The one-sided cycle shuffles, and other mysteries and wonders of the symmetric group algebra [talk slides]

Darij Grinberg
joint work with Nadia Lafrenière

George Washington University, 2023-04-10 (Sections 1–12);
Temple University, 2023-10-16 (Sections 1–15);
Uppsala Universitet, 2024-03-26

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 $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n$ in the group algebra of S_n by

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

where the cycle (i) is the identity permutation. The first of them, $\mathbf{t}_1$, is known as the top-to-random shuffle and has been studied by Diaconis, Fill, Pitman (among others).

The n elements $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n$ 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 many tempting conjectures.

This is joint work with Nadia Lafrenière.

***

Preprints on one-sided cycle shuffles:

- Darij Grinberg and Nadia Lafrenière, *The one-sided cycle shuffles in the symmetric group algebra*, submitted, arXiv:2212.06274,
`https://www.cip.ifi.lmu.de/~grinberg/algebra/s2b1.pdf`
- Darij Grinberg, *Commutator nilpotency for somewhere-to-below shuffles*, arXiv:2309.05340,
`https://darijgrinberg.gitlab.io/algebra/s2b2.pdf`
- Another preprint to follow on the representation theory.

Preprint on row-to-row-sums:

- Darij Grinberg, *Rook sums in the symmetric group algebra*, outline 2024.
`https://www.cip.ifi.lmu.de/~grinberg/algebra/rooksn.pdf`

Slides of this talk:

- `https://www.cip.ifi.lmu.de/~grinberg/algebra/dc2023.pdf`

Items marked with ⊛ are more important.

FPSAC abstract on one-sided cycle shuffles:

- `https://www.cip.ifi.lmu.de/~grinberg/algebra/fps2024sn.pdf`

1. Finite group algebras

1.1. 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

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

1.2. Left and right actions of u on $\mathbf{k}[G]$

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

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

and

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

(So $L(\mathbf{u})(\mathbf{x}) = \mathbf{ux}$ and $R(\mathbf{u})(\mathbf{x}) = \mathbf{xu}$.)

- (**Note:** I will try to consistently use boldface letters for elements of $\mathbf{k}[G]$, such as $\mathbf{x}$ and $\mathbf{u}$ here.)

- Both $L(\mathbf{u})$ and $R(\mathbf{u})$ 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, $L(\mathbf{u})$ and $R(\mathbf{u})$ can be viewed as $|G| \times |G|$-matrices.

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

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

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

1.3. Minimal polynomials

- (∗) Each $\mathbf{u} \in \mathbf{k}[G]$ has a **minimal polynomial**, i.e., a minimum-degree monic polynomial $P \in \mathbf{k}[X]$ such that $P(\mathbf{u}) = 0$. It is unique when $\mathbf{k}$ is a field.

  The minimal polynomial of $\mathbf{u}$ is also the minimal polynomial of the endomorphisms $L(\mathbf{u})$ and $R(\mathbf{u})$.

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

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

1.4. Left and right are usually conjugate

- **Theorem 1.2.** Assume that $\mathbf{k}$ is a field. Let $\mathbf{u} \in \mathbf{k}[G]$. Then, $L(\mathbf{u}) \sim R(\mathbf{u})$ 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:** $L(\mathbf{u}) \sim R(\mathbf{u})$ would fail if G was merely a monoid, or if $\mathbf{k}$ was merely a commutative ring (e.g., for $\mathbf{k} = \mathbb{Q}[t]$ and $G = S_3$).

1.5. The antipode

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

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

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

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

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

- **Lemma 1.5.** Let $\mathbf{u} \in \mathbf{k}[G]$. Then, $L(S(\mathbf{u})) \sim R(\mathbf{u})$ in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$.

- *Proof:* We have $R(\mathbf{u}) = S \circ L(S(\mathbf{u})) \circ S$ 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.** Let $\mathbf{u} \in \mathbf{k}[G]$. Even if $\mathbf{k} = \mathbb{C}$, we don't always have $\mathbf{u} \sim S(\mathbf{u})$ in $\mathbf{k}[G]$ (easy counterexample for $G = C_3$).

2. The symmetric group algebra

2.1. Symmetric groups

- 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!)

2.2. Symmetric group algebras

- 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.

  The best source I know (dated but readable and careful) is:
  - Daniel Edwin Rutherford, *Substitutional Analysis*, Edinburgh 1948.
- **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.

