ALGEBRAIC COMBINATORICS

Darij Grinberg & Nadia Lafrenière

**The one-sided cycle shuffles in the symmetric group algebra**

Volume 7, issue 2 (2024), p. 275-326.
https://doi.org/10.5802/alco.346



*Algebraic Combinatorics is published by The Combinatorics Consortium*
*and is a member of the Centre Mersenne for Open Scientific Publishing*
www.tccpublishing.org www.centre-mersenne.org
e-ISSN: 2589-5486

*Algebraic Combinatorics*
Volume 7, issue 2 (2024), p. 275–326
https://doi.org/10.5802/alco.346

# The one-sided cycle shuffles in the symmetric group algebra

Darij Grinberg & Nadia Lafrenière

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 $\ell$ to the next-higher element of $I$ (this "next-higher element" is understood to be $\ell$ 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.

## 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 [9], 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 [9], the riffle shuffle [4], the top-to-random shuffle [28] and the random-to-random shuffle [10], among several others. An interesting

*Manuscript received 17th March 2023, revised 21st October 2023 and 7th November 2023, accepted 7th November 2023.*

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

ISSN: 2589-5486 

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 $\frac{2(n+1-i)}{n(n+1)}$). 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 [4], the top-to-random and random-to-top shuffles [28], the pop shuffles and other 'BHR' shuffling operators [5], and the top-$m$-to-random shuffles [7]. 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 $t_\ell$ moves the card at position $\ell$ 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 $t_\ell$ 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 [29, 8, 10, 21, 3, 27, 25]. 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.

1.1. Remark. The arXiv version [17] of this paper is longer and includes some details that have been omitted from the present journal version. We will thus refer to [17] for some proofs that we leave to the reader here. See also the extended abstract [18] for a brief summary of this and some related work.

## 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 $[a, b] := \{a, a+1, \ldots, b\}$. 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 $\mathrm{cyc}_{i_1,i_2,\ldots,i_k}$ 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 $\mathrm{cyc}_i = \mathrm{id}$ 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 appears, e.g., under the name $B_1$ in [7], where it is studied extensively. (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 [19, 11, 28, 12, 5]), 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).

---

(1)The (German) diploma thesis [26] provides a detailed exposition of the results of [7] (in particular, [26, Satz 2.4.6] is [7, Theorem 4.2]).

See also [13] for an exposition of the most basic algebraic properties of $t_1$ (called $\mathbf{A}$ there). An unexpected application to machine learning has recently been given in [30, 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.

A probability distribution on the $n!$ possible orders of a deck of $n$ cards can be identified with the element $\sum_{w \in S_n} P(w)\, w$ of $\mathbb{R}[S_n]$, where $P(w)$ is the probability of the deck having order $w$. Likewise, a nonzero element $\sum_{\sigma \in S_n} P(\sigma)\, \sigma$ 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 $w\tau$ equals $\dfrac{P(\tau)}{\sum_{\sigma \in S_n} P(\sigma)}$ for each $w, \tau \in S_n$. This is an instance of a *right random walk on a group*, as defined (e.g.) in [22, 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 $t_\ell$ transforms a deck by picking its $\ell$-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 $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{R}_{\geqslant 0}$ being not all 0) picks a card at random – specifically, picking the $\ell$-th card from the top with probability $\dfrac{(n-\ell+1)\lambda_\ell}{\sum_{i=1}^{n}(n-i+1)\lambda_i}$ – 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

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

The $n! \times n!$-matrix $\left(Q(\tau,\sigma)\right)_{\tau,\sigma \in S_n}$ 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.

(1) **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 $w_1 := w\,(1)$, $w_2 := w\,(2)$ and $w_3 := w\,(3)$, 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 [28] 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 [5] and in terms of standard Young tableaux [29].

(2) **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 $P(i) = \frac{1}{n}$ for all $i \in [n]$). 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:

$$\mathrm{R2B}_3 = \begin{array}{cc} & \begin{array}{cccccc} [w_1w_2w_3] & [w_1w_3w_2] & [w_2w_1w_3] & [w_2w_3w_1] & [w_3w_1w_2] & [w_3w_2w_1] \end{array} \\ \begin{array}{c} [w_1w_2w_3] \\ [w_1w_3w_2] \\ [w_2w_1w_3] \\ [w_2w_3w_1] \\ [w_3w_1w_2] \\ [w_3w_2w_1] \end{array} & \begin{pmatrix} \frac{11}{18} & \frac{1}{6} & \frac{1}{9} & \frac{1}{9} & 0 & 0 \\ \frac{1}{6} & \frac{11}{18} & 0 & 0 & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{9} & \frac{1}{9} & \frac{11}{18} & \frac{1}{6} & 0 & 0 \\ 0 & 0 & \frac{1}{6} & \frac{11}{18} & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{9} & \frac{1}{9} & 0 & 0 & \frac{11}{18} & \frac{1}{6} \\ 0 & 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{6} & \frac{11}{18} \end{pmatrix} \end{array}.$$

A recently studied shuffle admits a similar description, namely the one-sided transposition shuffle [3], that picks a card uniformly at random and swaps it with a card chosen uniformly at random among the cards below.

(3)Actually, [28] 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.

Despite its similar-sounding description, it is not a one-sided cycle shuffle (unless $n \leqslant 2$), 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.

(3) **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 $i \leqslant j$, 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 $\frac{2}{n(n+1)}$ for all $i < j$, and the probability of applying the identity is $\frac{2}{n+1}$. This is the one-sided cycle shuffle governed by the probability distribution $P$ with $P(i) = \frac{2(n-i+1)}{n(n+1)}$. For $n = 3$, its transition matrix is

$$\begin{array}{c} \\ {[w_1w_2w_3]} \\ {[w_1w_3w_2]} \\ {[w_2w_1w_3]} \\ {[w_2w_3w_1]} \\ {[w_3w_1w_2]} \\ {[w_3w_2w_1]} \end{array}
\begin{array}{c} \begin{array}{cccccc} [w_1w_2w_3] & [w_1w_3w_2] & [w_2w_1w_3] & [w_2w_3w_1] & [w_3w_1w_2] & [w_3w_2w_1] \end{array} \\
\begin{pmatrix}
\frac{1}{2} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 0 & 0 \\
\frac{1}{6} & \frac{1}{2} & 0 & 0 & \frac{1}{6} & \frac{1}{6} \\
\frac{1}{6} & \frac{1}{6} & \frac{1}{2} & \frac{1}{6} & 0 & 0 \\
0 & 0 & \frac{1}{6} & \frac{1}{2} & \frac{1}{6} & \frac{1}{6} \\
\frac{1}{6} & \frac{1}{6} & 0 & 0 & \frac{1}{2} & \frac{1}{6} \\
0 & 0 & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{2}
\end{pmatrix} \end{array}.$$

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 $\mathrm{OSC}(P, n)$ 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 $\dfrac{m_{I,1}}{n}$. 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

$$\mathbf{k}[S_n] \to \mathbf{k}[S_n],$$
$$y \mapsto yx.$$

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 $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$ be arbitrary. 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 $\lambda_i = \frac{6}{i}$ 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

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

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 [1]) or as "Zeckendorf sets" (in [6], at least when they are finite subsets of $\{1,2,3,\ldots\}$).

It is known (see, e.g., [15, 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 $\{i-1 \mid i\in I\}\subseteq\mathbb{Z}$. 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

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

  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 $[n-1]\smallsetminus(I\cup(I-1))$. 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 $\{2,3\}'=[4]\smallsetminus\{1,2,3\}=\{4\}$.

## 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 $\ell\leqslant k$ in $[n]$. Thus, (1) rewrites as follows:

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

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

The following relationship between simple transpositions follows easily from (2):

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

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

## 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 **k**-submodule filtration of $\mathbf{k}[S_n]$ that is preserved by all the somewhere-to-below shuffles. In this section, we first define a 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 $0 \leqslant \operatorname{sum} I \leqslant n(n+1)/2$.
- We let
$$F(I) := \{q \in \mathbf{k}[S_n] \ \mid \ qs_i = q \text{ for all } i \in I'\}.$$
This is a **k**-submodule of $\mathbf{k}[S_n]$. Intuitively, it can be understood as follows: Write each permutation $\pi \in S_n$ as the $n$-tuple $[\pi(1) \ \pi(2) \ \ldots \ \pi(n)]$ (this is called *one-line notation*, and we write it without commas between the entries for the sake of brevity). Thus, each element $q \in \mathbf{k}[S_n]$ can be viewed as a **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 $[n] \setminus I$. 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 $[n] \setminus [i,j]$, the coefficient of $\sigma\tau$ in $q$ is also $c$. Moreover, this property characterizes the elements $q$ of $F(I)$.

Note that $F([n]) = \mathbf{k}[S_n]$, since $[n]' = \varnothing$.

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 **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
$$\begin{aligned} F(\{1\}) &= \{q \in \mathbf{k}[S_n] \ \mid \ qs_2 = q\} \\ &= \operatorname{span}([123] + [132], \quad [213] + [231], \quad [312] + [321]). \end{aligned}$$
- We have $\{3\}' = \{1\}$ and thus
$$\begin{aligned} F(\{3\}) &= \{q \in \mathbf{k}[S_n] \ \mid \ qs_1 = q\} \\ &= \operatorname{span}([123] + [213], \quad [132] + [312], \quad [231] + [321]). \end{aligned}$$

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

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

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 $i,j,k,\ell$, 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

$$F(<k) := \sum_{\substack{J \subseteq [n]; \\ \operatorname{sum} J < k}} F(J). \tag{4}$$

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 $\operatorname{sum} K < \operatorname{sum} I$. This will complete the proof. This is a long proof, and some claims might not be obvious at first sight. Proofs that have been omitted require no clever tricks, and can be found in the more detailed version of this paper [17].

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 $\ell$. Thus, $m_{I,\ell} = i_k - \ell$ (by the definition of $m_{I,\ell}$) and

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

Note that $k \geqslant 1$ (since $\ell \leqslant i_k$), so that $i_k \geqslant 1$.

