Séminaire Lotharingien de Combinatoire **91B** (2024)
Article #16, 12 pp.

Proceedings of the 36th Conference on Formal Power Series and Algebraic Combinatorics (Bochum)

The somewhere-to-below shuffles in the symmetric group and Hecke algebras

Darij Grinberg[*1] and Nadia Lafrenière[†2]

[1]*Mathematics Department, Drexel University, Philadelphia, PA, USA*
[2]*Department of Mathematics & Statistics, Concordia University, Montreal, QC, Canada*

Abstract. We introduce and study the *somewhere-to-below shuffles*, which are elements of the group algebra of the symmetric group S_n defined as sums of cycles. We show that these elements are simultaneously triangularizable (in an easily-defined basis of $\mathbf{k}[S_n]$), and compute their joint eigenvalues with multiplicities. We furthermore discuss some identities between them, a card shuffling interpretation and its probabilistic properties, and a possible generalization to the Hecke algebra.

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

1 Introduction

The group algebra $\mathbf{k}[S_n]$ of the symmetric group S_n is one of the most elementary, yet richest examples of an algebra in combinatorics. Over a characteristic-zero field, it is known (by the representation theory of the symmetric group) to be isomorphic to a direct product of matrix rings, a viewpoint that clarifies some of its features while obscuring others. The structure of $\mathbf{k}[S_n]$ becomes more interesting when $\mathbf{k}$ is less well-behaved (e.g., the ring $\mathbb{Z}$), but also when combinatorics is invited back onto the stage.

The latter can be done by defining a simple-looking family of elements of $\mathbf{k}[S_n]$ combinatorially and asking algebraic questions: Do its elements commute? Do they have integer eigenvalues (viewed as endomorphisms of $\mathbf{k}[S_n]$ by left multiplication)? What subalgebra do they generate? Such families often come with a rich provenance. Examples are the Young–Jucys–Murphy elements (originating from representation theory), the Eulerian idempotents (born in homological algebra) and the more recent Wronski–Purbhoo elements (inspired by mathematical physics).

A wide class of recent examples has come from probability theory, the most elementary example being perhaps the *top-to-random shuffle*

$$t_1 := \mathrm{cyc}_1 + \mathrm{cyc}_{1,2} + \mathrm{cyc}_{1,2,3} + \cdots + \mathrm{cyc}_{1,2,\ldots,n} \in \mathbf{k}[S_n],$$

*darijgrinberg@gmail.com
†nadia.lafreniere@concordia.ca

where $\mathrm{cyc}_{i_1,i_2,\ldots,i_m}$ denotes the m-cycle sending $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_m \mapsto i_1$. After this shuffle was fully analyzed in 1986 [6], several generalizations and extensions have come up and are still undergoing active research.

The work outlined in this abstract, and detailed in our papers [4] and [3] (and forthcoming work), concerns the perhaps simplest way to generalize the top-to-random shuffle: namely, by embedding it in the n-tuple $(t_1, t_2, \ldots, t_n)$ of the *somewhere-to-below shuffles*

$$t_i := \mathrm{cyc}_i + \mathrm{cyc}_{i,i+1} + \mathrm{cyc}_{i,i+1,i+2} + \cdots + \mathrm{cyc}_{i,i+1,\ldots,n} \in \mathbf{k}\left[S_n\right]$$

for all $i \in \{1, 2, \ldots, n\}$. These n shuffles have a simple probabilistic meaning (shuffling a deck of cards by picking the i-th card from the top and randomly moving it further down the deck), and are also related to the insertion sort algorithm and to subgroups (each t_i is a sum of coset representatives for a certain S_{n-i} subgroup inside S_{n-i+1}).

The somewhere-to-below shuffles $t_1, t_2, \ldots, t_n$ do not commute, but they "commute up to nilpotent error terms". In rigorous language, this means that there exists a basis $(a_1, a_2, \ldots, a_{n!})$ of the $\mathbf{k}$-module $\mathbf{k}\left[S_n\right]$ on which these elements act from the right as upper-triangular matrices (i.e., we have $a_k t_\ell \in \operatorname{span}(a_1, a_2, \ldots, a_k)$ for each k). This basis can be constructed explicitly over any ring $\mathbf{k}$, in contrast to the more classical diagonalizing bases that exist for various other known families but only over characteristic-0 fields. (A common diagonalizing basis is impossible for the $t_1, t_2, \ldots, t_n$, since some of their linear combinations fail to act semisimply.) A more conceptual but less catchy formulation of our main result is the existence of a filtration

$$0 = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}} = \mathbf{k}\left[S_n\right]$$

of the $\mathbf{k}$-module $\mathbf{k}\left[S_n\right]$ that is preserved by the somewhere-to-below shuffles $t_1, t_2, \ldots, t_n$ (acting from the right), and on whose quotients F_i/F_{i-1} these shuffles act as scalars. The length of this filtration is (rather unexpectedly) the $(n+1)$-st *Fibonacci number* f_{n+1}.