2.3. Antipodal conjugacy

Theorem 2.2. Let $\mathbf{k}$ be a field of characteristic 0. Let $\mathbf{u} \in \mathbf{k}[S_n]$. Then, $\mathbf{u} \sim S(\mathbf{u})$ 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 $S(\mathbf{u})$ are the transposes of the matrices corresponding to $\mathbf{u}$ (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 $\mathbf{u} \in \mathbf{k}[G]$. Then, $\mathbf{u} \sim S(\mathbf{u})$ in $\mathbf{k}[G]$. To prove this, pass to the algebraic closure of $\mathbf{k}$. By Artin–Wedderburn, it suffices to show that $\mathbf{u}$ and $S(\mathbf{u})$ 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

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

  (by Taussky–Zassenhaus).

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

3. The Young–Jucys–Murphy elements

- From now on, we shall discuss 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.** We have $\operatorname{cyc}_i = \operatorname{id}$; $\operatorname{cyc}_{i,j}$ is a transposition.

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

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

- **Note.** We have $\mathbf{m}_1 = 0$. Also, $S(\mathbf{m}_k) = \mathbf{m}_k$ for each $k \in [n]$.

- **Theorem 3.1.** The YJM elements $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n$ commute: We have $\mathbf{m}_i\mathbf{m}_j = \mathbf{m}_j\mathbf{m}_i$ for all i, j.

- *Proof:* Easy computational exercise.

- **Theorem 3.2.** The minimal polynomial of $\mathbf{m}_k$ 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 $\mathbf{m}_k$ 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 $\mathbf{m}_k$ and $\mathbf{m}_{k+1}$ are simultaneously diagonalizable over $\mathbb{C}$ (since they are symmetric as real matrices and commute) and satisfy $s_k\mathbf{m}_{k+1} = \mathbf{m}_k s_k + 1$, 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 $k \in \mathbb{N}$, we can evaluate the k-th elementary symmetric polynomial e_k at the YJM elements $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n$ to obtain

$$e_k(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n) = \sum_{\substack{\sigma \in S_n; \\ \sigma \text{ has exactly } n-k \text{ cycles}}} \sigma.$$

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

- There are formulas for other symmetric polynomials applied to $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n$ (see Garsia/Egecioglu).

- **Theorem 3.4 (Murphy).**

$$\{f(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n) \mid f \in \mathbf{k}[X_1, X_2, \ldots, X_n] \text{ symmetric}\}$$
$$= (\text{center of the group algebra } \mathbf{k}[S_n]).$$

- *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 $R(\mathbf{m}_k)$ by the YJM element $\mathbf{m}_k$ 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,

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

- 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 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 $S\left(\mathbf{B}_k\right)$.

- **Generalization (implicit in Reiner, Saliola, Welker).** For each $k \in \{0, 1, \ldots, n\}$, we let

$$\widetilde{\mathbf{R}}_k := \sum_{\sigma \in S_n} \sum_{\substack{I \subseteq [n]; \\ |I| = n-k; \\ \sigma \text{ increases on } I}} \sigma \otimes \prod_{i \in I} x_i$$

in the **twisted group algebra**

$$\mathcal{T} := \mathbf{k}\left[S_n\right] \otimes \mathbf{k}\left[x_1, x_2, \ldots, x_n\right]$$
$$\text{with multiplication } \left(\sigma \otimes f\right)\left(\tau \otimes g\right) = \sigma\tau \otimes \tau^{-1}\left(f\right) g.$$

Then, the $\widetilde{\mathbf{R}}_1, \widetilde{\mathbf{R}}_2, \ldots, \widetilde{\mathbf{R}}_n$ commute.

- This twisted group algebra $\mathcal{T}$ acts on $\mathbf{k}\left[x_1, x_2, \ldots, x_n\right]$ in two ways: by multiplication ($\left(\sigma \otimes f\right)\left(p\right) = \sigma\left(fp\right)$) or by differentiation ($\left(f \otimes \sigma\right)\left(p\right) = \sigma\left(f\left(\partial\right)\left(p\right)\right)$). (In either case, the S_n part permutes the variables.)

6. Somewhere-to-below shuffles

- In 2021, Nadia Lafrenière defined the **somewhere-to-below shuffles** $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n$ by setting

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

  for each $\ell \in [n]$. (These $\mathbf{t}_\ell$ are called t_ℓ in my papers.)

- Thus, $\mathbf{t}_1 = \mathbf{B}_1$ and $\mathbf{t}_n = \operatorname{id}$.