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

$$qt_\ell = \sum_{j=\ell}^{n} qs_\ell s_{\ell+1} \cdots s_{j-1} = \sum_{j=\ell}^{i_{p+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1} \qquad \text{(since } n = i_{p+1} - 1\text{)}$$

$$= \sum_{j=\ell}^{i_k-1} qs_\ell s_{\ell+1} \cdots s_{j-1} + \sum_{j=i_k}^{i_{p+1}-1} qs_\ell s_{\ell+1} \cdots s_{j-1}. \tag{6}$$

Now, from (5), it is easy to see that each $u \in [\ell, i_k - 2]$ belongs to the non-shadow $I'$, and thus 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

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

Subtracting $m_{I,\ell} q$ from both sides of this equality, we obtain

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

Next, recall that $i_k < i_{k+1} < \cdots < i_{p+1}$, and write the interval $[i_k, i_{p+1} - 1]$ as

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

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 view of (8), it is sufficient to show that

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

Let us fix some $r \in [k, p]$. We set

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

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

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

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

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

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

We define a set

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

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 $\operatorname{sum} K \leqslant \operatorname{sum} I - (r-k+1)$ (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). Hence, $\operatorname{sum} K \leqslant \operatorname{sum} I - (r-k+1) < \operatorname{sum} I$ (because $r \geqslant k$). Thus, $F(K) \subseteq F(< \operatorname{sum} I)$. Hence, in order to prove that $q' \in F(< \operatorname{sum} I)$, 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.

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 $i+1 \in [n]$.

Using the definition of $K$ (and the facts $i \notin K$ and $i+1 \notin K$), one can show that

$$i + 1 \notin I.$$

Thus, it is also relatively straightforward to show that

$$i \in I' \text{ if } i \notin [i_k, i_r] . \tag{10}$$

Similarly, one can see that

$$i + 1 \in I' \text{ if } i \in [\ell, i_r - 1] . \tag{11}$$

From (5) and $r \geqslant k$, we obtain $\ell \leqslant i_r < i_{r+1}$. 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 $\ell \leqslant i < i_r$.

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

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

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, $i < \ell - 1 < \ell \leqslant i_k$, so that $i \notin [i_k, i_r]$. Hence, from (10), 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

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

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

Let us next consider Case 2. In this case, we have $i = \ell - 1$. Thus, $i = \ell - 1 < \ell \leqslant i_k$, so that $i \notin [i_k, i_r]$, and therefore $i \in I'$ by (10). Hence, $q s_i = q$ (since $q \in F(I)$). We must prove that $q' s_i = q'$. This easily follows in the case when $\ell = n$ (since $q' = q$ in this case). Hence, for the rest of Case 2, we assume, without loss of generality, that

$\ell \neq n$. Therefore, $\ell \in [n-1]$. Hence, it is easy to see that $\ell \in I'$ (since $\ell = i+1 \notin K$ and $\ell = i+1 \notin I$ and $i_k - 1 \in K$ and since the smallest element of $\widehat{I}$ that is $\geqslant \ell$ is $i_k$). Hence, $qs_\ell = q$. From $\ell \in I'$, we furthermore obtain $\ell \notin I$ and thus $\ell \neq i_r$ (because $i_r \in I$). Hence, $\ell < i_r$. Now, (9) rewrites as

$$q' = \sum_{j=i_r}^{i_{r+1}-1} \underbrace{(qs_\ell)}_{=q} \cdot s_{\ell+1}s_{\ell+2}\cdots s_{j-1} = \sum_{j=i_r}^{i_{r+1}-1} qs_{\ell+1}s_{\ell+2}\cdots s_{j-1}. \tag{12}$$

From $i = \ell - 1$, we see that $s_i$ commutes with the permutations $s_{\ell+1}, s_{\ell+2}, \ldots, s_{i_{r+1}-2}$ that appear on the right hand side of (12), and, multiplying the equality (12) by $s_i$, we find

$$q's_i = \sum_{j=i_r}^{i_{r+1}-1} \underbrace{qs_i}_{=q} \cdot s_{\ell+1}s_{\ell+2}\cdots s_{j-1} = q'.$$

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

Let us now consider Case 3. In this case, we have $\ell \leqslant i < i_r$. Thus, $i < i_r - 1$ (since $i \notin K$ and $i \neq 0$, but $i_r - 1 \in K \cup \{0\}$). Hence, $i+1 < i_r \leqslant n$, and $i \in [\ell, i_r - 1]$. Thus, (11) yields $i+1 \in I'$. Hence, $qs_{i+1} = q$ (since $q \in F(I)$).

Let $j \in [i_r, i_{r+1}-1]$, so that $i < i_r - 1 \leqslant j-1$. Hence, $i \in [\ell, j-2]$, and, using Lemma 6.1,

$$q\ s_\ell s_{\ell+1}\cdots s_{j-1} \cdot s_i = \underbrace{qs_{i+1}}_{=q} \cdot s_\ell s_{\ell+1}\cdots s_{j-1} = qs_\ell s_{\ell+1}\cdots s_{j-1}. \tag{13}$$

Forget that we fixed $j$. We thus have proved (13) for each $j \in [i_r, i_{r+1}-1]$. Now, multiplying the equality (9) by $s_i$, we find

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

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

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

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
$$qs_\ell s_{\ell+1}\cdots s_{j-1} \cdot s_i = qs_\ell s_{\ell+1}\cdots s_{j-1}.$$
- *Claim 2:* We have
$$qs_\ell s_{\ell+1}\cdots s_{i-1} \cdot s_i = qs_\ell s_{\ell+1}\cdots s_i.$$
- *Claim 3:* We have
$$qs_\ell s_{\ell+1}\cdots s_i \cdot s_i = qs_\ell s_{\ell+1}\cdots s_{i-1}.$$

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:

- Let us first consider the subcase when $j < i$. In this subcase, $s_i$ commutes with each of $s_\ell, s_{\ell+1}, \ldots, s_{j-1}$. Thus, $s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i = s_i \cdot s_\ell s_{\ell+1} \cdots s_{j-1}$. Because $i > j \geqslant i_r$, $i \notin [i_k, i_r]$, and (10) yields $i \in I'$. Thus, $qs_i = q$ (since $q \in F(I)$). Now,

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

  We have thus proved Claim 1 in the subcase when $j < i$.
- Let us now consider the subcase when $j > i+1$ or, equivalently, $i \leqslant j-2$. Combining this with $\ell \leqslant i_r \leqslant i$, we obtain $i \in [\ell, j-2]$. Hence, Lemma 6.1 yields $s_\ell s_{\ell+1} \cdots s_{j-1} \cdot s_i = s_{i+1} \cdot s_\ell s_{\ell+1} \cdots s_{j-1}$. Moreover, from $j \in [i_r, i_{r+1}-1] \subseteq [n]$, we obtain $j \leqslant n$, so that $n \geqslant j > i+1$. Hence, $i+1 < n$, so that $i+1 \in [n-1]$.

  Furthermore, $i_r \leqslant i < i+1$. On the other hand, from $j > i+1$, we obtain $i+1 < j \leqslant i_{r+1}-1$ (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 $\widehat{I}$, nor to $I$ (since $I \subseteq \widehat{I}$). In other words, $i+1 \notin I \cup (I-1)$. Since $i+1 \in [n-1]$, we obtain $i+1 \in I'$ (by the definition of $I'$). Thus, $qs_{i+1} = q$ (since $q \in F(I)$). Now,

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

  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, 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

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

proving $q' s_i = q'$ in Case 4.

Finally, let us consider Case 5, in which $i \geqslant i_{r+1}$. Thus, $i \geqslant i_{r+1} > i_r$, so that $i \notin [i_k, i_r]$. From (10), we obtain $i \in I'$, so that $qs_i = q$. Furthermore, from $i \geqslant i_{r+1}$, 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). Hence, multiplying the equality (9) by $s_i$, we find

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

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

We have now proved $q's_i = q'$ in all five cases. 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. $\square$

## 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 the Fibonacci number $f_{n+1}$. Let $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ be all the lacunar subsets of $[n-1]$, listed in an order that satisfies

$$\operatorname{sum}(Q_1) \leqslant \operatorname{sum}(Q_2) \leqslant \cdots \leqslant \operatorname{sum}\left(Q_{f_{n+1}}\right). \tag{14}$$

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

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 (14), 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 (note that $F_0 = 0$):

| $i$ | 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 |

.

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 |
| $\delta_i$ | 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.

When $\mathbf{k}$ is a field, Theorem 8.1 entails that the endomorphisms $R(t_1)$, $R(t_2)$, ..., $R(t_n)$ on $\mathbf{k}[S_n]$ can be simultaneously triangularized (as endomorphisms of the $\mathbf{k}$-module $\mathbf{k}[S_n]$). So, in particular, a $\mathbf{k}$-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 $\operatorname{sum} J \leqslant \operatorname{sum} I$.

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.* (This is a sketch; see [17] for details.)

**(a)** Recall that the non-shadow $I'$ of $I$ is obtained by starting with the set $[n-1]$ and removing all the numbers $i$ and $i-1$ for $i \in I$. In particular, the numbers $j$ and $j-1$ have to be removed, since $j \in I$.

The set $K$ is obtained from $I$ by "moving the element $j$ one unit to the left" (and removing 0 if necessary). Hence, its non-shadow $K'$ is constructed in the same way as $I'$, but instead of removing the numbers $j$ and $j-1$, we now have to remove the numbers $j-1$ and $j-2$. Therefore, the only element of $K'$ that may fail to belong to $I'$ is $j$. In other words, $K' \subseteq I' \cup \{j\}$. This proves part **(a)**.

**(b)** Assume that $j+1 \in I$. Then, $j+1 \in K$ as well, so that $j \notin K'$. Hence, part **(b)** follows from part **(a)**. $\square$

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, $n \in I$. Setting $K := (I \setminus \{n\}) \cup \{n-1\}$ (or just $K := I \setminus \{n\}$ in the case when $n = 1$), one can easily verify that $\operatorname{sum} K < \operatorname{sum} I$ and $K' \subseteq I'$. 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. $\square$

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 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 (and observing that the sum of a subset of $[n]$ cannot keep decreasing forever), we obtain the following corollary:

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

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 a fact that follows directly from the definition of $F(I)$ (given at the beginning of Section 7): If $A$ and $B$ are two subsets of $[n]$ satisfying $B' \subseteq A'$, then $F(A) \subseteq F(B)$. As a consequence, the lacunar subset $J$ in Corollary 8.8 satisfies $F(I) \subseteq F(J)$. Thus, for any given $k \in \mathbb{N}$, the sum on the right hand side of (4) has many redundant addends, and we can restrict this sum to just those addends for which $I$ is a lacunar subset of $[n-1]$. In other words:

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

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

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

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

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 $\text{sum}(Q_i) < k$ (or $0$ if no such $i$ exists). Then, $F(<k) = F_{i_k}$.