A consequence of all this is that each linear combination $\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n$ of the somewhere-to-below shuffles has explicitly computable eigenvalues, which are all integers if the coefficients $\lambda_1, \lambda_2, \ldots, \lambda_n$ are, and of which at most f_{n+1} are distinct. Their multiplicities (in the generic case) are certain divisors of $n!$, counting some kinds of permutations. We give the constructions and say a few words on the proofs below; details can be found in [4]. Some variants of these results (replacing right by left multiplication, and replacing the $t_1, t_2, \ldots, t_n$ by their "antipodes") are briefly outlined in Section 8.

The filtration above explains much but not everything. In particular, it shows that the commutators $\left[t_i, t_j\right]$ are nilpotent, but gives fairly bad (exponential) bounds on their nilpotency degrees. The actual nilpotency degrees, however, are much smaller (in fact, no larger than $n/2+1$). This is elaborated upon in Section 9, but the detailed proofs are too long to even hint at; they can be found in [3].

The motivation for studying the somewhere-to-below shuffles comes largely from probability theory. Card shuffling can be thought of applying a permutation at random, according to some probability, to a deck of cards. For us, it means acting on the right by an element of $\mathbf{k}[S_n]$ whose coefficients are nonnegative reals. A question of interest is thus, given the choice of an element of $\mathbf{k}[S_n]$, how many applications of it would suffice to shuffle the deck of cards properly. In Section 10, we give an optimal strong stationary time for linear combinations of the somewhere-to-below shuffles.

Anything about $\mathbf{k}[S_n]$ is, of course, connected to integer partitions and Young diagrams, since the irreducible representations of $\mathbf{k}[S_n]$ are the *Specht modules* S^λ assigned to the partitions λ of n. Thus, one can wonder how the somewhere-to-below shuffles $t_1, t_2, \ldots, t_n$ act on a given Specht module S^λ. We answer this in Section 11; the proof will appear in forthcoming work.

In the last Section 12, we suggest a further potential generalization, replacing the symmetric group algebra $\mathbf{k}[S_n]$ by the Hecke algebra $\mathcal{H}_n(q)$. We have only just began the study of this setting, but it appears that many of our results extend to it. Research on this, as well as on our Specht module conjecture, is underway.

2 Definitions

2.1 Combinatorics

Let us first introduce some basic notations (more will be defined as needed). We set $\mathbb{N} := \{0, 1, 2, \ldots\}$. Furthermore, we set $[a, b] := \{x \in \mathbb{Z} \mid a \leq x \leq b\}$ for any $a, b \in \mathbb{Z}$. For any $k \in \mathbb{Z}$, we set $[k] := [1, k] = \{1, 2, \ldots, k\}$.

We fix a positive integer n. We let S_n denote the n-th symmetric group; it consists of the $n!$ permutations of $[n]$, with multiplication given by composition: $(\alpha\beta)(i) = \alpha(\beta(i))$ for each $\alpha, \beta \in S_n$ and $i \in [n]$.

2.2 Algebra

We fix a commutative ring $\mathbf{k}$. (The cases $\mathbf{k} = \mathbb{Z}$ and $\mathbf{k} = \mathbb{Q}$ are fully sufficient.)

We let $\mathbf{k}[S_n]$ denote the group algebra of S_n over $\mathbf{k}$. This $\mathbf{k}$-algebra consists of all formal $\mathbf{k}$-linear combinations $\sum_{\sigma \in S_n} \lambda_\sigma \sigma$ of the permutations $\sigma \in S_n$, and its multiplication is the $\mathbf{k}$-linear extension of the multiplication on S_n. Its unity is $1 = \mathrm{id}_{[n]} \in S_n$.

For each $u \in \mathbf{k}[S_n]$, we define the two $\mathbf{k}$-linear maps $L(u) : \mathbf{k}[S_n] \to \mathbf{k}[S_n]$ and $R(u) : \mathbf{k}[S_n] \to \mathbf{k}[S_n]$ by

$$(L(u))(a) = ua \qquad \text{and} \qquad (R(u))(a) = au \qquad \text{for each } a \in \mathbf{k}[S_n].$$

These are just the left multiplication and the right multiplication by u. Being endomorphisms of the $\mathbf{k}$-module $\mathbf{k}[S_n]$, they can be represented as $n! \times n!$-matrices over $\mathbf{k}$ (since $\mathbf{k}[S_n]$ is a free $\mathbf{k}$-module of rank $n!$, with basis $(w)_{w \in S_n}$), and thus have characteristic polynomials, eigenvalues and eigenvectors (at least when $\mathbf{k}$ is a field).

