The one-sided cycle shuffles in the symmetric group algebra [talk slides]

Darij Grinberg
joint work with Nadia Lafrenière

CAP 2022, 2022-11-29

Elements in the group algebra of a symmetric group S_n are known to have an interpretation in terms of card shuffling. I will discuss a new family of such elements, recently constructed by Nadia Lafrenière:

Given a positive integer n, we define n elements $t_1, t_2, \ldots, t_n$ in the group algebra of S_n by

$$t_i = \text{the sum of the cycles } (i), \ (i, i+1), \ (i, i+1, i+2), \ \ldots, \ (i, i+1, \ldots, n),$$

where the cycle (i) is the identity permutation. The first of them, t_1, is known as the top-to-random shuffle and has been studied by Diaconis, Fill, Pitman (among others).

The n elements $t_1, t_2, \ldots, t_n$ do not commute. However, we show that they can be simultaneously triangularized in an appropriate basis of the group algebra (the "descent-destroying basis"). As a consequence, any rational linear combination of these n elements has rational eigenvalues. The maximum number of possible distinct eigenvalues turns out to be the Fibonacci number f_{n+1}, and underlying this fact is a filtration of the group algebra connected to "lacunar subsets" (i.e., subsets containing no consecutive integers).

This talk will include an overview of other families (both well-known and exotic) of elements of these group algebras. I will also briefly discuss the probabilistic meaning of these elements as well as some tempting conjectures.

This is joint work with Nadia Lafrenière.

***

Preprint:

- Darij Grinberg and Nadia Lafrenière, *The one-sided cycle shuffles in the symmetric group algebra*, preprint, `https://www.cip.ifi.lmu.de/~grinberg/algebra/s2b1.pdf`

Slides of this talk:

- `https://www.cip.ifi.lmu.de/~grinberg/algebra/cap2022.pdf`

1. Finite group algebras

- This talk is mainly about a certain family of elements of the group algebra of the symmetric group S_n. But I shall begin with some generalities.

- Let $\mathbf{k}$ be any commutative ring (but $\mathbf{k} = \mathbb{Z}$ is enough for most of our results).

- Let G be a finite group. (It will be a symmetric group from the next chapter onwards.)

- Let $\mathbf{k}[G]$ be the group algebra of G over $\mathbf{k}$. Its elements are formal $\mathbf{k}$-linear combinations of elements of G. The multiplication is inherited from G and extended bilinearly.

- **Example:** Let G be the symmetric group S_3 on the set $\{1,2,3\}$. For $i \in \{1,2\}$, let $s_i \in S_3$ be the simple transposition that swaps i with $i+1$. Then, in $\mathbf{k}[G] = \mathbf{k}[S_3]$, we have

$$(1+s_1)(1-s_1) = 1+s_1-s_1-s_1^2 = 1+s_1-s_1-1 = 0;$$
$$(1+s_2)(1+s_1+s_1s_2) = 1+s_2+s_1+s_2s_1+s_1s_2+s_2s_1s_2 = \sum_{w\in S_3} w.$$

- For each $u \in \mathbf{k}[G]$, we define two $\mathbf{k}$-linear maps

$$L(u) : \mathbf{k}[G] \to \mathbf{k}[G], \quad x \mapsto ux \qquad (\text{“left multiplication by } u\text{”})$$

and

$$R(u) : \mathbf{k}[G] \to \mathbf{k}[G], \quad x \mapsto xu \qquad (\text{“right multiplication by } u\text{”}).$$

(So $L(u)(x) = ux$ and $R(u)(x) = xu$.)

- Both $L(u)$ and $R(u)$ belong to the endomorphism ring $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$ of the $\mathbf{k}$-module $\mathbf{k}[G]$. This ring is essentially a $|G| \times |G|$-matrix ring over $\mathbf{k}$. Thus, $L(u)$ and $R(u)$ can be viewed as $|G| \times |G|$-matrices.

- Studying u, $L(u)$ and $R(u)$ is often (but not always) equivalent, because the maps

$$L : \mathbf{k}[G] \to \operatorname{End}_{\mathbf{k}}(\mathbf{k}[G]) \qquad \text{and}$$
$$R : \underbrace{(\mathbf{k}[G])^{\mathrm{op}}}_{\text{opposite ring}} \to \operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$$

are two injective $\mathbf{k}$-algebra morphisms (known as the left and right regular representations of the group G).