[*Proof of Claim 0:* Recall that $\text{sum}(Q_1) \leqslant \text{sum}(Q_2) \leqslant \cdots \leqslant \text{sum}(Q_{f_{n+1}})$. Thus, the inequality $\text{sum}(Q_i) < k$ holds for each $i \leqslant i_k$ but does not hold for any other $i$. Therefore, the lacunar subsets $J$ of $[n-1]$ satisfying $\text{sum } J < k$ are precisely $Q_1, Q_2, \ldots, Q_{i_k}$, and we obtain

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

In view of Corollary 8.9, we can rewrite this as $F(<k) = F_{i_k}$, and 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 $k = \binom{n}{2} + 1$. Then, $\text{sum}[n] = \binom{n}{2} < k$, so that $F([n]) \subseteq F(<k)$. However, $F([n]) = \mathbf{k}[S_n]$ because the non-shadow $[n]' = \varnothing$. Thus, $\mathbf{k}[S_n] = F([n]) \subseteq F(<k) \subseteq F_{f_{n+1}}$ (since Claim 0 yields $F(<k) \subseteq F_{i_k}$ for some $i_k \in [f_{n+1}]$, and this $i_k$ in turn satisfies $F_{i_k} \subseteq F_{f_{n+1}}$). Thus, $F_{f_{n+1}} = \mathbf{k}[S_n]$. The proof of Claim 1 is thus finished.]

[*Proof of Claim 3:* Let $i \in [f_{n+1}]$ and $\ell \in [n]$.

The definition of $F_{i-1}$ yields $F_{i-1} = F(Q_1) + F(Q_2) + \cdots + F(Q_{i-1})$. Now, from Corollary 8.9, it is easy to see that each $i \in [k]$ satisfies

$$F(<\text{sum}(Q_k)) \subseteq F_{k-1} \tag{15}$$

(since the lacunar sets $Q_1, \ldots, Q_{f_{n+1}}$ are ordered by increasing sum, so that all of them that have a smaller sum than $Q_k$ must appear among $Q_1, Q_2, \ldots, Q_{k-1}$).

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,

$$F_i \cdot (t_\ell - m_{Q_i,\ell}) = \sum_{k=1}^{i} F(Q_k) \cdot (t_\ell - m_{Q_i,\ell})$$

$$\begin{aligned}
&= \sum_{k=1}^{i} F(Q_k) \cdot ((t_\ell - m_{Q_k,\ell}) + (m_{Q_k,\ell} - m_{Q_i,\ell})) \\
&\subseteq \sum_{k=1}^{i} \underbrace{F(Q_k) \cdot (t_\ell - m_{Q_k,\ell})}_{\substack{\subseteq F(<\operatorname{sum}(Q_k)) \\ \text{(by Theorem 7.3)}}} + \sum_{k=1}^{i} \underbrace{F(Q_k) \cdot (m_{Q_k,\ell} - m_{Q_i,\ell})}_{\substack{=0 \text{ for } k=i, \\ \text{and } \subseteq F(Q_k) \text{ for all other } k}} \\
&\subseteq \sum_{k=1}^{i} F(< \operatorname{sum}(Q_k)) + \sum_{k=1}^{i-1} F(Q_k) \\
&\subseteq \sum_{k=1}^{i} F_{k-1} + F_{i-1} \qquad \text{(by (15))} \\
&\subseteq F_{i-1} \qquad (\text{since } F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots).
\end{aligned}$$

This proves Claim 3.]

[*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. Thus, we assume, without loss of generality, that $i \neq 0$. Hence, $i \in [f_{n+1}]$, and Claim 3 yields $F_i \cdot (t_\ell - m_{Q_i,\ell}) \subseteq F_{i-1} \subseteq F_i$. Now,

$$F_i \cdot t_\ell = F_i \cdot ((t_\ell - m_{Q_i,\ell}) + m_{Q_i,\ell}) \subseteq F_i \cdot (t_\ell - m_{Q_i,\ell}) + F_i \cdot m_{Q_i,\ell} \subseteq F_i + F_i \subseteq F_i.$$

This proves Claim 2.]

We have now proved all Claims 1, 2 and 3. This proves Theorem 8.1. ☐

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

We 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 $S_n$.
- 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 $G(I) = \langle s_2, s_4 \rangle \leqslant S_5$.
- For each $w \in S_n$, we set

$$a_w := \sum_{\sigma \in G(\operatorname{Des} w)} w\sigma \in \mathbf{k}[S_n]. \tag{16}$$

Example 9.1. For this example, let $n = 3$. We write each permutation $w \in S_3$ in one-line notation (i.e., as the list $[w(1)\ w(2)\ w(3)]$). Then,

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

$$a_{[231]} = [231] + [213] ;$$
$$a_{[312]} = [312] + [132] ;$$
$$a_{[321]} = [321] + [312] + [231] + [213] + [132] + [123] .$$

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 $\sigma \neq \operatorname{id}$. Then, $w\sigma < w$ (with respect to the lexicographic order).*

*Proof sketch.* Here is an informal argument. See [17] for a detailed formal proof.

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 $\sigma$ 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 $k \in [p+1]$), because all the generators $s_i$ of $G(\operatorname{Des} w)$ preserve these intervals. 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, $w\sigma \leqslant w$. Combining this with $w\sigma \neq w$ (which follows from $\sigma \neq \operatorname{id}$), we obtain $w\sigma < w$. This proves Proposition 9.2. ☐

Corollary 9.3. *Let $w \in S_n$. Then,*

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

9.3. The basis property. Using Corollary 9.3, 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 9.4. *The family $(a_w)_{w \in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$.*

Proposition 9.5. *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 9.4 and Proposition 9.5 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 9.6. *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 9.6. $\square$

Now, we can state the general result from which both Proposition 9.4 and Proposition 9.5 will follow:

Proposition 9.7. *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.* We proceed in three steps. 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 precise arguments are fairly straightforward, so we shall only sketch them; more details can be found in [17].

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

$$[w](q\sigma) = \left[w\sigma^{-1}\right] q \tag{17}$$

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 $G(\operatorname{Des} w)$). Hence, the map $G(\operatorname{Des} w) \to G(\operatorname{Des} w),\ \sigma \mapsto \sigma s_i$ is a bijection (since $G(\operatorname{Des} w)$ is a group).

However, multiplying the equality (16) by $s_i$, we find

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

(due to the bijection from the previous paragraph). 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, $a_w \in Z(I)$ (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,

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

[*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 $u = x$.

Using our induction hypothesis, we can easily see that

$$Z(I) \cap \operatorname{span}\left((w)_{w \in S_n;\ w < x}\right) \subseteq \operatorname{span}\left((a_w)_{w \in S_n;\ I \subseteq \operatorname{Des} w}\right). \tag{18}$$

(Indeed, if $x$ is the smallest permutation in $S_n$, then this is clear because the left hand side is 0. In all other cases, this follows by applying our induction hypothesis to $u$ being the permutation that precedes $x$ in the lexicographic order.)

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

To do so, we let $q \in Z(I) \cap \operatorname{span}\left((w)_{w \in S_n;\ w \leqslant x}\right)$. Thus, $q \in \operatorname{span}\left((w)_{w \in S_n;\ w \leqslant x}\right)$, so that

$$[w]\, q = 0 \qquad \text{for every } w \in S_n \text{ satisfying } w > x. \tag{19}$$

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, $x(k) \leqslant x(k+1)$ (since $k \notin \operatorname{Des} x$), so that $x(k) < x(k+1)$. Hence, by the definition of lexicographic order, it follows that $xs_k > x$. Thus, (19) yields $[xs_k]\, q = 0$.

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, (17) yields

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

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 (19), we obtain

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

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 (18)). 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 $q \in Z(I)$ and $a_x \in Z(I)$). Moreover, Corollary 9.3 yields

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

Therefore, $a_x \in \operatorname{span}\left((w)_{w \in S_n;\ w \leqslant x}\right)$ and $[x]\,(a_x) = 1$.

Now, $r = q - \lambda a_x \in \operatorname{span}\left((w)_{w \in S_n;\ w \leqslant x}\right)$ (since both $q$ and $a_x$ lie in this span). That is, $r$ can be written as a linear combination of the permutations $w \in S_n$ satisfying $w \leqslant x$. Moreover, the permutation $x$ does not appear in this combination, since its coefficient in $r$ is

$$[x]\,r = [x]\,(q - \lambda a_x) = [x]\,q - \lambda\,[x]\,(a_x) = \lambda - \lambda \cdot 1 = 0.$$

Hence, $r$ is a linear combination of the permutations $w \in S_n$ satisfying $w < x$. In other words, $r \in \operatorname{span}\left((w)_{w\in S_n;\ w<x}\right)$. 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 (18)). Now, from $r = q - \lambda a_x$, we obtain

$$q = r + \lambda a_x \in \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$$

(since both $r$ and $a_x$ lie in this span). Hence, we 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.

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 $q \in Z\,(I) \cap \operatorname{span}\left((w)_{w\in S_n;\ w\leqslant x}\right)$. In other words, $Z\,(I) \cap \operatorname{span}\left((w)_{w\in S_n;\ w\leqslant x}\right) \subseteq \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$. 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 $Z\,(I)$. Indeed, let $u$ be the largest permutation in $S_n$, so that every $w \in S_n$ satisfies $w \leqslant u$, and $\operatorname{Des} u = [n-1]$. Then, $\operatorname{span}\left((w)_{w\in S_n}\right) = \operatorname{span}\left((w)_{w\in S_n;\ w\leqslant u}\right)$. Hence, $Z\,(I) \subseteq \mathbf{k}[S_n] = \operatorname{span}\left((w)_{w\in S_n;\ w\leqslant u}\right)$, and $Z\,(I) = Z\,(I) \cap \operatorname{span}\left((w)_{w\in S_n;\ w\leqslant u}\right) \subseteq \operatorname{span}\left((a_w)_{w\in S_n;\ I\subseteq \operatorname{Des} w}\right)$ (by Claim 2).

We shall now show that this family is $\mathbf{k}$-linearly independent. Slightly better:

*Claim 3:* The family $(a_w)_{w\in S_n}$ is $\mathbf{k}$-linearly independent.

