(i)}_{=a \in [k]}\right) \in \sigma^{-1}([k]) = [k],$$

so that $(w\sigma)^{-1}(i) \leq k$ and therefore $k \geq (w\sigma)^{-1}(i) > (w\sigma)^{-1}(j)$. In other words, $(w\sigma)^{-1}(j) < k$, so that $(w\sigma)^{-1}(j) \in [k]$. Therefore, $\sigma\left((w\sigma)^{-1}(j)\right) \in \sigma([k]) = [k]$. In view of $\sigma\left((w\sigma)^{-1}(j)\right) = \sigma\left(\sigma^{-1}\left(w^{-1}(j)\right)\right) = w^{-1}(j) = b$, this rewrites as $b \in [k]$. But this contradicts $b \notin [k]$. This contradiction shows that our assumption was false.

Hence, $a > b$ is proved. In view of $a = w^{-1}(i)$ and $b = w^{-1}(j)$, we can rewrite this as $w^{-1}(i) > w^{-1}(j)$. Combining this with $(i, j) \in [n] \times [n]$ and $i < j$, we conclude that (i, j) is an inversion of w^{-1}. In other words, $(i, j) \in \operatorname{Inv}\left(w^{-1}\right)$.

Forget that we fixed (i, j). We thus have shown that $(i, j) \in \operatorname{Inv}\left(w^{-1}\right)$ for each $(i, j) \in \operatorname{Inv}\left((w\sigma)^{-1}\right)$. In other words, $\operatorname{Inv}\left((w\sigma)^{-1}\right) \subseteq \operatorname{Inv}\left(w^{-1}\right)$. Lemma 9.3 is thus proven. $\square$

Proof of Lemma 9.4. We WLOG assume that $u \neq v$ (since otherwise, the claim is obvious). Thus, there exists some $i \in [n]$ satisfying $u(i) \neq v(i)$. Consider the **smallest** such i. We

[16] *Proof.* Assume the contrary. Thus, there exists no $k \in [a, b-1] \setminus \operatorname{Des} w$. In other words, the set $[a, b-1] \setminus \operatorname{Des} w$ is empty. In other words, $[a, b-1] \subseteq \operatorname{Des} w$. Hence, each $i \in [a, b-1]$ satisfies $i \in [a, b-1] \subseteq \operatorname{Des} w$ and therefore $w(i) > w(i+1)$ (by the definition of $\operatorname{Des} w$). In other words, we have

$$w(a) > w(a+1) > \cdots > w(b-1) > w(b).$$

This contradicts $w(a) < w(b)$. This contradiction shows that our assumption was false, qed.

[17] *Proof of (19):* We must show that each element of $G(I)$ preserves the set $[k]$.

We have defined $G(I)$ to be the subgroup of S_n generated by the subset $\{s_m \mid m \in I\}$. Hence, in order to prove that each element of $G(I)$ preserves the set $[k]$, it suffices to prove that each of the generators s_m preserves this set. In other words, it suffices to prove that $s_m([k]) = [k]$ for each $m \in I$.

But this is easy: Let $m \in I$. Then, $m \neq k$ (since $m \in I$ but $k \notin I$). Hence, we have either $m < k$ or $m > k$. In the former case, the simple transposition s_m swaps the two elements m and $m+1$, which both lie inside $[k]$; thus, $s_m([k]) = [k]$ in this case. In the latter case, the simple transposition s_m fixes all elements of $[k]$ (since neither m nor $m+1$ lies in $[k]$); thus, $s_m([k]) = [k]$ in this case as well. Hence, we have proved that $s_m([k]) = [k]$ in all cases. As explained above, this completes the proof of (19).

shall show that $u(i) < v(i)$. Once this is shown, we will immediately obtain $u < v$ (by the definition of lexicographic order), and thus Lemma 9.4 will follow.

So it remains to prove that $u(i) < v(i)$. For the sake of contradiction, we assume the contrary. Thus, $u(i) \geq v(i)$, so that $u(i) > v(i)$ (since $u(i) \neq v(i)$).

The maps u and v are permutations, and thus are injective.

Recall that i was defined to be the **smallest** element of $[n]$ satisfying $u(i) \neq v(i)$. Thus,

$$u(k) = v(k) \qquad \text{for each } k < i. \tag{20}$$

Let $p := u(i)$ and $q := v(i)$. Thus, $p > q$ (since $u(i) > v(i)$), so that $q < p$. Hence, $q \neq p$, so that $u^{-1}(q) \neq u^{-1}(p)$. Moreover, $u^{-1}(p) = i$ (since $p = u(i)$). If we had $u^{-1}(q) < i$, then we would have $u\left(u^{-1}(q)\right) = v\left(u^{-1}(q)\right)$ (by (20), applied to $k = u^{-1}(q)$), so that $v\left(u^{-1}(q)\right) = u\left(u^{-1}(q)\right) = q = v(i)$ and therefore $u^{-1}(q) = i$ (since the map v is injective); but this would contradict the very assumption $u^{-1}(q) < i$. Hence, we cannot have $u^{-1}(q) < i$. Thus, we must have $u^{-1}(q) \geq i = u^{-1}(p)$. Combining this with $u^{-1}(q) \neq u^{-1}(p)$, we obtain $u^{-1}(q) > u^{-1}(p)$.

Now we know that $(q, p) \in [n] \times [n]$ satisfies $q < p$ and $u^{-1}(q) > u^{-1}(p)$. In other words, (q, p) is an inversion of u^{-1}. Hence, $(q, p) \in \operatorname{Inv}\left(u^{-1}\right) \subseteq \operatorname{Inv}\left(v^{-1}\right)$. In other words, (q, p) is an inversion of v^{-1}. Hence, $v^{-1}(q) > v^{-1}(p)$. Since $v^{-1}(q) = i$ (because $q = v(i)$), this rewrites as $i > v^{-1}(p)$. Thus, $v^{-1}(p) < i$, so that we can apply (20) to $k = v^{-1}(p)$ and obtain

$$u\left(v^{-1}(p)\right) = v\left(v^{-1}(p)\right) = p = u(i).$$

Hence, $v^{-1}(p) = i$ (because u is injective). In other words, $p = v(i)$. This contradicts $p > q = v(i)$. This contradiction shows that our assumption was false. Hence, $u(i) < v(i)$ is proved, and Lemma 9.4 follows as explained above. ☐

Formal proof of Proposition 9.2. Lemma 9.3 yields $\operatorname{Inv}\left((w\sigma)^{-1}\right) \subseteq \operatorname{Inv}\left(w^{-1}\right)$. Hence, Lemma 9.4 (applied to $u = w\sigma$ and $v = w$) yields $w\sigma \leq w$. However, from $\sigma \neq \mathrm{id}$, we obtain $w\sigma \neq w$ (since S_n is a group). Combining this with $w\sigma \leq w$, we obtain $w\sigma < w$. This proves Proposition 9.2. ☐

Corollary 9.5. Let $w \in S_n$. Then,

$$a_w = w + (\text{a sum of permutations } v \in S_n \text{ satisfying } v < w).$$

Proof. The definition of a_w yields

$$\begin{aligned}
a_w &= \sum_{\sigma \in G(\operatorname{Des} w)} w\sigma = \underbrace{w\,\mathrm{id}}_{=w} + \sum_{\substack{\sigma \in G(\operatorname{Des} w); \\ \sigma \neq \mathrm{id}}} w\sigma \qquad \left(\begin{array}{c}\text{here, we have split off the} \\ \text{addend for } \sigma = \mathrm{id} \text{ from the sum}\end{array}\right) \\
&= w + \underbrace{\sum_{\substack{\sigma \in G(\operatorname{Des} w); \\ \sigma \neq \mathrm{id}}} w\sigma}_{\substack{=(\text{a sum of permutations } v \in S_n \text{ satisfying } v < w) \\ (\text{since Proposition 9.2 shows that each} \\ \text{addend } w\sigma \text{ of this sum satisfies } w\sigma < w)}} \\
&= w + (\text{a sum of permutations } v \in S_n \text{ satisfying } v < w).
\end{aligned}$$

This proves Corollary 9.5. $\square$

9.3. The basis property

Using Corollary 9.5, we can now see that the elements a_w for all $w \in S_n$ form a basis of $\mathbf{k}[S_n]$, and furthermore, by selecting an appropriate subset of these elements, we can find a basis of each $F(I)$. To wit, the following two propositions hold:

Proposition 9.6. The family $(a_w)_{w \in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$.

Proposition 9.7. For each $I \subseteq [n]$, the family $(a_w)_{w \in S_n;\ I' \subseteq \operatorname{Des} w}$ is a basis of the $\mathbf{k}$-module $F(I)$.

We shall derive both Proposition 9.6 and Proposition 9.7 from a more general result. To state the latter, we introduce another notation:

- For any subset I of $[n-1]$, we set

$$Z(I) := \{q \in \mathbf{k}[S_n] \mid qs_i = q \text{ for all } i \in I\}.$$

  This is a $\mathbf{k}$-submodule of $\mathbf{k}[S_n]$.

The definition of those $\mathbf{k}$-submodules reminds us of the definition of $F(I)$, so we make the relation between the two notions explicit:

Proposition 9.8. Let $I \subseteq [n]$. Then, $F(I) = Z(I')$.

Proof. Both $F(I)$ and $Z(I')$ are defined to be $\{q \in \mathbf{k}[S_n] \mid qs_i = q \text{ for all } i \in I'\}$. Thus, we have $F(I) = Z(I')$. This proves Proposition 9.8. $\square$

Now, we can state the general result from which both Proposition 9.6 and Proposition 9.7 will follow:

Proposition 9.9. Let I be a subset of $[n-1]$. Then, the family $(a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}$ is a basis of the $\mathbf{k}$-module $Z(I)$.

Proof. To prove that the family $(a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}$ forms a basis of $Z(I)$, there are three items to prove. First, we shall prove that each element of this family belongs to $Z(I)$ (Claim 1 below). Then, we will show that this family spans $Z(I)$ (a consequence of Claim 2 below). Finally, we will show that the (larger) family $(a_w)_{w \in S_n}$ is $\mathbf{k}$-linearly independent (Claim 3). The proofs of these three claims constitute the bulk of the proof of Proposition 9.9, although an experienced reader will likely find some (or even all) of them straightforward.

In the proof that follows, we shall use the notation $[w]\, q$ for the coefficient of a permutation $w \in S_n$ in an element $q \in \mathbf{k}[S_n]$. (Thus, each $q \in \mathbf{k}[S_n]$ satisfies

$q = \sum_{w \in S_n} ([w] q) w$.) The definition of multiplication in the group algebra $\mathbf{k}[S_n]$ shows that

$$[w](q\sigma) = \left[w\sigma^{-1}\right] q \tag{21}$$

for any $w \in S_n$, $\sigma \in S_n$ and $q \in \mathbf{k}[S_n]$.

We shall first show that the family $(a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}$ is a family of vectors in $Z(I)$. In other words, we shall show the following:

Claim 1: For each $w \in S_n$ satisfying $I \subseteq \operatorname{Des} w$, we have $a_w \in Z(I)$.

[*Proof of Claim 1:* Let $w \in S_n$ satisfy $I \subseteq \operatorname{Des} w$. Let $i \in I$. Then, $i \in I \subseteq \operatorname{Des} w$. Hence, s_i is one of the generators of the group $G(\operatorname{Des} w)$ (by the definition of $G(\operatorname{Des} w)$). Thus, $s_i \in G(\operatorname{Des} w)$. However, $G(\operatorname{Des} w)$ is a group. Thus, the map $G(\operatorname{Des} w) \to G(\operatorname{Des} w)$, $\sigma \mapsto \sigma s_i$ is a bijection (since $s_i \in G(\operatorname{Des} w)$).

However, the definition of a_w yields $a_w = \sum_{\sigma \in G(\operatorname{Des} w)} w\sigma$. Multiplying this equality by s_i, we find

$$a_w s_i = \left(\sum_{\sigma \in G(\operatorname{Des} w)} w\sigma \right) s_i = \sum_{\sigma \in G(\operatorname{Des} w)} w\sigma s_i = \sum_{\sigma \in G(\operatorname{Des} w)} w\sigma$$

(here, we have substituted σ for σs_i in the sum, since the map $G(\operatorname{Des} w) \to G(\operatorname{Des} w)$, $\sigma \mapsto \sigma s_i$ is a bijection). Comparing this with $a_w = \sum_{\sigma \in G(\operatorname{Des} w)} w\sigma$, we obtain $a_w s_i = a_w$.

Now, forget that we fixed i. We thus have shown that $a_w s_i = a_w$ for each $i \in I$. In other words,

$$a_w \in \{q \in \mathbf{k}[S_n] \mid q s_i = q \text{ for all } i \in I\} = Z(I)$$

(by the definition of $Z(I)$). This proves Claim 1.]

Next, we shall show that the family $(a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}$ spans the $\mathbf{k}$-module $Z(I)$. To achieve this, we will first prove the following:

Claim 2: Let $u \in S_n$. Then,[18]

$$Z(I) \cap \operatorname{span}\left((w)_{w \in S_n;\ w \leq u} \right) \subseteq \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w} \right).$$

[*Proof of Claim 2:* We proceed by strong induction on u (using the lexicographic order as a well-ordering on S_n). Thus, we fix some permutation $x \in S_n$, and we assume (as induction hypothesis) that Claim 2 has already been proved for each $u < x$. We must then prove Claim 2 for $u = x$.

[18] Here and in the following, $\operatorname{span}\left((f_i)_{i \in I}\right)$ denotes the $\mathbf{k}$-linear span of a family $(f_i)_{i \in I}$ of vectors.

Using our induction hypothesis, we can easily see that

$$Z(I) \cap \operatorname{span}\left((w)_{w\in S_n;\ w<x}\right) \subseteq \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right). \tag{22}$$

[19]

Our goal is to prove Claim 2 for $u = x$. In other words, our goal is to prove that $Z(I) \cap \operatorname{span}\left((w)_{w\in S_n;\ w\leq x}\right) \subseteq \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$.

To do so, we let $q \in Z(I) \cap \operatorname{span}\left((w)_{w\in S_n;\ w\leq x}\right)$. Thus, $q \in Z(I)$ and $q \in \operatorname{span}\left((w)_{w\in S_n;\ w\leq x}\right)$. From $q \in \operatorname{span}\left((w)_{w\in S_n;\ w\leq x}\right)$, we see that q is a $\mathbf{k}$-linear combination of the family $(w)_{w\in S_n;\ w\leq x}$. Thus,

$$[w]\, q = 0 \qquad \text{for every } w \in S_n \text{ satisfying } w > x. \tag{23}$$

We want to show that $q \in \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$.

We are in one of the following two cases:

Case 1: We have $I \not\subseteq \operatorname{Des} x$.

Case 2: We have $I \subseteq \operatorname{Des} x$.

First, let us consider Case 1. In this case, we have $I \not\subseteq \operatorname{Des} x$. Hence, there exists some $k \in I$ such that $k \notin \operatorname{Des} x$. Consider this k. Then, $k \in I \subseteq [n-1]$. Hence, if we had $x(k) > x(k+1)$, then we would have $k \in \operatorname{Des} x$ (by the definition of $\operatorname{Des} x$), which would contradict $k \notin \operatorname{Des} x$. Thus, we cannot have $x(k) > x(k+1)$. Hence, we have $x(k) \leq x(k+1)$. Since $x(k) \neq x(k+1)$ (because x is a permutation), we thus find $x(k) < x(k+1)$. Hence, it is easy to see that $xs_k > x$ [20]. Thus, (23) (applied to $w = xs_k$) yields $[xs_k]\, q = 0$.

[19] *Proof of (22):* If x is the smallest permutation in S_n (with respect to the lexicographic order), then the family $(w)_{w\in S_n;\ w<x}$ is empty (since there is no $w \in S_n$ satisfying $w < x$ in this case), and thus its span is $\operatorname{span}\left((w)_{w\in S_n;\ w<x}\right) = 0$, so that we have $Z(I) \cap \underbrace{\operatorname{span}\left((w)_{w\in S_n;\ w<x}\right)}_{=0} = 0 \subseteq \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$. Hence, if x is the smallest permutation in S_n, then (22) holds. Thus, for the rest of this proof, we WLOG assume that x is not the smallest permutation in S_n. Thus, there exists some $w \in S_n$ such that $w < x$. Let y be the **largest** such w (this is well-defined, since the lexicographic order is a total order on the finite set S_n). Then, the permutations $w \in S_n$ satisfying $w < x$ are precisely the permutations $w \in S_n$ satisfying $w \leq y$. Thus, $\operatorname{span}\left((w)_{w\in S_n;\ w<x}\right) = \operatorname{span}\left((w)_{w\in S_n;\ w\leq y}\right)$. Note also that $y < x$ (by the definition of y).

However, our induction hypothesis says that Claim 2 has already been proved for each $u < x$. Hence, in particular, Claim 2 holds for $u = y$ (since $y < x$). In other words, we have $Z(I) \cap \operatorname{span}\left((w)_{w\in S_n;\ w\leq y}\right) \subseteq \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$. In view of $\operatorname{span}\left((w)_{w\in S_n;\ w<x}\right) = \operatorname{span}\left((w)_{w\in S_n;\ w\leq y}\right)$, we can rewrite this as $Z(I) \cap \operatorname{span}\left((w)_{w\in S_n;\ w<x}\right) \subseteq \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$. This completes the proof of (22).

[20] *Proof.* Let $y := xs_k$. Then, recalling how s_k was defined, we see that all values of y are equal to the corresponding values of x except for the values at k and $k+1$, which are swapped. In other

On the other hand, $q \in Z(I)$, and therefore $qs_i = q$ for all $i \in I$ (by the definition of $Z(I)$). Applying this to $i = k$, we obtain $qs_k = q$ (since $k \in I$). However, (21) (applied to $w = x$ and $\sigma = s_k$) yields

$$[x](qs_k) = \left[xs_k^{-1}\right] q = [xs_k] q \qquad \left(\text{since } s_k^{-1} = s_k\right)$$
$$= 0.$$

In view of $qs_k = q$, this rewrites as $[x] q = 0$. In other words, $[w] q = 0$ holds for $w = x$. Combining this with (23), we obtain

$$[w] q = 0 \qquad \text{for every } w \in S_n \text{ satisfying } w \geq x. \tag{24}$$

Hence, $q \in \operatorname{span}\left((w)_{w\in S_n;\ w<x}\right)$. Combining this with $q \in Z(I)$, we obtain

$$q \in Z(I) \cap \operatorname{span}\left((w)_{w\in S_n;\ w<x}\right) \subseteq \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$$

(by (22)). Hence, we have proved that $q \in \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$ in Case 1.

Let us next consider Case 2. In this case, we have $I \subseteq \operatorname{Des} x$. Hence, $a_x \in Z(I)$ (by Claim 1, applied to $w = x$). Moreover, a_x is an element of the family $(a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}$ (since $x \in S_n$ satisfies $I \subseteq \operatorname{Des} x$). Hence, $a_x \in \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$.

Let $\lambda := [x] q$. Let $r := q - \lambda a_x \in \mathbf{k}[S_n]$. Then, $r \in Z(I)$ (since $Z(I)$ is a $\mathbf{k}$-module, and since both q and a_x belong to $Z(I)$). Moreover, Corollary 9.5 (applied to $w = x$) yields

$$a_x = x + (\text{a sum of permutations } v \in S_n \text{ satisfying } v < x).$$

Hence, $[x](a_x) = 1$ and

$$[w](a_x) = 0 \qquad \text{for each } w \in S_n \text{ satisfying } w > x. \tag{25}$$

Now, from $r = q - \lambda a_x$, we obtain

$$[x] r = [x](q - \lambda a_x) = [x] q - \underbrace{\lambda}_{=[x]q} \cdot \underbrace{[x](a_x)}_{=1} = [x] q - [x] q = 0.$$

---

words,

$$(y(1), y(2), \ldots, y(k-1), y(k), y(k+1), y(k+2), \ldots, y(n))$$
$$= (x(1), x(2), \ldots, x(k-1), x(k+1), x(k), x(k+2), \ldots, x(n)).$$

Thus, the smallest $i \in [n]$ satisfying $x(i) \neq y(i)$ is k, and this smallest i satisfies $x(i) < y(i)$ (since we have $x(k) < x(k+1) = y(k)$). Therefore, the definition of lexicographic order shows that $x < y$. Hence, $x < y = xs_k$, so that $xs_k > x$.

Moreover, for each $w \in S_n$ satisfying $w > x$, we have

$$\begin{aligned} [w]\, r &= [w]\,(q - \lambda a_x) \qquad (\text{since } r = q - \lambda a_x) \\ &= \underbrace{[w]\, q}_{\substack{=0 \\ (\text{by (23)})}} - \lambda \cdot \underbrace{[w]\,(a_x)}_{\substack{=0 \\ (\text{by (25)})}} = 0 - \lambda \cdot 0 = 0. \end{aligned}$$

This equality also holds for $w = x$ (since we have just seen that $[x]\, r = 0$). Hence, it holds for all $w \geq x$. Thus, we have shown that $[w]\, r = 0$ for each $w \in S_n$ satisfying $w \geq x$. In other words, we have $r \in \operatorname{span}\left((w)_{w \in S_n;\ w < x}\right)$. Combining this with $r \in Z(I)$, we obtain

$$r \in Z(I) \cap \operatorname{span}\left((w)_{w \in S_n;\ w < x}\right) \subseteq \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right)$$

(by (22)). Now, from $r = q - \lambda a_x$, we obtain

$$\begin{aligned} q &= \underbrace{r}_{\in \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right)} + \lambda \underbrace{a_x}_{\in \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right)} \\ &\in \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right) + \lambda \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right) \\ &\subseteq \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right) \qquad \left(\text{since } \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right) \text{ is a } \mathbf{k}\text{-module}\right). \end{aligned}$$

Hence, we have proved $q \in \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right)$ in Case 2.