2.3 Cycles, somewhere-to-below and other random-to-below shuffles

For any distinct elements $i_1, i_2, \ldots, i_k$ of $[n]$, we let $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ be the permutation in S_n that cyclically permutes $i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_k \mapsto i_1$ and leaves all other elements of $[n]$ unchanged. In particular, $\operatorname{cyc}_{i,j}$ is a transposition, while $\operatorname{cyc}_i = \operatorname{id} = 1$.

We are now ready for our main definition: For each $\ell \in [n]$, we define the element

$$t_\ell := \operatorname{cyc}_\ell + \operatorname{cyc}_{\ell,\ell+1} + \operatorname{cyc}_{\ell,\ell+1,\ell+2} + \cdots + \operatorname{cyc}_{\ell,\ell+1,\ldots,n} \in \mathbf{k}\left[S_n\right].$$

These n elements $t_1, t_2, \ldots, t_n$ will be called the *somewhere-to-below shuffles*. The first of these elements, t_1, is also known as the *top-to-random shuffle* or the *Tsetlin library*, whereas the last is just the identity ($t_n = \operatorname{cyc}_n = 1$).

Linear combinations of the somewhere-to-below shuffles are also interesting. Assuming the coefficients $\lambda_1, \lambda_2, \ldots, \lambda_n$ are nonnegative reals, $\lambda_1 t_1 + \lambda_2 t_2 + \ldots + \lambda_n t_n$ represents the action of choosing the i-th somewhere-to-below shuffle with some probability dictated by λ_i. In particular, the *random-to-below shuffle* is the shuffle in which we pick i with uniform probability (among $[n]$), and then apply the i-th somewhere-to-below shuffle. In terms of card shuffling, this amounts to drawing a card (uniformly) at random and moving it weakly below. See [4, §3] for other interesting shuffles of this sort.

3 The descent-destroying basis

The n somewhere-to-below shuffles do not commute (e.g., we have $t_1 t_2 \neq t_2 t_1$ for $n = 3$). Nevertheless, they behave far better than a "random" family of elements of $\mathbf{k}\left[S_n\right]$. In particular, there exists a basis of the $\mathbf{k}$-module $\mathbf{k}\left[S_n\right]$ in which all of the endomorphisms $R\left(t_1\right), R\left(t_2\right), \ldots, R\left(t_n\right)$ are represented by upper-triangular matrices. We shall construct this basis now. This requires some more definitions.

For each $w \in S_n$, we define the *descent set* of w to be the set

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

For each $i \in [n-1]$, we define the *simple transposition* $s_i := \operatorname{cyc}_{i,i+1} \in S_n$.

For each $I \subseteq [n-1]$, we define the *Young subgroup* $G(I)$ to be the subgroup of S_n generated by the s_i for $i \in I$. This can be viewed as a product $S_{n_1} \times S_{n_2} \times \cdots \times S_{n_k}$ with $n_1 + n_2 + \cdots + n_k = n$, embedded into S_n via the canonical homomorphism.

For each $w \in S_n$, we define

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

The following is easy to see by triangularity:

Proposition 1. *The family $\left(a_w\right)_{w \in S_n}$ is a basis of the $\mathbf{k}$-module $\mathbf{k}\left[S_n\right]$.*

Example 1. *For $n = 3$, we have*

$$
\begin{array}{ll|ll}
a_{[123]} &= [123]\,; & a_{[231]} &= [231] + [213]\,; \\
a_{[132]} &= [132] + [123]\,; & a_{[312]} &= [312] + [132]\,; \\
a_{[213]} &= [213] + [123]\,; & a_{[321]} &= [321] + [312] + [231] + [213] + [132] + [123]
\end{array}
$$

(where we use one-line notation for permutations: $[i_1 i_2 \cdots i_n]$ means the permutation of $[n]$ that sends $1, 2, \ldots, n$ to $i_1, i_2, \ldots, i_n$).