[*Proof of Claim 3:* Corollary 9.3 shows that this family is obtained from the family $(w)_{w\in S_n}$ by a unitriangular change-of-basis matrix (where we arrange the permutations $w \in S_n$ in lexicographic order). Since the latter family is a basis of the $\mathbf{k}$-module $\mathbf{k}\,[S_n]$, we thus conclude that the former family is a basis as well. In particular, it is thus $\mathbf{k}$-linearly independent. This proves Claim 3.]

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 we also know that it spans the $\mathbf{k}$-module $Z\,(I)$, we thus conclude that this subfamily is a basis of $Z\,(I)$. This proves Proposition 9.7. $\square$

*Proof of Proposition 9.4.* 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 9.7 (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 $(a_w)_{w\in S_n}$, 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 9.4. $\square$

*Proof of Proposition 9.5.* Let $I \subseteq [n]$. Then, Proposition 9.6 yields $F\,(I) = Z\,(I')$.

However, Proposition 9.7 (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 9.5. ☐

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 9.8. *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 9.9. For this example, let $n = 4$. We write each permutation $w \in S_4$ as the in one-line notation. 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 belong to $\{0, 1, -1\}$. However, the smallest $n$ for which this is not the case is $n = 8$.

## 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" depends 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 $[n-1]$. 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 $j \in [n-1]$ lies either in $I$ (if $j \equiv n-1 \mod 2$) or in $I-1$ (if not). Thus, the definition of $I'$ yields $I' = \varnothing \subseteq \operatorname{Des} w$. In other words, $Q'_i \subseteq \operatorname{Des} w$ (since $I = Q_i$). This proves Lemma 10.1. ☐

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, $\operatorname{Qind} w = 4$.

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 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,

$$\operatorname{sum} I = \operatorname{sum}(I \setminus K) + \operatorname{sum}(I \cap K). \tag{20}$$

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

$$\operatorname{sum} K = \operatorname{sum}(K \setminus I) + \operatorname{sum}(K \cap I). \tag{21}$$

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 assume, without loss of generality, 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

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

Therefore, the right hand side of (20) is smaller than that of (21) (since $K \cap I = I \cap K$). Thus, the same holds for the left hand sides. That is, we have $\operatorname{sum} I < \operatorname{sum} K$. This proves Lemma 10.4. □

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 $j$ 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 $\operatorname{sum} J \leqslant \operatorname{sum} R$ and $J' \subseteq R'$. Consider this $J$. Then, $\operatorname{sum} J \leqslant \operatorname{sum} R < \operatorname{sum} I$ 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. □

*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

$$Q_k' \not\subseteq \operatorname{Des} w \qquad \text{for each } k < i. \tag{22}$$

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 $\operatorname{sum}(Q_k) = \operatorname{sum} K < \operatorname{sum}(Q_i)$. In view of (14), this entails that $k < i$. Therefore, (22) 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, $\operatorname{Des} w$ is disjoint from $Q_i$. Hence, $\operatorname{Des} w \subseteq [n-1] \setminus Q_i$. 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, $\operatorname{sum}(Q_k) \leqslant \operatorname{sum}(Q_i)$ (by (14)) and $Q_k \neq Q_i$ (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 $\operatorname{sum}(Q_k) \leqslant \operatorname{sum}(Q_i)$. 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). That is, $\operatorname{Qind} w = i$. Thus, we have proved the "$\Longleftarrow$" direction of Proposition 10.3. $\square$

### 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* $(a_w)_{w \in S_n;\ \operatorname{Qind} w \leqslant i}$*.*
- **(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 9.4 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

$$F(Q_k) = \operatorname{span}\left((a_w)_{w \in S_n;\ Q_k' \subseteq \operatorname{Des} w}\right) \tag{23}$$

(since Proposition 9.5 (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

$$F_i = F(Q_1) + F(Q_2) + \cdots + F(Q_i) = \sum_{k=1}^{i} F(Q_k)$$
$$= \sum_{k=1}^{i} \operatorname{span}\left((a_w)_{w\in S_n;\ Q'_k\subseteq \operatorname{Des} w}\right) \qquad \text{(by (23))}$$
$$= \operatorname{span}\left((a_w)_{w\in S_n;\ Q'_k\subseteq \operatorname{Des} w \text{ for some } k\in[i]}\right). \tag{24}$$

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 "$\operatorname{Qind} w \leqslant i$" (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 $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leqslant i}$. Hence, we can rewrite (24) as follows:

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

In other words, the family $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leqslant i}$ 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 $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leqslant i}$. 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 $\operatorname{Qind} w \leqslant i$. 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 $\operatorname{Qind} w \leqslant i$ are precisely the permutations $w \in A(i)$. Hence, the family $(a_w)_{w\in S_n;\ \operatorname{Qind} w\leqslant i}$ is precisely the family $(a_w)_{w\in A(i)}$.

In view of this, Theorem 10.6 **(a)** yields that the $\mathbf{k}$-module $F_i$ is free with basis $(a_w)_{w\in A(i)}$ . The same argument 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 $(\overline{a_w})_{w\in A(i)\setminus A(i-1)}$.

However, $A(i) \setminus A(i-1) = \{w \in S_n \mid \operatorname{Qind} w = i\}$ (by the definitions of $A(i)$ and $A(i-1)$). Thus, the family $(\overline{a_w})_{w\in A(i)\setminus A(i-1)}$ is exactly the family $(\overline{a_w})_{w\in S_n;\ \operatorname{Qind} w=i}$. The previous paragraph is thus saying that the $\mathbf{k}$-module $F_i/F_{i-1}$ is free with basis $(\overline{a_w})_{w\in S_n;\ \operatorname{Qind} w=i}$. This proves Theorem 10.6 **(b)**. $\square$

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. $\square$

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 $i \in [f_{n+1}]$. Theorem 10.6 **(b)** yields that the $\mathbf{k}$-module $F_i / F_{i-1}$ is free with basis $(\overline{a_w})_{w \in S_n;\ \operatorname{Qind} w = i}$. This basis is nonempty (by Lemma 10.7). Hence, $F_i / F_{i-1} \neq 0$, so that $F_i \neq F_{i-1}$. Thus, Corollary 10.8 is proved. $\square$

## 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,*

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

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

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

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 $(a_v)_{v \in S_n;\ \operatorname{Qind} v \leqslant i-1}$. (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, $(a_v)_{v \in S_n;\ \operatorname{Qind} v \leqslant i-1}$ is a basis of the $\mathbf{k}$-module $F_{i-1}$. Hence, $F_{i-1} = \operatorname{span}\left((a_v)_{v \in S_n;\ \operatorname{Qind} v \leqslant i-1}\right)$. Now,

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

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

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

Equivalently,

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

This proves Theorem 11.1. $\square$

## 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,*

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

*(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 note that

$$F_i \cdot (t - g_i) \subseteq F_{i-1} \qquad \text{for each } i \in [f_{n+1}], \tag{25}$$

which follows easily from Theorem 8.1 **(c)**. Details can be found in [17].

Using this, we can easily show that

$$F_m \cdot \prod_{j=1}^{m} (t - g_j) = 0 \qquad \text{for each } m \in [0, f_{n+1}]. \tag{26}$$

(Again, the product $\prod_{j=1}^{m}(t-g_j)$ 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.) Equation (26) can be proven by induction on $m$, where the base case ($m=0$) follows from $F_0=0$, and the induction step follows from (25). More details can be found in [17].

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

$$\begin{aligned}
&\prod_{\substack{I\subseteq[n-1] \text{ is}\\ \text{lacunar}}} (t-(\lambda_1 m_{I,1}+\lambda_2 m_{I,2}+\cdots+\lambda_n m_{I,n}))\\
&=\prod_{j=1}^{f_{n+1}}\left(t-\left(\lambda_1 m_{Q_j,1}+\lambda_2 m_{Q_j,2}+\cdots+\lambda_n m_{Q_j,n}\right)\right)\\
&=\prod_{j=1}^{f_{n+1}}(t-g_j)=1\cdot\prod_{j=1}^{f_{n+1}}(t-g_j)\in F_{f_{n+1}}\cdot\prod_{j=1}^{f_{n+1}}(t-g_j)=0
\end{aligned}$$

(by (26)). In other words,

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

This proves Theorem 12.1. □

12.2. The spectrum. We now describe the spectrum of $R(\lambda_1 t_1+\lambda_2 t_2+\cdots+\lambda_n t_n)$ 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,*

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

*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.(4)

*Proof of Corollary 12.2.* Let

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

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

$$\operatorname{Qind}(w_1)\leqslant\operatorname{Qind}(w_2)\leqslant\cdots\leqslant\operatorname{Qind}(w_{n!}). \tag{27}$$

(This ordering is not the lexicographic order!)

(4)This is due to the fact that (when $\mathbf{k}$ is a $\mathbb{Q}$-algebra) $\mathbf{k}[S_n]$ decomposes into a direct sum of *Specht modules* indexed by partitions of $n$, and that the Specht module corresponding to the partition $\lambda$ appears $f^\lambda$ many times, where $f^\lambda$ is the number of standard tableaux of shape $\lambda$. Since $R(a)$ 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 $R(a)$ 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 $[n]$.

Proposition 9.4 says that the family $(a_w)_{w\in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$. In other words, the list $(a_{w_1}, a_{w_2}, \ldots, a_{w_{n!}})$ is a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$. We shall refer to this basis as the *a-basis*. Let $M = (\mu_{i,j})_{i,j\in[n!]}$ be the matrix that represents the endomorphism $\rho$ with respect to this a-basis $(a_{w_1}, a_{w_2}, \ldots, a_{w_{n!}})$. Then, for each $j \in [n!]$, we have

$$\rho\left(a_{w_j}\right) = \sum_{k=1}^{n!} \mu_{k,j} a_{w_k}. \tag{28}$$

On the other hand, recall that $\rho = R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n) = R\left(\sum_{\ell=1}^{n} \lambda_\ell t_\ell\right)$. Hence, by the definition of $R(x)$, we have

$$\rho\left(a_{w_j}\right) = a_{w_j} \cdot \sum_{\ell=1}^{n} \lambda_\ell t_\ell = \sum_{\ell=1}^{n} \lambda_\ell a_{w_j} t_\ell. \tag{29}$$

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

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

*Claim 1:* The diagonal entries of $M$ satisfy $\mu_{j,j} = g_{\mathrm{Qind}(w_j)}$ for each $j \in [n!]$.