- When $\mathbf{k}$ is a field, each $u \in \mathbf{k}[G]$ has a **minimal polynomial**, i.e., a minimum-degree monic polynomial $P \in \mathbf{k}[X]$ such that $P(u) = 0$. This is also the minimal polynomial of the endomorphisms $L(u)$ and $R(u)$.

- Minimal polynomials also exist for $\mathbf{k} = \mathbb{Z}$:

- **Proposition 1.1.** Let $u \in \mathbb{Z}[G]$. Then, the minimal polynomial of u over $\mathbb{Q}$ is actually in $\mathbb{Z}[X]$.

- *Proof:* Follow the standard proof that the minimal polynomial of an algebraic number is in $\mathbb{Z}[X]$. (Use Gauss's Lemma.)

- **Theorem 1.2.** Assume that $\mathbf{k}$ is a field. Let $u \in \mathbf{k}[G]$. Then, $L(u) \sim R(u)$ as endomorphisms of $\mathbf{k}[G]$.

  Note: The symbol $\sim$ means "conjugate to". Thinking of these endomorphisms as $|G| \times |G|$-matrices, this is just similarity of matrices.

- We will see a proof of this soon.

- **Note:** $L(u) \sim R(u)$ would fail if we allowed G to be a monoid.

- The **antipode** of the group algebra $\mathbf{k}[G]$ is defined to be the $\mathbf{k}$-linear map

$$\begin{aligned} S : \mathbf{k}[G] &\to \mathbf{k}[G], \\ g &\mapsto g^{-1} \qquad \text{for each } g \in G. \end{aligned}$$

- **Proposition 1.3.** The antipode S is an involution (that is, $S \circ S = \mathrm{id}$) and a $\mathbf{k}$-algebra anti-automorphism (that is, $S(ab) = S(b) \cdot S(a)$ for all a, b).

- **Lemma 1.4.** Assume that $\mathbf{k}$ is a field. Let $u \in \mathbf{k}[G]$. Then, $L(u) \sim L(S(u))$ in $\mathrm{End}_{\mathbf{k}}(\mathbf{k}[G])$.

- *Proof:* Consider the standard basis $(g)_{g \in G}$ of $\mathbf{k}[G]$. The matrix representing the endomorphism $L(S(u))$ in this basis is the transpose of the matrix representing $L(u)$. But the Taussky–Zassenhaus theorem says that over a field, each matrix A is similar to its transpose A^T.

- **Lemma 1.5.** Let $u \in \mathbf{k}[G]$. Then, $L(S(u)) \sim R(u)$ in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$.
- *Proof:* We have $R(u) = S \circ L(S(u)) \circ S$ and $S = S^{-1}$.
- *Proof of Theorem 1.2:* Combine Lemma 1.4 with Lemma 1.5.
- **Remark (Martin Lorenz).** Theorem 1.2 generalizes to arbitrary Frobenius algebras.
- **Remark.** The conjugacy $L(u) \sim R(u)$ can fail if $\mathbf{k}$ is not a field (e.g., for $\mathbf{k} = \mathbb{Q}[t]$ and $G = S_3$).
- **Remark.** Let $u \in \mathbf{k}[G]$. Even if $\mathbf{k} = \mathbb{C}$, we don't always have $u \sim S(u)$ in $\mathbf{k}[G]$ (easy counterexample for $G = C_3$).

2. The symmetric group algebra

- Let $\mathbb{N} := \{0, 1, 2, \ldots\}$.
- Let $[k] := \{1, 2, \ldots, k\}$ for each $k \in \mathbb{N}$.
- Now, fix a positive integer n, and let S_n be the **n-th symmetric group**, i.e., the group of permutations of the set $[n]$.

  Multiplication in S_n is composition:

  $$(\alpha\beta)(i) = (\alpha \circ \beta)(i) = \alpha(\beta(i)) \qquad \text{for all } \alpha, \beta \in S_n \text{ and } i \in [n].$$

  (**Warning:** SageMath has a different opinion!)

- What can we say about the group algebra $\mathbf{k}[S_n]$ that doesn't hold for arbitrary $\mathbf{k}[G]$?
- There is a classical theory ("Young's seminormal form") of the structure of $\mathbf{k}[S_n]$ when $\mathbf{k}$ has characteristic 0. Two modern treatments are
  - Adriano M. Garsia, Ömer Egecioglu, *Lectures in Algebraic Combinatorics*, Springer 2020.
  - Murray Bremner, Sara Madariaga, Luiz A. Peresi, *Structure theory for the group algebra of the symmetric group, ...*, Commentationes Mathematicae Universitatis Carolinae, 2016.
- **Theorem 2.1 (Artin–Wedderburn–Young).** If $\mathbf{k}$ is a field of characteristic 0, then

  $$\mathbf{k}[S_n] \cong \prod_{\lambda \text{ is a partition of } n} \underbrace{\mathrm{M}_{f_\lambda}(\mathbf{k})}_{\text{matrix ring}} \qquad (\text{as } \mathbf{k}\text{-algebras}),$$

  where f_λ is the number of standard Young tableaux of shape λ.