Now, we claim that the endomorphisms $R(t_1), R(t_2), \ldots, R(t_n)$ are upper-triangular with respect to this basis (appropriately ordered). More concretely:

Theorem 1. *There is some partial order $\prec$ on S_n such that for any $w \in S_n$ and $\ell \in [n]$, we have*

$$a_w t_\ell = \mu_{w,\ell} a_w + \sum_{\substack{v \in S_n; \\ v \prec w}} \lambda_{w,\ell,v} a_v \qquad \text{for some } \mu_{w,\ell} \in \mathbb{N} \text{ and } \lambda_{w,\ell,v} \in \mathbb{Z}.$$

Example 2. *For $n = 4$, we have* $a_{[4312]} t_2 = a_{[4312]} + \underbrace{a_{[4321]} - a_{[4231]} - a_{[3241]} - a_{[2143]}}_{\text{subscripts are } \prec [4312]}.$

4 The invariant spaces $F(I)$

To prove Theorem 1 directly, we would need to understand how $R(t_\ell)$ acts on each single a_w. But this is not easy. Thus, we shall instead analyze the action of $R(t_\ell)$ on a certain filtration $0 = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}} = \mathbf{k}[S_n]$ of $\mathbf{k}[S_n]$ by left ideals (which are preserved by the $R(t_\ell)$). The basis $(a_w)_{w \in S_n}$ will then reveal itself to be compatible with this filtration (i.e., each F_i is spanned by some subfamily of this basis), and thus we will be able to draw conclusions about $a_w t_\ell$ from the action of $R(t_\ell)$ on the filtration. Essentially, the filtration will act as a "middleman" between the t_ℓ and the a_w.

In order to construct the filtration, we shall in turn need another middleman: some left ideals $F(I)$ defined for each $I \subseteq [n]$. These are easy to define:

For each subset I of $[n]$, we define the number

$$\operatorname{sum} I := \sum_{i \in I} i,$$

and the sets

$$\widehat{I} := \{0\} \cup I \cup \{n+1\} \qquad \text{and} \qquad I' := [n-1] \setminus (I \cup (I-1))$$

(where $I - 1 := \{i - 1 \mid i \in I\}$), and finally the left ideal

$$F(I) := \left\{ u \in \mathbf{k}[S_n] \mid u s_i = u \text{ for all } i \in I' \right\} \subseteq \mathbf{k}[S_n]$$

(the "*invariant space*" corresponding to I).

Example 3. *Let $n = 9$ and $I = \{2,3,7\}$. Then, $\widehat{I} = \{0,2,3,7,10\}$ and $I' = [8] \setminus \{1,2,3,6,7\} = \{4,5,8\}$ and $F(I) = \{u \in \mathbf{k}[S_n] \mid us_4 = us_5 = us_8 = u\}$.*

The following is easy to see:

Proposition 2. *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 $F(I)$.*

The main workhorse of our study of the somewhere-to-below shuffles is a lemma which, for each $I \subseteq [n]$ and $\ell \in [n]$ and $u \in F(I)$, expresses the product ut_ℓ as a scalar multiple of u plus a sum of "error terms" in "smaller" invariant spaces $F(J)$ (to be precise: invariant spaces $F(J)$ for subsets $J \subseteq [n]$ satisfying $\operatorname{sum} J < \operatorname{sum} I$). We can actually be more specific and characterize the scalar in front of the u as follows:

For any $\ell \in [n]$, we let $m_{I,\ell}$ be the distance from ℓ to the next-higher element of $\widehat{I}$. In other words,

$$m_{I,\ell} := \left(\text{smallest element of } \widehat{I} \text{ that is } \geq \ell\right) - \ell \in \{0,1,\ldots,n\}.$$

Example 4. *If $n = 9$ and $I = \{2,3,7\}$, then $\widehat{I} = \{0,2,3,7,10\}$ and*

$$(m_{I,1},\ m_{I,2},\ \ldots,\ m_{I,9}) = (1,0,0,3,2,1,0,2,1).$$

Lemma 1 (Workhorse lemma)**.** *Let $I \subseteq [n]$ and $\ell \in [n]$. Then,*

$$ut_\ell \in m_{I,\ell} u + \sum_{\substack{J \subseteq [n]; \\ \operatorname{sum} J < \operatorname{sum} I}} F(J) \qquad \text{for each } u \in F(I).$$

Proof idea. Expand ut_ℓ by the definition of t_ℓ, and break up the resulting sum into smaller bunches using the interval decomposition

$$[\ell, n] = [\ell, i_k - 1] \sqcup [i_k, i_{k+1} - 1] \sqcup [i_{k+1}, i_{k+2} - 1] \sqcup \cdots \sqcup [i_p, n]$$

(where $i_k < i_{k+1} < \cdots < i_p$ are the elements of I larger or equal to ℓ). The $[\ell, i_k - 1]$ bunch gives the $m_{I,\ell} u$ term; the others live in appropriate $F(J)$'s. See [4, Theorem 7.3] for details. □

5 The Fibonacci filtration

The filtration $0 = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}} = \mathbf{k}[S_n]$ that we want to construct will consist of sums of certain invariant spaces $F(I)$. However, we do not need all $F(I)$, but only the ones that correspond to certain subsets I: namely, those that are *lacunar* (i.e., contain no two consecutive integers) and do not contain n. Arranging these lacunar subsets I in order of increasing sum, we will define F_i as the sum of the $F(I)$ corresponding to the first i many I's.