- As a card shuffle, $\mathbf{t}_\ell$ takes the ℓ-th card from the top and moves it further down the deck.

- Their linear combinations

$$\lambda_1 \mathbf{t}_1 + \lambda_2 \mathbf{t}_2 + \cdots + \lambda_n \mathbf{t}_n \qquad \text{with } \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$$

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

- **Fact:** $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n$ do not commute for $n \geq 3$. For $n = 3$, we have

$$\left[\mathbf{t}_1, \mathbf{t}_2\right] = \operatorname{cyc}_{1,2} + \operatorname{cyc}_{1,2,3} - \operatorname{cyc}_{1,3,2} - \operatorname{cyc}_{1,3}.$$

- 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 $R\left(\mathbf{t}_1\right), R\left(\mathbf{t}_2\right), \ldots, R\left(\mathbf{t}_n\right)$ 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

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

In other words, you get $\mathbf{a}_w$ by breaking up the word w into maximal decreasing factors and re-sorting each factor arbitrarily (without mixing different factors). (The $\mathbf{a}_w$ are called a_w in my papers.)

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

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

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

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

$$\mathbf{a}_w \mathbf{t}_\ell = \mu_{w,\ell} \mathbf{a}_w + \sum_{\substack{v \in S_n;\\ v \prec w}} \lambda_{w,\ell,v} \mathbf{a}_v$$

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 $R(\mathbf{t}_1), R(\mathbf{t}_2), \ldots, R(\mathbf{t}_n)$ are upper-triangular with respect to the basis $(\mathbf{a}_w)_{w \in S_n}$.

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

$$\mathbf{a}_{[4312]}\mathbf{t}_2 = \mathbf{a}_{[4312]} + \underbrace{\mathbf{a}_{[4321]} - \mathbf{a}_{[4231]} - \mathbf{a}_{[3241]} - \mathbf{a}_{[2143]}}_{\text{subscripts are } \prec [4312]}.$$

  - For $n = 3$, the endomorphism $R(\mathbf{t}_1)$ is represented by the matrix

	$\mathbf{a}_{[321]}$	$\mathbf{a}_{[231]}$	$\mathbf{a}_{[132]}$	$\mathbf{a}_{[213]}$	$\mathbf{a}_{[312]}$	$\mathbf{a}_{[123]}$
$\mathbf{a}_{[321]}$	3	1	1		1	
$\mathbf{a}_{[231]}$				1	-1	1
$\mathbf{a}_{[132]}$				1		
$\mathbf{a}_{[213]}$				1		
$\mathbf{a}_{[312]}$					1	
$\mathbf{a}_{[123]}$						1

  (empty cells = zero entries). For instance, the last column means $\mathbf{a}_{[123]}\mathbf{t}_1 = \mathbf{a}_{[123]} + \mathbf{a}_{[231]}$.

- **Corollary 7.2.** The eigenvalues of these endomorphisms $R(\mathbf{t}_1), R(\mathbf{t}_2), \ldots, R(\mathbf{t}_n)$ and of all their linear combinations

$$R(\lambda_1\mathbf{t}_1 + \lambda_2\mathbf{t}_2 + \cdots + \lambda_n\mathbf{t}_n)$$

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

- How many different eigenvalues do they have?

- $R(\mathbf{t}_1) = R(\mathbf{B}_1)$ has only n eigenvalues: $0, 1, \ldots, n-2, n$, as we have seen before. The other $R(\mathbf{t}_\ell)$'s have even fewer.

- But their linear combinations $R(\lambda_1\mathbf{t}_1 + \lambda_2\mathbf{t}_2 + \cdots + \lambda_n\mathbf{t}_n)$ 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: $f_0 = 0$, $f_1 = 1$, $f_n = f_{n-1} + f_{n-2}$.)

- ∗ **Theorem 8.2.** When $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{C}$ are generic, the number of distinct eigenvalues of $R(\lambda_1 \mathbf{t}_1 + \lambda_2 \mathbf{t}_2 + \cdots + \lambda_n \mathbf{t}_n)$ is f_{n+1}. In this case, the endomorphism $R(\lambda_1 \mathbf{t}_1 + \lambda_2 \mathbf{t}_2 + \cdots + \lambda_n \mathbf{t}_n)$ is diagonalizable.