*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 $\mu_{j,j} = g_{\mathrm{Qind}(w_j)}$.

The equality (28) 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 $i := \mathrm{Qind}(w_j)$. Then, Equation (29) becomes

$$\begin{aligned}\rho\left(a_{w_j}\right) &= \sum_{\ell=1}^{n} \lambda_\ell a_{w_j} t_\ell \\ &= \sum_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell} a_{w_j} \\ &\qquad + (\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \mathrm{Qind}\, v < i)\end{aligned}$$

(by Theorem 11.1, applied to $w = w_j$). In view of

$$\sum_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell} = g_i,$$

we can rewrite this as

$$\rho\left(a_{w_j}\right) = g_i a_{w_j} + (\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \mathrm{Qind}\, v < i)\,. \tag{30}$$

The right hand side of (30) is clearly a $\mathbf{k}$-linear combination of the a-basis. The basis vector $a_{w_j}$ appears in this combination with coefficient $g_i$ (since the $\mathbf{k}$-linear combination of $a_v$'s for $v \in S_n$ satisfying $\mathrm{Qind}\, v < i$ does not contain $a_{w_j}$, because $w_j$ is not such a $v$). 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 expanded as a $\mathbf{k}$-linear combination of the a-basis). In view of $i = \mathrm{Qind}(w_j)$, this rewrites as $\mu_{j,j} = g_{\mathrm{Qind}(w_j)}$. 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 (28) 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.

Let $i := \mathrm{Qind}(w_j)$. Just as in the proof of Claim 1, we obtain the equality (30), which expands $\rho\left(a_{w_j}\right)$ as a $\mathbf{k}$-linear combination of the a-basis. The right hand side of this equality is clearly a $\mathbf{k}$-linear combination of the a-basis. The element $a_{w_k}$ of the a-basis does not appear in this combination (since $k > j$ and (27) ensure that $w_k$ is neither $w_j$ nor a permutation $v \in S_n$ satisfying $\operatorname{Qind} v < i$). Thus, 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. Thus,

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

by Claim 1.

The values $\operatorname{Qind} w$ for all $w \in S_n$ belong to the set $[f_{n+1}]$ (by their definition). Conversely, each $i \in [f_{n+1}]$ 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 $\rho$ 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, $\operatorname{Spec} M = \operatorname{Spec} \rho$. Hence,

$$\begin{aligned}
\operatorname{Spec} \rho = \operatorname{Spec} M &= \left\{g_{\operatorname{Qind}(w_j)} \ \mid \ j \in [n!]\right\} = \{g_{\operatorname{Qind} w} \ \mid \ w \in S_n\} \\
&= \{g_i \ \mid \ i \in [f_{n+1}]\} \qquad \left(\text{since } \{\operatorname{Qind} w \ \mid \ w \in S_n\} = [f_{n+1}]\right) \\
&= \{\lambda_1 m_{Q_i,1} + \lambda_2 m_{Q_i,2} + \cdots + \lambda_n m_{Q_i,n} \ \mid \ i \in [f_{n+1}]\} \\
&= \{\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n} \ \mid \ I \subseteq [n-1] \text{ is lacunar}\}
\end{aligned}$$

(since $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are exactly the lacunar subsets $I$ of $[n-1]$). This proves Corollary 12.2 (since $\rho = R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$). ☐

12.3. Diagonalizability. We have already seen in Remark 4.2 that the endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ of $\mathbf{k}[S_n]$ 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 $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ of $\mathbf{k}[S_n]$ 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

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

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 $A^{\mathrm{op}}$ to $B$, where $A^{\mathrm{op}}$ 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. 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 $\rho$ be the endomorphism $R(t)$ of $\mathbf{k}[S_n]$. We shall show that $\rho$ 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 $\prod_{\substack{I \subseteq [n-1] \\ \text{is lacunar}}} (X - (\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n})) \in \mathbf{k}[X]$. 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 $R(P(t)) = P(R(t)) = P(\rho)$. Hence, $P(\rho) = R(P(t)) = R(0) = 0$. Therefore, the minimal polynomial of $\rho$ divides $P$. (Note that the minimal polynomial of $\rho$ is indeed well-defined, since $\rho$ 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 $\rho$ is split separable (since this minimal polynomial divides $P$, which is split separable).

Now, recall the following fact (see, e.g., [20, §6.4, Theorem 6]): 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 $\rho$ is diagonalizable (since the minimal polynomial of $\rho$ is split separable). Since $\rho = R(t) = R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$, then $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is diagonalizable. 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 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 for $\mathbf{k}[S_n]$, $n \leqslant 11$. It is 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 [7, 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 $\delta_i$ 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 $\delta_i$. (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 $\delta_i$ 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,*

$$\delta_i = \binom{n}{j_1, j_2, \ldots, j_{p+1}} \cdot \prod_{k=2}^{p+1} (j_k - 1). \tag{31}$$

*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 $\delta_i$ (by the definition of $\delta_i$). This proves Theorem 13.1 **(a)**.

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

$$\begin{aligned}
&(\operatorname{Qind} w = i) \\
\iff\ &(Q'_i \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i) \qquad \text{(by Proposition 10.3 )} \\
\iff\ &(Q'_i \subseteq \operatorname{Des} w \text{ and } \operatorname{Des} w \subseteq [n-1] \setminus Q_i) \\
\iff\ &((j \in \operatorname{Des} w \text{ for all } j \in Q'_i) \text{ and } (\operatorname{Des} w \text{ is disjoint from } Q_i)) \\
\iff\ &((j \in \operatorname{Des} w \text{ for all } j \in Q'_i) \text{ and } (j \notin \operatorname{Des} w \text{ for all } j \in Q_i))
\end{aligned}$$

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

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

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

(because $\delta_i$ was defined as the number of 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 $h \geqslant 2$ 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 assume, without loss of generality, 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,

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

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

$$Q_i = \{i_1, i_2, \ldots, i_p\} \tag{32}$$

and

$$Q_i' = \{1,\ 2,\ \ldots,\ i_1 - 2\} \cup \bigcup_{k=2}^{p+1} \{i_{k-1} + 1,\ i_{k-1} + 2,\ \ldots,\ i_k - 2\}. \tag{33}$$

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 $|J_k| = i_k - i_{k-1} = j_k$.

The set $\{i_1 < i_2 < \cdots < i_p\} = Q_i$ is a lacunar subset of $[n-1]$ (since it is one of the sets $Q_1, Q_2, \ldots, Q_{f_{n+1}}$). Thus, inserting $i_{p+1} = n + 1$ into it, we still obtain a lacunar set (since $n + 1$ is at least by 2 larger than any element of $[n-1]$). In other words, the set $\{i_1 < i_2 < \cdots < i_{p+1}\}$ is lacunar. The $p$ integers $j_2, j_3, \ldots, j_{p+1}$ are (by their definition) the distances between adjacent elements of this lacunar set, and thus are $\geqslant 2$. In other words, we have

$$j_k \geqslant 2 \qquad \text{for each } k \in [2, p+1]\,. \tag{34}$$

Moreover, $j_1 = i_1 - i_0 \geqslant 0$ (since $i_0 \leqslant i_1$).

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

$$w(j) < w(j+1) \qquad \text{for all } j \in Q_i \tag{35}$$

and

$$w(j) > w(j+1) \qquad \text{for all } j \in Q'_i. \tag{36}$$

In view of (32) and (33), we can rewrite this as follows: $\delta_i$ 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, $\delta_i$ 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 $\binom{n}{j_1, j_2, \ldots, j_{p+1}}$ 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 (34) yields $j_k \geqslant 2$). Hence, in total, we have $\prod_{k=2}^{p+1}(j_k - 1)$ options at this step.

Altogether, the total number of possibilities to perform this construction is thus $\binom{n}{j_1, j_2, \ldots, j_{p+1}} \cdot \prod_{k=2}^{p+1}(j_k - 1)$. 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 $j_k \geqslant 2$ for each $k \in [2, p+1]$ (in fact, this is the inequality (34), which has been shown in our above proof of Theorem 13.1 **(c)**).

The definition of a multinomial coefficient yields

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

Hence, we can rewrite (31) as

$$\delta_i = \frac{n!}{j_1! \prod_{k=2}^{p+1} j_k!} \cdot \prod_{k=2}^{p+1} (j_k - 1) = \frac{n!}{j_1! \cdot \prod_{k=2}^{p+1} (j_k! \diagup (j_k - 1))} = \frac{n!}{j_1! \cdot \prod_{k=2}^{p+1} ((j_k - 2)! \cdot j_k)}$$

(since a straightforward computation shows that each $k \in [2, p+1]$ satisfies $j_k! \diagup (j_k - 1) = (j_k - 2)! \cdot j_k$).