Let us elaborate on this. A set S of integers is called *lacunar* if it contains no two consecutive integers (i.e., we have $s+1 \notin S$ for all $s \in S$). The number of lacunar subsets of $[n-1]$ is known to be the Fibonacci number f_{n+1}. (Recall that the Fibonacci numbers $f_0, f_1, f_2, \ldots$ are defined by $f_0 = 0$ and $f_1 = 1$ and $f_k = f_{k-1} + f_{k-2}$ for each $k \geq 2$.)

The following lemma (essentially [4, Proposition 8.7]) is easy to check:

Lemma 2. *Let $J \subseteq [n]$ be a subset that fails to be lacunar or contains n. Then, there exists some subset $K \subseteq [n]$ such that $\operatorname{sum} K < \operatorname{sum} J$ and $K' \subseteq J'$ (so that $F(J) \subseteq F(K)$).*

Now, we let $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ be the f_{n+1} lacunar subsets of $[n-1]$, listed in such an order that $\operatorname{sum}(Q_1) \leq \operatorname{sum}(Q_2) \leq \cdots \leq \operatorname{sum}\left(Q_{f_{n+1}}\right)$. (We fix such an order once and for all.) Then, for each $i \in [0, f_{n+1}]$, define a left ideal

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

(so that $F_0 = 0$). The resulting filtration

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

satisfies the following crucial property:

Theorem 2. *For each $i \in [f_{n+1}]$ and $\ell \in [n]$, we have $F_i \cdot \left(t_\ell - m_{Q_i,\ell}\right) \subseteq F_{i-1}$ (so that $R(t_\ell)$ preserves F_i and F_{i-1}, and acts as multiplication by $m_{Q_i,\ell}$ on F_i / F_{i-1}).*

Proof idea. This follows from Lemmas 1 and 2. See [4, Theorem 8.1 **(c)**] for details. □

Now we claim that our basis $(a_w)_{w \in S_n}$ of $\mathbf{k}[S_n]$ respects the filtration $0 = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{f_{n+1}} = \mathbf{k}[S_n]$. To make this precise, we introduce some more notation:

The *Q-index* $\operatorname{Qind} w$ of a permutation $w \in S_n$ is defined to be the **smallest** $i \in [f_{n+1}]$ such that $Q_i' \subseteq \operatorname{Des} w$. (Note that this depends on our ordering of $Q_1, Q_2, \ldots, Q_{f_{n+1}}$.)

The following facts ([4, §10]) are not hard to see:

Proposition 3. *Let $w \in S_n$ and $i \in [f_{n+1}]$. Then, $\operatorname{Qind} w = i$ if and only if $Q_i' \subseteq \operatorname{Des} w \subseteq [n-1] \setminus Q_i$.*

Theorem 3. *For each $i \in [0, f_{n+1}]$, the $\mathbf{k}$-module F_i is free with basis $(a_w)_{w \in S_n;\ \operatorname{Qind} w \leq i}$.*

Corollary 1. *For each $i \in [f_{n+1}]$, the $\mathbf{k}$-module F_i / F_{i-1} is free with basis $\left(\overline{a_w}\right)_{w \in S_n;\ \operatorname{Qind} w = i}$.*

6 Triangularizability

Combining Theorem 3 with Theorem 2, we easily obtain the following concretization of Theorem 1 ([4, Theorem 11.1]):

Theorem 4. *Let $w \in S_n$ and $\ell \in [n]$. Let $i = \operatorname{Qind} w$. Then,*

$$a_w t_\ell = m_{Q_i,\ell} a_w + \sum_{\substack{v \in S_n; \\ \operatorname{Qind} v < \operatorname{Qind} w}} \lambda_{w,\ell,v} a_v \qquad \text{for some integers } \lambda_{w,\ell,v}.$$

Thus, the endomorphisms $R(t_1), R(t_2), \ldots, R(t_n)$ are upper-triangular with respect to the basis $(a_w)_{w \in S_n}$, as long as the permutations $w \in S_n$ are ordered by increasing Q-index. Their diagonal entries are the numbers $m_{Q_{\operatorname{Qind} w},\ell} \in \mathbb{N}$.