- *Proof:* This follows from Young's seminormal form. For the shortest readable proof, see Theorem 1.45 in Bremner/Madariaga/Peresi.
- **Theorem 2.2.** Let $\mathbf{k}$ be a field of characteristic 0. Let $u \in \mathbf{k}[S_n]$. Then, $u \sim S(u)$ in $\mathbf{k}[S_n]$.
- *Proof:* Again use Young's seminormal form. Under the isomorphism $\mathbf{k}[S_n] \cong \prod_{\lambda \text{ is a partition of } n} \mathrm{M}_{f_\lambda}(\mathbf{k})$, the matrices corresponding to $S(u)$ are the transposes of the matrices corresponding to

u (this follows from (2.3.40) in Garsia/Egecioglu). Now, use the Taussky–Zassenhaus theorem again.

- *Alternative proof:* More generally, let G be an *ambivalent* finite group (i.e., a finite group in which each $g \in G$ is conjugate to g^{-1}). Let $u \in \mathbf{k}[G]$. Then, $u \sim S(u)$ in $\mathbf{k}[G]$. To prove this, pass to the algebraic closure of $\mathbf{k}$. By Artin–Wedderburn, it suffices to show that u and $S(u)$ act by similar matrices on each irreducible G-module V. But this is easy: Since G is ambivalent, we have $V \cong V^*$ and thus

$$(u \mid_V) \sim (u \mid_{V^*}) \sim (S(u) \mid_V)^T \sim (S(u) \mid_V)$$

  (by Taussky–Zassenhaus).

- **Note.** Characteristic 0 is needed!

3. The Young–Jucys–Murphy elements

- We now go further down the abstraction pole and study concrete elements in $\mathbf{k}[S_n]$.

- For any distinct elements $i_1, i_2, \ldots, i_k$ of $[n]$, 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.

- **Note.** $\operatorname{cyc}_i = \operatorname{id}$; $\operatorname{cyc}_{i,j}$ is a transposition.

- For each $k \in [n]$, we define the k**-th Young–Jucys–Murphy (YJM) element**

$$m_k := \operatorname{cyc}_{1,k} + \operatorname{cyc}_{2,k} + \cdots + \operatorname{cyc}_{k-1,k} \in \mathbf{k}[S_n].$$

- **Note.** We have $m_1 = 0$. Also, $S(m_k) = m_k$ for each $k \in [n]$.

- **Theorem 3.1.** The YJM elements $m_1, m_2, \ldots, m_n$ commute: We have $m_i m_j = m_j m_i$ for all i, j.

- *Proof:* Easy computational exercise.

- **Theorem 3.2.** The minimal polynomial of m_k over $\mathbb{Q}$ divides

$$\prod_{i=-k+1}^{k-1} (X - i) = (X - k + 1)(X - k + 2) \cdots (X + k - 1).$$

  (For $k \leq 3$, some factors here are redundant.)

- *First proof:* Study the action of m_k on each Specht module (simple S_n-module). See, e.g., G. E. Murphy, *A New Construction of Young's Seminormal Representation ...*, 1981 for details.

- *Second proof (Igor Makhlin):* Some linear algebra does the trick. Induct on k using the facts that m_k and m_{k+1} are simultaneously diagonalizable over $\mathbb{C}$ (since they are symmetric as real matrices and commute) and satisfy $s_k m_{k+1} = m_k s_k + 1$, where $s_k := \operatorname{cyc}_{k,k+1}$. See `https://mathoverflow.net/a/83493/` for details.

- More results and context can be found in §3.3 in Ceccherini-Silberstein/Scarabotti/Tolli, *Representation Theory of the Symmetric Groups*, 2010.

- **Question.** Is there a self-contained algebraic/combinatorial proof of Theorem 3.2 without linear algebra or representation theory? (Asked on MathOverflow: `https://mathoverflow.net/questions/420318/` .)