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

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 $\delta_i$, where $i \in [f_{n+1}]$ is chosen such that $I = Q_i$ (and where $\delta_i$ 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 $\delta_i$'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 $\delta_i$ 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 $\kappa \in \mathbf{k}$ be arbitrary. Then, the algebraic multiplicity of $\kappa$ 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). Using Claim 1 from the proof of Corollary 12.2, we recall that the entries on the diagonal of $M$ satisfy $\mu_{j,j} = g_{\operatorname{Qind}(w_j)}$ for each $j \in [n!]$. We thus conclude that

$$\begin{aligned}
&(\text{the algebraic multiplicity of } \kappa \text{ as an eigenvalue of } M) \\
&= (\text{the number of times that } \kappa \text{ appears on the main diagonal of } M) \\
&= (\text{the number of } j \in [n!] \text{ such that } \mu_{j,j} = \kappa) \qquad \left(\text{since } M = (\mu_{i,j})_{i,j \in [n!]}\right) \\
&= \left(\text{the number of } j \in [n!] \text{ such that } g_{\operatorname{Qind}(w_j)} = \kappa\right) \\
&= (\text{the number of } w \in S_n \text{ such that } g_{\operatorname{Qind} w} = \kappa) \\
&= \sum_{\substack{i \in [f_{n+1}];\\ g_i = \kappa}} (\text{the number of } w \in S_n \text{ such that } \operatorname{Qind} w = i)
\end{aligned}$$

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

This proves Theorem 13.2. □

## 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

$$t'_\ell := \mathrm{cyc}_\ell + \mathrm{cyc}_{\ell+1,\ell} + \mathrm{cyc}_{\ell+2,\ell+1,\ell} + \cdots + \mathrm{cyc}_{n,n-1,\ldots,\ell} \in \mathbf{k}[S_n]. \tag{37}$$

In terms of card shuffling, this element $t'_\ell$ corresponds to randomly picking a card from the bottommost $n-\ell+1$ positions in the deck (with uniform probabilities) and moving it to position $\ell$. 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., [24, 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

$$\begin{aligned} S\left(\mathrm{cyc}_{i_1,i_2,\ldots,i_k}\right) &= \left(\mathrm{cyc}_{i_1,i_2,\ldots,i_k}\right)^{-1} \qquad \text{(by the definition of } S\text{)} \\ &= \mathrm{cyc}_{i_k,i_{k-1},\ldots,i_1}. \end{aligned} \tag{38}$$

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

$$\begin{aligned} S(t_\ell) &= S\left(\mathrm{cyc}_\ell + \mathrm{cyc}_{\ell,\ell+1} + \mathrm{cyc}_{\ell,\ell+1,\ell+2} + \cdots + \mathrm{cyc}_{\ell,\ell+1,\ldots,n}\right) \qquad \text{(by (1))} \\ &= S(\mathrm{cyc}_\ell) + S\left(\mathrm{cyc}_{\ell,\ell+1}\right) + S\left(\mathrm{cyc}_{\ell,\ell+1,\ell+2}\right) + \cdots + S\left(\mathrm{cyc}_{\ell,\ell+1,\ldots,n}\right) \\ &= \mathrm{cyc}_\ell + \mathrm{cyc}_{\ell+1,\ell} + \mathrm{cyc}_{\ell+2,\ell+1,\ell} + \cdots + \mathrm{cyc}_{n,n-1,\ldots,\ell} \qquad \text{(by (38))} \\ &= t'_\ell \qquad \text{(by (37))}. \end{aligned} \tag{39}$$

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,

$$\begin{aligned} S(t) &= S(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n) \\ &= \lambda_1 S(t_1) + \lambda_2 S(t_2) + \cdots + \lambda_n S(t_n) \qquad (\text{since } S \text{ is } \mathbf{k}\text{-linear}) \\ &= \lambda_1 t_1' + \lambda_2 t_2' + \cdots + \lambda_n t_n' \qquad (\text{by ( 39 )}) \\ &= t' \qquad (\text{by the definition of } t'). \end{aligned}$$

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

Then,

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

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

However, $S$ is a $\mathbf{k}$-algebra antihomomorphism. Thus, Proposition 12.4 (applied to $A = \mathbf{k}[S_n]$, $B = \mathbf{k}[S_n]$, $f = S$ and $u = t$) yields that $S(P(t)) = P(S(t))$. In view of $S(t) = t'$, we can rewrite this as

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

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

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

This proves Theorem 14.1. □

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.[(5)]

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

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

  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.

(5) 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.

- If $U$ and $V$ are two $\mathbf{k}$-modules with bases $(u_w)_{w\in W}$ and $(v_w)_{w\in W}$, respectively[(6)], 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

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

  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 (see [17] for proofs):

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.*

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 $f$.*

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*

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

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

$$f(p, q) = [p = q] \qquad \text{for all } p, q \in S_n. \tag{40}$$

(This defines a unique bilinear form, since $(w)_{w\in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$.) Clearly, the basis $(w)_{w\in S_n}$ of $\mathbf{k}[S_n]$ is dual to itself with respect to this form $f$. Thus, Proposition 14.2 (applied to $U = \mathbf{k}[S_n]$, $V = \mathbf{k}[S_n]$, $W = S_n$, $(u_w)_{w\in W} = (w)_{w\in S_n}$ 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 $U = \mathbf{k}[S_n]$, $V = \mathbf{k}[S_n]$, $W = S_n$ 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 9.4 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

$$f(a_p, b_q) = [p = q] \qquad \text{for all } p, q \in S_n. \tag{41}$$

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,*

$$b_w t'_\ell = m_{Q_i,\ell} b_w + (a\ \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v > i).$$

[(6)] Note that the bases must have the same indexing set in this definition.

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 (40):

Lemma 14.6. *We have*

$$f(u, vS(x)) = f(ux, v) \qquad \textit{for all } x, u, v \in \mathbf{k}[S_n].$$

*Proof.* This is an easy consequence of the $\mathbf{k}$-bilinearity of $f$ (which allows us to assume that $x, u, v$ all belong to $S_n$) and of the definition of $S$ (which shows that $S(x) = x^{-1}$ when $x \in S_n$). Details can be found in [17]. □

*Proof of Theorem 14.5.* Forget that we fixed $w$ and $i$ (but keep $\ell$ fixed). For each $u \in S_n$, define two elements

$$\widetilde{a}_u := a_u t_\ell - m_{Q_{\operatorname{Qind} u},\ell} a_u \qquad \text{and} \qquad \widetilde{b}_u := b_u t'_\ell - m_{Q_{\operatorname{Qind} u},\ell} b_u$$

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)** shows that each $u \in \mathbf{k}[S_n]$ satisfies

$$u = \sum_{w\in S_n} f(u, b_w)\, a_w. \tag{42}$$

Furthermore, Proposition 14.4 **(b)** shows that each $v \in \mathbf{k}[S_n]$ satisfies

$$v = \sum_{w\in S_n} f(a_w, v)\, b_w. \tag{43}$$

For each $u \in S_n$, we have

$$\widetilde{a}_u = \sum_{w\in S_n} f(\widetilde{a}_u, b_w)\, a_w \tag{44}$$

(by (42)).

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 (43)). 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

$$\widetilde{b}_w = \sum_{v\in S_n} f\left(a_v, \widetilde{b}_w\right) b_v. \tag{45}$$

We shall now prove the following:

*Claim 1:* Let $u, w \in S_n$ be such that $\operatorname{Qind} w \geqslant \operatorname{Qind} u$. 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 $\operatorname{Qind} w \geqslant \operatorname{Qind} u = j$. Thus, $w$ does not satisfy $\operatorname{Qind} w < j$.

Theorem 11.1 (applied to $u$ and $j$ instead of $w$ and $i$) yields

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

In view of $\widetilde{a}_u = a_u t_\ell - m_{Q_{\operatorname{Qind} u},\ell} a_u = a_u t_\ell - m_{Q_j,\ell} a_u$, we can rewrite this as

$$\widetilde{a}_u = (\text{a } \mathbf{k}\text{-linear combination of } a_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} v < j).$$

The $\mathbf{k}$-linear combination on the right hand side here does not contain $a_w$ (since $w \in S_n$ does not satisfy $\operatorname{Qind} w < j$). Thus, 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 (44) shows that this coefficient is $f(\widetilde{a}_u, b_w)$. 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,

$$\begin{aligned}
f(\widetilde{a}_u, b_w) &= f\left(a_u t_\ell - m_{Q_{\operatorname{Qind} u},\ell} a_u,\ b_w\right) \\
&= f(a_u t_\ell, b_w) - m_{Q_{\operatorname{Qind} u},\ell} f(a_u, b_w) && \text{(since } f \text{ is a bilinear form)} \\
&= f(a_u t_\ell, b_w) - m_{Q_{\operatorname{Qind} u},\ell} [u = w], && \text{(by (41))}. \qquad (46)
\end{aligned}$$

However, it is easy to see that

$$m_{Q_{\operatorname{Qind} w},\ell} [u = w] = m_{Q_{\operatorname{Qind} u},\ell} [u = w] \qquad (47)$$

(indeed, this equality is obvious when $u = w$ and otherwise).

On the other hand, the definition of $\widetilde{b}_w$ yields $\widetilde{b}_w = b_w t'_\ell - m_{Q_{\operatorname{Qind} w},\ell} b_w$. Since $f$ is $\mathbf{k}$-bilinear, we thus obtain

$$\begin{aligned}
f\left(a_u, \widetilde{b}_w\right) &= f(a_u, b_w t'_\ell) - m_{Q_{\operatorname{Qind} w},\ell} f(a_u, b_w) \\
&= f(a_u, b_w S(t_\ell)) - m_{Q_{\operatorname{Qind} w},\ell} [u = w] && \text{(by (39) and (41))} \\
&= f(a_u t_\ell, b_w) - m_{Q_{\operatorname{Qind} u},\ell} [u = w] && \text{(by Lemma 14.6 and (47))} \\
&= f(\widetilde{a}_u, b_w)
\end{aligned}$$

by (46). 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, (45) yields

$$\begin{aligned}
\widetilde{b}_w &= \sum_{v \in S_n} f\left(a_v, \widetilde{b}_w\right) b_v = \sum_{v \in S_n} f(\widetilde{a}_v, b_w) b_v && \text{(by Claim 2)} \\
&= \sum_{\substack{v \in S_n; \\ \operatorname{Qind} w < \operatorname{Qind} v}} f(\widetilde{a}_v, b_w) b_v && \left(\begin{array}{c}\text{since Claim 1 shows that all} \\ \text{addends with } \operatorname{Qind} w \geqslant \operatorname{Qind} v \text{ are zero}\end{array}\right) \\
&= (\text{a } \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } \operatorname{Qind} w < \operatorname{Qind} v) \\
&= (\text{a } \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } i < \operatorname{Qind} v).
\end{aligned}$$

In view of $\widetilde{b}_w = b_w t'_\ell - m_{Q_i,\ell} b_w$, this can be rewritten as

$$b_w t'_\ell = m_{Q_i,\ell} b_w + (\text{a } \mathbf{k}\text{-linear combination of } b_v\text{'s for } v \in S_n \text{ satisfying } i < \operatorname{Qind} v).$$

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

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

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:(7)

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*

$$R(S(x)) = S \circ (L(x)) \circ S^{-1}. \tag{48}$$

*Proof.* 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

$$S(xz) = S(z)\, S(x) \qquad \text{for each } z \in \mathbf{k}[S_n]. \tag{49}$$

Now, for each $y \in \mathbf{k}[S_n]$, we obtain

$$(R(S(x)))(y) = \left(S \circ (L(x)) \circ S^{-1}\right)(y)$$

as a result of comparing

$$(R(S(x)))(y) = yS(x) \qquad \text{(by the definition of } R(S(x)))$$

with

$$\begin{aligned}\left(S \circ (L(x)) \circ S^{-1}\right)(y) &= S\left((L(x))\left(S^{-1}(y)\right)\right) = S\left(xS^{-1}(y)\right) \\ &= S\left(S^{-1}(y)\right) S(x) \qquad \text{(by (49))} \\ &= yS(x).\end{aligned}$$

In other words, $R(S(x)) = S \circ (L(x)) \circ S^{-1}$. This proves (49), and the rest of Proposition 14.7 follows. ☐

Corollary 14.8. *Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$ be arbitrary. 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*

$$R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n) = S \circ (L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)) \circ S^{-1}.$$

*Proof.* It is easy to see that the map

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

is $\mathbf{k}$-linear. Hence,

$$R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n) = \lambda_1 R(t'_1) + \lambda_2 R(t'_2) + \cdots + \lambda_n R(t'_n) = \sum_{\ell=1}^{n} \lambda_\ell R(t'_\ell).$$

Similarly,

$$L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n) = \sum_{\ell=1}^{n} \lambda_\ell L(t_\ell).$$

(7)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 $w^{-1}$.