Therefore, any $\mathbf{k}$-linear combination $R\left(\sum_{\ell=1}^{n} \lambda_\ell t_\ell\right) = \sum_{\ell=1}^{n} \lambda_\ell R(t_\ell)$ of these endomorphisms $R(t_1), R(t_2), \ldots, R(t_n)$ (with $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$) is upper-triangular with respect to this basis as well, and its diagonal entries will be the appropriate $\mathbf{k}$-linear combinations $\sum_{\ell=1}^{n} \lambda_\ell m_{Q_{\operatorname{Qind} w},\ell}$. Hence, regarded as an $n! \times n!$-matrix, $R\left(\sum_{\ell=1}^{n} \lambda_\ell t_\ell\right)$ is triangularizable with eigenvalues $\sum_{\ell=1}^{n} \lambda_\ell m_{Q_{\operatorname{Qind} w},\ell}$ for $w \in S_n$.

This matrix is not always diagonalizable. A sufficient (but far from necessary) criterion can nevertheless be given:

Theorem 5. *Let $\mathbf{k}$ be a field, and let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Then, the eigenvalues of the operator $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ are the linear combinations*

$$\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n} \qquad \text{for } I \subseteq [n-1] \text{ lacunar}$$

(with multiplicities discussed below). If all these f_{n+1} linear combinations are distinct, then $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is diagonalizable.

Proof idea. The first claim follows from the discussion above; the second uses Theorem 2 and some linear algebra. See [4, Corollary 12.2 and Theorem 12.3] for details. □

7 Multiplicities of the eigenvalues

We can also describe the multiplicities of the eigenvalues of $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ ([4, Theorem 13.2]):

Theorem 6. *Assume that $\mathbf{k}$ is a field. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. For each $i \in [f_{n+1}]$, let δ_i be the number of all permutations $w \in S_n$ satisfying $\operatorname{Qind} w = i$, and let*

$$g_i := \sum_{\ell=1}^{n} \lambda_\ell m_{Q_i,\ell} \in \mathbf{k}.$$

Let $\kappa \in \mathbf{k}$. Then, the algebraic multiplicity of κ as an eigenvalue of $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ equals the sum of the δ_i over all $i \in [f_{n+1}]$ satisfying $g_i = \kappa$.

Furthermore, these δ_i can be expressed by an explicit formula (similar to but simpler than the famous hook-length formula), and are divisors of $n!$ (just like in the hook-length formula); we refer to [4, Theorem 13.1] for details.

8 Variants

So far, we have directed our attention at the right multiplication maps $R(t_1), R(t_2), \ldots, R(t_n)$, while neglecting their left counterparts $L(t_1), L(t_2), \ldots, L(t_n)$. However, almost all our claims about the former can be extended to the latter using general properties of group algebras. In particular, there exists a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$ in which all of the endomorphisms $L(t_1), L(t_2), \ldots, L(t_n)$ are represented by upper-triangular matrices. This basis is not the basis $(a_w)_{w \in S_n}$, but rather its dual basis with respect to a certain bilinear form (and its order is modified). Theorems 5 and 6 remain valid if "R" is replaced by "L" throughout them. For the proofs of all these claims, we refer to [4, §14]; all we shall say here is that they are derived from the analogous properties of R purely algebraically, with no further combinatorial input.

It is also natural to study the *below-to-somewhere shuffles* $t'_1, t'_2, \ldots, t'_n$, where

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

for each $\ell \in [n]$. Again, Theorems 5 and 6 remain valid if each t_ℓ is replaced by the corresponding t'_ℓ; but this is again not too surprising, since the t'_ℓ are the images of t_ℓ under a very simple $\mathbf{k}$-algebra anti-automorphism of $\mathbf{k}[S_n]$ called the *antipode* (sending each permutation $w \in S_n$ to its inverse w^{-1}). Thus, again, most properties can be transferred between the t_ℓ and the t'_ℓ by purely algebraic tools (see [4, §14] for details).

9 Nilpotent commutators

Since the endomorphisms $R(t_1), R(t_2), \ldots, R(t_n)$ are simultaneously triangularizable, their pairwise commutators are nilpotent. Hence, the pairwise commutators $[t_i, t_j]$ in $\mathbf{k}[S_n]$ are also nilpotent. A natural question is: How small is the required exponent?