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

- ∗ We prove this 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 $R(\mathbf{t}_\ell)$ acts as a **scalar** on each of its quotients F_i / F_{i-1}. In matrix terms, this means bringing $R(\mathbf{t}_\ell)$ 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

$$\widehat{I} := \{0\} \cup I \cup \{n+1\} \qquad (\text{"enclosure" of } I)$$

and

$$I' := [n-1] \setminus (I \cup (I-1)) \qquad (\text{"non-shadow" of } I)$$

and

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

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,

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

- *Proof:* Expand $\mathbf{q}\mathbf{t}_\ell$ by the definition of $\mathbf{t}_\ell$, 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 $m_{I,\ell}\mathbf{q}$ 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 $F_i \cdot (\mathbf{t}_\ell - m_{Q_i,\ell}) \subseteq F_{i-1}$ (so that $R(\mathbf{t}_\ell)$ 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 $R(\lambda_1 \mathbf{t}_1 + \lambda_2 \mathbf{t}_2 + \cdots + \lambda_n \mathbf{t}_n)$ 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 $(\mathbf{a}_w)_{w\in S_n}$ is compatible with our filtration:

⊛ **Theorem 10.1.** For each $I \subseteq [n]$, the family $(\mathbf{a}_w)_{w\in S_n;\ I'\subseteq \operatorname{Des} w}$ 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 $(\mathbf{a}_w)_{w\in S_n;\ \operatorname{Qind} w \leq i}$.

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

- 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

$$\mathbf{a}_w \mathbf{t}_\ell = \mu_{w,\ell} \mathbf{a}_w + \sum_{\substack{v\in S_n;\\ \operatorname{Qind} v < \operatorname{Qind} w}} \lambda_{w,\ell,v} \mathbf{a}_v$$

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

Thus, the endomorphisms $R(\mathbf{t}_1), R(\mathbf{t}_2), \ldots, R(\mathbf{t}_n)$ are upper-triangular with respect to the basis $(\mathbf{a}_w)_{w\in S_n}$ 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 $R(\mathbf{t}_\ell)$'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 $R(\lambda_1 \mathbf{t}_1 + \lambda_2 \mathbf{t}_2 + \cdots + \lambda_n \mathbf{t}_n)$ 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 $\delta_i \mid n!$.

- **Note.** This reminds of the hook-length formula for standard tableaux, but is much simpler.

12. Variants

- Most of what we said about the somewhere-to-below shuffles $\mathbf{t}_\ell$ can be extended to their antipodes $S(\mathbf{t}_\ell)$ (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 $R(S(\mathbf{t}_1)), R(S(\mathbf{t}_2)), \ldots, R(S(\mathbf{t}_n))$ 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 $L(\mathbf{t}_1), L(\mathbf{t}_2), \ldots, L(\mathbf{t}_n)$ 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 $L(\mathbf{t}_\ell) \sim R(\mathbf{t}_\ell)$ in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[S_n])$ when $\mathbf{k}$ is not a field?

- **Remark.** The similarity $\mathbf{t}_\ell \sim S(\mathbf{t}_\ell)$ 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. Commutators

- The simultaneous trigonalizability of the endomorphisms $R(\mathbf{t}_1), R(\mathbf{t}_2), \ldots, R(\mathbf{t}_n)$ yields that their pairwise commutators are nilpotent. Hence, the pairwise commutators $[\mathbf{t}_i, \mathbf{t}_j]$ are also nilpotent.

- **Question.** How small an exponent works in $[\mathbf{t}_i, \mathbf{t}_j]^* = 0$?

- **Theorem 13.1.** We have $[\mathbf{t}_i, \mathbf{t}_j]^{j-i+1} = 0$ for any $1 \leq i \leq j \leq n$.

- **Theorem 13.2.** We have $[\mathbf{t}_i, \mathbf{t}_j]^{\lceil (n-j)/2 \rceil + 1} = 0$ for any $i, j \in [n]$.

- Depending on i and j, one of the exponents is better than the other.

  Conjecture. The better one is optimal! (Checked for all $n \leq 12$.)

- Stronger results hold, replacing powers by products.

- Several other curious facts hold: For example,

  $$\mathbf{t}_{i+1}\mathbf{t}_i = (\mathbf{t}_i - 1)\,\mathbf{t}_i \qquad \text{and} \qquad \mathbf{t}_{i+2}(\mathbf{t}_i - 1) = (\mathbf{t}_i - 1)(\mathbf{t}_{i+1} - 1)$$

  and

  $$\mathbf{t}_{n-1}[\mathbf{t}_i, \mathbf{t}_{n-1}] = 0 \qquad \text{and} \qquad [\mathbf{t}_i, \mathbf{t}_{n-1}][\mathbf{t}_j, \mathbf{t}_{n-1}] = 0$$

  for all i and j.