Hence,

$$S \circ (L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)) \circ S^{-1} = S \circ \left( \sum_{\ell=1}^{n} \lambda_\ell L(t_\ell) \right) \circ S^{-1} = \sum_{\ell=1}^{n} \lambda_\ell S \circ (L(t_\ell)) \circ S^{-1}$$

(by linearity). Comparing this with

$$R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n) = \sum_{\ell=1}^{n} \lambda_\ell R(t'_\ell) = \sum_{\ell=1}^{n} \lambda_\ell R(S(t_\ell)) \qquad (\text{since } t'_\ell = S(t_\ell))$$
$$= \sum_{\ell=1}^{n} \lambda_\ell S \circ (L(t_\ell)) \circ S^{-1} \qquad (\text{by (48)}),$$

we obtain

$$R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n) = S \circ (L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)) \circ S^{-1}.$$

Thus, Corollary 14.8 follows. ☐

Using Corollary 14.8, we can derive properties of $L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ from properties of $R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n)$ by conjugating with $S^{-1}$. In particular, we obtain an analogue of Theorem 4.1 for $L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ instead of $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$, since we already know (from Subsection 14.1) that such an analogue exists for $R(\lambda_1 t'_1 + \lambda_2 t'_2 + \cdots + \lambda_n t'_n)$. Thus, we shall not discuss $L(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ any further.

14.3. A Boolean interval partition of $\mathcal{P}([n-1])$. 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 [1] 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.* As in our proof of Lemma 10.7, we can construct a permutation $w \in S_n$ satisfying $\operatorname{Des} w = J$. Fix such a $w$.

There exists a unique $i \in [f_{n+1}]$ such that $\operatorname{Qind} w = i$. In view of Proposition 10.3, we can rewrite this as follows: There exists a unique $i \in [f_{n+1}]$ such that $Q'_i \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i$. Since $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ are all the lacunar subsets of $[n-1]$ (listed without repetition), we can rewrite this as follows: There exists a unique lacunar subset $I$ of $[n-1]$ satisfying $I' \subseteq \operatorname{Des} w \subseteq [n-1] \setminus I$. But this is precisely the claim of Corollary 14.9 (since $\operatorname{Des} w = J$). ☐

In the language of Boolean interval partitions (see [14, §4.4]), Corollary 14.9 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 [7, Theorem 4.1]). Unfortunately, the fact that $R(t_1)$ is diagonalizable when $\mathbf{k}$ is a field of characteristic 0 (see, e.g., [7, Theorem 4.1]) cannot be recovered from our above results (as the assumptions of Theorem 12.3 are not satisfied when $n \geqslant 4$ 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 ([2]). 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 [2], or in [22, §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.[8] 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 $\tau$ 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 $t \geqslant \tau$, meaning that $\tau$ 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.

[8] We agree that if a card moves into the space that contains the bookmark, then it is inserted below (not above) the bookmark.

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.

- 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 $j \geqslant i$) 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 $H_i := \sum\limits_{k=1}^{i} \dfrac{1}{k}$ 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

$$\frac{1}{\dfrac{i}{n}\left(H_n - H_{i-1}\right)} = \frac{n}{i\left(H_n - H_{i-1}\right)}.$$

  (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 $n \geqslant 2$. 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:*

$$\sum_{i=2}^{n} \frac{n}{i\left(H_n - H_{i-1}\right)} \leqslant n \log n + n \log(\log n) + n \log(2) + 1.$$

*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. We begin with three properties of the logarithm function that can be proved fairly straightforwardly (see [17] for details):

LEMMA 15.3. *Let $a$ and $b$ be two positive reals. Then:*

***(a)*** *We have* $\log \dfrac{a+b}{a} \leqslant \dfrac{b}{a}$.

***(b)*** *We have* $\log \dfrac{a+b}{a} \geqslant \dfrac{b}{a+b}$.

LEMMA 15.4. *Let $m$ be a positive real. Then, the function $f : (0,m) \to \mathbb{R}$ given by*

$$f(x) = \frac{1}{x \log \dfrac{m}{x}} \qquad \text{for all } x \in (0,m)$$

*is convex.*

LEMMA 15.5. *If $n \geqslant 3$, then* $\dfrac{n+1}{n} - \dfrac{n+1}{3} < \dfrac{\log n}{2n}$.

LEMMA 15.6. *Let $i \leqslant n$ be a positive integer. Then,*

$$H_n - H_{i-1} \geqslant \log \frac{n+1}{i}.$$

*Proof of Lemma 15.6.* For each $j \in \{i, i+1, \ldots, n\}$, we have

$$\begin{aligned} H_j - H_{j-1} = \frac{1}{j} &\geqslant \log \frac{j+1}{j} \qquad \text{(by Lemma 15.3 } \textbf{(a)}\text{)} \\ &= \log(j+1) - \log j. \end{aligned}$$

Summing up these inequalities yields $H_n - H_{i-1} \geqslant \log(n+1) - \log i = \log \dfrac{n+1}{i}$. ☐

The next lemma we need is a simple inequality between integrals and their Riemann sums for convex functions:

LEMMA 15.7. *Let $a$ and $b$ be two integers satisfying $a \leqslant b$. Let $f : (a-1, b+1) \to \mathbb{R}$ be a convex function. Then,*

$$\sum_{i=a}^{b} f(i) \leqslant \int_{a-1/2}^{b+1/2} f(x)\, dx.$$

*Proof of Lemma 15.7.* See [17]. The idea is that the convexity of $f$ entails $f(i) \leqslant \int_{i-1/2}^{i+1/2} f(x)\, dx$ for each $i \in [a,b]$. ☐

Now, we return to the proof of the upper bound

$$\sum_{i=2}^{n} \frac{n}{i(H_n - H_{i-1})} \leqslant n \log n + n \log(\log n) + n \log 2 + 1 \tag{50}$$

claimed in Theorem 15.2.

Indeed, this upper bound can be checked by straightforward computations for $n = 2$. So let us assume, without loss of generality, that $n \geqslant 3$.

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

$$\begin{aligned} \sum_{i=2}^{n} \frac{n}{i(H_n - H_{i-1})} &\leqslant \sum_{i=2}^{n} \frac{n}{i \log \dfrac{n+1}{i}} = \sum_{i=2}^{n} \frac{n}{i \log \dfrac{m}{i}} \qquad (\text{since } n+1 = m) \\ &= n \cdot \sum_{i=2}^{n} \frac{1}{i \log \dfrac{m}{i}} = n \cdot \sum_{i=2}^{n} f(i). \end{aligned}$$

Hence, in order to prove (50), we only need to show that

$$\sum_{i=2}^{n} f(i) \leqslant \log n + \log(\log n) + \log 2 + \frac{1}{n}. \tag{51}$$

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

$$\begin{aligned}
\sum_{i=2}^{n} f(i) &\leqslant \int_{3/2}^{n+1/2} f(x)\, dx \\
&= \left(-\log\left(\log \frac{m}{n+1/2}\right)\right) - \left(-\log\left(\log \frac{m}{3/2}\right)\right) \\
&= \log\left(\log \frac{m}{3/2}\right) - \log\left(\log \frac{(n+1/2)+1/2}{n+1/2}\right) \\
&\leqslant \log\left(\log \frac{m}{3/2}\right) - \log \frac{1/2}{n+1} \qquad \text{(by Lemma 15.3 \textbf{(b)})} \\
&= \log\left(\left(\log \frac{m}{3/2}\right) \Big/ \frac{1/2}{m}\right) = \log\left(2m \log \frac{m}{3/2}\right).
\end{aligned}$$

Thus, in order to prove (51), it suffices to show that

$$\log\left(2m \log \frac{m}{3/2}\right) \leqslant \log n + \log(\log n) + \log 2 + \frac{1}{n}.$$

After exponentiation, this rewrites as

$$2m \log \frac{m}{3/2} \leqslant 2n \log n \cdot e^{1/n}. \tag{52}$$

Upon division by 2, this rewrites as

$$m \log \frac{m}{3/2} \leqslant n \log n \cdot e^{1/n}. \tag{53}$$

However, since Lemma 15.3 **(a)** yields $\log \hat{A}\frac{m}{n} \leqslant \frac{1}{n}$ and because $\log \frac{3}{2} \geqslant \frac{1}{3}$,

$$\log \frac{m}{3/2} = \log\left(n \cdot \frac{m}{n} \Big/ \frac{3}{2}\right) = \log n + \log \frac{m}{n} - \log \frac{3}{2} \leqslant \log n + \frac{1}{n} - \frac{1}{3},$$

so that

$$\begin{aligned}
m \log \frac{m}{3/2} &\leqslant m\left(\log n + \frac{1}{n} - \frac{1}{3}\right) = (n+1)\left(\log n + \frac{1}{n} - \frac{1}{3}\right) \\
&= (n+1) + \frac{n+1}{n} - \frac{n+1}{3} \\
&< n \log n + \log n + \frac{\log n}{2n} \qquad \text{(by Lemma 15.5)} \\
&= n \log n \cdot \left(1 + \frac{1}{n} + \frac{1}{2n^2}\right) \leqslant n \log n \cdot e^{1/n}
\end{aligned}$$