Now, we have proved $q \in \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right)$ in both Cases 1 and 2. Hence, $q \in \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right)$ always holds.

Forget that we fixed q. We thus have shown that $q \in \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right)$ for each $q \in Z(I) \cap \operatorname{span}\left((w)_{w \in S_n;\ w \leq x}\right)$. In other words, $Z(I) \cap \operatorname{span}\left((w)_{w \in S_n;\ w \leq x}\right) \subseteq \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right)$. In other words, we have proved Claim 2 for $u = x$. This completes the induction step. Thus, Claim 2 is proven.]

Now, it is easy to see that the family $(a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}$ spans the $\mathbf{k}$-module $Z(I)$ [21]. We shall now show that this family is $\mathbf{k}$-linearly independent. Slightly better, we will show that the family $(a_w)_{w \in S_n}$ is $\mathbf{k}$-linearly independent:

[21] *Proof.* Let u be the largest permutation in S_n (with respect to the lexicographic order). Thus, every $w \in S_n$ satisfies $w \leq u$.

Let $q \in Z(I)$. Then, $q \in Z(I) \subseteq \mathbf{k}[S_n] = \operatorname{span}\left((w)_{w \in S_n}\right)$ (since the family $(w)_{w \in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$). However, the family $(w)_{w \in S_n}$ is the same as the family $(w)_{w \in S_n;\ w \leq u}$ (since every $w \in S_n$ satisfies $w \leq u$). Hence, $q \in \operatorname{span}\left((w)_{w \in S_n;\ w \leq u}\right)$ (since $q \in \operatorname{span}\left((w)_{w \in S_n}\right)$). Combining this with $q \in Z(I)$, we obtain $q \in Z(I) \cap \operatorname{span}\left((w)_{w \in S_n;\ w \leq u}\right) \subseteq \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right)$ (by Claim 2).

Claim 3: Let $(\lambda_w)_{w\in S_n}$ be a family of elements of $\mathbf{k}$ such that $\sum\limits_{w\in S_n} \lambda_w a_w = 0$. Then, $\lambda_w = 0$ for each $w \in S_n$.

[*Proof of Claim 3:* This follows by a straightforward triangularity argument (where the triangularity is provided by Corollary 9.5). Purely for the sake of completeness, we present the argument in full:

We must prove that

$$\lambda_w = 0 \qquad \text{for each } w \in S_n. \tag{26}$$

In order to prove (26), we proceed by strong induction on w, but this time we use the **reverse** of the lexicographic order on S_n as our well-ordering. Thus, we fix some $x \in S_n$, and we assume (as the induction hypothesis) that (26) has already been proved for each $w > x$ (not for each $w < x$ as in our previous induction proof). Our goal is then to prove that (26) holds for $w = x$. In other words, our goal is to prove that $\lambda_x = 0$.

The induction hypothesis yields that (26) holds for each $w > x$. In other words, $\lambda_w = 0$ for each $w \in S_n$ satisfying $w > x$. Hence, $\sum\limits_{\substack{w\in S_n;\\ w>x}} \underbrace{\lambda_w}_{=0} a_w = \sum\limits_{\substack{w\in S_n;\\ w>x}} 0 a_w = 0$. However, each $w \in S_n$ satisfies exactly one of the three statements $w < x$ and $w = x$ and $w > x$. Hence, we can split the sum $\sum\limits_{w\in S_n} \lambda_w a_w$ as follows:

$$\sum_{w\in S_n} \lambda_w a_w = \sum_{\substack{w\in S_n;\\ w<x}} \lambda_w a_w + \underbrace{\sum_{\substack{w\in S_n;\\ w=x}} \lambda_w a_w}_{=\lambda_x a_x} + \underbrace{\sum_{\substack{w\in S_n;\\ w>x}} \lambda_w a_w}_{=0} = \sum_{\substack{w\in S_n;\\ w<x}} \lambda_w a_w + \lambda_x a_x.$$

Comparing this with $\sum\limits_{w\in S_n} \lambda_w a_w = 0$, we obtain

$$0 = \sum_{\substack{w\in S_n;\\ w<x}} \lambda_w a_w + \lambda_x a_x.$$

Taking the x-coefficients on both sides of this equality, we obtain

$$\begin{aligned} [x]\, 0 &= [x] \left(\sum_{\substack{w\in S_n;\\ w<x}} \lambda_w a_w + \lambda_x a_x \right) \\ &= \sum_{\substack{w\in S_n;\\ w<x}} \lambda_w \cdot [x]\,(a_w) + \lambda_x \cdot [x]\,(a_x). \end{aligned} \tag{27}$$

Forget that we fixed q. We thus have shown that each $q \in Z(I)$ satisfies $q \in \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$. In other words, $Z(I) \subseteq \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$. In other words, the family $(a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}$ spans the $\mathbf{k}$-module $Z(I)$ (since Claim 1 shows that this family is a family of vectors in $Z(I)$). Qed.

Now, let $w \in S_n$ be such that $w < x$. Then, $x > w$. However, Corollary 9.5 yields

$$a_w = w + (\text{a sum of permutations } v \in S_n \text{ satisfying } v < w).$$

Hence, $[y](a_w) = 0$ for all $y \in S_n$ satisfying $y > w$. Applying this to $y = x$, we obtain $[x](a_w) = 0$ (since $x > w$).

Forget that we fixed w. We thus have shown that

$$[x](a_w) = 0 \qquad \text{for each } w \in S_n \text{ satisfying } w < x. \tag{28}$$

Also, Corollary 9.5 (applied to $w = x$) yields

$$a_x = x + (\text{a sum of permutations } v \in S_n \text{ satisfying } v < x).$$

Hence, $[x](a_x) = 1$. Now,

$$\begin{aligned} 0 = [x]\,0 &= \sum_{\substack{w \in S_n;\\ w < x}} \lambda_w \cdot \underbrace{[x](a_w)}_{\substack{=0\\ \text{(by (28))}}} + \lambda_x \cdot \underbrace{[x](a_x)}_{=1} \qquad \text{(by (27))} \\ &= \underbrace{\sum_{\substack{w \in S_n;\\ w < x}} \lambda_w \cdot 0}_{=0} + \lambda_x = \lambda_x. \end{aligned}$$

Thus, $\lambda_x = 0$. In other words, (26) holds for $w = x$. This completes the induction step. Thus, (26) is proved, and Claim 3 follows.]

Now, we have proved Claim 3. In other words, we have proved that the family $(a_w)_{w \in S_n}$ is $\mathbf{k}$-linearly independent. Hence, its subfamily $(a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}$ is $\mathbf{k}$-linearly independent as well (since a subfamily of a $\mathbf{k}$-linearly independent family must itself be $\mathbf{k}$-linearly independent family). Since we also know that this subfamily spans the $\mathbf{k}$-module $Z(I)$, we thus conclude that this subfamily is a basis of $Z(I)$. This proves Proposition 9.9. □

Proof of Proposition 9.6. The definition of $Z(\varnothing)$ yields

$$Z(\varnothing) = \{q \in \mathbf{k}[S_n] \mid qs_i = q \text{ for all } i \in \varnothing\} = \mathbf{k}[S_n]$$

(because the statement "$qs_i = q$ for all $i \in \varnothing$" is vacuously true for each $q \in \mathbf{k}[S_n]$). However, Proposition 9.9 (applied to $I = \varnothing$) yields that the family $(a_w)_{w \in S_n;\ \varnothing \subseteq \operatorname{Des} w}$ is a basis of the $\mathbf{k}$-module $Z(\varnothing)$. Since the family $(a_w)_{w \in S_n;\ \varnothing \subseteq \operatorname{Des} w}$ is nothing other than the family $(a_w)_{w \in S_n}$ (because the statement "$\varnothing \subseteq \operatorname{Des} w$" holds for each $w \in S_n$), we can rewrite this as follows: The family $(a_w)_{w \in S_n}$ is a basis of the $\mathbf{k}$-module $Z(\varnothing)$. In other words, the family $(a_w)_{w \in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$ (since $Z(\varnothing) = \mathbf{k}[S_n]$). This proves Proposition 9.6. □

Proof of Proposition 9.7. Let $I \subseteq [n]$. Then, Proposition 9.8 yields $F(I) = Z(I')$.

However, Proposition 9.9 (applied to I' instead of I) yields that the family $(a_w)_{w \in S_n;\ I' \subseteq \operatorname{Des} w}$ is a basis of the $\mathbf{k}$-module $Z(I')$. Since $F(I) = Z(I')$, we can rewrite this as follows: The family $(a_w)_{w \in S_n;\ I' \subseteq \operatorname{Des} w}$ is a basis of the $\mathbf{k}$-module $F(I)$. This proves Proposition 9.7. □

We refer to the basis $(a_w)_{w\in S_n}$ of $\mathbf{k}[S_n]$ as the *descent-destroying basis*, due to how a_w is defined in terms of "removing" descents from w. As with any basis, we can ask the following rather natural question about it:

Question 9.10. How can we explicitly expand a permutation $v \in S_n$ in the basis $(a_w)_{w\in S_n}$ of $\mathbf{k}[S_n]$?

Example 9.11. For this example, let $n = 4$. We write each permutation $w \in S_4$ as the list $[w(1)\ w(2)\ w(3)\ w(4)]$ (written without commas for brevity, and using square brackets to distinguish it from a parenthesized integer). Then,

$$[3412] = a_{[1234]} - a_{[1324]} + a_{[1342]} + a_{[3124]} - a_{[3142]} + a_{[3412]}.$$

We note that it is **not** generally true that when we express a permutation $v \in S_n$ as a $\mathbf{k}$-linear combination of the basis $(a_w)_{w\in S_n}$, all coefficients will belong to $\{0, 1, -1\}$. However, the smallest n for which this is not the case is $n = 8$, which suggests that the coefficients are not too complicated.

10. Q-indices and bases of F_i

10.1. Definition

We can now use our basis $(a_w)_{w\in S_n}$ and its subfamilies $(a_w)_{w\in S_n;\ I'\subseteq \operatorname{Des} w}$ to obtain a basis for each piece F_i of the filtration $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}}$. First, for the sake of convenience, we define a certain permutation statistic we call the "Q-index". It is worth pointing out that this "Q-index" will depend on the way how we numbered the lacunar subsets of $[n-1]$ by $Q_1, Q_2, \ldots, Q_{f_{n+1}}$, so it is not really a natural permutation statistic. We will show in Proposition 10.3, however, that the assignment of the lacunar set Q_i (where i is the Q-index of w) to a permutation w is canonical (i.e., does not depend on the numbering of the lacunar subsets).

First, we prove a lemma:

Lemma 10.1. Let $w \in S_n$. Then, there exists some $i \in [f_{n+1}]$ such that $Q_i' \subseteq \operatorname{Des} w$.

Proof. Let $I = \{j \in [n-1] \mid j \equiv n-1 \bmod 2\}$. Then, I is a lacunar subset of $[n-1]$ (in fact, I is lacunar since all elements of I have the same parity). Thus, there exists some $i \in [f_{n+1}]$ such that $I = Q_i$ (since $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are all lacunar subsets of $[n-1]$). Consider this i. We shall show that $Q_i' \subseteq \operatorname{Des} w$.

The definition of I yields that each element of $[n-1]$ is either in I (if it has the same parity as $n-1$) or in $I-1$ (if it has not). In other words, $[n-1] \subseteq I \cup (I-1)$. The definition of I' yields $I' = [n-1] \setminus (I \cup (I-1)) = \varnothing$ (since $[n-1] \subseteq I \cup (I-1)$). In view of $I = Q_i$, this rewrites as $Q_i' = \varnothing$. Hence, $Q_i' = \varnothing \subseteq \operatorname{Des} w$. This proves Lemma 10.1. $\square$

Now, we can define the Q-index:

- If $w \in S_n$ is any permutation, then the *Q-index* of w is defined to be the **smallest** $i \in [f_{n+1}]$ such that $Q_i' \subseteq \operatorname{Des} w$. (This is well-defined, because Lemma 10.1 shows that such an i exists.) We denote the Q-index of w by $\operatorname{Qind} w$.

Example 10.2. For this example, let $n = 4$. Recall Example 8.3, in which we listed all the lacunar subsets of $[3]$ in order. Let $w \in S_n$ be the permutation such that $(w(1), w(2), \ldots, w(n)) = (4, 3, 1, 2)$. Then, $\operatorname{Des} w = \{1, 2\}$. Hence, $Q_4' = \{1\} \subseteq \operatorname{Des} w$, but it is easy to see that $Q_i' \not\subseteq \operatorname{Des} w$ for all $i < 4$. Hence, the smallest $i \in [f_{n+1}]$ such that $Q_i' \subseteq \operatorname{Des} w$ is 4. In other words, the Q-index of w is 4. In other words, $\operatorname{Qind} w = 4$.

10.2. An equivalent description

As we said, the Q-index of a permutation $w \in S_n$ depends on the ordering of $Q_1, Q_2, \ldots, Q_{f_{n+1}}$. However, the dependence is not as strong as it might appear from the definition; indeed, we have the following alternative characterization:

Proposition 10.3. Let $w \in S_n$ and $i \in [f_{n+1}]$. Then, $\operatorname{Qind} w = i$ if and only if $Q_i' \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i$.

Before we prove this proposition, we need two further lemmas about lacunar subsets:

Lemma 10.4. Let I and K be two subsets of $[n-1]$ such that I is lacunar and $K \neq I$ and $K' \subseteq [n-1] \setminus I$. Then, $\operatorname{sum} I < \operatorname{sum} K$.

Proof of Lemma 10.4. First, we observe that $I \setminus K \subseteq (K \setminus I) - 1$.

[*Proof:* Let $i \in I \setminus K$. Thus, $i \in I$ and $i \notin K$.

If we had $i + 1 \notin K$, then we would have $i \in K'$ (since $i \in I \subseteq [n-1]$ and $i \notin K$ and $i + 1 \notin K$), which would entail $i \in K' \subseteq [n-1] \setminus I$; but this would contradict $i \in I$. Thus, we cannot have $i + 1 \notin K$. In other words, we have $i + 1 \in K$. Furthermore, I is lacunar; thus, from $i \in I$, we obtain $i + 1 \notin I$. Combining this with $i + 1 \in K$, we find $i + 1 \in K \setminus I$. Hence, $i \in (K \setminus I) - 1$.

Forget that we fixed i. We thus have proved that $i \in (K \setminus I) - 1$ for each $i \in I \setminus K$. In other words, $I \setminus K \subseteq (K \setminus I) - 1$.]

Now, the set I is the union of its two disjoint subsets $I \setminus K$ and $I \cap K$. Hence,

$$\operatorname{sum} I = \operatorname{sum}(I \setminus K) + \operatorname{sum}(I \cap K). \tag{29}$$

The same argument (with the roles of I and K swapped) yields

$$\operatorname{sum} K = \operatorname{sum}(K \setminus I) + \operatorname{sum}(K \cap I). \tag{30}$$

Our goal is to prove that $\operatorname{sum} I < \operatorname{sum} K$. If $I \subseteq K$, then this is obvious (since we have $K \neq I$, so that I must be a **proper** subset of K in this case). Thus, we WLOG assume that $I \not\subseteq K$ from now on. Hence, $I \setminus K \neq \varnothing$. In view of $I \setminus K \subseteq (K \setminus I) - 1$, this entails $(K \setminus I) - 1 \neq \varnothing$, so that $K \setminus I \neq \varnothing$. Hence, $|K \setminus I| > 0$.

Now, from $I \setminus K \subseteq (K \setminus I) - 1$, we obtain

$$\operatorname{sum}(I \setminus K) \leq \operatorname{sum}((K \setminus I) - 1) = \operatorname{sum}(K \setminus I) - \underbrace{|K \setminus I|}_{>0} < \operatorname{sum}(K \setminus I).$$

However, (29) becomes

$$\operatorname{sum} I = \underbrace{\operatorname{sum}(I \setminus K)}_{<\operatorname{sum}(K \setminus I)} + \operatorname{sum}\left(\underbrace{I \cap K}_{=K \cap I}\right) < \operatorname{sum}(K \setminus I) + \operatorname{sum}(K \cap I) = \operatorname{sum} K$$

(by (30)). This proves Lemma 10.4. $\square$

Lemma 10.5. Let I be a subset of $[n]$. Let $j \in I$. Then, there exists a lacunar subset K of $[n-1]$ satisfying $\operatorname{sum} K < \operatorname{sum} I$ and $K' \subseteq I' \cup \{j\}$.

Proof. Set $R := (I \setminus \{j\}) \cup \{j-1\}$ if $j > 1$, and otherwise set $R := I \setminus \{j\}$. Thus, the set R is obtained from I by replacing the element j (which was in I, because $j \in I$) by the smaller element $j-1$ (unless $j = 1$, in which case j is just removed). In either case, we therefore have $\operatorname{sum} R < \operatorname{sum} I$. Also, it is easy to see that $R \subseteq [n]$ and $R' \subseteq I' \cup \{j\}$ (by Proposition 8.6 **(a)**, applied to $K = R$). Thus, Corollary 8.8 (applied to R instead of I) yields that there exists a lacunar subset J of $[n-1]$ such that $\operatorname{sum} J \leq \operatorname{sum} R$ and $J' \subseteq R'$. Consider this J. Then, $\operatorname{sum} J \leq \operatorname{sum} R < \operatorname{sum} I$ and $J' \subseteq R' \subseteq I' \cup \{j\}$. Hence, there exists a lacunar subset K of $[n-1]$ satisfying $\operatorname{sum} K < \operatorname{sum} I$ and $K' \subseteq I' \cup \{j\}$ (namely, $K = J$). This proves Lemma 10.5. $\square$

Proof of Proposition 10.3. $\Longrightarrow$: Assume that $\operatorname{Qind} w = i$. We must prove that $Q_i' \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i$.

In view of the definition of the Q-index, our assumption $\operatorname{Qind} w = i$ means that $Q_i' \subseteq \operatorname{Des} w$ and that i is the smallest element of $[f_{n+1}]$ with this property. The latter statement means that

$$Q_k' \not\subseteq \operatorname{Des} w \qquad \text{for each } k < i. \tag{31}$$

Now, let $j \in (\operatorname{Des} w) \cap Q_i$. We shall derive a contradiction.

Indeed, we have $j \in (\operatorname{Des} w) \cap Q_i \subseteq Q_i$. Hence, Lemma 10.5 (applied to $I = Q_i$) shows that there exists a lacunar subset K of $[n-1]$ satisfying $\operatorname{sum} K < \operatorname{sum}(Q_i)$ and $K' \subseteq Q_i' \cup \{j\}$. Consider this K. Since K is a lacunar subset of $[n-1]$, we have $K = Q_k$ for some $k \in [f_{n+1}]$ (since the lacunar subsets of $[n-1]$ are $Q_1, Q_2, \ldots, Q_{f_{n+1}}$). Consider this k. Thus, $Q_k = K$, so that $\operatorname{sum}(Q_k) = \operatorname{sum} K < \operatorname{sum}(Q_i)$. However, if we had $i \leq k$, then we would have $\operatorname{sum}(Q_i) \leq \operatorname{sum}(Q_k)$ (by (15)), which would contradict $\operatorname{sum}(Q_k) < \operatorname{sum}(Q_i)$. Thus, we cannot have $i \leq k$.

Hence, we must have $i > k$, so that $k < i$. Therefore, (31) yields $Q'_k \not\subseteq \operatorname{Des} w$. In other words, $K' \not\subseteq \operatorname{Des} w$ (since $Q_k = K$).

However, $K' \subseteq \underbrace{Q'_i}_{\subseteq \operatorname{Des} w} \cup \{j\} \subseteq (\operatorname{Des} w) \cup \{j\} = \operatorname{Des} w$ (since $j \in (\operatorname{Des} w) \cap Q_i \subseteq \operatorname{Des} w$). This contradicts $K' \not\subseteq \operatorname{Des} w$.

Forget that we fixed j. We thus have obtained a contradiction for each $j \in (\operatorname{Des} w) \cap Q_i$. Hence, there exists no such j. In other words, the set $(\operatorname{Des} w) \cap Q_i$ is empty. In other words, $\operatorname{Des} w$ is disjoint from Q_i. Hence, $\operatorname{Des} w \subseteq [n-1] \setminus Q_i$ (since $\operatorname{Des} w \subseteq [n-1]$). Combining this with $Q'_i \subseteq \operatorname{Des} w$, we obtain $Q'_i \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i$. Thus, we have proved the "$\Longrightarrow$" direction of Proposition 10.3.

$\Longleftarrow$: Assume that $Q'_i \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i$. We must prove that $\operatorname{Qind} w = i$.

We shall show that $Q'_k \not\subseteq \operatorname{Des} w$ for each $k < i$. Indeed, let us fix a positive integer $k < i$. Thus, $\operatorname{sum}(Q_k) \leq \operatorname{sum}(Q_i)$ (by (15)). Also, from $k < i$, we obtain $Q_k \neq Q_i$ (since the sets $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are distinct). Also, the set Q_i is lacunar (since the sets $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are lacunar).

Now, assume (for the sake of contradiction) that $Q'_k \subseteq \operatorname{Des} w$. Then, $Q'_k \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i$. Therefore, Lemma 10.4 (applied to $I = Q_i$ and $K = Q_k$) yields $\operatorname{sum}(Q_i) < \operatorname{sum}(Q_k)$. This contradicts $\operatorname{sum}(Q_k) \leq \operatorname{sum}(Q_i)$. This contradiction shows that our assumption (that $Q'_k \subseteq \operatorname{Des} w$) was false. Hence, we have $Q'_k \not\subseteq \operatorname{Des} w$.