- All this is completely elementary but surprisingly hard to prove (dozens of pages of manipulations with sums and cycles). The proofs can be found in arXiv:2309.05340v2 aka

  `https://www.cip.ifi.lmu.de/~grinberg/algebra/s2b2.pdf`

- What is “really” going on? No idea...

14. Representation theory

- Where groups go, representations are not far away...

  If you know representation theory, you will have asked yourself two questions:

  1. The $F(I)$ and the F_i are left ideals of $\mathbf{k}[S_n]$; how do they decompose into Specht modules?
  2. How do $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n$ act on a given Specht module?

- We can answer these (in characteristic 0):

- The answer uses symmetric functions, specifically:

  - Let s_λ mean the Schur function for a partition λ.
  - Let $h_m = s_{(m)}$ be the m-th complete homogeneous symmetric function for each $m \geq 0$.
  - Let $z_m = s_{(m-1,1)} = h_{m-1}h_1 - h_m$ for each $m > 0$.

- For each subset I of $[n]$, we define a symmetric function

$$z_I := h_{i_1 - 1} \prod_{j=2}^{k} z_{i_j - i_{j-1}},$$

  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 $I = \{i_1 < i_2 < \cdots < i_{k-1}\}$).

- For each $I \subseteq [n]$ and each partition λ of n, we let c^I_λ be the coefficient of s_λ in the Schur expansion of z_I.

  This is a nonnegative integer (actually a Littlewood–Richardson coefficient, since z_I is a skew Schur function).

- **Theorem 14.1.** Let ν be a partition. Let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{k}$. Then, the one-sided cycle shuffle $\lambda_1 \mathbf{t}_1 + \lambda_2 \mathbf{t}_2 + \cdots + \lambda_n \mathbf{t}_n$ acts on the Specht module S^ν as a linear map with eigenvalues

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

  and the multiplicity of each such eigenvalue is c^I_ν 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 this linear map is diagonalizable.

- **Theorem 14.2.** As a representation of S_n, the quotient module F_i / F_{i-1} has Frobenius characteristic z_{Q_i}.
- Proofs will appear in forthcoming work.

15. Conjectures and questions

- **Question.** What can be said about the $\mathbf{k}$-subalgebra $\mathbf{k}[\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n]$ of $\mathbf{k}[S_n]$? Note:

n	1	2	3	4	5	6	7	8
$\dim(\mathbb{Q}[\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n])$	1	2	4	9	23	66	212	761

(this sequence is not in the OEIS as of 2024-03-17).

Also, the Lie subalgebra $\mathcal{L}(\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n)$ of $\mathbb{Q}[S_n]$ has dimensions

n	1	2	3	4	5	6	7
$\dim(\mathcal{L}(\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n))$	1	2	4	8	20	59	196

(also not in the OEIS).

- **Question ("Is there a q-deformation?").** Much of the above (e.g., Theorems 10.5, 13.1, 13.2) seems to still hold if $\mathbb{Q}[S_n]$ is replaced by the Iwahori–Hecke algebra (but $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n$ are defined in the exact same way, with w replaced by T_w). Even $\dim(\mathbb{Q}[\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_n])$ appears to be the same for the Hecke algebra, suggesting that all identities come from the Hecke algebra. Why?

16. The Gaudin Bethe subalgebras

- We now leave the topic of one-sided cycle shuffles, and return to surveying other (families of) elements of $\mathbf{k}[S_n]$.
- The following was found (at least in a significant case) by Mukhin, Tarasov and Varchenko (2013), and recently extended and reproved by Purbhoo (2022) and Karp and Purbhoo (2023).
- **Definition.** Let $z_1, z_2, \ldots, z_n$ be any $n+2$ elements of $\mathbf{k}$.