As it turns out, it is much smaller than one might expect:

Theorem 7. *Let $1 \leq i \leq j \leq n$. Then,*

$$[t_i, t_j]^m = 0 \qquad \textit{holds for } m = \min\{j - i + 1,\ \lceil (n-j)/2 \rceil + 1\}.$$

We conjecture (and have verified for all $n \leq 12$) that this choice of m is optimal (i.e., that $[t_i, t_j]^{m-1} \neq 0$, at least for $\mathbf{k} = \mathbb{Z}$).

Actually, Theorem 7 can be generalized, replacing the m-th power of a single $[t_i, t_j]$ by a product of several $[t_i, t_j]$'s (with the same j but possibly different i's). The reader can find this generalization in [3, Theorems 8.15 and 9.10], where it is proved by long and tricky but completely elementary manipulations of permutations and sums.

Several other curious facts hold, such as the following ([3, Theorems 5.1 and 6.1, Corollaries 7.6 and 8.20]):

Proposition 4. *If $i \in [n-1]$, then $t_{i+1}t_i = (t_i - 1)\, t_i$.*
If $i \in [n-2]$, then $t_{i+2}\,(t_i - 1) = (t_i - 1)\,(t_{i+1} - 1)$.

Proposition 5. *Let $i, j \in [n]$. Then, $t_{n-1}\,[t_i, t_{n-1}] = 0$ and $[t_i, t_{n-1}]\,[t_j, t_{n-1}] = 0$.*

These facts suggest that the $\mathbf{k}$-subalgebra $\mathbf{k}\,[t_1, t_2, \ldots, t_n]$ of $\mathbf{k}\,[S_n]$ has some interesting structure (apart from the "split-semisimple-by-nilpotent" decomposition following from Theorem 1). Yet it remains mysterious in many ways. For $\mathbf{k} = \mathbb{Q}$ and $n \in [8]$, here is its dimension as a $\mathbb{Q}$-vector space (the sequence is not in the OEIS as of 2023-11-07!):

n	1	2	3	4	5	6	7	8
$\dim(\mathbb{Q}\,[t_1, t_2, \ldots, t_n])$	1	2	4	9	23	66	212	761

. (9.1)

10 Probability theory

We shall now make a few comments on the probabilistic side of the one-sided cycle shuffles. Viewing them as shuffling operators, we are interested in the number of iterations needed to get a well-mixed deck of cards. We describe a strong stationary time for all one-sided cycle shuffles (see [4, §10]), imitating a similar result for the top-to-random shuffle ([1]). Once the strong stationary time is reached, the deck is perfectly mixed.

Theorem 8. *If $\lambda_1 \neq 0$, then the one-sided cycle shuffle $\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n$ admits a stopping time τ obtained as follows: Place a bookmark right above the bottommost card of the deck. The bookmark itself does not move (but cards can move down past it). We let τ be the time it takes for the bookmark to reach the top of the deck.*

The distribution of the deck is uniform at time τ and any time afterwards; i.e., τ is a strong stationary time. Furthermore, this stopping time is optimal.

If $\lambda_1 = 0$, then the top card never moves, so the deck will never be uniformly mixed.

For the random-to-below shuffle, we can compute the waiting time explicitly:

Theorem 9. *Let H_n be the n-th harmonic number. The expected number of steps to get to the strong stationary time for the random-to-below shuffle is*

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

We conjecture that the strong stationary time for the random-to-below shuffle satisfies $\mathbb{E}(\tau) = n\,(\log n + \log(\log n) + O(1))$, which makes the random-to-below shuffle slower than top-to-random, for which the strong stationary time approaches $n \log n$ ([1]).

11 Representation theory

Recall the maps $L(u)$ and $R(u)$ defined in Subsection 2.2 for any $u \in \mathbf{k}[S_n]$. Any representation theorist will recognize them as the actions of u on the left and the right regular representation of S_n. Similar maps can be defined for any other representation of S_n. It thus is natural to ask about analogues of Theorems 5 and 6 for arbitrary representations. We shall briefly summarize the answer (yet unpublished).

In this section, we assume that $\mathbf{k}$ is a field of characteristic 0. We shall use some basic notions from the representation theory of S_n and from symmetric functions; the reader can find all prerequisites in [2, Chapters 6 and 7]. For any partition λ of n, a Specht module S^λ is defined, which is an irreducible representation of S_n with a basis indexed by standard tableaux of shape λ. Each $u \in \mathbf{k}[S_n]$ acts (on the left) on this Specht module S^λ; we let $L_\lambda(u)$ denote this action (viewed as a $\mathbf{k}$-module endomorphism of S^λ).