Forget that we fixed k. We thus have shown that $Q'_k \not\subseteq \operatorname{Des} w$ for each $k < i$. Since we also know that $Q'_i \subseteq \operatorname{Des} w$ (by assumption), we thus conclude that i is the **smallest** element of $[f_{n+1}]$ such that $Q'_i \subseteq \operatorname{Des} w$. In other words, i is the Q-index of w (since this is how the Q-index of w is defined). In other words, $i = \operatorname{Qind} w$. That is, $\operatorname{Qind} w = i$. Thus, we have proved the "$\Longleftarrow$" direction of Proposition 10.3. □

10.3. Bases of the F_i and F_i / F_{i-1}

Theorem 10.6. Recall the $\mathbf{k}$-module filtration $0 = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}} = \mathbf{k}[S_n]$ from Theorem 8.1. Then:

- **(a)** For each $i \in [0, f_{n+1}]$, the $\mathbf{k}$-module F_i is free with basis $(a_w)_{w \in S_n;\ \operatorname{Qind} w \leq i}$.
- **(b)** For each $i \in [f_{n+1}]$, the $\mathbf{k}$-module F_i / F_{i-1} is free with basis $(\overline{a_w})_{w \in S_n;\ \operatorname{Qind} w = i}$. Here, $\overline{x}$ denotes the projection of an element $x \in F_i$ onto the quotient F_i / F_{i-1}.

Proof. **(a)** Proposition 9.6 yields that the family $(a_w)_{w \in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$. Hence, this family $(a_w)_{w \in S_n}$ is $\mathbf{k}$-linearly independent.

Let $i \in [0, f_{n+1}]$. For each $k \in [i]$, we have

$$F(Q_k) = \operatorname{span}\left((a_w)_{w \in S_n;\ Q'_k \subseteq \operatorname{Des} w}\right) \tag{32}$$

(since Proposition 9.7 (applied to $I = Q_k$) shows that the family $(a_w)_{w\in S_n;\ Q'_k\subseteq \operatorname{Des} w}$ is a basis of the $\mathbf{k}$-module $F(Q_k)$). However, the definition of F_i yields

$$
\begin{aligned}
F_i &= F(Q_1) + F(Q_2) + \cdots + F(Q_i) = \sum_{k=1}^{i} \underbrace{F(Q_k)}_{\substack{=\operatorname{span}\left((a_w)_{w\in S_n;\ Q'_k\subseteq \operatorname{Des} w}\right) \\ \text{(by (32))}}} \\
&= \sum_{k=1}^{i} \operatorname{span}\left((a_w)_{w\in S_n;\ Q'_k\subseteq \operatorname{Des} w}\right) \\
&= \operatorname{span}\left((a_w)_{w\in S_n;\ Q'_k\subseteq \operatorname{Des} w \text{ for some } k\in[i]}\right) \qquad (33)
\end{aligned}
$$

(since the sum of the spans of some families of vectors is the span of the union of these families). However, if $w \in S_n$ is a permutation, then the statement "$Q'_k \subseteq \operatorname{Des} w$ for some $k \in [i]$" is equivalent to the statement "$\operatorname{Qind} w \leq i$" (since $\operatorname{Qind} w$ is defined as the **smallest** $j \in [f_{n+1}]$ such that $Q'_j \subseteq \operatorname{Des} w$). Thus, the family $(a_w)_{w\in S_n;\ Q'_k\subseteq \operatorname{Des} w \text{ for some } k\in[i]}$ is precisely the family $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leq i}$. Hence, we can rewrite (33) as follows:

$$F_i = \operatorname{span}\left((a_w)_{w\in S_n;\ \operatorname{Qind} w\leq i}\right).$$

In other words, the family $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leq i}$ spans the $\mathbf{k}$-module F_i. Furthermore, this family is $\mathbf{k}$-linearly independent (since it is a subfamily of the $\mathbf{k}$-linearly independent family $(a_w)_{w\in S_n}$). Thus, this family is a basis of the $\mathbf{k}$-module F_i. In other words, the $\mathbf{k}$-module F_i is free with basis $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leq i}$. This proves Theorem 10.6 **(a)**.

(b) For each $i \in [0, f_{n+1}]$, we let $A(i)$ denote the set of all permutations $w \in S_n$ satisfying $\operatorname{Qind} w \leq i$. Clearly, $A(0) \subseteq A(1) \subseteq \cdots \subseteq A(f_{n+1})$.

Let $i \in [f_{n+1}]$. Then, the permutations $w \in S_n$ satisfying $\operatorname{Qind} w \leq i$ are precisely the permutations $w \in A(i)$ (by the definition of $A(i)$). Hence, the family $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leq i}$ is precisely the family $(a_w)_{w\in A(i)}$.

However, Theorem 10.6 **(a)** yields that the $\mathbf{k}$-module F_i is free with basis $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leq i}$. In other words, the $\mathbf{k}$-module F_i is free with basis $(a_w)_{w\in A(i)}$ (since the family $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leq i}$ is precisely the family $(a_w)_{w\in A(i)}$). The same argument (applied to $i-1$ instead of i) yields that the $\mathbf{k}$-module F_{i-1} is free with basis $(a_w)_{w\in A(i-1)}$. Note that $A(i-1) \subseteq A(i)$ and that F_{i-1} is a $\mathbf{k}$-submodule of F_i.

However, the following fact is simple and well-known:

> *Fact 1:* Let B and C be two sets such that $C \subseteq B$. Let U be a $\mathbf{k}$-module that is free with a basis $(f_w)_{w\in B}$. Let V be a $\mathbf{k}$-submodule of U that is free with basis $(f_w)_{w\in C}$. Then, the $\mathbf{k}$-module U/V is free with basis $\left(\overline{f_w}\right)_{w\in B\setminus C}$. Here, $\overline{x}$ denotes the projection of an element $x \in U$ onto the quotient U/V.

We apply Fact 1 to $B = A(i)$ and $C = A(i-1)$ and $U = F_i$ and $V = F_{i-1}$. As a consequence, we conclude that the $\mathbf{k}$-module F_i / F_{i-1} is free with basis $\left(\overline{a_w}\right)_{w \in A(i) \setminus A(i-1)}$.

However,

$$\begin{aligned}
&A(i) \setminus A(i-1) \\
&= \{w \in A(i) \mid w \notin A(i-1)\} \\
&= \{w \in S_n \mid w \in A(i) \text{ but not } w \in A(i-1)\} \\
&= \{w \in S_n \mid \operatorname{Qind} w \leq i \text{ but not } \operatorname{Qind} w \leq i-1\} \\
&\qquad \left(\begin{array}{c}\text{since } A(i) \text{ is the set of all } w \in S_n \text{ satisfying } \operatorname{Qind} w \leq i, \\ \text{whereas } A(i-1) \text{ is the set of all } w \in S_n \text{ satisfying } \operatorname{Qind} w \leq i-1\end{array}\right) \\
&= \{w \in S_n \mid \operatorname{Qind} w = i\}
\end{aligned}$$

(since a $w \in S_n$ satisfies "$\operatorname{Qind} w \leq i$ but not $\operatorname{Qind} w \leq i-1$" if and only if it satisfies $\operatorname{Qind} w = i$). Thus, the family $\left(\overline{a_w}\right)_{w \in A(i) \setminus A(i-1)}$ is exactly the family $\left(\overline{a_w}\right)_{w \in S_n;\ \operatorname{Qind} w = i}$. Hence, the $\mathbf{k}$-module F_i / F_{i-1} is free with basis $\left(\overline{a_w}\right)_{w \in S_n;\ \operatorname{Qind} w = i}$ (because we have previously showed that the $\mathbf{k}$-module F_i / F_{i-1} is free with basis $\left(\overline{a_w}\right)_{w \in A(i) \setminus A(i-1)}$). This proves Theorem 10.6 **(b)**. □

10.4. Our filtration has no equal terms

For our next corollary, we need a simple existence result:

Lemma 10.7. Let $i \in [f_{n+1}]$. Then, there exists some permutation $w \in S_n$ satisfying $\operatorname{Qind} w = i$.

Proof. We shall construct such a permutation w as follows:

Let $J := [n-1] \setminus Q_i$. Thus, J is a subset of $[n-1]$.

Let $m := |J|$. Let $w \in S_n$ be the permutation that sends the m elements of J (from smallest to largest) to the m numbers $n, n-1, n-2, \ldots, n-m+1$ (in this order) while sending the remaining $n-m$ elements of $[n]$ (from smallest to largest) to the $n-m$ numbers $1, 2, \ldots, n-m$ (in this order). For example, if $n = 8$ and $J = \{2, 4, 5\}$, then $m = 3$ and $(w(1), w(2), \ldots, w(n)) = (1, 8, 2, 7, 6, 3, 4, 5)$. The definition of w easily yields that $\operatorname{Des} w = J$.

Thus, we have $\operatorname{Des} w = J = [n-1] \setminus Q_i$. The definition of Q_i' yields

$$Q_i' = [n-1] \setminus \underbrace{(Q_i \cup (Q_i - 1))}_{\supseteq Q_i} \subseteq [n-1] \setminus Q_i = J = \operatorname{Des} w.$$

Combining this with $\operatorname{Des} w \subseteq \operatorname{Des} w = [n-1] \setminus Q_i$, we obtain $Q_i' \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i$. However, the latter chain of inclusions is equivalent to $\operatorname{Qind} w = i$ (because of Proposition 10.3). Thus, we have $\operatorname{Qind} w = i$.

So we have constructed a permutation $w \in S_n$ satisfying $\operatorname{Qind} w = i$. As explained above, this proves Lemma 10.7. □

Combining Lemma 10.7 with Theorem 10.6, we obtain the following corollary (which, roughly speaking, says that our filtration $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}}$ cannot be shortened):

Corollary 10.8. Assume that $\mathbf{k} \neq 0$. Then, $F_i \neq F_{i-1}$ for each $i \in [f_{n+1}]$.

Proof. Let $i \in [f_{n+1}]$. We must prove that $F_i \neq F_{i-1}$. In other words, we must prove that $F_i / F_{i-1} \neq 0$ (since F_{i-1} is a $\mathbf{k}$-submodule of F_i). However, Theorem 10.6 **(b)** yields that the $\mathbf{k}$-module F_i / F_{i-1} is free with basis $(\overline{a_w})_{w \in S_n;\ \operatorname{Qind} w = i}$. Hence, in order to prove that $F_i / F_{i-1} \neq 0$, it suffices to show that this basis $(\overline{a_w})_{w \in S_n;\ \operatorname{Qind} w = i}$ is nonempty. In other words, it suffices to show that there exists some permutation $w \in S_n$ satisfying $\operatorname{Qind} w = i$. However, this follows from Lemma 10.7. Thus, Corollary 10.8 is proved. □

11. Triangularizing the endomorphism

We are now ready to prove Theorem 4.1, made concrete as follows:

Theorem 11.1. Let $w \in S_n$ and $\ell \in [n]$. Let $i = \operatorname{Qind} w$. Then,

$$a_w t_\ell = m_{Q_i,\ell} a_w + \left(\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < i\right).$$

This theorem shows that for each $\ell \in [n]$, the $n! \times n!$-matrix that represents the endomorphism $R(t_\ell)$ of $\mathbf{k}[S_n]$ with respect to the basis $(a_w)_{w \in S_n}$ is upper-triangular if we order the set S_n by increasing Q-index (note that this is not the lexicographic order!). Thus, the same holds for any $\mathbf{k}$-linear combination

$$R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n) = \lambda_1 R(t_1) + \lambda_2 R(t_2) + \cdots + \lambda_n R(t_n).$$

Theorem 4.1 therefore follows, if we can prove Theorem 11.1. We shall do this in a moment; first, let us give an example:

Example 11.2. For this example, let $n = 4$. We write each permutation $w \in S_4$ as the list $[w(1)\ \ w(2)\ \ w(3)\ \ w(4)]$ (written without commas for brevity, and using square brackets to distinguish it from a parenthesized integer). Then,

$$a_{[4312]} t_2 = a_{[4312]} + \underbrace{a_{[4321]} - a_{[4231]} - a_{[3241]} - a_{[2143]}}_{\substack{\text{this is a } \mathbf{k}\text{-linear combination of } a_v\text{'s} \\ \text{for } v \in S_n \text{ satisfying } \operatorname{Qind} v < i, \text{ where } i = \operatorname{Qind}[4312]}}.$$

Indeed, Example 8.3 tells us that $\operatorname{Qind}[4312] = 4$, whereas $\operatorname{Qind}[4321] = 1$ and $\operatorname{Qind}[4231] = \operatorname{Qind}[3241] = \operatorname{Qind}[2143] = 3$.

Proof of Theorem 11.1. Theorem 10.6 **(a)** yields that the $\mathbf{k}$-module F_i is free with basis $(a_v)_{v\in S_n;\ \operatorname{Qind} v\leq i}$. (Here, we have renamed the index w from Theorem 10.6 **(a)** as v in order to avoid confusion with the already-fixed permutation w.)

Now, $w \in S_n$ and $\operatorname{Qind} w \leq i$ (since $\operatorname{Qind} w = i$). Hence, a_w is an element of the family $(a_v)_{v\in S_n;\ \operatorname{Qind} v\leq i}$. Since the latter family $(a_v)_{v\in S_n;\ \operatorname{Qind} v\leq i}$ is a basis of F_i, this entails that $a_w \in F_i$. Hence,

$$\underbrace{a_w}_{\in F_i} \cdot \left(t_\ell - m_{Q_i,\ell}\right) \in F_i \cdot \left(t_\ell - m_{Q_i,\ell}\right) \subseteq F_{i-1} \qquad \text{(by Theorem 8.1 \textbf{(c)})}.$$

However, Theorem 10.6 **(a)** (applied to $i-1$ instead of i) yields that the $\mathbf{k}$-module F_{i-1} is free with basis $(a_v)_{v\in S_n;\ \operatorname{Qind} v\leq i-1}$. (Here, again, we have renamed the index w from Theorem 10.6 **(a)** as v in order to avoid confusion with the already-fixed permutation w.) Thus, in particular, $(a_v)_{v\in S_n;\ \operatorname{Qind} v\leq i-1}$ is a basis of the $\mathbf{k}$-module F_{i-1}. Hence, $F_{i-1} = \operatorname{span}\left((a_v)_{v\in S_n;\ \operatorname{Qind} v\leq i-1}\right)$. Now,

$$a_w \cdot \left(t_\ell - m_{Q_i,\ell}\right) \in F_{i-1} = \operatorname{span}\left((a_v)_{v\in S_n;\ \operatorname{Qind} v\leq i-1}\right) = \operatorname{span}\left((a_v)_{v\in S_n;\ \operatorname{Qind} v< i}\right)$$

(since the condition "$\operatorname{Qind} v \leq i-1$" is equivalent to "$\operatorname{Qind} v < i$"). In other words,

$$a_w \cdot \left(t_\ell - m_{Q_i,\ell}\right) = \left(\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < i\right).$$

In view of $a_w \cdot \left(t_\ell - m_{Q_i,\ell}\right) = a_w t_\ell - m_{Q_i,\ell} a_w$, this can be rewritten as

$$a_w t_\ell - m_{Q_i,\ell} a_w = \left(\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < i\right).$$

Equivalently,

$$a_w t_\ell = m_{Q_i,\ell} a_w + \left(\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < i\right).$$

This proves Theorem 11.1. □

12. The eigenvalues of the endomorphism

12.1. An annihilating polynomial

We have now shown enough to easily obtain a polynomial that annihilates any given $\mathbf{k}$-linear combination $\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n$ of the shuffles $t_1, t_2, \ldots, t_n$ (and therefore the corresponding endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$):

Theorem 12.1. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Let $t := \lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n$. Then,

$$\prod_{\substack{I\subseteq[n-1] \text{ is} \\ \text{lacunar}}} \left(t - \left(\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}\right)\right) = 0.$$

(Here, the product on the left hand side is well-defined, since all its factors $t - (\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n})$ lie in the commutative subalgebra $\mathbf{k}[t]$ of $\mathbf{k}[S_n]$ and therefore commute with each other.)

Proof. For each $i \in [f_{n+1}]$, we set

$$g_i := \lambda_1 m_{Q_i,1} + \lambda_2 m_{Q_i,2} + \cdots + \lambda_n m_{Q_i,n} = \sum_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell} \in \mathbf{k}.$$

First, we shall show that

$$F_i \cdot (t - g_i) \subseteq F_{i-1} \qquad \text{for each } i \in [f_{n+1}]. \tag{34}$$

[*Proof of (34):* Let $i \in [f_{n+1}]$. From $t = \lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n = \sum\limits_{\ell=1}^{n} \lambda_\ell t_\ell$ and $g_i = \sum\limits_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell}$, we obtain

$$t - g_i = \sum_{\ell=1}^{n} \lambda_\ell t_\ell - \sum_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell} = \sum_{\ell=1}^{n} \lambda_\ell \left(t_\ell - m_{Q_i,\ell}\right).$$

Therefore,

$$\begin{aligned} F_i \cdot (t - g_i) &= F_i \cdot \sum_{\ell=1}^{n} \lambda_\ell \left(t_\ell - m_{Q_i,\ell}\right) = \sum_{\ell=1}^{n} \lambda_\ell \underbrace{F_i \cdot \left(t_\ell - m_{Q_i,\ell}\right)}_{\substack{\subseteq F_{i-1} \\ \text{(by Theorem 8.1 } \textbf{(c)}\text{)}}} \\ &\subseteq \sum_{\ell=1}^{n} \lambda_\ell F_{i-1} \subseteq F_{i-1} \qquad \left(\text{since } F_{i-1} \text{ is a } \mathbf{k}\text{-module}\right). \end{aligned}$$

This proves (34).]

Next, we claim that

$$F_m \cdot \prod_{j=1}^{m} \left(t - g_j\right) = 0 \qquad \text{for each } m \in [0, f_{n+1}]. \tag{35}$$

(Here, the product $\prod\limits_{j=1}^{m} \left(t - g_j\right)$ is well-defined, since all its factors $t - g_j$ lie in the commutative subalgebra $\mathbf{k}[t]$ of $\mathbf{k}[S_n]$ and therefore commute with each other.)

[*Proof of (35):* We proceed by induction on m:

Induction base: For $m = 0$, the equality (35) says that $F_0 \cdot (\text{empty product}) = 0$, which is true (since $F_0 = 0$).

Induction step: Let $i \in [f_{n+1}]$. Assume (as the induction hypothesis) that (35) holds for $m = i - 1$. We must prove that (35) holds for $m = i$.

We have

$$F_i \cdot \underbrace{\prod_{j=1}^{i} \left(t - g_j\right)}_{=(t-g_i)\cdot \prod_{j=1}^{i-1}\left(t-g_j\right)} = \underbrace{F_i \cdot (t - g_i)}_{\substack{\subseteq F_{i-1} \\ \text{(by (34))}}} \cdot \prod_{j=1}^{i-1} \left(t - g_j\right) \subseteq F_{i-1} \cdot \prod_{j=1}^{i-1} \left(t - g_j\right) = 0$$

(since we assumed that (35) holds for $m = i-1$). Hence, $F_i \cdot \prod_{j=1}^{i} \left(t - g_j\right) = 0$. In other words, (35) holds for $m = i$. This completes the induction step. Thus, the proof of (35) is complete.]

Now, recall that $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are all the lacunar subsets of $[n-1]$, listed without repetition. Hence,

$$\begin{aligned}
&\prod_{\substack{I \subseteq [n-1] \text{ is} \\ \text{lacunar}}} \left(t - \left(\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}\right)\right) \\
&= \prod_{j=1}^{f_{n+1}} \left(t - \underbrace{\left(\lambda_1 m_{Q_j,1} + \lambda_2 m_{Q_j,2} + \cdots + \lambda_n m_{Q_j,n}\right)}_{\substack{= g_j \\ \text{(by the definition of } g_j\text{)}}} \right) \\
&= \prod_{j=1}^{f_{n+1}} \left(t - g_j\right) = \underbrace{1}_{\substack{\in \mathbf{k}[S_n] = F_{f_{n+1}} \\ \text{(since } F_{f_{n+1}} = \mathbf{k}[S_n] \\ \text{(by Theorem 8.1 } \textbf{(a)}\text{))}}} \cdot \prod_{j=1}^{f_{n+1}} \left(t - g_j\right) \in F_{f_{n+1}} \cdot \prod_{j=1}^{f_{n+1}} \left(t - g_j\right) = 0
\end{aligned}$$

(by (35), applied to $m = f_{n+1}$). In other words,

$$\prod_{\substack{I \subseteq [n-1] \text{ is} \\ \text{lacunar}}} \left(t - \left(\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}\right)\right) = 0.$$

This proves Theorem 12.1. □

12.2. The spectrum

We can now describe the spectrum of $R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)$ when $\mathbf{k}$ is a field:

Corollary 12.2. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Assume that $\mathbf{k}$ is a field. Then,

$$\begin{aligned}
&\operatorname{Spec}\left(R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)\right) \\
&= \left\{\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n} \ \mid\ I \subseteq [n-1] \text{ is lacunar}\right\}.
\end{aligned}$$

Here, $\operatorname{Spec} f$ denotes the spectrum (i.e., the set of all eigenvalues) of a $\mathbf{k}$-linear operator f.

An interesting fact here is that the number of distinct eigenvalues cannot exceed the number of lacunar subsets of $[n-1]$, which was shown in Section 5 to be the Fibonacci number f_{n+1}. This is a surprisingly low number compared to the number of distinct eigenvalues that $R(a)$ can have for an arbitrary $a \in \mathbf{k}[S_n]$. In fact, the latter number is the number of involutions of $[n]$, or equivalently the number of standard Young tableaux with n cells.[22]

Proof of Corollary 12.2. Let

$$\rho := R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right) : \mathbf{k}\left[S_n\right] \to \mathbf{k}\left[S_n\right].$$

Let $w_1, w_2, \ldots, w_{n!}$ be the $n!$ permutations in S_n, ordered in such a way that

$$\operatorname{Qind}\left(w_1\right) \leq \operatorname{Qind}\left(w_2\right) \leq \cdots \leq \operatorname{Qind}\left(w_{n!}\right). \tag{36}$$

(This ordering is not the lexicographic order!)