- **Theorem 3.3.** For each $k \in \{0, 1, \ldots, n\}$, we can evaluate the k-th elementary symmetric polynomial e_k at the YJM elements $m_1, m_2, \ldots, m_n$ to obtain

$$e_k(m_1, m_2, \ldots, m_n) = \sum_{\substack{\sigma \in S_n; \\ \sigma \text{ has exactly } n-k \text{ cycles}}} \sigma.$$

- *Proof:* Nice homework exercise (once stripped of the algebra).

- There are formulas for other symmetric polynomials applied to $m_1, m_2, \ldots, m_n$ (see Garsia/Egecioglu).

- **Theorem 3.4 (Murphy).**

$$\begin{aligned} &\{f(m_1, m_2, \ldots, m_n) \mid f \in \mathbf{k}[X_1, X_2, \ldots, X_n] \text{ symmetric}\} \\ &= (\text{center of the group algebra } \mathbf{k}[S_n]). \end{aligned}$$

- *Proof:* See any of:
  - Gadi Moran, *The center of $\mathbb{Z}[S_{n+1}]$ ...*, 1992.
  - G. E. Murphy, *The Idempotents of the Symmetric Group ...*, 1983, Theorem 1.9 (for the case $\mathbf{k} = \mathbb{Z}$, but the general case easily follows).

  (For $\mathbf{k} = \mathbb{Q}$, this is Theorem 4.4.5 in CS/S/T as well.)

A. The card shuffling point of view

- Permutations are often visualized as shuffled decks of cards:

  Imagine a deck of cards labeled $1, 2, \ldots, n$.

  A permutation $\sigma \in S_n$ corresponds to the **state** in which the cards are arranged $\sigma(1), \sigma(2), \ldots, \sigma(n)$ from top to bottom.

- A **random state** is an element $\sum\limits_{\sigma \in S_n} a_\sigma \sigma$ of $\mathbb{R}[S_n]$ whose coefficients $a_\sigma \in \mathbb{R}$ are nonnegative and add up to 1. This is interpreted as a distribution on the $n!$ possible states, where a_σ is the probability for the deck to be in state σ.

- We drop the "add up to 1" condition, and only require that $\sum\limits_{\sigma \in S_n} a_\sigma > 0$. The probabilities must then be divided by $\sum\limits_{\sigma \in S_n} a_\sigma$.

- For instance, $1 + \operatorname{cyc}_{1,2,3}$ corresponds to the random state in which the deck is sorted as $1, 2, 3$ with probability $\frac{1}{2}$ and sorted as $2, 3, 1$ with probability $\frac{1}{2}$.

- An $\mathbb{R}$-vector space endomorphism of $\mathbb{R}[S_n]$, such as $L(u)$ or $R(u)$ for some $u \in \mathbb{R}[S_n]$, acts as a **(random) shuffle**, i.e., a transformation of random states. This is just the standard way how Markov chains are constructed from transition matrices.

- For example, if $k > 1$, then the right multiplication $R(m_k)$ by the YJM element m_k corresponds to swapping the k-th card with some card above it chosen uniformly at random.

- Transposing such a matrix performs a time reversal of a random shuffle.

4. Top-to-random and random-to-top shuffles

* Another family of elements of $\mathbf{k}[S_n]$ are the k-**top-to-random shuffles**

$$\mathbf{B}_k := \sum_{\substack{\sigma \in S_n; \\ \sigma^{-1}(k+1) < \sigma^{-1}(k+2) < \cdots < \sigma^{-1}(n)}} \sigma$$

defined for all $k \in \{0, 1, \ldots, n\}$. Thus,

$$\mathbf{B}_{n-1} = \mathbf{B}_n = \sum_{\sigma \in S_n} \sigma;$$
$$\mathbf{B}_1 = \mathrm{cyc}_1 + \mathrm{cyc}_{1,2} + \mathrm{cyc}_{1,2,3} + \cdots + \mathrm{cyc}_{1,2,\ldots,n};$$
$$\mathbf{B}_0 = \mathrm{id}.$$

- As a random shuffle, $\mathbf{B}_k$ (to be precise, $R(\mathbf{B}_k)$) takes the top k cards and moves them to random positions.

- $\mathbf{B}_1$ is known as the **top-to-random shuffle** or the **Tsetlin library**.

- **Theorem 4.1 (Diaconis, Fill, Pitman).** We have

$$\mathbf{B}_{k+1} = (\mathbf{B}_1 - k)\,\mathbf{B}_k \qquad \text{for each } k \in \{0, 1, \ldots, n-1\}.$$

- **Corollary 4.2.** The $n+1$ elements $\mathbf{B}_0, \mathbf{B}_1, \ldots, \mathbf{B}_n$ commute and are polynomials in $\mathbf{B}_1$.