(since $1 + \frac{1}{n} + \frac{1}{2n^2} = \sum_{k=0}^{2} \frac{1}{k!}\left(\frac{1}{n}\right)^k \leqslant \sum_{k=0}^{\infty} \frac{1}{k!}\left(\frac{1}{n}\right)^k = e^{1/n}$). This proves (53). 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 $n \geqslant 2$. The expected number of steps to get to the strong stationary time for the random-to-below shuffle satisfies the following lower bound:*

$$\mathbb{E}(\tau) = \sum_{i=2}^{n} \frac{n}{i\,(H_n - H_{i-1})} \geqslant n \log n + n \log(\log n)\,.$$

*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 $\tau$ for the one-sided cycle shuffles. Our stopping time $\tau$ 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 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 $\mathfrak{gl}(\mathbf{k}[S_n])$ 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 $[t_i, t_j] := t_i t_j - t_j t_i$ satisfy $[t_i, t_j]^2 = 0$ whenever $n \leqslant 5$ (but not when $n = 6$ and $i = 1$ and $j = 3$). This can be generalized as follows:

Theorem 16.1. *We have $[t_i, t_j]^{j-i+1} = 0$ for any $1 \leqslant i < j \leqslant n$.*

Theorem 16.2. *We have $[t_i, t_j]^{\lceil (n-j)/2 \rceil + 1} = 0$ for any $1 \leqslant i < j \leqslant n$.*

Both of these theorems are proved in the preprint [16]. 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 [16]:

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 $m \geqslant j - k_m + 1$. Then,*

$$[t_{k_1}, t_j]\,[t_{k_2}, t_j] \cdots [t_{k_m}, t_j] = 0.$$

Theorem 16.4. *Let $j \in [n]$ and $m \in \mathbb{N}$ be such that $2m \geqslant n - j + 2$. Let $i_1, i_2, \ldots, i_m$ be $m$ elements of $[j]$ (not necessarily distinct). Then,*

$$[t_{i_1}, t_j]\,[t_{i_2}, t_j] \cdots [t_{i_m}, t_j] = 0.$$

The following identities are proved in [16] 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* $(1 + s_j)[t_i, t_j] = 0$ *for any* $1 \leqslant i < j \leqslant n$.

Proposition 16.7. *We have* $t_{n-1}[t_i, t_{n-1}] = 0$ *for any* $1 \leqslant i \leqslant n$.

Proposition 16.8. *We have* $[t_i, t_j] = [s_i s_{i+1} \cdots s_{j-1}, t_j] t_j$ *for any* $1 \leqslant i < j \leqslant n$.

Proposition 16.9. *We have* $t_{i+1} t_i = (t_i - 1) t_i$ *for any* $1 \leqslant i < n$.

Proposition 16.10. *We have* $t_{i+2}(t_i - 1) = (t_i - 1)(t_{i+1} - 1)$ *for any* $1 \leqslant i < n - 1$.

16.2. Open questions. The above results (particularly Propositions 16.9 and 16.10) might suggest that the **k**-subalgebra $\mathbf{k}[t_1, t_2, \ldots, t_n]$ of $\mathbf{k}[S_n]$ 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* **k** *to be a field.) What is its dimension (as a* **k***-vector space)?*

Any reader acquainted with the standard arsenal of card-shuffling will spot another peculiarity: We have not once used any result about $\mathbf{k}[S_n]$-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 $\mathbf{k}[S_n]$-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* **k** *is a field of characteristic* $0$*?*

We have been able to answer this question (see [18]), 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 [23]. 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* $t_\ell$ *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, a filtration might be easier to find. Thus, the following question is quite natural:

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?*

We have proven that the somewhere-to-below shuffles are triangularizable, as well as that they are diagonalizable for a sufficiently generic choice of coefficients. However, the coefficients of the shuffles arising naturally have a lot of structure, as exhibited in Remark 4.2 (about the unweighted one-sided cycle shuffle), Example 12.6 (about the random-to-below shuffle), and Example 12.7 (about the top-to-random shuffle). Hence, we are prompted to ask the following:

Question 16.15. *(Question* 12.8*) Can a necessary and sufficient criterion be found for the diagonalizability of a one-sided shuffle?*

*Acknowledgements.* The authors would like to thank Eran Assaf, Sarah Brauner, 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, as well as the referees for improving the paper. This work was made possible thanks to [31].

## References

[1] Marcelo Aguiar, Kathryn Nyman, and Rosa Orellana, *New results on the peak algebra*, J. Algebraic Combin. **23** (2006), no. 2, 149–188.

[2] David Aldous and Persi Diaconis, *Shuffling cards and stopping times*, Amer. Math. Monthly **93** (1986), no. 5, 333–348.

[3] Michael E. Bate, Stephen B. Connor, and Oliver Matheau-Raven, *Cutoff for a one-sided transposition shuffle*, Ann. Appl. Probab. **31** (2021), no. 4, 1746–1773.

[4] Dave Bayer and Persi Diaconis, *Trailing the dovetail shuffle to its lair*, Ann. Appl. Probab. **2** (1992), no. 2, 294–313.

[5] Pat Bidigare, Phil Hanlon, and Dan Rockmore, *A combinatorial description of the spectrum for the Tsetlin library and its generalization to hyperplane arrangements*, Duke Math. J. **99** (1999), no. 1, 135–174.

[6] Hùng Viêt Chu, *The Fibonacci sequence and Schreier-Zeckendorf sets*, J. Integer Seq. **22** (2019), no. 6, article no. 19.6.5 (12 pages).

[7] Persi Diaconis, James Allen Fill, and Jim Pitman, *Analysis of top to random shuffles*, Combin. Probab. Comput. **1** (1992), no. 2, 135–155.

[8] Persi Diaconis, C. Y. Amy Pang, and Arun Ram, *Hopf algebras and Markov chains: two examples and a theory*, J. Algebraic Combin. **39** (2014), no. 3, 527–585.

[9] Persi Diaconis and Mehrdad Shahshahani, *Generating a random permutation with random transpositions*, Z. Wahrsch. Verw. Gebiete **57** (1981), no. 2, 159–179.

[10] A. B. Dieker and F. V. Saliola, *Spectral analysis of random-to-random Markov chains*, Adv. Math. **323** (2018), 427–485.

[11] Peter Donnelly, *The heaps process, libraries, and size-biased permutations*, J. Appl. Probab. **28** (1991), no. 2, 321–335.

[12] James Allen Fill, *An exact formula for the move-to-front rule for self-organizing lists*, J. Theoret. Probab. **9** (1996), no. 1, 113–160.

[13] Darij Grinberg, *Answers to "Is this sum of cycles invertible in $\mathbb{Q}S_n$?"*, 2018, `https://mathoverflow.net/questions/308536/`, MathOverflow thread #308536.

[14] ———, *The Elser nuclei sum revisited*, Discrete Math. Theor. Comput. Sci. **23** (2021), no. 1, article no. 15 (25 pages).

[15] ———, *Enumerative Combinatorics*, 2022, `http://www.cip.ifi.lmu.de/~grinberg/t/19fco/n/n.pdf`, unpublished notes.

[16] ———, *Commutator nilpotency for somewhere-to-below shuffles*, 2023, `https://arxiv.org/abs/2309.05340`.

[17] Darij Grinberg and Nadia Lafrenière, *The one-sided cycle shuffles in the symmetric group algebra*, 2022, https://arxiv.org/abs/2212.06274.

[18] ———, *The somewhere-to-below shuffles in the symmetric group and Hecke algebras*, 2023, extended abstract accepted in the FPSAC 2024 conference.

[19] W. J. Hendricks, *The stationary distribution of an interesting Markov chain*, J. Appl. Probability **9** (1972), 231–233.

[20] Kenneth Hoffman and Ray Kunze, *Linear algebra*, second ed., Prentice-Hall, Inc., Englewood Cliffs, NJ, 1971.

[21] Nadia Lafrenière, *Valeurs propres des opérateurs de mélange symétrisés*, Phd thesis, Université du Québec à Montréal, 2019, https://arxiv.org/abs/1912.07718, pp. xvi+160.

[22] David A. Levin, Yuval Peres, and Elizabeth L Wilmer, *Markov chains and mixing times*, second ed., American Mathematical Society, Providence, RI, 2017.

[23] Andrew Mathas, *Iwahori-Hecke algebras and Schur algebras of the symmetric group*, University Lecture Series, vol. 15, American Mathematical Society, Providence, RI, 1999.

[24] Catherine Meusburger, *Hopf Algebras and Representation Theory of Hopf Algebras*, 2021, https://en.www.math.fau.de/lie-groups/scientific-staff/prof-dr-catherine-meusburger/teaching/lecture-notes/, unpublished lecture notes.

[25] Evita Nestoridi and Kenny Peng, *Mixing times of one-sided $k$-transposition shuffles*, 2021, https://arxiv.org/abs/2112.05085.

[26] Christian Palmes, *Top-to-Random-Shuffles*, diploma thesis, Westfälische Wilhelms-Universität Münster, 2010, pp. ii+110, https://www.uni-muenster.de/stochastik/alsmeyer/diplomarbeiten/palmes.pdf.

[27] C. Y. Amy Pang, *The eigenvalues of hyperoctahedral descent operators and applications to card-shuffling*, Electron. J. Combin. **29** (2022), no. 1, article no. 1.32 (50 pages).

[28] R. M. Phatarfod, *On the matrix occurring in a linear search problem*, J. Appl. Probab. **28** (1991), no. 2, 336–346.

[29] Victor Reiner, Franco Saliola, and Volkmar Welker, *Spectra of symmetrized shuffling operators*, Mem. Amer. Math. Soc. **228** (2014), no. 1072, vi+109.

[30] Jeremy Francis Reizenstein, *Iterated-Integral Signatures in Machine Learning*, Phd thesis, University of Warwick, 2019, http://wrap.warwick.ac.uk/131162/, pp. ix+107.

[31] The Sagemath developers, *SageMath, (Version 9.4)*, 2022, https://www.sagemath.org.

Darij Grinberg, Drexel University, Korman Center, 15 S 33rd Street, Office #263, Philadelphia, PA 19104 (USA)
*E-mail :* darijgrinberg@gmail.com
*Url :* http://www.cip.ifi.lmu.de/~grinberg/

Nadia Lafrenière, Concordia University, J.W. McConnell Building (LB), 1400 De Maisonneuve Blvd. W., Montreal, QC H3G 1M8 (Canada)
*E-mail :* nadia.lafreniere@concordia.ca
*Url :* https://nadialafreniere.github.io/