We let $\mathcal{R}$ denote the representation ring of the symmetric groups (called R in [2, §7.3]), and Λ denote the ring of symmetric functions over $\mathbb{Z}$ (defined in [2, §6.2]). An isomorphism $\varphi : \Lambda \to \mathcal{R}$ (often called the *Frobenius characteristic map*) is defined in [2, §7.3], and the famous *Schur function* $s_\lambda \in \Lambda$ corresponding to a partition λ is the preimage of the Specht module S^λ under this isomorphism φ.

For each $m \in \mathbb{N}$, we let $h_m \in \Lambda$ denote the m-th complete homogeneous symmetric polynomial. For each $m > 0$, we let $z_m \in \Lambda$ denote the Schur function $s_{(m-1,1)} = h_{m-1}h_1 - h_m \in \Lambda$. (This is 0 for $m = 1$.)

For each subset I of $[n]$, we define a symmetric function $z_I := h_{i_1-1} \prod_{j=2}^{k} z_{i_j - i_{j-1}} \in \Lambda$, where $i_1, i_2, \ldots, i_k$ are the elements of $I \cup \{n+1\}$ in increasing order (so that $i_k = n+1$ and $I = \{i_1 < i_2 < \cdots < i_{k-1}\}$). When this symmetric function z_I is expanded in the basis $(s_\lambda)_{\lambda \text{ is a partition}}$ of Λ, the coefficient of a given Schur function s_λ shall be called c_λ^I. This coefficient c_λ^I is actually a Littlewood–Richardson coefficient (since z_I is a skew Schur function), hence $\in \mathbb{N}$.

We now claim the following:

Theorem 10. *Let ν be a partition. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Then, the eigenvalues of the operator $L_\nu(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ on the Specht module S^ν are the linear combinations*

$$\lambda_1 m_{I,1} + \lambda_2 m_{I,2} + \cdots + \lambda_n m_{I,n} \qquad \text{for } I \subseteq [n-1] \text{ lacunar satisfying } c_\nu^I \neq 0,$$

and their respective multiplicities are the c_ν^I in the generic case (i.e., if no two I's produce the same linear combination; otherwise the multiplicities of colliding eigenvalues should be added together). If all these linear combinations are distinct, then $L_\nu(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is diagonalizable.

Relatedly, (the isomorphism class of) the representation F_i / F_{i-1} of S_n is $\varphi(z_{Q_i})$.

12 Into the Hecke algebra

Like many objects originating in combinatorics, the symmetric group algebra $\mathbf{k}[S_n]$ has a q-deformation. This deformation is the *type-A Hecke algebra* (or *Iwahori-Hecke algebra*), defined in terms of a 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 $\mathbf{k}[S_n]$. We refer to [5] for the definition of this multiplication, and much more about $\mathcal{H}$. 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 $t_1, t_2, \ldots, t_n$. In particular, the analogues of Theorems 1 and 7 in $\mathcal{H}$ (where the t_ℓ are replaced by the $t_\ell^{\mathcal{H}}$) seem to hold. Even more surprisingly perhaps, the dimensions of $\mathbb{Q}[t_1, t_2, \ldots, t_n]$ tabulated in (9.1) (at least for $n \leq 6$) appear to be the same for the $\mathcal{H}$-analogue, which suggests that all algebraic relations between the $t_1, t_2, \ldots, t_n$ are "coming from" the Hecke algebra. Attempts to prove these conjectures are underway.

Acknowledgements

We thank Eran Assaf, Sarah Brauner, Colin Defant, Persi Diaconis, Theo Douvropoulos, Maxim Kontsevich, Martin Lorenz, Oliver Matheau-Raven, Amy Pang, Karol Penson, Victor Reiner and Franco Saliola for inspiring discussions and insightful comments.

References

[1] D. Aldous and P. Diaconis. "Shuffling cards and stopping times". *American Mathematical Monthly* **93**.5 (1986), pp. 333–348. DOI.

[2] W. Fulton. *Young Tableaux*. Vol. 35. London Mathematical Society Student Texts. Cambridge University Press, 1997. DOI.

[3] D. Grinberg. "Commutator nilpotency for somewhere-to-below shuffles". 2023. arXiv:2309.05340.

[4] D. Grinberg and N. Lafrenière. "The one-sided cycle shuffles in the symmetric group algebra". 2023. arXiv:2212.06274.

[5] A. Mathas. *Iwahori-Hecke Algebras and Schur Algebras of the Symmetric Group*. Vol. 15. University Lecture Series. American Mathematical Society, 1999. Link.

[6] N. R. Wallach. "Lie Algebra Cohomology and Holomorphic Continuation of Generalized Jacquet Integrals". *Advanced Studies in Pure Mathematics 14, 1988, Representations of Lie Groups, Kyoto, Hiroshima, 1986* (1988), pp. 123–151. DOI.