- **Theorem 4.3 (Wallach).** The minimal polynomial of $\mathbf{B}_1$ over $\mathbb{Q}$ is

$$\prod_{i \in \{0,1,\ldots,n-2,n\}} (X - i) = (X - n) \prod_{i=0}^{n-2} (X - i).$$

- These are not hard to prove in this order. See `https://mathoverflow.net/questions/308536` for the details.

- More can be said: in particular, the multiplicities of the eigenvalues $0, 1, \ldots, n-2, n$ of $R(\mathbf{B}_1)$ over $\mathbb{Q}$ are known.

- The antipodes $S(\mathbf{B}_0), S(\mathbf{B}_1), \ldots, S(\mathbf{B}_n)$ are known as the **random-to-top shuffles** and have essentially the same properties (since S is an algebra anti-automorphism).

- Main references:

– Nolan R. Wallach, *Lie Algebra Cohomology and Holomorphic Continuation of Generalized Jacquet Integrals*, 1988, Appendix.

– Persi Diaconis, James Allen Fill and Jim Pitman, *Analysis of Top to Random Shuffles*, 1992.

5. Random-to-random shuffles

- Here is a further family. For each $k \in \{0, 1, \ldots, n\}$, we let

$$\mathbf{R}_k := \sum_{\sigma \in S_n} \operatorname{noninv}_{n-k}(\sigma) \cdot \sigma,$$

  where $\operatorname{noninv}_{n-k}(\sigma)$ denotes the number of $(n-k)$-element subsets of $[n]$ on which σ is increasing.

- **Theorem 5.1 (Reiner, Saliola, Welker).** The $n+1$ elements $\mathbf{R}_0, \mathbf{R}_1, \ldots, \mathbf{R}_n$ commute (but are not polynomials in $\mathbf{R}_1$ in general).

- **Theorem 5.2 (Dieker, Saliola, Lafrenière).** The minimal polynomial of each $\mathbf{R}_i$ over $\mathbb{Q}$ is a product of $X - i$'s for distinct integers i. For example, the one of $\mathbf{R}_1$ divides

$$\prod_{i=-n^2}^{n^2} (X - i).$$

  The exact factors can be given in terms of certain statistics on Young diagrams.

- Main references:
  - Victor Reiner, Franco Saliola, Volkmar Welker, *Spectra of Symmetrized Shuffling Operators*, arXiv:1102.2460.
  - A.B. Dieker, F.V. Saliola, *Spectral analysis of random-to-random Markov chains*, 2018.
  - Nadia Lafrenière, *Valeurs propres des opérateurs de mélanges symétrisés*, thesis, 2019.

- **Question:** Simpler proofs? (Even commutativity takes a dozen pages!)

- **Question (Reiner):** How big is the subalgebra of $\mathbb{Q}[S_n]$ generated by $\mathbf{R}_0, \mathbf{R}_1, \ldots, \mathbf{R}_n$? Does it have dimension $O(n^2)$? Some small values:

n	1	2	3	4	5	6
$\dim(\mathbb{Q}[\mathbf{R}_0, \mathbf{R}_1, \ldots, \mathbf{R}_n])$	1	2	4	7	15	30

- **Remark 5.3.** We have
$$\mathbf{R}_k = \frac{1}{k!} \cdot S\left(\mathbf{B}_k\right) \cdot \mathbf{B}_k,$$
but this isn't all that helpful, since the $\mathbf{B}_k$ don't commute with the $S\left(\mathbf{B}_k\right)$.

6. Somewhere-to-below shuffles

- In 2021, Nadia Lafrenière defined the **somewhere-to-below shuffles** $t_1, t_2, \ldots, t_n$ by setting

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

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

- Thus, $t_1 = \mathbf{B}_1$ and $t_n = \mathrm{id}$.

- As a card shuffle, t_ℓ takes the ℓ-th card from the top and moves it further down the deck.

- Their linear combinations

$$\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n \qquad \text{with } \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$$

are called **one-sided cycle shuffles** and also have a probabilistic meaning when $\lambda_1, \lambda_2, \ldots, \lambda_n \geq 0$.

- **Fact:** $t_1, t_2, \ldots, t_n$ do not commute for $n \geq 3$. For $n = 3$, we have

$$[t_1, t_2] = \mathrm{cyc}_{1,2} + \mathrm{cyc}_{1,2,3} - \mathrm{cyc}_{1,3,2} - \mathrm{cyc}_{1,3}.$$

- However, they come pretty close to commuting!