Proposition 9.6 says that the family $\left(a_w\right)_{w \in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}\left[S_n\right]$. In other words, the list $\left(a_{w_1}, a_{w_2}, \ldots, a_{w_{n!}}\right)$ is a basis of the $\mathbf{k}$-module $\mathbf{k}\left[S_n\right]$ (since this list is just a reindexing of the family $\left(a_w\right)_{w \in S_n}$). We shall refer to this basis as the *a-basis*. Let $M = \left(\mu_{i,j}\right)_{i,j \in [n!]}$ be the matrix that represents the endomorphism ρ with respect to this a-basis $\left(a_{w_1}, a_{w_2}, \ldots, a_{w_{n!}}\right)$. Then, for each $j \in [n!]$, we have

$$\rho\left(a_{w_j}\right) = \sum_{k=1}^{n!} \mu_{k,j} a_{w_k}. \tag{37}$$

On the other hand,

$$\begin{aligned}
\rho\left(a_{w_j}\right) &= \left(R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)\right)\left(a_{w_j}\right) \\
&\qquad \left(\text{since } \rho = R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)\right) \\
&= a_{w_j} \cdot \underbrace{\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)}_{= \sum_{\ell=1}^{n} \lambda_\ell t_\ell} \\
&\qquad \left(\text{by the definition of } R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)\right) \\
&= a_{w_j} \cdot \sum_{\ell=1}^{n} \lambda_\ell t_\ell = \sum_{\ell=1}^{n} \lambda_\ell a_{w_j} t_\ell.
\end{aligned} \tag{38}$$

Define an element $g_i \in \mathbf{k}$ for each $i \in \left[f_{n+1}\right]$ as in the proof of Theorem 12.1.

We shall now prove the following two properties of our matrix $M = \left(\mu_{i,j}\right)_{i,j \in [n!]}$:

Claim 1: We have $\mu_{j,j} = g_{\operatorname{Qind}\left(w_j\right)}$ for each $j \in [n!]$.

[22]This is due to the fact that (when $\mathbf{k}$ is a $\mathbb{Q}$-algebra) $\mathbf{k}\left[S_n\right]$ decomposes into a direct sum of *Specht modules* indexed by partitions of n, and that the Specht module corresponding to the partition λ appears f^λ many times, where f^λ is the number of standard tableaux of shape λ. Since $R\left(a\right)$ acts by the same endomorphism on all copies of a single Specht module, but can act independently on all non-isomorphic Specht modules, we see that the maximum number of distinct eigenvalues of $R\left(a\right)$ equals the sum of the dimensions of all non-isomorphic Specht modules. But this number is the number of standard tableaux with n cells, i.e., the number of involutions of $[n]$.

Claim 2: For any $j,k \in [n!]$ satisfying $k > j$, we have $\mu_{k,j} = 0$.

[*Proof of Claim 1:* Let $j \in [n!]$. We must prove that $\mu_{j,j} = g_{\operatorname{Qind}(w_j)}$.

The equality (37) shows that $\mu_{j,j}$ is the coefficient of a_{w_j} when $\rho\left(a_{w_j}\right)$ is expanded as a $\mathbf{k}$-linear combination of the a-basis.

Let $i := \operatorname{Qind}\left(w_j\right)$. Then, (38) becomes

$$\begin{aligned}
&\rho\left(a_{w_j}\right) \\
&= \sum_{\ell=1}^{n} \lambda_\ell \underbrace{a_{w_j} t_\ell}_{\substack{=m_{Q_i,\ell} a_{w_j} + (\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < i) \\ (\text{by Theorem 11.1, applied to } w = w_j)}} \\
&= \sum_{\ell=1}^{n} \lambda_\ell \left(m_{Q_i,\ell} a_{w_j} + (\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < i)\right) \\
&= \sum_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell} a_{w_j} + (\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < i) .
\end{aligned}$$

In view of

$$\sum_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell} a_{w_j} = \underbrace{\left(\sum_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell}\right)}_{\substack{=g_i \\ (\text{by the definition of } g_i)}} a_{w_j} = g_i a_{w_j},$$

we can rewrite this as

$$\rho\left(a_{w_j}\right) = g_i a_{w_j} + (\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < i) . \tag{39}$$

The right hand side of (39) is clearly a $\mathbf{k}$-linear combination of the a-basis. Let us compute the coefficient of a_{w_j} in this combination. Indeed, the first addend $g_i a_{w_j}$ clearly contributes g_i to this coefficient. On the other hand, the $\mathbf{k}$-linear combination of a_v's for $v \in S_n$ satisfying $\operatorname{Qind} v < i$ does not contain a_{w_j} (because w_j is not a $v \in S_n$ satisfying $\operatorname{Qind} v < i$ [23]), and thus does not contribute to the coefficient of a_{w_j} on the right hand side of (39). Thus, the total coefficient with which the basis element a_{w_j} appears on the right hand side of (39) is g_i. Thus, the equality (39) expresses $\rho\left(a_{w_j}\right)$ as a $\mathbf{k}$-linear combination of the a-basis, and the basis element a_{w_j} appears in this combination with coefficient g_i. Hence, when $\rho\left(a_{w_j}\right)$ is expanded as a $\mathbf{k}$-linear combination of the a-basis, the basis element a_{w_j} appears with coefficient g_i. In other words, $\mu_{j,j} = g_i$ (since $\mu_{j,j}$ is the coefficient of a_{w_j} when $\rho\left(a_{w_j}\right)$ is

[23] *Proof.* We have $\operatorname{Qind}\left(w_j\right) = i$. Thus, we do not have $\operatorname{Qind}\left(w_j\right) < i$. Hence, w_j is not a $v \in S_n$ satisfying $\operatorname{Qind} v < i$.

expanded as a $\mathbf{k}$-linear combination of the a-basis). In view of $i = \operatorname{Qind}\left(w_j\right)$, this rewrites as $\mu_{j,j} = g_{\operatorname{Qind}\left(w_j\right)}$. This completes our proof of Claim 1.]

[*Proof of Claim 2:* Let $j, k \in [n!]$ satisfy $k > j$. We must prove that $\mu_{k,j} = 0$.

The equality (37) shows that $\mu_{k,j}$ is the coefficient of a_{w_k} when $\rho\left(a_{w_j}\right)$ is expanded as a $\mathbf{k}$-linear combination of the a-basis. Thus, our goal is to show that this coefficient is 0 (since we must prove that $\mu_{k,j} = 0$). In other words, our goal is to show that when $\rho\left(a_{w_j}\right)$ is expanded as a $\mathbf{k}$-linear combination of the a-basis, the basis element a_{w_k} appears with coefficient 0.

Let $i := \operatorname{Qind}\left(w_j\right)$. Just as in the proof of Claim 1, we obtain the equality (39). The right hand side of this equality is clearly a $\mathbf{k}$-linear combination of the a-basis. Let us see whether the element a_{w_k} of the a-basis appears in this combination. Indeed, a_{w_k} clearly does not appear in the addend $g_i a_{w_j}$, because $k \neq j$ (since $k > j$). Furthermore, a_{w_k} does not appear in the $\mathbf{k}$-linear combination of a_v's for $v \in S_n$ satisfying $\operatorname{Qind} v < i$ either, because w_k is not a $v \in S_n$ satisfying $\operatorname{Qind} v < i$ [24]. Hence, a_{w_k} appears nowhere on the right hand side of (39). Thus, the equality (39) expresses $\rho\left(a_{w_j}\right)$ as a $\mathbf{k}$-linear combination of the a-basis, but without the basis element a_{w_k} ever appearing in this combination. Hence, when $\rho\left(a_{w_j}\right)$ is expanded as a $\mathbf{k}$-linear combination of the a-basis, the basis element a_{w_k} appears with coefficient 0. This completes our proof of Claim 2.]

Claim 2 shows that the matrix M is upper-triangular. Hence, its eigenvalues are its diagonal entries. In other words,

$$\operatorname{Spec} M = \{\text{all diagonal entries of } M\} = \left\{\mu_{j,j} \mid j \in [n!]\right\} = \left\{g_{\operatorname{Qind}\left(w_j\right)} \mid j \in [n!]\right\}$$

(since Claim 1 yields that $\mu_{j,j} = g_{\operatorname{Qind}\left(w_j\right)}$ for each $j \in [n!]$).

The values $\operatorname{Qind} w$ for all $w \in S_n$ belong to the set $[f_{n+1}]$ (by the definition of $\operatorname{Qind} w$). Conversely, each element i of $[f_{n+1}]$ can be written as $\operatorname{Qind} w$ for at least one permutation $w \in S_n$ (by Lemma 10.7). Combining these two observations, we obtain

$$\{\operatorname{Qind} w \mid w \in S_n\} = [f_{n+1}].$$

Now, recall that the matrix M represents the endomorphism ρ with respect to the basis $(a_{w_1}, a_{w_2}, \ldots, a_{w_{n!}})$. Hence, its eigenvalues are the eigenvalues of the latter endomorphism. In other words, $\operatorname{Spec} M = \operatorname{Spec} \rho$. In view of $\rho = R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)$,

[24] *Proof.* From $k > j$, we obtain $j \leq k$ and thus $\operatorname{Qind}\left(w_j\right) \leq \operatorname{Qind}\left(w_k\right)$ (by (36)). Hence, $\operatorname{Qind}\left(w_k\right) \geq \operatorname{Qind}\left(w_j\right) = i$. Thus, we do not have $\operatorname{Qind}\left(w_k\right) < i$. Hence, w_k is not a $v \in S_n$ satisfying $\operatorname{Qind} v < i$.

this rewrites as $\operatorname{Spec} M = \operatorname{Spec}\left(R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)\right)$. Hence,

$$\begin{aligned}
&\operatorname{Spec}\left(R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)\right) \\
&= \operatorname{Spec} M \\
&= \left\{ g_{\operatorname{Qind}\left(w_j\right)} \ \mid \ j \in [n!] \right\} \\
&= \left\{ g_{\operatorname{Qind} w} \ \mid \ w \in S_n \right\} \qquad \left(\text{since } w_1, w_2, \ldots, w_{n!} \text{ are the } n! \text{ permutations in } S_n\right) \\
&= \left\{ g_i \ \mid \ i \in [f_{n+1}] \right\} \qquad \left(\text{since } \left\{\operatorname{Qind} w \ \mid \ w \in S_n\right\} = [f_{n+1}]\right) \\
&= \left\{ \lambda_1 m_{Q_i,1} + \lambda_2 m_{Q_i,2} + \cdots + \lambda_n m_{Q_i,n} \ \mid \ i \in [f_{n+1}] \right\} \\
&\qquad\qquad \left(\text{since } g_i \text{ is defined as } \lambda_1 m_{Q_i,1} + \lambda_2 m_{Q_i,2} + \cdots + \lambda_n m_{Q_i,n}\right) \\
&= \left\{ \lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n} \ \mid \ I \subseteq [n-1] \text{ is lacunar} \right\}
\end{aligned}$$

(since $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are exactly the lacunar subsets I of $[n-1]$). This proves Corollary 12.2. □

12.3. Diagonalizability

We have already seen in Remark 4.2 that the endomorphism $R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)$ of $\mathbf{k}\left[S_n\right]$ may fail to be diagonalizable (even if $\mathbf{k} = \mathbb{C}$). However, in a large class of cases, it is diagonalizable:

Theorem 12.3. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Assume that $\mathbf{k}$ is a field. Assume that the elements $\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}$ for all lacunar subsets $I \subseteq [n-1]$ are distinct. Then, the endomorphism $R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)$ of $\mathbf{k}\left[S_n\right]$ is diagonalizable.

In order to prove Theorem 12.3, we will need a slightly apocryphal concept from algebra:

- A $\mathbf{k}$-*algebra antihomomorphism* from a $\mathbf{k}$-algebra A to a $\mathbf{k}$-algebra B means a $\mathbf{k}$-linear map $f : A \to B$ that satisfies $f(1) = 1$ and

$$f\left(a_1 a_2\right) = f\left(a_2\right) f\left(a_1\right) \qquad \text{for all } a_1, a_2 \in A.$$

Thus, a $\mathbf{k}$-algebra antihomomorphism from a $\mathbf{k}$-algebra A to a $\mathbf{k}$-algebra B is the same as a $\mathbf{k}$-algebra homomorphism from A^{op} to B, where A^{op} is the opposite algebra of A (that is, the $\mathbf{k}$-algebra A with its multiplication reversed).

It is well-known that $\mathbf{k}$-algebra homomorphisms preserve univariate polynomials: That is, if f is a $\mathbf{k}$-algebra homomorphism from a $\mathbf{k}$-algebra A to a $\mathbf{k}$-algebra B, and if $P \in \mathbf{k}[X]$ is a polynomial, then $f(P(u)) = P(f(u))$ for any $u \in A$. The same holds for $\mathbf{k}$-algebra antihomomorphisms:

Proposition 12.4. Let f be a $\mathbf{k}$-algebra antihomomorphism from a $\mathbf{k}$-algebra A to a $\mathbf{k}$-algebra B. Let $P \in \mathbf{k}[X]$ be a polynomial. Then, $f(P(u)) = P(f(u))$ for any $u \in A$.

Proof. This can be proved in the same way as the analogous result about $\mathbf{k}$-algebra homomorphisms. □

Proof of Theorem 12.3. Consider the endomorphism ring $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n])$ of the $\mathbf{k}$-algebra $\mathbf{k}[S_n]$.

We have defined an endomorphism $R(x) \in \operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n])$ of the $\mathbf{k}$-module $\mathbf{k}[S_n]$ for each $x \in \mathbf{k}[S_n]$. Thus, we obtain a map

$$\begin{aligned} R : \mathbf{k}[S_n] &\to \operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n]), \\ x &\mapsto R(x). \end{aligned}$$

It is well-known (and straightforward to check) that this map R is a $\mathbf{k}$-algebra antihomomorphism (i.e., a $\mathbf{k}$-linear map satisfying $R(1) = 1$ and $R(xy) = R(y) \cdot R(x)$ for all $x, y \in \mathbf{k}[S_n]$). In fact, R is the standard right action of the $\mathbf{k}$-algebra $\mathbf{k}[S_n]$ on itself.

Let

$$t := \lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n \in \mathbf{k}[S_n].$$

Let ρ be the endomorphism $R(t)$ of $\mathbf{k}[S_n]$. We shall show that ρ is diagonalizable.

A univariate polynomial $P \in \mathbf{k}[X]$ is said to be *split separable* if it can be factored as a product of distinct monic polynomials of degree 1 (that is, if it can be written as $P = \prod_{j=1}^{k} (X - p_j)$, where $p_1, p_2, \ldots, p_k$ are k **distinct** elements of $\mathbf{k}$).

Let P be the polynomial $\prod_{\substack{I \subseteq [n-1] \text{ is} \\ \text{lacunar}}} (X - (\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n})) \in \mathbf{k}[X]$.

This polynomial P is split separable, since we assumed that the elements $\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}$ for all lacunar subsets $I \subseteq [n-1]$ are distinct.

Moreover, the definition of P yields

$$P(t) = \prod_{\substack{I \subseteq [n-1] \text{ is} \\ \text{lacunar}}} (t - (\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n})) = 0$$

by Theorem 12.1. However, R is a $\mathbf{k}$-algebra antihomomorphism. Hence, Proposition 12.4 (applied to $A = \mathbf{k}[S_n]$, $B = \operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n])$ and $f = R$) yields that $R(P(u)) = P(R(u))$ for any $u \in \mathbf{k}[S_n]$. Applying this to $u = t$, we obtain $R(P(t)) = P\left(\underbrace{R(t)}_{=\rho}\right) = P(\rho)$. Hence, $P(\rho) = R\left(\underbrace{P(t)}_{=0}\right) = R(0) = 0$. Therefore, the minimal polynomial of ρ divides P. (Note that the minimal polynomial of ρ is indeed well-defined, since ρ is an endomorphism of the finite-dimensional $\mathbf{k}$-vector space $\mathbf{k}[S_n]$.)

It is easy to see that any polynomial $Q \in \mathbf{k}[X]$ that divides a split separable polynomial must itself be split separable. Hence, the minimal polynomial of ρ is split separable (since this minimal polynomial divides P, but we know that P is split separable).

Now, recall the following fact (see, e.g., [Conrad22, Theorem 4.11] or [HofKun71, §6.4, Theorem 6] or [StoLui19, Proposition 3.8]): If the minimal polynomial of an endomorphism of a finite-dimensional $\mathbf{k}$-vector space is split separable, then this endomorphism is diagonalizable. Hence, the endomorphism ρ is diagonalizable (since the minimal polynomial of ρ is split separable). In other words, $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is diagonalizable (since $\rho = R\left(\underbrace{t}_{=\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n}\right) = R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$). This proves Theorem 12.3. $\square$

Note that Theorem 12.3 is not an "if and only if" statement. We do not know if there is an easy way to characterize when $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is diagonalizable.

Remark 12.5. Let I be a subset of $[n]$. Then, the numbers $m_{I,1}, m_{I,2}, \ldots, m_{I,n}$ together uniquely determine I. Indeed, a moment's thought reveals that

$$I = \{\ell \in [n] \mid m_{I,\ell} = 0\}.$$

Hence, if $\mathbf{k}$ is a field of characteristic 0, then the main assumption of Theorem 12.3 (viz., that the elements $\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}$ for all lacunar subsets $I \subseteq [n-1]$ are distinct) will be satisfied for any "sufficiently" generic $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$.

Example 12.6. We cannot use Theorem 12.3 to show that the random-to-below shuffle is always diagonalizable. For example, when $n = 12$, two lacunar sets ($\{1,6,8,10\}$ and $\{6,8,11\}$) yield $\sum\limits_{\ell=1}^{n} \frac{m_{I,\ell}}{n+1-\ell} = \frac{13573}{3960}$. This is the smallest example we could find, meaning that the shuffle is certainly diagonalizable when $\mathbf{k} = \mathbb{Q}$ and $n \leq 11$. It remains an open question whether the random-to-below shuffle is diagonalizable.

Example 12.7. There are diagonalizable one-sided cycle shuffles that do not satisfy the hypotheses of Theorem 12.3. For example, it is known since [DiFiPi92, Theorem 4.1] that the top-to-random shuffle (t_1) is diagonalizable. In our notation, it corresponds to $\lambda_1 = 1$ and $\lambda_2 = \lambda_3 = \ldots = \lambda_n = 0$, which does not satisfy the conditions of Theorem 12.3 in general.

Question 12.8. Can a necessary and sufficient criterion be found for the diagonalizability of a one-sided shuffle (as opposed to the merely sufficient one in Theorem 12.3)?

13. The multiplicities of the eigenvalues

13.1. The dimensions of F_i/F_{i-1}, explicitly

In Theorem 10.6 **(b)**, we have given bases for all the quotient $\mathbf{k}$-modules F_i/F_{i-1}. The sizes of these bases are the dimensions of these quotient $\mathbf{k}$-modules. Let us now characterize these dimensions more explicitly:

Theorem 13.1. Let $i \in [f_{n+1}]$. Let δ_i be the number of all permutations $w \in S_n$ satisfying $\operatorname{Qind} w = i$. Then:

(a) The $\mathbf{k}$-module F_i/F_{i-1} is free and has dimension (i.e., rank) equal to δ_i. (Here, of course, $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}}$ is the filtration from Theorem 8.1.)

(b) The number δ_i equals the number of all permutations $w \in S_n$ that satisfy

$$w(j) < w(j+1) \qquad \text{for all } j \in Q_i$$

and

$$w(j) > w(j+1) \qquad \text{for all } j \in Q_i'.$$

(c) Write the set Q_i in the form $Q_i = \{i_1 < i_2 < \cdots < i_p\}$, and set $i_0 = 1$ and $i_{p+1} = n+1$. Let $j_k = i_k - i_{k-1}$ for each $k \in [p+1]$. Then,

$$\delta_i = \binom{n}{j_1, j_2, \ldots, j_{p+1}} \cdot \prod_{k=2}^{p+1} (j_k - 1). \tag{40}$$

Here, $\binom{n}{j_1, j_2, \ldots, j_{p+1}}$ denotes the multinomial coefficient $\dfrac{n!}{j_1! j_2! \cdots j_{p+1}!}$.

(d) We have $\delta_i \mid n!$.

Proof. **(a)** Theorem 10.6 **(b)** shows that the $\mathbf{k}$-module F_i/F_{i-1} is free with basis $(\overline{a_w})_{w \in S_n;\ \operatorname{Qind} w = i}$. Hence, its dimension is the number of all permutations $w \in S_n$ satisfying $\operatorname{Qind} w = i$. But this latter number is δ_i (by the definition of δ_i). This proves Theorem 13.1 **(a)**.