- **Theorem 6.1 (Lafreniere, G., 2022+).** 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.

7. The descent-destroying basis

- This basis is not hard to define, but I haven't seen it before.

- For each $w \in S_n$, we let

$$\operatorname{Des} w := \{i \in [n-1] \mid w(i) > w(i+1)\} \qquad \text{(the **descent set** of } w\text{)}.$$

- For each $i \in [n-1]$, we let $s_i := \operatorname{cyc}_{i,i+1}$.

- For each $I \subseteq [n-1]$, we let

$$G(I) := (\text{the subgroup of } S_n \text{ generated by the } s_i \text{ for } i \in I).$$

- For each $w \in S_n$, we let

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

  In other words, you get a_w by breaking up the word w into maximal decreasing factors and re-sorting each factor arbitrarily (without mixing different factors).

- The family $(a_w)_{w \in S_n}$ is a basis of $\mathbf{k}[S_n]$ (by triangularity).

- For instance, for $n = 3$, we have

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

- **Theorem 7.1 (Lafrenière, G.).** For any $w \in S_n$ and $\ell \in [n]$, we have

$$a_w t_\ell = \mu_{w,\ell} a_w + \sum_{\substack{v \in S_n; \\ v \prec w}} \lambda_{w,\ell,v} a_v$$

  for some nonnegative integer $\mu_{w,\ell}$, some integers $\lambda_{w,\ell,v}$ and a certain partial order $\prec$ on S_n.

  Thus, the endomorphisms $R(t_1), R(t_2), \ldots, R(t_n)$ are upper-triangular with respect to the basis $(a_w)_{w \in S_n}$.

- *Examples:*
  - For $n = 4$, we have

$$a_{[4312]}t_2 = a_{[4312]} + \underbrace{a_{[4321]} - a_{[4231]} - a_{[3241]} - a_{[2143]}}_{\text{subscripts are } \prec [4312]} .$$

  - For $n = 3$, the endomorphism $R(t_1)$ is represented by the matrix

	$a_{[321]}$	$a_{[231]}$	$a_{[132]}$	$a_{[213]}$	$a_{[312]}$	$a_{[123]}$
$a_{[321]}$	3	1	1		1	
$a_{[231]}$				1	-1	1
$a_{[132]}$				1		
$a_{[213]}$				1		
$a_{[312]}$					1	
$a_{[123]}$						1

(empty cells = zero entries). For instance, the last column means $a_{[123]}t_1 = a_{[123]} + a_{[231]}$.

- **Corollary 7.2.** The eigenvalues of these endomorphisms $R(t_1), R(t_2), \ldots, R(t_n)$ and of all their linear combinations

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

are integers as long as $\lambda_1, \lambda_2, \ldots, \lambda_n$ are.

- How many different eigenvalues do they have?
- $R(t_1) = R(\mathbf{B}_1)$ has only n eigenvalues: $0, 1, \ldots, n-2, n$, as we have seen before. The other $R(t_\ell)$'s have even fewer.
- But their linear combinations $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ can have many more. How many?

8. Lacunar sets and Fibonacci numbers

- 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 $s \in S$).

- **Theorem 8.1 (combinatorial interpretation of Fibonacci numbers, folklore).** The number of lacunar subsets of $[n-1]$ is the **Fibonacci number** f_{n+1}.

  (Recall: $f_0 = 0, \qquad f_1 = 1, \qquad f_n = f_{n-1} + f_{n-2}$.)

- **Theorem 8.2.** When $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{C}$ are generic, the number of distinct eigenvalues of $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is f_{n+1}. In this case, the endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ is diagonalizable.

- Note that $f_{n+1} \ll n!$.

- One way such a theorem can be proved is by finding a filtration

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

  of the $\mathbf{k}$-module $\mathbf{k}[S_n]$ such that each $R(t_\ell)$ acts as a **scalar** on each of its quotients F_i / F_{i-1}. In matrix terms, this means bringing $R(t_\ell)$ to a block-triangular form, with the diagonal blocks being "scalar times I" matrices.

- It is only natural that the quotients should correspond to the lacunar subsets of $[n-1]$.

- Let us approach the construction of this filtration.