(b) For any permutation $w \in S_n$, we have the following chain of equivalences:

$$\begin{aligned}
&(\operatorname{Qind} w = i) \\
\Longleftrightarrow\ & \left(Q_i' \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i\right) \qquad \text{(by Proposition 10.3)} \\
\Longleftrightarrow\ & \left(\underbrace{Q_i' \subseteq \operatorname{Des} w}_{\Longleftrightarrow\ (j \in \operatorname{Des} w \text{ for all } j \in Q_i')} \quad \text{and} \quad \underbrace{\operatorname{Des} w \subseteq [n-1] \setminus Q_i}_{\substack{\Longleftrightarrow\ (\operatorname{Des} w \text{ is disjoint from } Q_i) \\ (\text{since } \operatorname{Des} w \subseteq [n-1] \text{ always holds})}} \right) \\
\Longleftrightarrow\ & \left(\left(j \in \operatorname{Des} w \text{ for all } j \in Q_i'\right) \text{ and } \underbrace{(\operatorname{Des} w \text{ is disjoint from } Q_i)}_{\Longleftrightarrow\ (j \notin \operatorname{Des} w \text{ for all } j \in Q_i)} \right) \\
\Longleftrightarrow\ & \left(\left(\underbrace{j \in \operatorname{Des} w}_{\substack{\Longleftrightarrow\ (w(j) > w(j+1)) \\ (\text{by the definition of } \operatorname{Des} w)}} \quad \text{for all } j \in Q_i' \right) \text{ and } \left(\underbrace{j \notin \operatorname{Des} w}_{\substack{\Longleftrightarrow\ (w(j) \leq w(j+1)) \\ (\text{by the definition of } \operatorname{Des} w)}} \quad \text{for all } j \in Q_i \right) \right) \\
\Longleftrightarrow\ & \left(\left(w(j) > w(j+1) \text{ for all } j \in Q_i'\right) \text{ and } \left(\underbrace{w(j) \leq w(j+1)}_{\substack{\Longleftrightarrow\ (w(j) < w(j+1)) \\ (\text{since } w(j) \neq w(j+1) \\ (\text{because } w \text{ is a permutation}))}} \quad \text{for all } j \in Q_i \right) \right) \\
\Longleftrightarrow\ & \left(\left(w(j) > w(j+1) \text{ for all } j \in Q_i'\right) \text{ and } \left(w(j) < w(j+1) \text{ for all } j \in Q_i\right) \right) \\
\Longleftrightarrow\ & \left(\left(w(j) < w(j+1) \text{ for all } j \in Q_i\right) \text{ and } \left(w(j) > w(j+1) \text{ for all } j \in Q_i'\right) \right).
\end{aligned}$$

Thus, δ_i equals the number of all permutations $w \in S_n$ satisfying

$$\left(w(j) < w(j+1) \text{ for all } j \in Q_i\right) \text{ and } \left(w(j) > w(j+1) \text{ for all } j \in Q_i'\right)$$

(because δ_i was defined as the number of all permutations $w \in S_n$ satisfying $\operatorname{Qind} w = i$). This proves Theorem 13.1 **(b)**.

(c) We introduce a bit of terminology: If $K = [u, v]$ is an interval of $\mathbb{Z}$, and if T is an arbitrary subset of $\mathbb{Z}$, then a map $f : K \to T$ will be called *up-decreasing* if it satisfies

$$f(u) < f(u+1) > f(u+2) > f(u+3) > \cdots > f(v)$$

(that is, if it is increasing on $[u, u+1]$ and decreasing on $[u+1, v]$). For instance, the map $[5] \to [-3, 0]$ that sends each $k \in [5]$ to $-|k-2|$ is up-decreasing.

The following fact is easy to see:

> *Claim 1:* Let $h \geq 2$ be an integer. Let $K = [u, v]$ be an interval of $\mathbb{Z}$ having size $|K| = v - u + 1 = h$. Let T be a subset of $\mathbb{Z}$ that has size h. Then, the number of up-decreasing bijections $f : K \to T$ is $h - 1$.

[*Proof of Claim 1:* We WLOG assume that $K = [h]$ and $T = [h]$, because we can otherwise rename the elements of K and of T while preserving their relative order. Thus, the bijections $f : K \to T$ are precisely the permutations of $[h]$, and we must show that the number of up-decreasing permutations of $[h]$ is $h - 1$.

But this is easy to show: An up-decreasing permutation of $[h]$ is a permutation f of $[h]$ satisfying $f(1) < f(2) > f(3) > f(4) > \cdots > f(h)$. Thus, any up-decreasing permutation f of $[h]$ is uniquely determined by its first value $f(1)$, because its remaining values must be the remaining elements of $[h]$ in decreasing order (to ensure that $f(2) > f(3) > f(4) > \cdots > f(h)$ holds). The first value $f(1)$ cannot be h (since this would violate $f(1) < f(2)$), but can be any of the other $h - 1$ elements of $[h]$. Thus, there are $h - 1$ choices for $f(1)$, and each of these choices leads to a unique up-decreasing permutation f of $[h]$. Hence, there are $h - 1$ such permutations in total. This completes the proof of Claim 1.]

Recall that $i_1 < i_2 < \cdots < i_p$ are the p elements of $Q_i \subseteq [n-1]$, and we have furthermore set $i_0 = 1$ and $i_{p+1} = n + 1$. Hence,

$$1 = i_0 \leq i_1 < i_2 < \cdots < i_p < i_{p+1} = n + 1.$$

Define an interval

$$J_k := [i_{k-1},\ i_k - 1] \qquad \text{for each } k \in [p+1].$$

Then, the interval $[n]$ is the disjoint union $J_1 \sqcup J_2 \sqcup \cdots \sqcup J_{p+1}$. We have

$$Q_i = \{i_1, i_2, \ldots, i_p\} \tag{41}$$

and

$$Q_i' = \{1,\ 2,\ \ldots,\ i_1 - 2\} \cup \bigcup_{k=2}^{p+1} \{i_{k-1} + 1,\ i_{k-1} + 2,\ \ldots,\ i_k - 2\}. \tag{42}$$

Note further that each $k \in [p+1]$ satisfies $|J_k| = i_k - i_{k-1}$ (since $J_k = [i_{k-1},\ i_k - 1]$) and therefore $|J_k| = i_k - i_{k-1} = j_k$. Furthermore, note that $j_1, j_2, \ldots, j_{p+1}$ are nonnegative integers (since each $k \in [p+1]$ satisfies $j_k = i_k - \underbrace{i_{k-1}}_{\leq i_k} \geq i_k - i_k = 0$).

Finally, it is easy to see that

$$j_k \geq 2 \qquad \text{for each } k \in [2, p+1]. \tag{43}$$

[*Proof of (43):* Let $k \in [2, p+1]$. Then, both $k - 1$ and k belong to $[p+1]$.

The set Q_i is a lacunar subset of $[n-1]$ (since $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are all the lacunar subsets of $[n-1]$). Thus, the set $Q_i \cup \{n+1\}$ is lacunar as well (since each element of Q_i is $\leq n - 1$ and thus differs by at least 2 from the new element $n + 1$). Hence, any two distinct elements of the set $Q_i \cup \{n+1\}$ differ by at least 2.

However, from $Q_i = \{i_1 < i_2 < \cdots < i_p\}$ and $i_{p+1} = n + 1$, we obtain $Q_i \cup \{n+1\} = \{i_1 < i_2 < \cdots < i_p < i_{p+1}\}$ (since $Q_i \subseteq [n-1]$). Therefore, i_{k-1} and i_k are two distinct elements of the set $Q_i \cup \{n+1\}$ (since both $k - 1$ and k belong to $[p+1]$). Consequently,

i_{k-1} and i_k differ by at least 2 (since any two distinct elements of the set $Q_i \cup \{n+1\}$ differ by at least 2). In other words, $i_k - i_{k-1} \geq 2$ (since $i_{k-1} < i_k$). But the definition of j_k yields $j_k = i_k - i_{k-1} \geq 2$. This proves (43).]

Now, Theorem 13.1 **(b)** shows that δ_i is the number of all permutations $w \in S_n$ that satisfy

$$w(j) < w(j+1) \qquad \text{for all } j \in Q_i \tag{44}$$

and

$$w(j) > w(j+1) \qquad \text{for all } j \in Q_i'. \tag{45}$$

In view of (41) and (42), we can rewrite this as follows: δ_i is the number of all permutations $w \in S_n$ that satisfy

$$w(1) > w(2) > w(3) > \cdots > w(i_1 - 1)$$

and

$$w(i_{k-1}) < w(i_{k-1}+1) > w(i_{k-1}+2) > w(i_{k-1}+3) > \cdots > w(i_k - 1)$$

for each $k \in [2, p+1]$. In other words, δ_i is the number of all permutations $w \in S_n$ such that the restriction $w\mid_{J_1}$ is strictly decreasing whereas the restrictions $w\mid_{J_2}$, $w\mid_{J_3}$, $\ldots$, $w\mid_{J_{p+1}}$ are up-decreasing (since $J_k = [i_{k-1},\ i_k - 1]$ for each $k \in [p+1]$). We can construct such a permutation w as follows:

- First, we choose the **sets** $w(J_k)$ for all $k \in [p+1]$. In doing so, we must ensure that these $p+1$ sets are disjoint and cover the entire set $[n]$, and have the size $|w(J_k)| = |J_k| = j_k$ for each k. Thus, there are $\dbinom{n}{j_1, j_2, \ldots, j_{p+1}}$ many options at this step.
- At this point, the restriction $w\mid_{J_1}$ is already uniquely determined, since $w\mid_{J_1}$ has to be strictly decreasing and its image $w(J_1)$ is already chosen.
- Now, for each $k \in [2, p+1]$, we choose the restriction $w\mid_{J_k}$. This restriction has to be an up-decreasing bijection from the interval J_k to the (already chosen) set $w(J_k)$, which has size $|w(J_k)| = |J_k| = j_k$; thus, by Claim 1 (applied to $h = j_k$ and $K = J_k$ and $T = w(J_k)$), there are $j_k - 1$ options for this restriction $w\mid_{J_k}$ (since (43) yields $j_k \geq 2$). Hence, in total, we have $\prod\limits_{k=2}^{p+1}(j_k - 1)$ options at this step.

Altogether, the total number of possibilities to perform this construction is thus $\dbinom{n}{j_1, j_2, \ldots, j_{p+1}} \cdot \prod\limits_{k=2}^{p+1}(j_k - 1)$. Hence,

$$\delta_i = \binom{n}{j_1, j_2, \ldots, j_{p+1}} \cdot \prod_{k=2}^{p+1}(j_k - 1).$$

This proves Theorem 13.1 **(c)**.

(d) Define the integers $i_0, i_1, \ldots, i_{p+1}$ and $j_1, j_2, \ldots, j_{p+1}$ as in Theorem 13.1 **(c)**. Then, we have $j_k \geq 2$ for each $k \in [2, p+1]$ (in fact, this is the inequality (43), which has been shown in our above proof of Theorem 13.1 **(c)**). Hence, for each $k \in [2, p+1]$, we have

$$j_k! = \underbrace{1 \cdot 2 \cdot \cdots \cdot (j_k - 2)}_{=(j_k-2)!} \cdot (j_k - 1) \cdot j_k = (j_k - 2)! \cdot (j_k - 1) \cdot j_k$$

and therefore

$$j_k - 1 = \frac{j_k!}{(j_k - 2)! \cdot j_k}. \tag{46}$$

The definition of a multinomial coefficient yields

$$\binom{n}{j_1, j_2, \ldots, j_{p+1}} = \frac{n!}{j_1! j_2! \cdots j_{p+1}!} = \frac{n!}{\prod\limits_{k=1}^{p+1} j_k!} = \frac{n!}{j_1! \prod\limits_{k=2}^{p+1} j_k!}.$$

From (40), we now obtain

$$\delta_i = \underbrace{\binom{n}{j_1, j_2, \ldots, j_{p+1}}}_{= \frac{n!}{j_1! \prod\limits_{k=2}^{p+1} j_k!}} \cdot \prod_{k=2}^{p+1} \underbrace{(j_k - 1)}_{\substack{= \frac{j_k!}{(j_k-2)! \cdot j_k} \\ \text{(by (46))}}} = \frac{n!}{j_1! \prod\limits_{k=2}^{p+1} j_k!} \cdot \prod_{k=2}^{p+1} \frac{j_k!}{(j_k - 2)! \cdot j_k}$$

$$= \frac{n!}{j_1!} \cdot \prod_{k=2}^{p+1} \left(\frac{j_k!}{(j_k - 2)! \cdot j_k} / j_k! \right) = \frac{n!}{j_1! \cdot \prod\limits_{k=2}^{p+1} ((j_k - 2)! \cdot j_k)}.$$

Thus, we obtain $\delta_i \mid n!$ (since the denominator $j_1! \cdot \prod\limits_{k=2}^{p+1} ((j_k - 2)! \cdot j_k)$ in this equality is clearly an integer). This proves Theorem 13.1 **(d)**. □

13.2. The multiplicities of the eigenvalues

Finally, we can find the algebraic multiplicities of the eigenvalues of the endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ (when $\mathbf{k}$ is a field and $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$ are arbitrary). Roughly speaking, we want to claim that each eigenvalue $\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}$ (where $I \subseteq [n-1]$ is a lacunar subset) has algebraic multiplicity δ_i, where $i \in [f_{n+1}]$ is chosen such that $I = Q_i$ (and where δ_i is as in Theorem 13.1). This is not fully precise; indeed, if some lacunar subsets $I \subseteq [n-1]$ produce the same eigenvalues $\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}$, then their respective δ_i's need to be added together to form the right algebraic multiplicity. The technically correct statement of our claim is thus as follows:

Theorem 13.2. Assume that $\mathbf{k}$ is a field. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. For each $i \in [f_{n+1}]$, let δ_i be the number of all permutations $w \in S_n$ satisfying $\operatorname{Qind} w = i$. For each $i \in [f_{n+1}]$, we set

$$g_i := \lambda_1 m_{Q_i,1} + \lambda_2 m_{Q_i,2} + \cdots + \lambda_n m_{Q_i,n} = \sum_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell} \in \mathbf{k}.$$

Let $\kappa \in \mathbf{k}$. Then, the algebraic multiplicity of κ as an eigenvalue of $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ equals

$$\sum_{\substack{i \in [f_{n+1}];\\ g_i = \kappa}} \delta_i.$$

Proof. We shall use the notations introduced in the proof of Corollary 12.2. In that proof, we have shown that the matrix M is upper-triangular.

Recall that the eigenvalues of a triangular matrix are its diagonal entries, and moreover, the algebraic multiplicity of an eigenvalue is the number of times that it appears on the main diagonal. We can apply this fact to the matrix M (since M is upper-triangular), and thus conclude that

$$\begin{aligned}
&(\text{the algebraic multiplicity of } \kappa \text{ as an eigenvalue of } M)\\
&= (\text{the number of times that } \kappa \text{ appears on the main diagonal of } M)\\
&= \left(\text{the number of } j \in [n!] \text{ such that } \mu_{j,j} = \kappa\right) \qquad \left(\text{since } M = \left(\mu_{i,j}\right)_{i,j \in [n!]}\right)\\
&= \left(\text{the number of } j \in [n!] \text{ such that } g_{\operatorname{Qind}(w_j)} = \kappa\right)\\
&\qquad\qquad \left(\begin{array}{c}\text{since Claim 1 from the proof of Corollary 12.2}\\ \text{yields that } \mu_{j,j} = g_{\operatorname{Qind}(w_j)} \text{ for each } j \in [n!]\end{array}\right)\\
&= \left(\text{the number of } w \in S_n \text{ such that } g_{\operatorname{Qind} w} = \kappa\right)\\
&\qquad\qquad (\text{since } w_1, w_2, \ldots, w_{n!} \text{ are the } n! \text{ permutations in } S_n)\\
&= \sum_{\substack{i \in [f_{n+1}];\\ g_i = \kappa}} \underbrace{(\text{the number of } w \in S_n \text{ such that } \operatorname{Qind} w = i)}_{\substack{=\delta_i \\ (\text{by the definition of } \delta_i)}}\\
&\qquad\qquad (\text{here we have split the sum up according to the value of } \operatorname{Qind} w)\\
&= \sum_{\substack{i \in [f_{n+1}];\\ g_i = \kappa}} \delta_i.
\end{aligned}$$

This proves Theorem 13.2. $\square$

14. Further algebraic consequences

In this section, we shall derive some more corollaries from the above. To be more specific, we first study the algebraic properties of the antipode of the one-sided cycle shuffle $\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n$; this corresponds to the reversal of the corresponding Markov chain. Then, we discuss the endomorphism $L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ corresponding to left multiplication (as opposed to right multiplication, which we have studied before) by the shuffle. We next use our notions of Q-index and non-shadow to subdivide the Boolean algebra of the set $[n-1]$ into Boolean intervals indexed by the lacunar subsets of $[n-1]$. Finally, we explore what known results about the top-to-random shuffle our results can and cannot prove.

14.1. Below-to-somewhere shuffles

We have so far been considering the somewhere-to-below shuffles $t_1, t_2, \ldots, t_n$, which are sums of cycles. If we invert these cycles (i.e., reverse the order of cycling), we obtain new elements of $\mathbf{k}[S_n]$, which may be called the "below-to-somewhere shuffles". Here is their precise definition:

For each $\ell \in [n]$, we define the element

$$t'_\ell := \mathrm{cyc}_\ell + \mathrm{cyc}_{\ell+1,\ell} + \mathrm{cyc}_{\ell+2,\ell+1,\ell} + \cdots + \mathrm{cyc}_{n,n-1,\ldots,\ell} \in \mathbf{k}[S_n]. \tag{47}$$

In terms of card shuffling, this element t'_ℓ corresponds to randomly picking a card from the bottommost $n-\ell+1$ positions in the deck (with uniform probabilities) and moving it to position ℓ. Thus, we call $t'_1, t'_2, \ldots, t'_n$ the *below-to-somewhere shuffles*. The first of them, t'_1, is known as the *random-to-top shuffle* (as it picks a random card and surfaces it to the top of the deck).

It is natural to ask whether our above properties of $t_1, t_2, \ldots, t_n$ have analogues for these new elements $t'_1, t'_2, \ldots, t'_n$. For example, an analogue of Theorem 12.1 holds:

Theorem 14.1. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Let $t' := \lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n$. Then,

$$\prod_{\substack{I \subseteq [n-1] \text{ is} \\ \text{lacunar}}} \left(t' - (\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n})\right) = 0.$$

Theorem 14.1 can actually be deduced from Theorem 12.1 pretty easily:

Let S be the $\mathbf{k}$-linear map $\mathbf{k}[S_n] \to \mathbf{k}[S_n]$ that sends each permutation $w \in S_n$ to its inverse w^{-1}. This map S is known as the *antipode* of the group algebra $\mathbf{k}[S_n]$ (see, e.g., [Meusbu21, Example 2.2.8]); it is an involution (i.e., it satisfies $S \circ S = \mathrm{id}$) and a $\mathbf{k}$-algebra antihomomorphism (i.e., it is $\mathbf{k}$-linear and satisfies $S(1) = 1$ and $S(uv) = S(v) \cdot S(u)$ for all $u, v \in \mathbf{k}[S_n]$). For any k distinct elements $i_1, i_2, \ldots, i_k$ of

$[n]$, we have

$$S\left(\operatorname{cyc}_{i_1,i_2,\ldots,i_k}\right) = \left(\operatorname{cyc}_{i_1,i_2,\ldots,i_k}\right)^{-1} \qquad \text{(by the definition of } S\text{)}$$
$$= \operatorname{cyc}_{i_k,i_{k-1},\ldots,i_1}. \tag{48}$$

Hence, for each $\ell \in [n]$, we have

$$\begin{aligned} S\left(t_\ell\right) &= S\left(\operatorname{cyc}_\ell + \operatorname{cyc}_{\ell,\ell+1} + \operatorname{cyc}_{\ell,\ell+1,\ell+2} + \cdots + \operatorname{cyc}_{\ell,\ell+1,\ldots,n}\right) \qquad \text{(by (1))} \\ &= S\left(\operatorname{cyc}_\ell\right) + S\left(\operatorname{cyc}_{\ell,\ell+1}\right) + S\left(\operatorname{cyc}_{\ell,\ell+1,\ell+2}\right) + \cdots + S\left(\operatorname{cyc}_{\ell,\ell+1,\ldots,n}\right) \\ &= \operatorname{cyc}_\ell + \operatorname{cyc}_{\ell+1,\ell} + \operatorname{cyc}_{\ell+2,\ell+1,\ell} + \cdots + \operatorname{cyc}_{n,n-1,\ldots,\ell} \qquad \text{(by (48))} \\ &= t'_\ell \qquad \text{(by (47))}. \end{aligned} \tag{49}$$

Thus, we can obtain properties of $t'_1, t'_2, \ldots, t'_n$ by applying the map S to corresponding properties of $t_1, t_2, \ldots, t_n$. In particular, we can obtain Theorem 14.1 this way:

Proof of Theorem 14.1. Let $t := \lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n$. Thus,

$$\begin{aligned} S\left(t\right) &= S\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right) \\ &= \lambda_1 S\left(t_1\right) + \lambda_2 S\left(t_2\right) + \cdots + \lambda_n S\left(t_n\right) \qquad \text{(since } S \text{ is } \mathbf{k}\text{-linear)} \\ &= \lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n \qquad \text{(by (49))} \\ &= t' \qquad \text{(by the definition of } t'\text{)}. \end{aligned}$$

Now, let P be the polynomial $\prod\limits_{\substack{I\subseteq[n-1] \text{ is} \\ \text{lacunar}}} \left(X - \left(\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}\right)\right) \in \mathbf{k}\left[X\right]$. Then,

$$P\left(t\right) = \prod_{\substack{I\subseteq[n-1] \text{ is} \\ \text{lacunar}}} \left(t - \left(\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}\right)\right) = 0$$

(by Theorem 12.1). Thus, $S\left(P\left(t\right)\right) = S\left(0\right) = 0$.

However, S is a $\mathbf{k}$-algebra antihomomorphism. Thus, Proposition 12.4 (applied to $A = \mathbf{k}\left[S_n\right]$, $B = \mathbf{k}\left[S_n\right]$, $f = S$ and $u = t$) yields that

$$S\left(P\left(t\right)\right) = P\left(\underbrace{S\left(t\right)}_{=t'}\right) = P\left(t'\right) = \prod_{\substack{I\subseteq[n-1] \text{ is} \\ \text{lacunar}}} \left(t' - \left(\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}\right)\right)$$

(by the definition of P). Comparing this with $S\left(P\left(t\right)\right) = 0$, we obtain

$$\prod_{\substack{I\subseteq[n-1] \text{ is} \\ \text{lacunar}}} \left(t' - \left(\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n}\right)\right) = 0.$$

This proves Theorem 14.1. $\square$

A more interesting question is to find an analogue of Theorem 4.1 for the below-to-somewhere shuffles: Is there a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$ with respect to which the $\mathbf{k}$-module endomorphisms $R(\lambda_1 t_1' + \lambda_2 t_2' + \cdots + \lambda_n t_n')$ are represented by triangular matrices for all $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$? Again, the answer is "yes", but this basis is no longer the descent-destroying basis $(a_w)_{w \in S_n}$ (ordered by increasing Q-index); instead, it is the **dual** basis to $(a_w)_{w \in S_n}$ with respect to a certain bilinear form (ordered by **decreasing** Q-index). Let us elaborate on this now.[25]

First, we recall some concepts from linear algebra (although we are working at a slightly unusual level of generality, since we do not require $\mathbf{k}$ to be a field):

- The *dual* of a $\mathbf{k}$-module U is defined to be the $\mathbf{k}$-module $\operatorname{Hom}_{\mathbf{k}}(U, \mathbf{k})$ of all $\mathbf{k}$-linear maps from U to $\mathbf{k}$. We denote this dual by $U^\vee$.