9. The $F(I)$ filtration

- For each $I \subseteq [n]$, we set
$$\operatorname{sum} I := \sum_{i \in I} i$$
and
$$\widehat{I} := \{0\} \cup I \cup \{n+1\}$$
and
$$I' := [n-1] \setminus (I \cup (I-1))$$
and
$$F(I) := \{q \in \mathbf{k}[S_n] \mid qs_i = q \text{ for all } i \in I'\} \subseteq \mathbf{k}[S_n].$$
In probabilistic terms, $F(I)$ consists of those random states of the deck that do not change if we swap the i-th and $(i+1)$-st cards from the top as long as neither i nor $i+1$ is in I. To put it informally: $F(I)$ consists of those random states that are "fully shuffled" between any two consecutive $\widehat{I}$-positions.

- 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,
$$m_{I,\ell} := \left(\text{smallest element of } \widehat{I} \text{ that is } \geq \ell\right) - \ell \in \{0, 1, \ldots, n\}.$$
For example, if $n = 5$ and $I = \{2, 3\}$, then $\widehat{I} = \{0, 2, 3, 6\}$ and
$$(m_{I,1},\ m_{I,2},\ m_{I,3},\ m_{I,4},\ m_{I,5}) = (1,\ 0,\ 0,\ 2,\ 1).$$
We note that, for any $\ell \in [n]$, we have the equivalence
$$m_{I,\ell} = 0 \iff \ell \in \widehat{I} \iff \ell \in I.$$

- **Crucial Lemma 9.1.** Let $I \subseteq [n]$ and $\ell \in [n]$. Then,
$$qt_\ell \in m_{I,\ell} q + \sum_{\substack{J \subseteq [n]; \\ \operatorname{sum} J < \operatorname{sum} I}} F(J) \qquad \text{for each } q \in F(I).$$

  - *Proof*: Expand qt_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 $m_{I,\ell} q$ term; the others live in appropriate $F(J)$'s.

See the paper for the details.

- Thus, we obtain a filtration of $\mathbf{k}[S_n]$ if we label the subsets I of $[n]$ in the order of increasing $\operatorname{sum} I$ and add up the respective $F(I)$s.

- Unfortunately, this filtration has 2^n, not f_{n+1} terms.

- Fortunately, that's because many of its terms are redundant. The ones that aren't correspond precisely to the I's that are lacunar subsets of $[n-1]$:

- **Lemma 9.2.** Let $k \in \mathbb{N}$. Then,

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

- *Proof:* If $J \subseteq [n]$ contains n or fails to be lacunar, then $F(J)$ is a submodule of some $F(K)$ with $\operatorname{sum} K < \operatorname{sum} J$. (Exercise!)

- 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

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

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 $F_0 = 0$). 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 properties we need:

- **Theorem 9.3.** For each $i \in [f_{n+1}]$ and $\ell \in [n]$, we have $F_i \cdot (t_\ell - m_{Q_i,\ell}) \subseteq F_{i-1}$ (so that $R(t_\ell)$ acts as multiplication by $m_{Q_i,\ell}$ on F_i / F_{i-1}).

- *Proof:* Lemma 9.1 + Lemma 9.2.

- **Lemma 9.4.** The quotients F_i / F_{i-1} are nontrivial for all $i \in [f_{n+1}]$.

- *Proof:* See below.

Corollary 9.5. Let $\mathbf{k}$ be a field, and let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Then, the eigenvalues of $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ are the linear combinations

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

- Theorem 8.2 easily follows by some linear algebra.

10. Back to the basis

- The descent-destroying basis $(a_w)_{w\in S_n}$ is compatible with our filtration:

* **Theorem 10.1.** 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 $F(I)$.

* 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 $Q_i' \subseteq \operatorname{Des} w$. We call this Q-index $\operatorname{Qind} w$.

- **Proposition 10.2.** 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 10.3.** 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 10.4.** For each $i \in [f_{n+1}]$, the $\mathbf{k}$-module F_i/F_{i-1} is free with basis $(\overline{a_w})_{w\in S_n;\ \operatorname{Qind} w = i}$.

- This yields Lemma 9.4 and also leads to Theorem 7.1, made precise as follows:

* **Theorem 10.5 (Lafrenière, G.).** For any $w \in S_n$ and $\ell \in [n]$, we have

$$a_w t_\ell = \mu_{w,\ell} a_w + \sum_{\substack{v\in S_n;\\ \operatorname{Qind} v < \operatorname{Qind} w}} \lambda_{w,\ell,v} a_v$$

  for some nonnegative integer $\mu_{w,\ell}$ and 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.