- A *bilinear form* on two $\mathbf{k}$-modules U and V is defined to be a map $f : U \times V \to \mathbf{k}$ that is $\mathbf{k}$-linear in each of its two arguments. A bilinear form $f : U \times V \to \mathbf{k}$ canonically induces a $\mathbf{k}$-module homomorphism

$$\begin{aligned} f^\circ : V &\to U^\vee, \\ v &\mapsto (\text{the map } U \to \mathbf{k} \text{ that sends each } u \in U \text{ to } f(u, v)). \end{aligned}$$

  A bilinear form $f : U \times V \to \mathbf{k}$ is called *nondegenerate* if the $\mathbf{k}$-module homomorphism $f^\circ : V \to U^\vee$ is an isomorphism.

- If U and V are two $\mathbf{k}$-modules with bases $(u_w)_{w \in W}$ and $(v_w)_{w \in W}$, respectively[26], and if $f : U \times V \to \mathbf{k}$ is a bilinear form, then we say that the basis $(v_w)_{w \in W}$ is *dual* to $(u_w)_{w \in W}$ with respect to f if and only if we have

$$\left(f(u_p, v_q) = [p = q] \qquad \text{for all } p, q \in W \right).$$

  Here, we are using the *Iverson bracket notation*: For each statement $\mathcal{A}$, we let $[\mathcal{A}]$ denote the truth value of $\mathcal{A}$ (that is, 1 if $\mathcal{A}$ is true and 0 if $\mathcal{A}$ is false).

The following three general facts about dual bases are easy and known:

Proposition 14.2. Let U and V be two $\mathbf{k}$-modules, and let $f : U \times V \to \mathbf{k}$ be a bilinear form. Let $(u_w)_{w \in W}$ be a basis of the $\mathbf{k}$-module U such that the set W is finite. Let $(v_w)_{w \in W}$ be a basis of the $\mathbf{k}$-module V that is dual to $(u_w)_{w \in W}$. Then, the bilinear form f is nondegenerate.

Proof sketch. Recall that $(u_w)_{w \in W}$ is a basis of U. For each $w \in W$, let $c_w : U \to \mathbf{k}$ be the map that sends each $u \in U$ to the u_w-coordinate of u with respect to this basis.

[25] Note that, with respect to the **standard** basis $(w)_{w \in S_n}$ of $\mathbf{k}[S_n]$, the matrix representing the endomorphism $R(\lambda_1 t_1' + \lambda_2 t_2' + \cdots + \lambda_n t_n')$ is the transpose of the matrix representing the endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$. However, neither of these two matrices is triangular.

[26] Note that the bases must have the same indexing set in this definition.

This map c_w is $\mathbf{k}$-linear and thus belongs to $U^\vee$. Now, it is easy to see that $(c_w)_{w\in W}$ is a basis of $U^\vee$ (since W is finite).

However, the basis $(v_w)_{w\in W}$ is dual to $(u_w)_{w\in W}$. Thus, $f^\circ(v_w) = c_w$ for each $w \in W$ (since any $w, p \in W$ satisfy $(f^\circ(v_w))(u_p) = f(u_p, v_w) = [p = w] = c_w(u_p)$). In other words, the map f° sends the basis $(v_w)_{w\in W}$ of V to the basis $(c_w)_{w\in W}$ of $U^\vee$. This entails that f° is an isomorphism (since any $\mathbf{k}$-linear map that sends a basis of its domain to a basis of its target must be an isomorphism). In other words, f is nondegenerate. This proves Proposition 14.2. □

Proposition 14.3. Let U and V be two $\mathbf{k}$-modules, and let $f : U \times V \to \mathbf{k}$ be a nondegenerate bilinear form. Let $(u_w)_{w\in W}$ be a basis of the $\mathbf{k}$-module U, where W is a finite set. Then, there is a unique basis of V that is dual to $(u_w)_{w\in W}$ with respect to f.

Proof sketch. Since f is nondegenerate, the map $f^\circ : V \to U^\vee$ is an isomorphism. Thus, we can WLOG assume that $V = U^\vee$ and that f is the standard pairing between U and $U^\vee$ (that is, the bilinear form $U \times U^\vee \to \mathbf{k}$ that sends each pair (u, f) to $f(u) \in \mathbf{k}$). Now, recall that $(u_w)_{w\in W}$ is a basis of U. For each $w \in W$, let $c_w : U \to \mathbf{k}$ be the map that sends each $u \in U$ to the u_w-coordinate of u with respect to this basis. This map c_w is $\mathbf{k}$-linear and thus belongs to $U^\vee$. Now, it is easy to see that $(c_w)_{w\in W}$ is a basis of $U^\vee = V$ that is dual to $(u_w)_{w\in W}$ with respect to f, and moreover it is the only such basis. Hence, Proposition 14.3 follows. □

Proposition 14.4. Let U and V be two $\mathbf{k}$-modules, and let $f : U \times V \to \mathbf{k}$ be a bilinear form. Let $(u_w)_{w\in W}$ be a basis of the $\mathbf{k}$-module U such that the set W is finite. Let $(v_w)_{w\in W}$ be a basis of the $\mathbf{k}$-module V that is dual to $(u_w)_{w\in W}$. Then:

(a) For any $u \in U$, we have

$$u = \sum_{w\in W} f(u, v_w)\, u_w.$$

(b) For any $v \in V$, we have

$$v = \sum_{w\in W} f(u_w, v)\, v_w.$$

Proof. **(a)** Let $u \in U$. Recall that $(u_w)_{w\in W}$ is a basis of the $\mathbf{k}$-module U. Thus, we can write u as a $\mathbf{k}$-linear combination of this basis. In other words, there exists a family $(\lambda_w)_{w\in W} \in \mathbf{k}^W$ of scalars such that

$$u = \sum_{w\in W} \lambda_w u_w. \tag{50}$$

Consider this family.

We have assumed that the basis $(v_w)_{w\in W}$ is dual to $(u_w)_{w\in W}$. In other words, we have

$$\left(f\left(u_p, v_q\right) = [p = q] \qquad \text{for all } p, q \in W\right). \tag{51}$$

Now, for each $q \in W$, we have

$$\begin{aligned}
f\left(u, v_q\right) &= f\left(\sum_{w\in W} \lambda_w u_w,\ v_q\right) \qquad \left(\text{since } u = \sum_{w\in W} \lambda_w u_w\right) \\
&= \sum_{w\in W} \lambda_w \underbrace{f\left(u_w, v_q\right)}_{\substack{=[w=q] \\ \text{(by (51), applied to } p=w)}} \qquad \text{(since } f \text{ is a bilinear form)} \\
&= \sum_{w\in W} \lambda_w [w = q] = \lambda_q \underbrace{[q = q]}_{=1} + \sum_{\substack{w\in W; \\ w\neq q}} \lambda_w \underbrace{[w = q]}_{\substack{=0 \\ \text{(since } w\neq q)}} \\
&\qquad \text{(here, we have split off the addend for } w = q \text{ from the sum)} \\
&= \lambda_q + \underbrace{\sum_{\substack{w\in W; \\ w\neq q}} \lambda_w 0}_{=0} = \lambda_q.
\end{aligned}$$

Renaming the variable q as w in this result, we obtain the following: For each $w \in W$, we have

$$f\left(u, v_w\right) = \lambda_w. \tag{52}$$

Now, (50) becomes

$$u = \sum_{w\in W} \underbrace{\lambda_w}_{\substack{=f(u,v_w) \\ \text{(by (52))}}} u_w = \sum_{w\in W} f\left(u, v_w\right) u_w.$$

This proves Proposition 14.4 **(a)**.

(b) This is analogous to the proof of part **(a)** (but, of course, the obvious changes need to be made – e.g., the equality (50) is replaced by $v = \sum_{w\in W} \lambda_w v_w$, and the equality (52) is replaced by $f\left(u_w, v\right) = \lambda_w$). $\square$

Now, we apply the above to the $\mathbf{k}$-module $\mathbf{k}\left[S_n\right]$. We define a bilinear form $f : \mathbf{k}\left[S_n\right] \times \mathbf{k}\left[S_n\right] \to \mathbf{k}$ by setting

$$f\left(p, q\right) = [p = q] \qquad \text{for all } p, q \in S_n. \tag{53}$$

(This defines a unique bilinear form, since $(w)_{w\in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}\left[S_n\right]$.) Clearly, the basis $(w)_{w\in S_n}$ of $\mathbf{k}\left[S_n\right]$ is dual to itself with respect to this form f. Thus, Proposition 14.2 (applied to $U = \mathbf{k}\left[S_n\right]$, $V = \mathbf{k}\left[S_n\right]$, $W = S_n$, $(u_w)_{w\in W} = (w)_{w\in S_n}$ and $(v_w)_{w\in W} = (w)_{w\in S_n}$) yields that the bilinear form f is nondegenerate. Hence, Proposition 14.3 (applied to $U = \mathbf{k}\left[S_n\right]$, $V = \mathbf{k}\left[S_n\right]$, $W = S_n$

and $(u_w)_{w \in W} = (a_w)_{w \in S_n}$) yields that there is a unique basis of $\mathbf{k}[S_n]$ that is dual to $(a_w)_{w \in S_n}$ with respect to f (since Proposition 9.6 tells us that $(a_w)_{w \in S_n}$ is a basis of $\mathbf{k}[S_n]$). Let us denote this basis by $(b_w)_{w \in S_n}$. Thus, the basis $(b_w)_{w \in S_n}$ is dual to $(a_w)_{w \in S_n}$; in other words, we have

$$f(a_p, b_q) = [p = q] \qquad \text{for all } p, q \in S_n. \tag{54}$$

Now, we claim the following analogue to Theorem 11.1:

Theorem 14.5. Let $w \in S_n$ and $\ell \in [n]$. Let $i = \operatorname{Qind} w$. Then,

$$b_w t'_\ell = m_{Q_i,\ell} b_w + (\text{a } \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v > i).$$

Once we have proved Theorem 14.5, it will follow that if we order the basis $(b_w)_{w \in S_n}$ in the order of decreasing Q-index, the endomorphisms $R(t'_1), R(t'_2), \ldots, R(t'_n)$ (and thus also their linear combinations $R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n)$) will be represented by upper-triangular matrices. The analogue of Theorem 4.1 for below-to-somewhere shuffles will thus follow. So it remains to prove Theorem 14.5. In order to do so, we need a simple lemma about the bilinear form $f : \mathbf{k}[S_n] \times \mathbf{k}[S_n] \to \mathbf{k}$ defined by (53):

Lemma 14.6. We have

$$f(u, vS(x)) = f(ux, v) \qquad \text{for all } x, u, v \in \mathbf{k}[S_n].$$

Proof. Let $x, u, v \in \mathbf{k}[S_n]$. We must prove the equality $f(u, vS(x)) = f(ux, v)$. Both sides of this equality depend $\mathbf{k}$-linearly on each of the three elements x, u, v (since the map f is $\mathbf{k}$-linear in each argument, whereas the map S is $\mathbf{k}$-linear). Hence, in order to prove this equality, we can WLOG assume that all of x, u, v belong to the basis $(w)_{w \in S_n}$ of the $\mathbf{k}$-module $\mathbf{k}[S_n]$. Assume this.

Thus, $x, u, v \in S_n$. The definition of S now yields $S(x) = x^{-1}$ (since $x \in S_n$). Moreover, $vx^{-1} \in S_n$ (since v and x^{-1} belong to S_n) and $ux \in S_n$ (since u and x belong to S_n). Furthermore, (53) (applied to $p = u$ and $q = vx^{-1}$) yields $f(u, vx^{-1}) = [u = vx^{-1}]$ (since u and vx^{-1} belong to S_n). Likewise, (53) (applied to $p = ux$ and $q = v$) yields $f(ux, v) = [ux = v]$.

However, the two statements $u = vx^{-1}$ and $ux = v$ are clearly equivalent. Thus, their truth values are equal. In other words, $[u = vx^{-1}] = [ux = v]$. Combining what we have shown above, we obtain

$$f\left(u, v\underbrace{S(x)}_{=x^{-1}}\right) = f\left(u, vx^{-1}\right) = \left[u = vx^{-1}\right] = [ux = v] = f(ux, v)$$

(since $f(ux, v) = [ux = v]$). This is precisely the equality that we wanted to prove. Thus, Lemma 14.6 is proved. $\square$

Proof of Theorem 14.5. Forget that we fixed w and i (but keep ℓ fixed). For each $u \in S_n$, define two elements

$$\widetilde{a}_u := a_u t_\ell - m_{\mathrm{Q}_{\operatorname{Qind} u},\ell} a_u \qquad \text{and} \qquad \widetilde{b}_u := b_u t'_\ell - m_{\mathrm{Q}_{\operatorname{Qind} u},\ell} b_u$$

of $\mathbf{k}[S_n]$.

We know that the family $(a_w)_{w \in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$; we called this basis the descent-destroying basis. We also know that $(b_w)_{w \in S_n}$ is a basis of $\mathbf{k}[S_n]$ that is dual to $(a_w)_{w \in S_n}$ with respect to f. Thus, Proposition 14.4 **(a)** (applied to $U = \mathbf{k}[S_n]$, $V = \mathbf{k}[S_n]$, $W = S_n$, $(u_w)_{w \in W} = (a_w)_{w \in S_n}$ and $(v_w)_{w \in W} = (b_w)_{w \in S_n}$) shows that each $u \in \mathbf{k}[S_n]$ satisfies

$$u = \sum_{w \in S_n} f(u, b_w)\, a_w. \tag{55}$$

Furthermore, Proposition 14.4 **(b)** (applied to $U = \mathbf{k}[S_n]$, $V = \mathbf{k}[S_n]$, $W = S_n$, $(u_w)_{w \in W} = (a_w)_{w \in S_n}$ and $(v_w)_{w \in W} = (b_w)_{w \in S_n}$) shows that each $v \in \mathbf{k}[S_n]$ satisfies

$$v = \sum_{w \in S_n} f(a_w, v)\, b_w. \tag{56}$$

For each $u \in S_n$, we have

$$\widetilde{a}_u = \sum_{w \in S_n} f(\widetilde{a}_u, b_w)\, a_w \tag{57}$$

(by (55), applied to $\widetilde{a}_u$ instead of u).

For each $v \in S_n$, we have

$$\widetilde{b}_v = \sum_{w \in S_n} f\left(a_w, \widetilde{b}_v\right) b_w$$

(by (56), applied to $\widetilde{b}_v$ instead of v). Renaming the indices v and w as w and v in this sentence, we obtain the following: For each $w \in S_n$, we have

$$\widetilde{b}_w = \sum_{v \in S_n} f\left(a_v, \widetilde{b}_w\right) b_v. \tag{58}$$

We shall now prove the following:

> *Claim 1:* Let $u, w \in S_n$ be such that $\operatorname{Qind} w \geq \operatorname{Qind} u$. Then, $f(\widetilde{a}_u, b_w) = 0$.
>
> *Claim 2:* Let $u, w \in S_n$. Then, $f\left(a_u, \widetilde{b}_w\right) = f(\widetilde{a}_u, b_w)$.

[*Proof of Claim 1:* Let $j = \operatorname{Qind} u$. By assumption, we have $\operatorname{Qind} w \geq \operatorname{Qind} u = j$. Thus, w does not satisfy $\operatorname{Qind} w < j$.

Theorem 11.1 (applied to u and j instead of w and i) yields

$$a_u t_\ell = m_{Q_j,\ell} a_u + \left(\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < j\right)$$

(since $j = \operatorname{Qind} u$). In other words,

$$a_u t_\ell - m_{Q_j,\ell} a_u = \left(\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < j\right).$$

In view of

$$\widetilde{a}_u = a_u t_\ell - m_{Q_{\operatorname{Qind} u},\ell} a_u = a_u t_\ell - m_{Q_j,\ell} a_u \qquad (\text{since } \operatorname{Qind} u = j),$$

we can rewrite this as

$$\widetilde{a}_u = \left(\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < j\right).$$

This equality shows that $\widetilde{a}_u$ can be written as a $\mathbf{k}$-linear combination of the descent-destroying basis, and the only basis elements that appear (with nonzero coefficients) in this combination are the a_v for $v \in S_n$ satisfying $\operatorname{Qind} v < j$. Hence, if $v \in S_n$ does not satisfy $\operatorname{Qind} v < j$, then a_v does not appear in the expansion of $\widetilde{a}_u$ as a $\mathbf{k}$-linear combination of the descent-destroying basis. Applying this to $v = w$, we conclude that a_w does not appear in the expansion of $\widetilde{a}_u$ as a $\mathbf{k}$-linear combination of the descent-destroying basis (since $w \in S_n$ does not satisfy $\operatorname{Qind} w < j$). In other words, the coefficient of a_w when $\widetilde{a}_u$ is expanded as a $\mathbf{k}$-linear combination of the descent-destroying basis is 0.

However, the equality (57) shows that $f(\widetilde{a}_u, b_w)$ is the coefficient of a_w when $\widetilde{a}_u$ is expanded as a $\mathbf{k}$-linear combination of the descent-destroying basis. But we have just shown that this coefficient is 0. Thus, we conclude that $f(\widetilde{a}_u, b_w) = 0$. This proves Claim 1.]

[*Proof of Claim 2:* The definition of $\widetilde{a}_u$ yields $\widetilde{a}_u = a_u t_\ell - m_{Q_{\operatorname{Qind} u},\ell} a_u$. Thus,

$$\begin{aligned}
f(\widetilde{a}_u, b_w) &= f\left(a_u t_\ell - m_{Q_{\operatorname{Qind} u},\ell} a_u,\ b_w\right) \\
&= f(a_u t_\ell, b_w) - m_{Q_{\operatorname{Qind} u},\ell} \underbrace{f(a_u, b_w)}_{\substack{=[u=w] \\ \text{(by (54), applied to } p=u \\ \text{and } q=w)}} \qquad (\text{since } f \text{ is a bilinear form}) \\
&= f(a_u t_\ell, b_w) - m_{Q_{\operatorname{Qind} u},\ell} [u = w]. \qquad (59)
\end{aligned}$$

However, it is easy to see that

$$m_{Q_{\operatorname{Qind} u},\ell} [u = w] = m_{Q_{\operatorname{Qind} w},\ell} [u = w] \qquad (60)$$

[27].

On the other hand, the definition of $\widetilde{b}_w$ yields $\widetilde{b}_w = b_w t'_\ell - m_{Q_{\operatorname{Qind} w},\ell} b_w$. Hence,

$$\begin{aligned}
f\left(a_u, \widetilde{b}_w\right) &= f\left(a_u,\ b_w t'_\ell - m_{Q_{\operatorname{Qind} w},\ell} b_w\right) \\
&= f\left(a_u, b_w \underbrace{t'_\ell}_{\substack{=S(t_\ell) \\ \text{(by (49))}}}\right) - m_{Q_{\operatorname{Qind} w},\ell} \underbrace{f(a_u, b_w)}_{\substack{=[u=w] \\ \text{(by (54), applied to } p=u \\ \text{and } q=w)}} \\
&\qquad (\text{since } f \text{ is a bilinear form}) \\
&= \underbrace{f(a_u, b_w S(t_\ell))}_{\substack{=f(a_u t_\ell, b_w) \\ \text{(by Lemma 14.6, applied to } a_u,\ b_w \text{ and } t_\ell \\ \text{instead of } u,\ v \text{ and } x)}} - \underbrace{m_{Q_{\operatorname{Qind} w},\ell} [u=w]}_{\substack{=m_{Q_{\operatorname{Qind} u},\ell}[u=w] \\ \text{(by (60))}}} \\
&= f(a_u t_\ell, b_w) - m_{Q_{\operatorname{Qind} u},\ell} [u=w] = f(\widetilde{a}_u, b_w)
\end{aligned}$$

(by (59)). This proves Claim 2.]

Now, let $w \in S_n$. Let $i = \operatorname{Qind} w$. Then, the definition of $\widetilde{b}_w$ yields $\widetilde{b}_w = b_w t'_\ell - m_{Q_{\operatorname{Qind} w},\ell} b_w = b_w t'_\ell - m_{Q_i,\ell} b_w$ (since $\operatorname{Qind} w = i$). However, (58) yields

$$\begin{aligned}
\widetilde{b}_w &= \sum_{v \in S_n} \underbrace{f\left(a_v, \widetilde{b}_w\right)}_{\substack{=f(\widetilde{a}_v, b_w) \\ \text{(by Claim 2, applied to } u=v)}} b_v = \sum_{v \in S_n} f(\widetilde{a}_v, b_w) b_v \\
&= \sum_{\substack{v \in S_n; \\ \operatorname{Qind} w \geq \operatorname{Qind} v}} \underbrace{f(\widetilde{a}_v, b_w)}_{\substack{=0 \\ \text{(by Claim 1, applied to } u=v)}} b_v + \sum_{\substack{v \in S_n; \\ \operatorname{Qind} w < \operatorname{Qind} v}} f(\widetilde{a}_v, b_w) b_v \\
&\qquad \left(\begin{array}{c} \text{since each } v \in S_n \text{ satisfies either } \operatorname{Qind} w \geq \operatorname{Qind} v \\ \text{or } \operatorname{Qind} w < \operatorname{Qind} v \text{ (but not both)} \end{array}\right) \\
&= \underbrace{\sum_{\substack{v \in S_n; \\ \operatorname{Qind} w \geq \operatorname{Qind} v}} 0 b_v}_{=0} + \sum_{\substack{v \in S_n; \\ \operatorname{Qind} w < \operatorname{Qind} v}} f(\widetilde{a}_v, b_w) b_v = \sum_{\substack{v \in S_n; \\ \operatorname{Qind} w < \operatorname{Qind} v}} f(\widetilde{a}_v, b_w) b_v \\
&= (\text{a } \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} w < \operatorname{Qind} v) \\
&= (\text{a } \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } i < \operatorname{Qind} v) \\
&\qquad (\text{since } \operatorname{Qind} w = i) \\
&= (\text{a } \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v > i)
\end{aligned}$$

[27] *Proof of (60):* If $u = w$, then (60) is obvious. Hence, we WLOG assume that $u \neq w$. Thus, $[u = w] = 0$. Hence, both sides of (60) equal 0 (since they contain the factor $[u = w] = 0$). Thus, (60) holds, qed.