- Note that the numbering $Q_1, Q_2, \ldots, Q_{f_{n+1}}$ of the lacunar subsets of $[n-1]$ is not unique; we just picked one. Nevertheless, our construction is "essentially" independent of choices, since Proposition 10.2 describes $Q_{\operatorname{Qind} w}$ independently of this numbering (it is the unique lacunar $L \subseteq [n-1]$ satisfying $L' \subseteq \operatorname{Des} w \subseteq [n-1] \setminus L$). To get rid of the dependence on the numbering, we should think of the filtration as being indexed by a poset.

11. The multiplicities

- With Corollary 10.4, we know not only the eigenvalues of the $R(t_\ell)$'s, but also their multiplicities:

Corollary 11.1. 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 we 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 the endomorphism $R(\lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_n t_n)$ equals

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

- Can we compute the δ_i explicitly? Yes!

Theorem 11.2. Let $i \in [f_{n+1}]$. Let δ_i be the number of all permutations $w \in S_n$ satisfying $\operatorname{Qind} w = i$. Then:

(a) 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,

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

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

- **Question.** This reminds of the hook-length formula for standard tableaux. Is it connected to Fibonacci tableaux (paths in the Young–Fibonacci lattice)?

12. Variants

- Most of what we said about the somewhere-to-below shuffles t_ℓ can be extended to their antipodes $S(t_\ell)$ (the "**below-to-somewhere shuffles**"). For instance:

- **Theorem 12.1.** There exists a basis of the $\mathbf{k}$-module $\mathbf{k}[S_n]$ in which all of the endomorphisms $R(S(t_1)), R(S(t_2)), \ldots, R(S(t_n))$ are represented by upper-triangular matrices.

- We can also use left instead of right multiplication:

- **Theorem 12.2.** 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.

- These follow from Theorem 6.1 using dual bases, transpose matrices and Proposition 1.3. No new combinatorics required!

- **Question.** Do we have $L(t_\ell) \sim R(t_\ell)$ in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n])$ when $\mathbf{k}$ is not a field?

- **Remark.** The similarity $t_\ell \sim S(t_\ell)$ in $\mathbf{k}[S_n]$ holds when $\operatorname{char} \mathbf{k} = 0$, but not for general fields $\mathbf{k}$. (E.g., it fails for $\mathbf{k} = \mathbb{F}_2$ and $n = 4$ and $\ell = 1$.)

13. Conjectures and questions

- The simultaneous trigonalizability of the endomorphisms $R(t_1), R(t_2), \ldots, R(t_n)$ yields that their pairwise commutators are nilpotent. Hence, the pairwise commutators $[t_i, t_j]$ are also nilpotent.

- **Question.** How small an exponent works in $[t_i, t_j]^* = 0$?

- **Conjecture 13.1.** We have $[t_i, t_j]^{j-i+1} = 0$ for any $1 \leq i < j \leq n$.

- **Conjecture 13.2.** We have $[t_i, t_j]^{n-j+1} = 0$ for any $1 \leq i < j \leq n$.

- **Conjecture 13.3.** We have $[t_i, t_j]^{n-j} = 0$ for any $1 \leq i < j < n-1$.

- We can prove Conjecture 13.1 for $j = i+1$ and Conjecture 13.2 for $j = n-1$. We can also show that

$$t_{n-1}[t_i, t_{n-1}] = 0 \qquad \text{and} \qquad [t_i, t_{n-1}][t_j, t_{n-1}] = 0$$

and $\quad t_{i+1} t_i = (t_i - 1) t_i$

for all i and j.

- **Question.** What can be said about the $\mathbf{k}$-subalgebra $\mathbf{k}[t_1, t_2, \ldots, t_n]$ of $\mathbf{k}[S_n]$? Note:

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

(this sequence is not in the OEIS as of 2022-11-28).

To answer a question: The Lie subalgebra $\mathcal{L}(t_1, t_2, \ldots, t_n)$of $\mathbb{Q}[S_n]$has dimensions

n	1	2	3	4	5	6	7
$\dim(\mathcal{L}(t_1, t_2, \ldots, t_n))$	1	2	4	8	20	59	196

(also not in the OEIS).

- **Question.** How do the $F(I)$ and the F_i decompose into Specht modules when $\mathbf{k}$ is a field of characteristic 0 ?

- **Question.** How do $t_1, t_2, \ldots, t_n$ act on a given Specht module?

14. I thank

- **Nadia Lafrenière** for obvious reasons.
- **Martin Lorenz, Franco Saliola, Marcelo Aguiar, Vic Reiner, Travis Scrimshaw** for helpful conversations recent and not so recent.
- **Gérard Duchamp** for the invitation.
- **you** for your patience.