(since $i < \operatorname{Qind} v$ is equivalent to $\operatorname{Qind} v > i$). In view of $\widetilde{b}_w = b_w t'_\ell - m_{Q_i,\ell} b_w$, this can be rewritten as

$$b_w t'_\ell - m_{Q_i,\ell} b_w = \left(\text{a } \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v > i\right).$$

In other words,

$$b_w t'_\ell = m_{Q_i,\ell} b_w + \left(\text{a } \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v > i\right).$$

This proves Theorem 14.5. □

14.2. Left multiplication

For each element $x \in \mathbf{k}[S_n]$, let $L(x)$ denote the $\mathbf{k}$-linear map

$$\mathbf{k}[S_n] \to \mathbf{k}[S_n], \qquad y \mapsto xy.$$

This is a "left" analogue to the right multiplication map $R(x)$. It is interesting to study from a shuffling perspective, as this corresponds to shuffling on the labels of a permutation instead of shuffling on the positions. Thus, having studied $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ in detail, we may wonder which of our results extend to $L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$. In particular, does an analogue of Theorem 4.1 hold for $L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ instead of $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$?

The answer is "yes", and in fact it turns out that this question is equivalent to the analogous question for $R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n)$ answered (in the positive) in Subsection 14.1, because the endomorphisms $L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ and $R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n)$ are conjugate via the antipode S. More generally, the following holds:[28]

Proposition 14.7. Let $x \in \mathbf{k}[S_n]$. Then, the endomorphisms $L(x)$ and $R(S(x))$ of $\mathbf{k}[S_n]$ are mutually conjugate in the endomorphism ring $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n])$ of the $\mathbf{k}$-module $\mathbf{k}[S_n]$. Namely, we have

$$R(S(x)) = S \circ (L(x)) \circ S^{-1}. \qquad (61)$$

Proof. Let $y \in \mathbf{k}[S_n]$. Recall that S is an involution; thus, S is invertible. Hence, S^{-1} exists. Moreover, recall that S is a $\mathbf{k}$-algebra antihomomorphism; thus, we have

$$S(xz) = S(z)\,S(x) \qquad \text{for each } z \in \mathbf{k}[S_n]. \qquad (62)$$

Now, comparing

$$(R(S(x)))(y) = yS(x) \qquad (\text{by the definition of } R(S(x)))$$

[28] Recall that S is the $\mathbf{k}$-linear map from $\mathbf{k}[S_n]$ to $\mathbf{k}[S_n]$ that sends each $w \in S_n$ to w^{-1}.

with

$$\left(S \circ (L(x)) \circ S^{-1}\right)(y) = S\left(\underbrace{(L(x))\left(S^{-1}(y)\right)}_{\substack{=xS^{-1}(y) \\ \text{(by the definition of } L(x))}}\right) = S\left(xS^{-1}(y)\right)$$
$$= \underbrace{S\left(S^{-1}(y)\right)}_{=y} S(x) \qquad \left(\text{by (62), applied to } z = S^{-1}(y)\right)$$
$$= yS(x),$$

we obtain $(R(S(x)))(y) = \left(S \circ (L(x)) \circ S^{-1}\right)(y)$.

Forget that we fixed y. We thus have shown that $(R(S(x)))(y) = \left(S \circ (L(x)) \circ S^{-1}\right)(y)$ for each $y \in \mathbf{k}[S_n]$. In other words, $R(S(x)) = S \circ (L(x)) \circ S^{-1}$. Hence, the endomorphisms $L(x)$ and $R(S(x))$ of $\mathbf{k}[S_n]$ are mutually conjugate in the endomorphism ring $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n])$ of the $\mathbf{k}$-module $\mathbf{k}[S_n]$. This proves Proposition 14.7. □

Corollary 14.8. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Then, the endomorphisms $L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ and $R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n)$ of $\mathbf{k}[S_n]$ are mutually conjugate in the endomorphism ring $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n])$ of the $\mathbf{k}$-module $\mathbf{k}[S_n]$. Namely, we have

$$R\left(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n\right) = S \circ (L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)) \circ S^{-1}.$$

Proof. It is easy to see that the map

$$R : \mathbf{k}[S_n] \to \operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n]),$$
$$x \mapsto R(x)$$

is $\mathbf{k}$-linear. Hence,

$$R\left(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n\right) = \lambda_1 R\left(t'_1\right) + \lambda_2 R\left(t'_2\right) + \cdots + \lambda_n R\left(t'_n\right) = \sum_{\ell=1}^{n} \lambda_\ell R\left(t'_\ell\right).$$

Similarly,

$$L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n) = \sum_{\ell=1}^{n} \lambda_\ell L(t_\ell).$$

Hence,

$$S \circ (L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)) \circ S^{-1} = S \circ \left(\sum_{\ell=1}^{n} \lambda_\ell L(t_\ell)\right) \circ S^{-1}$$
$$= \sum_{\ell=1}^{n} \lambda_\ell S \circ (L(t_\ell)) \circ S^{-1}$$

(since composition of $\mathbf{k}$-linear maps is $\mathbf{k}$-bilinear). Comparing this with

$$R\left(\lambda_1 t_1' + \lambda_2 t_2' + \cdots + \lambda_n t_n'\right) = \sum_{\ell=1}^{n} \lambda_\ell R\left(\underbrace{t_\ell'}_{\substack{=S(t_\ell) \\ \text{(by (49))}}}\right) = \sum_{\ell=1}^{n} \lambda_\ell \underbrace{R\left(S\left(t_\ell\right)\right)}_{\substack{=S\circ(L(t_\ell))\circ S^{-1} \\ \text{(by (61),} \\ \text{applied to } x=t_\ell)}}$$
$$= \sum_{\ell=1}^{n} \lambda_\ell S \circ \left(L\left(t_\ell\right)\right) \circ S^{-1},$$

we obtain

$$R\left(\lambda_1 t_1' + \lambda_2 t_2' + \cdots + \lambda_n t_n'\right) = S \circ \left(L\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)\right) \circ S^{-1}.$$

Thus, the endomorphisms $L\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)$ and $R\left(\lambda_1 t_1' + \lambda_2 t_2' + \cdots + \lambda_n t_n'\right)$ of $\mathbf{k}\left[S_n\right]$ are mutually conjugate in the endomorphism ring $\operatorname{End}_{\mathbf{k}}\left(\mathbf{k}\left[S_n\right]\right)$ of the $\mathbf{k}$-module $\mathbf{k}\left[S_n\right]$. This proves Corollary 14.8. □

Using Corollary 14.8, we can derive properties of $L\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)$ from properties of $R\left(\lambda_1 t_1' + \lambda_2 t_2' + \cdots + \lambda_n t_n'\right)$ by conjugating with S^{-1}. In particular, we obtain an analogue of Theorem 4.1 for $L\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)$ instead of $R\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)$, since we already know (from Subsection 14.1) that such an analogue exists for $R\left(\lambda_1 t_1' + \lambda_2 t_2' + \cdots + \lambda_n t_n'\right)$. Thus, we shall not discuss $L\left(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n\right)$ any further.

14.3. A Boolean interval partition of $\mathcal{P}\left([n-1]\right)$

Our results on Q-indices and lacunar subsets shown above quickly lead to a curious result, which may be of independent interest (similar results appear in [AgNyOr06] and other references on peak algebras and cd-indices):

Corollary 14.9. Let J be a subset of $[n-1]$. Then, there exists a unique lacunar subset I of $[n-1]$ satisfying $I' \subseteq J \subseteq [n-1] \setminus I$.

Proof. First of all, we observe that there exists a permutation $w \in S_n$ satisfying $\operatorname{Des} w = J$ (indeed, we have already constructed such a w in our proof of Lemma 10.7[29]). Fix such a w.

There exists a unique $i \in \left[f_{n+1}\right]$ such that $\operatorname{Qind} w = i$ (since $\operatorname{Qind} w$ is a well-defined element of $\left[f_{n+1}\right]$). In view of Proposition 10.3, we can rewrite this as follows: There exists a unique $i \in \left[f_{n+1}\right]$ such that $Q_i' \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i$. In view of $\operatorname{Des} w = J$, we can rewrite this as follows: There exists a unique $i \in \left[f_{n+1}\right]$ such that $Q_i' \subseteq J \subseteq [n-1] \setminus Q_i$. Since $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are all the lacunar subsets

[29] Arguably, the set J in the proof of Lemma 10.7 was not an arbitrary subset of $[n-1]$, but a specially constructed one; however, the construction of w works equally well for any J.

of $[n-1]$ (listed without repetition), we can rewrite this as follows: There exists a unique lacunar subset I of $[n-1]$ satisfying $I' \subseteq J \subseteq [n-1] \setminus I$. Corollary 14.9 is thus proven. $\square$

We can rewrite Corollary 14.9 in the language of Boolean interval partitions (see [Grinbe21, §4.4]): Namely, it says that there is a Boolean interval partition of the powerset $\mathcal{P}([n-1])$ whose blocks are the intervals $[I', [n-1] \setminus I]$ for all lacunar subsets I of $[n-1]$.

14.4. Consequences for the top-to-random shuffle

Let us briefly comment on what our above results yield for the top-to-random shuffle t_1. It is easy to derive from Corollary 12.2 that when $\mathbf{k}$ is a field, we have

$$\operatorname{Spec}(R(t_1)) = \{m_{I,1} \mid I \subseteq [n-1] \text{ is lacunar}\} = \{0, 1, \ldots, n-2, n\}$$

(the latter equality sign here is a consequence of the definition of $m_{I,1}$ and the fact that $\widehat{I} \subseteq \{0, 1, \ldots, n-1, n+1\}$). This, of course, is a fairly well-known result (e.g., being part of [DiFiPi92, Theorem 4.1]). Unfortunately, the fact that $R(t_1)$ is diagonalizable when $\mathbf{k}$ is a field of characteristic 0 (see, e.g., [DiFiPi92, Theorem 4.1]) cannot be recovered from our above results (as the assumptions of Theorem 12.3 are not satisfied when $n \geq 4$ and $\lambda_2 = \lambda_3 = \cdots = \lambda_n = 0$).

15. Strong stationary time for the random-to-below shuffle

We now leave the realm of algebra for some probabilistic analysis of the one-sided cycle shuffles.

We shall start this section by recalling how a strong stationary time for the top-to-random shuffle has been obtained ([AldDia86]). Using a similar but subtler strategy, we will then describe a strong stationary time for the one-sided cycle shuffles, and compute its waiting time in the specific case of the random-to-below shuffle.

15.1. Strong stationary time for the top-to-random shuffle

A stopping time for the top-to-random shuffle can be obtained using the following clever argument: At any given time, the cards that have already been moved from the top position will appear in a uniformly random relative order. Hence, once all cards have been moved from the top position, all permutations of the deck are equally likely. To estimate the time for this event to happen, we follow the position of the card that is originally at the bottom of the deck. This card occasionally moves up a position, but never moves down until it reaches the top of the deck.

It moves from the bottommost position to the next-higher one with probability $\frac{1}{n}$, then to one position higher with probability $\frac{2}{n}$, etc., until (as we said) it reaches the top. One iteration of the top-to-random shuffle later, the deck will be fully mixed, therefore giving a strong stationary time. The waiting time for this event can be easily seen to approach $n \log n$. Details can be found in the introduction of [AldDia86], or in [LePeWi09, §6.1 and §6.5.3].

15.2. A similar argument for the one-sided cycle shuffles

A similar argument can be used for the one-sided cycle shuffles. However, unlike for the top-to-random shuffle, we do not follow the bottommost card any more, since it may fall down before reaching the top (and is thus much more difficult to track). Thus, instead of following a specific card, we follow a space between two cards.

Namely, we stick a *bookmark* right above the card that was initially at the bottom. This bookmark will serve as a marker that will distinguish the fully mixed part (which is the part below the bookmark) from the rest of the deck. The bookmark itself is not considered to be a card in the deck, so the only way it moves is when a card that was above it is inserted below it.[30] Thus, the bookmark never moves down but occasionally moves up the deck. The deck is mixed once the bookmark is at the top.

The following theorem follows:

Theorem 15.1. If $P(1) \neq 0$, then the one-sided cycle shuffle $\mathrm{OSC}(P, n)$ admits a stopping time τ corresponding to the first time that all cards have been inserted below a bookmark initially placed right above the card at the bottom of the deck before the shuffling process. If X_t is the random variable for $\mathrm{OSC}(P, n)$, the distribution of X_t is uniform for all $t \geq \tau$, meaning that τ is a strong stationary time.

If $P(1) = 0$, then the top card never moves, and the stationary distribution is not the uniform distribution over all permutations.

15.3. The waiting time for the strong stationary time of the random-to-below shuffle

Knowing the existence of a strong stationary time for the one-sided cycle shuffle (with $P(1) \neq 0$), one might be interested to know when it is reasonable to expect this phenomenon to occur. We shall compute this waiting time for the random-to-below shuffle; the computations for other one-sided cycle shuffles would result in other numbers.

[30] We agree that if a card moves into the space that contains the bookmark, then it is inserted below (not above) the bookmark.

- If the bookmark is below the i-th card from the bottom, the probability for it to move in one iteration of the random-to-below shuffle is the sum of the probabilities for cards above it to move below it. The card at position j (counting from the bottom) is selected with probability $P(j) = \frac{1}{n}$, and (assuming that $j \geq i$) is inserted below the bookmark with probability $\frac{i}{j}$ (this includes the case when it is moved inbetween positions i and $i-1$, because in this case we insert it below the bookmark). Hence, the bookmark climbs up one position in the deck with probability

$$\sum_{j=i}^{n} \frac{1}{n} \cdot \frac{i}{j} = \frac{i}{n} \sum_{j=i}^{n} \frac{1}{j} = \frac{i}{n} \left(H_n - H_{i-1} \right),$$

where $H_i := \sum_{k=1}^{i} \frac{1}{k}$ is the i-th harmonic number.

Thus, the probability of the bookmark climbing from position i to $i+1$ at any single step follows a geometric distribution with parameter $\frac{i}{n} \left(H_n - H_{i-1} \right)$, and therefore the expected time needed for the event to happen is

$$\frac{1}{\frac{i}{n} \left(H_n - H_{i-1} \right)} = \frac{n}{i \left(H_n - H_{i-1} \right)}.$$

(Recall that the expected time for an event with probability p to happen is $\frac{1}{p}$.)

- The stopping time is the time required for the bookmark to reach the top of the deck (position n). This is achieved in an expected time corresponding to

$$\sum_{i=2}^{n} \frac{n}{i \left(H_n - H_{i-1} \right)}.$$

Theorem 15.2. Let $n \geq 2$. The expected number of steps to get to the strong stationary time for the random-to-below shuffle is

$$\mathbb{E}(\tau) = \sum_{i=2}^{n} \frac{n}{i \left(H_n - H_{i-1} \right)}.$$

Moreover, this time satisfies the following bound:

$$\sum_{i=2}^{n} \frac{n}{i \left(H_n - H_{i-1} \right)} \leq n \log n + n \log \left(\log n \right) + n \log(2) + 1.$$

Here, log denotes the natural logarithm ln.

Proof. The statement that the expected number of steps is $\sum\limits_{i=2}^{n} \dfrac{n}{i\left(H_n - H_{i-1}\right)}$ follows from the discussion above. Hence, we only need to prove the upper bound.

For this purpose, we shall show several analytic lemmas. The first is a known property of logarithms:[31]

Lemma 15.3. Let a and b be two positive reals. Then:

(a) We have $\log \dfrac{a+b}{a} \leq \dfrac{b}{a}$.

(b) We have $\log \dfrac{a+b}{a} \geq \dfrac{b}{a+b}$.

Proof of Lemma 15.3. Since the logarithm function is the antiderivative of the function $f\left(x\right) = \dfrac{1}{x}$, we have $\int_a^{a+b} \dfrac{1}{x} dx = \log\left(a+b\right) - \log a = \log \dfrac{a+b}{a}$. Hence,

$$\log \frac{a+b}{a} = \int_a^{a+b} \underbrace{\frac{1}{x}}_{\leq \frac{1}{a}} dx \leq \int_a^{a+b} \frac{1}{a} dx = \frac{b}{a},$$

which proves part **(a)**. Furthermore,

$$\log \frac{a+b}{a} = \int_a^{a+b} \underbrace{\frac{1}{x}}_{\geq \frac{1}{a+b}} dx \geq \int_a^{a+b} \frac{1}{a+b} dx = \frac{b}{a+b},$$

which proves part **(b)**. □

Lemma 15.4. Let m be a positive real. Then, the function $f : \left(0, m\right) \to \mathbb{R}$ given by

$$f\left(x\right) = \frac{1}{x \log \frac{m}{x}} \qquad \text{for all } x \in \left(0, m\right)$$

is convex.

Proof of Lemma 15.4. The second derivative $f^{(2)}$ of this function is easily computed as

$$f^{(2)}\left(x\right) = \frac{2\left(\log \frac{m}{x}\right)^2 - 3 \log \frac{m}{x} + 2}{x^3 \left(\log \frac{m}{x}\right)^3},$$

[31] Throughout this proof, the notations $\left[a, b\right]$, $\left[a, b\right)$, $\left(a, b\right]$ and $\left(a, b\right)$ are used in their familiar meanings from real analysis. In particular, $\left[a, b\right]$ means the set of all real numbers x satisfying $a \leq x \leq b$, contrary to our convention from Subsection 2.1.

and this is ≥ 0 because the numerator can be rewritten as $2y^2 - 3y + 2 = 2(y-1)^2 + y$ for $y = \log \frac{m}{x} \geq 0$. $\square$

Lemma 15.5. If $n \geq 3$, then $\frac{n+1}{n} - \frac{n+1}{3} < \frac{\log n}{2n}$.

Proof of Lemma 15.5. Consider the function $f : (0, \infty) \to \mathbb{R}$ given by $f(x) := \frac{\log x}{2} - (x+1)\left(1 - \frac{x}{3}\right)$. This function f is weakly increasing on $(2, \infty)$ (since its derivative is $f'(x) = \frac{-4x + 4x^2 + 3}{6x} = \frac{(2x-1)^2 + 2}{6x} \geq 0$). Thus, for $n \geq 3$, we have $f(n) \geq f(3) = \frac{\log 3}{2} > 0$. Since $f(n) = \frac{\log n}{2} - (n+1)\left(1 - \frac{n}{3}\right)$, we can rewrite this as

$$(n+1)\left(1 - \frac{n}{3}\right) < \frac{\log n}{2}.$$

Dividing both sides by n and expanding the left hand side, we transform this into

$$\frac{n+1}{n} - \frac{n+1}{3} < \frac{\log n}{2n}.$$

This proves Lemma 15.5. $\square$

Lemma 15.6. Let $i \leq n$ be a positive integer. Then,

$$H_n - H_{i-1} \geq \log \frac{n+1}{i}.$$

Proof of Lemma 15.6. The definition of H_m yields

$$\begin{aligned}
H_n - H_{i-1} &= \frac{1}{i} + \frac{1}{i+1} + \cdots + \frac{1}{n} \\
&\geq \int_i^{i+1} \frac{1}{x} dx + \int_{i+1}^{i+2} \frac{1}{x} dx + \cdots + \int_n^{n+1} \frac{1}{x} dx \\
&\qquad \left(\begin{array}{c} \text{indeed, } \frac{1}{j} \geq \int_j^{j+1} \frac{1}{x} dx \text{ for each } j > 0, \\ \text{since the function } \frac{1}{x} \text{ is decreasing} \end{array}\right) \\
&= \int_i^{n+1} \frac{1}{x} dx = \log(n+1) - \log i = \log \frac{n+1}{i}.
\end{aligned}$$

$\square$

Lemma 15.7. Let a and b be two integers satisfying $a \leq b$. Let $f : (a-1, b+1) \to \mathbb{R}$ be a convex function. Then,

$$\sum_{i=a}^{b} f(i) \leq \int_{a-1/2}^{b+1/2} f(x)\, dx.$$

Proof of Lemma 15.7. The interval $[a-1/2,\ b+1/2)$ can be decomposed as a disjoint union

$$[a-1/2,\ a+1/2) \sqcup [a+1/2,\ a+3/2) \sqcup [a+3/2,\ a+5/2) \sqcup \cdots \sqcup [b-1/2,\ b+1/2)$$
$$= \bigsqcup_{i=a}^{b} [i-1/2,\ i+1/2).$$

Hence,

$$\begin{aligned}
\int_{a-1/2}^{b+1/2} f(x)\, dx &= \sum_{i=a}^{b} \underbrace{\int_{i-1/2}^{i+1/2} f(x)\, dx}_{\substack{=\frac{1}{2}\left(\int_{i-1/2}^{i+1/2} f(x)dx+\int_{i-1/2}^{i+1/2} f(x)dx\right) \\ \text{(since } p=\frac{1}{2}(p+p) \text{ for any } p\text{)}}} \\
&= \sum_{i=a}^{b} \frac{1}{2}\left(\int_{i-1/2}^{i+1/2} f(x)\, dx + \int_{i-1/2}^{i+1/2} f(x)\, dx\right) \\
&= \sum_{i=a}^{b} \frac{1}{2}\left(\int_{i-1/2}^{i+1/2} f(x)\, dx + \int_{i-1/2}^{i+1/2} f(2i-x)\, dx\right) \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } 2i-x \text{ for } x \\ \text{in the second integral}\end{array}\right) \\
&= \sum_{i=a}^{b} \int_{i-1/2}^{i+1/2} \underbrace{\frac{1}{2}\left(f(x) + f(2i-x)\right)}_{\substack{\geq f(i) \\ \text{(since } f \text{ is convex, and} \\ \text{since } i \text{ is the midpoint} \\ \text{between } x \text{ and } 2i-x\text{)}}} dx \\
&\geq \sum_{i=a}^{b} \underbrace{\int_{i-1/2}^{i+1/2} f(i)\, dx}_{=f(i)} = \sum_{i=a}^{b} f(i).
\end{aligned}$$

This proves Lemma 15.7. □

Now, we return to the proof of the upper bound

$$\sum_{i=2}^{n} \frac{n}{i(H_n - H_{i-1})} \leq n \log n + n \log(\log n) + n \log 2 + 1 \qquad (63)$$

claimed in Theorem 15.2.

Indeed, this upper bound can be checked by straightforward computations for $n = 2$. So let us WLOG assume that $n \geq 3$.

Let $m := n+1$. Define a function $f : (0, m) \to \mathbb{R}$ as in Lemma 15.4. Then, Lemma 15.4 says that this function f is convex. We note also that the function f has antiderivative $F : (0, m) \to \mathbb{R}$ given by

$$F(x) = -\log\left(\log \frac{m}{x}\right).$$

(This can be easily verified by hand.)

From Lemma 15.6, we obtain

$$\begin{aligned}\sum_{i=2}^{n} \frac{n}{i(H_n - H_{i-1})} &\leq \sum_{i=2}^{n} \frac{n}{i \log \dfrac{n+1}{i}} = \sum_{i=2}^{n} \frac{n}{i \log \dfrac{m}{i}} \qquad (\text{since } n+1 = m) \\ &= n \cdot \sum_{i=2}^{n} \underbrace{\frac{1}{i \log \dfrac{m}{i}}}_{\substack{=f(i) \\ (\text{by the definition of } f)}} = n \cdot \sum_{i=2}^{n} f(i).\end{aligned}$$

Hence, in order to prove (63), we only need to show that

$$\sum_{i=2}^{n} f(i) \leq \log n + \log(\log n) + \log 2 + \frac{1}{n}. \tag{64}$$

So let us prove this inequality now.

Since f is convex on $(0, m)$, we can apply Lemma 15.7 to $a = 2$ and $b = n = m - 1$.

We thus obtain

$$\begin{aligned}
\sum_{i=2}^{n} f(i) &\leq \int_{3/2}^{n+1/2} f(x)\,dx \\
&= \left(-\log\left(\log \frac{m}{n+1/2}\right)\right) - \left(-\log\left(\log \frac{m}{3/2}\right)\right) \\
&\qquad \left(\begin{array}{c}\text{since } f \text{ has antiderivative } F \text{ given} \\ \text{by } F(x) = -\log\left(\log \frac{m}{x}\right)\end{array}\right) \\
&= \log\left(\log \frac{m}{3/2}\right) - \log \underbrace{\left(\log \frac{m}{n+1/2}\right)}_{\substack{=\log \frac{n+1/2+1/2}{n+1/2} \\ (\text{since } m=n+1=n+1/2+1/2)}} \\
&= \log\left(\log \frac{m}{3/2}\right) - \log \underbrace{\left(\log \frac{n+1/2+1/2}{n+1/2}\right)}_{\substack{\geq \frac{1/2}{n+1/2+1/2} \\ (\text{by Lemma 15.3 } \textbf{(b)}, \\ \text{applied to } a=n+1/2 \text{ and } b=1/2)}} \\
&\leq \log\left(\log \frac{m}{3/2}\right) - \log \frac{1/2}{n+1/2+1/2} \\
&= \log\left(\log \frac{m}{3/2}\right) - \log \frac{1/2}{m} \qquad (\text{since } n+1/2+1/2 = n+1 = m) \\
&= \log\left(\left(\log \frac{m}{3/2}\right) \Big/ \frac{1/2}{m}\right) = \log\left(2m \log \frac{m}{3/2}\right).
\end{aligned}$$

Thus, in order to prove (64), it will suffice to show that

$$\log\left(2m \log \frac{m}{3/2}\right) \leq \log n + \log(\log n) + \log 2 + \frac{1}{n}.$$

After exponentiation, this rewrites as

$$2m \log \frac{m}{3/2} \leq 2n \log n \cdot e^{1/n}. \tag{65}$$

Upon division by 2, this rewrites as

$$m \log \frac{m}{3/2} \leq n \log n \cdot e^{1/n}. \tag{66}$$

However,

$$\log\frac{m}{3/2} = \log\left(n\cdot\frac{m}{n}\Big/\frac{3}{2}\right) = \log n + \underbrace{\log\frac{m}{n}}_{\substack{=\log\frac{n+1}{n}\leq\frac{1}{n} \\ \text{(by Lemma 15.3 (a),} \\ \text{applied to } a=n \text{ and } b=1)}} - \underbrace{\log\frac{3}{2}}_{\geq\frac{1}{3}} \leq \log n + \frac{1}{n} - \frac{1}{3},$$

so that

$$\begin{aligned} m\log\frac{m}{3/2} &\leq \underbrace{m}_{=n+1}\left(\log n+\frac{1}{n}-\frac{1}{3}\right) = (n+1)\left(\log n+\frac{1}{n}-\frac{1}{3}\right) \\ &= \underbrace{(n+1)\log n}_{=n\log n+\log n} + \underbrace{\frac{n+1}{n}-\frac{n+1}{3}}_{\substack{<\frac{\log n}{2n} \\ \text{(by Lemma 15.5)}}} \\ &< n\log n+\log n+\frac{\log n}{2n} = n\log n\cdot\underbrace{\left(1+\frac{1}{n}+\frac{1}{2n^2}\right)}_{\substack{=\sum_{k=0}^{2}\frac{1}{k!}\left(\frac{1}{n}\right)^k \\ \leq\sum_{k=0}^{\infty}\frac{1}{k!}\left(\frac{1}{n}\right)^k \\ =e^{1/n}}} \leq n\log n\cdot e^{1/n}. \end{aligned}$$

This proves (66). Thus, the proof of Theorem 15.2 is complete. □

One might ask if this is a good upper bound, or, in other terms, if the order of magnitude of the bound given in Theorem 15.2 is also the order of magnitude of $\mathbb{E}(\tau)$. Numerical checks suggest that this is indeed the case, allowing us to make the following conjecture.

Conjecture 15.8. Let $n \geq 2$. The expected number of steps to get to the strong stationary time for the random-to-below shuffle satisfies the following lower bound:

$$\mathbb{E}(\tau) = \sum_{i=2}^{n}\frac{n}{i\left(H_n - H_{i-1}\right)} \geq n\log n + n\log(\log n).$$

Here, log denotes the natural logarithm ln.

15.4. Optimality of our strong stationary time

A legitimate question to ask is whether there is a strong stationary time that occurs faster than τ for the one-sided cycle shuffles. Our stopping time τ is the waiting time for the bookmark to reach the top of the deck. We now shall explain why there is no faster stopping time, i.e., why we need to wait for the bookmark to reach the top. To do so, we claim that some permutations cannot be reached until the bookmark reaches the top.

Consider the card that was initially at the bottom. This card was initially the only card to be below the bookmark. For this card to go up, a card needs to be inserted below it, and thus below the bookmark. Hence, all the cards that are above the bookmark are atop of the card that was initially at the bottom. Note that cards that are below the bookmark can still be above the card initially at the bottom. As long as there are k cards above the bookmark, the card initially at the bottom cannot be among the top k cards. Hence, for any permutation of our deck to be likely, we need the bookmark to reach the top, showing that our stopping time is optimal.

A consequence of this fact is that, assuming Conjecture 15.8, the random-to-below shuffle would be slower than top-to-random, for which the strong stationary time approaches $n \log n$. We attribute the fact that random-to-below is slower to its greater *laziness*, in other words, to the fact that the probability of applying the identity permutation is higher for random-to-below than for top-to-random.

16. Further remarks and questions

16.1. Some identities for $t_1, t_2, \ldots, t_n$

We have now seen various properties of the somewhere-to-below shuffles $t_1, t_2, \ldots, t_n$. In particular, from Theorem 4.1, we know that they can all be represented as upper-triangular matrices of size $n! \times n!$. Thus, the Lie subalgebra of $\mathfrak{gl}\left(\mathbf{k}\left[S_n\right]\right)$ they generate is solvable. In a sense, this can be understood as an "almost-commutativity": It is not true in general that $t_1, t_2, \ldots, t_n$ commute, but one can think of them as commuting "up to error terms". There might be several ways to make this rigorous. One striking observation is that the commutators $\left[t_i, t_j\right] := t_i t_j - t_j t_i$ satisfy $\left[t_i, t_j\right]^2 = 0$ whenever $n \leq 5$ (but not when $n = 6$ and $i = 1$ and $j = 3$). This can be generalized as follows:

Theorem 16.1. We have $\left[t_i, t_j\right]^{j-i+1} = 0$ for any $1 \leq i < j \leq n$.

Theorem 16.2. We have $\left[t_i, t_j\right]^{\lceil (n-j)/2 \rceil + 1} = 0$ for any $1 \leq i < j \leq n$.

Both of these theorems are proved in the preprint [Grinbe23]. The proofs are surprisingly difficult, even though they rely on nothing but elementary manipulations of cycles and sums. Actually, the following two more general results are proved in [Grinbe23]:

Theorem 16.3. Let $j \in [n]$, and let m be a positive integer. Let $k_1, k_2, \ldots, k_m$ be m elements of $[j]$ (not necessarily distinct) satisfying $m \geq j - k_m + 1$. Then,

$$\left[t_{k_1}, t_j\right] \left[t_{k_2}, t_j\right] \cdots \left[t_{k_m}, t_j\right] = 0.$$

Theorem 16.4. Let $j \in [n]$ and $m \in \mathbb{N}$ be such that $2m \geq n - j + 2$. Let $i_1, i_2, \ldots, i_m$ be m elements of $[j]$ (not necessarily distinct). Then,

$$\left[t_{i_1}, t_j\right] \left[t_{i_2}, t_j\right] \cdots \left[t_{i_m}, t_j\right] = 0.$$

The following identities are proved in [Grinbe23] as well:

Proposition 16.5. We have $t_i = 1 + s_i t_{i+1}$ for any $i \in [n-1]$.

Proposition 16.6. We have $\left(1 + s_j\right) \left[t_i, t_j\right] = 0$ for any $1 \leq i < j \leq n$.

Proposition 16.7. We have $t_{n-1} \left[t_i, t_{n-1}\right] = 0$ for any $1 \leq i \leq n$.

Proposition 16.8. We have $\left[t_i, t_j\right] = \left[s_i s_{i+1} \cdots s_{j-1}, t_j\right] t_j$ for any $1 \leq i < j \leq n$.

Proposition 16.9. We have $t_{i+1} t_i = \left(t_i - 1\right) t_i$ for any $1 \leq i < n$.

Proposition 16.10. We have $t_{i+2} \left(t_i - 1\right) = \left(t_i - 1\right) \left(t_{i+1} - 1\right)$ for any $1 \leq i < n - 1$.

16.2. Open questions

The above results (particularly Propositions 16.9 and 16.10) might suggest that the $\mathbf{k}$-subalgebra $\mathbf{k}\left[t_1, t_2, \ldots, t_n\right]$ of $\mathbf{k}\left[S_n\right]$ can be described by explicit generators and relations. This is probably overly optimistic, but we believe that it has some more properties left to uncover. In particular, one can ask:

Question 16.11. What is the representation theory (indecomposable modules, etc.) of this algebra? What power of its Jacobson radical is 0? (These likely require $\mathbf{k}$ to be a field.) What is its dimension (as a $\mathbf{k}$-vector space)?

Any reader acquainted with the standard arsenal of card-shuffling will spot another peculiarity of the above work: We have not once used any result about $\mathbf{k}\left[S_n\right]$-modules (i.e., representations of the symmetric group S_n). The subject is, of course, closely related: Each of the $F(I)$'s and thus also the F_i's is a left $\mathbf{k}\left[S_n\right]$-module, and it is natural to ask for its isomorphism type:

Question 16.12. How do the $F(I)$ and the F_i decompose into Specht modules when $\mathbf{k}$ is a field of characteristic 0 ?

We have been able to answer this question (see [GriLaf24]), and will prove our answer in forthcoming work.

A different direction in which our results seem to extend is the *Hecke algebra*. In a nutshell, the *type-A Hecke algebra* (or *Iwahori-Hecke algebra*) is a deformation of the group algebra $\mathbf{k}[S_n]$ that involves a new parameter $q \in \mathbf{k}$. It is commonly denoted by $\mathcal{H} = \mathcal{H}_q(S_n)$; it has a basis $(T_w)_{w \in S_n}$ indexed by the permutations $w \in S_n$, but a more intricate multiplication than $\mathbf{k}[S_n]$. A definition of the latter multiplication can be found in [Mathas99]. We can now define the *q-deformed somewhere-to-below shuffles* $t_1^{\mathcal{H}}, t_2^{\mathcal{H}}, \ldots, t_n^{\mathcal{H}}$ by

$$t_\ell^{\mathcal{H}} := T_{\mathrm{cyc}_\ell} + T_{\mathrm{cyc}_{\ell,\ell+1}} + T_{\mathrm{cyc}_{\ell,\ell+1,\ell+2}} + \cdots + T_{\mathrm{cyc}_{\ell,\ell+1,\ldots,n}} \in \mathcal{H}.$$

Surprisingly, these q-deformed shuffles appear to share many properties of the original $t_1, t_2, \ldots, t_n$; for example:

Conjecture 16.13. Theorem 4.1 seems to hold in $\mathcal{H}$ when the t_ℓ are replaced by the $t_\ell^{\mathcal{H}}$.

Attempts to prove this conjecture are underway.

Thus ends our study of the somewhere-to-below shuffles $t_1, t_2, \ldots, t_n$ and their linear combinations. From a bird's eye view, the most prominent feature of this study might have been its use of a strategically defined filtration of $\mathbf{k}[S_n]$ (as opposed to, e.g., working purely algebraically with the operators, or combining them into generating functions, or finding a joint eigenbasis). In the language of matrices, this means that we found a joint triangular basis for our shuffles (i.e., a basis of $\mathbf{k}[S_n]$ such that each of our shuffles is represented by an upper-triangular matrix in this basis). In our case, this method was essentially forced upon us by the lack of a joint eigenbasis (as we saw in Remark 4.2). However, even when a family of linear operators has a joint eigenbasis, it might be easier to find a filtration than to find such an eigenbasis. Thus, a question naturally appears:

Question 16.14. Are there other families of shuffles for which a filtration like ours (i.e., with properties similar to Theorem 8.1) exists and can be used to simplify the spectral analysis?

References

[AgNyOr06] M. Aguiar, K. Nyman, and R. Orellana. New results on the peak algebra. *J. Algebraic Combin.*, 23(2):149–188, 2006.

[AldDia86] D. Aldous and P. Diaconis. Shuffling cards and stopping times. *American Mathematical Monthly*, 93(5):333–348, 1986. doi:10.2307/2323590.

[BaCoMR21] M. E. Bate, S. B. Connor, and O. Matheau-Raven. Cutoff for a one-sided transposition shuffle. *Ann. Appl. Probab.*, 31(4):1746–1773, 2021.

[BayDia92] D. Bayer and P. Diaconis. Trailing the dovetail shuffle to its lair. *The Annals of Applied Probability*, 2(2):294–313, 1992.

[BiHaRo99] P. Bidigare, P. Hanlon, and D. Rockmore. A combinatorial description of the spectrum for the Tsetlin library and its generalization to hyperplane arrangements. *Duke Mathematical Journal*, 99(1):135–174, 1999. doi:10.1215/S0012-7094-99-09906-4.

[Chu19] H. V. Chu. The Fibonacci sequence and Schreier-Zeckendorf sets. *J. Integer Seq.*, 22(6):Art. 19.6.5, 12, 2019. URL `https://www.emis.de/journals/JIS/VOL22/Chu2/chu9.html`.

[Conrad22] K. Conrad. The minimal polynomial and some applications. 2022. URL `https://kconrad.math.uconn.edu/blurbs/linmultialg/minpolyandappns.pdf`.

[DiaSha81] P. Diaconis and M. Shahshahani. Generating a random permutation with random transpositions. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 57(2):159–179, 1981. doi:10.1007/BF00535487.

[DieSal18] A. B. Dieker and F. Saliola. Spectral analysis of random-to-random Markov chains. *Advances in Mathematics*, 323:427–485, 2018. doi:10.1016/j.aim.2017.10.034.

[DiFiPi92] P. Diaconis, J. A. Fill, and J. Pitman. Analysis of top to random shuffles. *Combinatorics, Probability and Computing*, 1(2):135–155, 1992. URL `https://statweb.stanford.edu/~cgates/PERSI/papers/randomshuff92.pdf`.

[DiPaRa14] P. Diaconis, C. Y. A. Pang, and A. Ram. Hopf algebras and Markov chains: two examples and a theory. *J. Algebraic Combin.*, 39(3):527–585, 2014.

[Donnel91] P. Donnelly. The heaps process, libraries, and size-biased permutations. *Journal of Applied Probability*, 28(2):321–335, 1991. doi:10.2307/3214869.

[Fill96] J. A. Fill. An exact formula for the move-to-front rule for self-organizing lists. *Journal of Theoretical Probability*, 9(1):113–160, 1996. doi:10.1007/BF02213737.

[GriLaf24] D. Grinberg and N. Lafrenière. The somewhere-to-below shuffles in the symmetric group and Hecke algebras. extended abstract at the FPSAC 2024 conference, 2023.

[Grinbe18] D. Grinberg. Answers to "is this sum of cycles invertible in $\mathbb{Q}S_n$?". MathOverflow thread #308536. URL `https://mathoverflow.net/questions/308536/is-this-sum-of-cycles-invertible-in-mathbb-qs-n`.

[Grinbe20] D. Grinberg. Enumerative combinatorics. Drexel Fall 2019 Math 222 notes, 2022. URL `http://www.cip.ifi.lmu.de/~grinberg/t/19fco/n/n.pdf`.

[Grinbe21] D. Grinberg. The Elser nuclei sum revisited. *DMTCS*, 23(1):Art. #15, 2021. doi:10.46298/dmtcs.7012.

[Grinbe23] D. Grinberg. Commutator nilpotency for somewhere-to-below shuffles. arXiv:2309.05340v2, 2023.

[Hendri72] W. J. Hendricks. The stationary distribution of an interesting Markov chain. *J. Appl. Probability*, 9:231–233, 1972. URL `https://doi.org/10.2307/3212655`.

[HofKun71] K. Hoffman and R. Kunze. *Linear algebra*. Prentice-Hall, Inc., Englewood Cliffs, N.J., second edition, 1971.

[Lafren19] N. Lafrenière. *Valeurs propres des opérateurs de mélange symétrisés*. Phd thesis, Université du Québec à Montréal, 2019. URL `https://arxiv.org/abs/1912.07718v1`.

[LePeWi09] D. A. Levin, Y. Peres, and E. L. Wilmer. *Markov Chains and Mixing Times*. American Mathematical Society, second edition, 2017. URL `http://www.ams.org/bookpages/mbk-107`. preprint available at `https://pages.uoregon.edu/dlevin/MARKOV/mcmt2e.pdf`.

[Mathas99] A. Mathas. *Iwahori-Hecke Algebras and Schur Algebras of the Symmetric Group*, volume 15 of *University Lecture Series*. American Mathematical Society, 1999. URL `https://bookstore.ams.org/ulect-15`.

[Meusbu21] C. Meusburger. Hopf algebras and representation theory of Hopf algebras. Lecture notes, 2021. URL `https://en.www.math.fau.de/lie-groups/scientific-staff/prof-dr-catherine-meusburger/teaching/lecture-notes/`.

[NesPen22] E. Nestoridi and K. Peng. Mixing times of one-sided k-transposition shuffles. ArXiv:2112.05085, 2021.

[Palmes10] C. Palmes. Top-to-random-shuffles. diploma thesis at Westfälische Wilhelms-Universität Münster, `https://www.uni-muenster.de/Stochastik/alsmeyer/Diplomarbeiten/Palmes.pdf`, 2010.

[Pang22] A. Pang. The eigenvalues of hyperoctahedral descent operators and applications to card-shuffling. *Electronic Journal of Combinatorics*, 29:Article #P1.32, 2022. doi:10.37236/10678. ArXiv:2108.09097.

[Phatar91] R. M. Phatarfod. On the matrix occurring in a linear search problem. *Journal of Applied Probability*, 28(2):336–346, 1991. doi:10.1017/s0021900200039723.

[Reizen19] J. F. Reizenstein. *Iterated-Integral Signatures in Machine Learning*. Phd thesis, University of Warwick, 2019. URL `http://wrap.warwick.ac.uk/131162/`.

[ReSaWe14] V. Reiner, F. Saliola, and V. Welker. Spectra of symmetrized shuffling operators. *Memoirs of the American Mathematical Society*, 228(1072):vi+109, 2014.

[SageMath] The SageMath developers. *SageMath, (Version 10.1)*, 2023. `https://www.sagemath.org`.

[StoLui19] M. Stoll. Linear algebra II. Lecture notes. With some additions by Ronald van Luijk, 2019. URL `https://pub.math.leidenuniv.nl/~luijkrmvan/linalg2/2019/`.