  For any subset T of $[n]$, we set

  $$\boldsymbol{\alpha}_T^+ := \sum_{\sigma \in S_T} \sigma \in \mathbf{k}[S_n]$$

  (where S_T is embedded into S_n in the obvious way: all elements $\notin T$ are fixed).
- **Theorem 16.1 (Mukhin/Tarasov/Varchenko/Purbhoo).** Set

  $$\boldsymbol{\beta}_k^+(u) := \sum_{\substack{T \subseteq [n];\\ |T|=k}} \boldsymbol{\alpha}_T^+ \prod_{m \in [n] \setminus T} (z_m + u) \qquad \text{for any } k \in \mathbb{N} \text{ and } u \in \mathbf{k}.$$

  Then, $\boldsymbol{\beta}_i^+(u)$ and $\boldsymbol{\beta}_j^+(v)$ commute for all $i, j \in \mathbb{N}$ and $u, v \in \mathbf{k}$.
- More generally:
- **Theorem 16.2 (Karp/Purbhoo).** Fix $i, j \in \mathbb{N}$ and $u, v \in \mathbf{k}$. Fix a class function φ on the symmetric group S_i, and a class function ψ on the symmetric group S_j. For any i-element subset T of $[n]$, set

  $$\boldsymbol{\alpha}_T^\varphi := \sum_{\sigma \in S_T} \varphi(\sigma)\, \sigma \in \mathbf{k}[S_n],$$

  where φ is transported onto S_T via any bijection $[i] \to T$ (the choice does not matter). Set

  $$\boldsymbol{\beta}_i^\varphi(u) := \sum_{\substack{T \subseteq [n];\\ |T|=i}} \boldsymbol{\alpha}_T^\varphi \prod_{m \in [n] \setminus T} (z_m + u).$$

  Similarly define $\boldsymbol{\beta}_j^\psi(v)$. Then, $\boldsymbol{\beta}_i^\varphi(u)$ and $\boldsymbol{\beta}_j^\psi(v)$ commute.
- The proofs are not very long but surprisingly complicated. A major ingredient is the group version of antipodal conjugacy: Each permutation $\sigma \in S_n$ is conjugate to its inverse. (A trickier refinement of this is used.)

- Both Mukhin/Tarasov/Varchenko and Purbhoo prove further results about the (commutative) subalgebra of $\mathbf{k}[S_n]$ generated by the $\boldsymbol{\beta}_i^{\varphi}(u)$. In particular, Purbhoo shows that the subalgebra generated by $\boldsymbol{\beta}_i^{+}(u)$ is that generated by $\boldsymbol{\beta}_i^{\mathrm{sign}}(u)$.

- **Question:** Simpler proofs?

17. Excendances and anti-excedances

- **Definition.** Let $\sigma \in S_n$ be a permutation. Then, we define

$$\operatorname{exc}\sigma := (\text{\# of } i \in [n] \text{ such that } \sigma(i) > i) \qquad \text{and}$$
$$\operatorname{anxc}\sigma := (\text{\# of } i \in [n] \text{ such that } \sigma(i) < i)$$

(the "**excedance number**" and the "**anti-excedance number**" of σ).

- **Conjecture 17.1.** For any $a, b \in \mathbb{N}$, define

$$\mathbf{X}_{a,b} := \sum_{\substack{\sigma \in S_n; \\ \operatorname{exc}\sigma = a; \\ \operatorname{anxc}\sigma = b}} \sigma \in \mathbf{k}[S_n].$$

Then, the elements $\mathbf{X}_{a,b}$ for all $a, b \in \mathbb{N}$ commute (for fixed n).

- Checked for all $n \leq 7$ using SageMath. Inspired by the Mukhin /Tarasov/Varchenko results from the previous section (thanks Theo Douvropoulos for the idea!).

- The antipode plays well with these elements:

$$S(\mathbf{X}_{a,b}) = \mathbf{X}_{b,a}.$$

- **Question.** What can be said about the $\mathbf{k}$-subalgebra $\mathbf{k}[\mathbf{X}_{a,b} \mid a, b \in \{0, 1, \ldots, n\}]$ of $\mathbf{k}[S_n]$? Note:

n	1	2	3	4	5	6
$\dim(\mathbb{Q}[\mathbf{X}_{a,b}])$	1	2	4	10	26	76

.

So far, this looks like the # of involutions in S_n, which is exactly the dimension of the Gelfand–Zetlin subalgebra (generated by the Young–Jucys–Murphy elements)!

What is the exact relation?

18. Riffle shuffles

- For a change, here is something classical.

- For each $k \in \mathbb{N}$, we define an element

$$\mathbf{S}_k := \sum_{\substack{\mathbf{i}=(i_1,i_2,\ldots,i_k)\in\mathbb{N}^k;\\ i_1+i_2+\cdots+i_k=n}} \ \sum_{\substack{\sigma\in S_n;\\ \sigma \text{ is increasing on}\\ \text{every } \mathbf{i}\text{-interval}}} \sigma$$

  of $\mathbf{k}[S_n]$. Here, for any k-tuple $\mathbf{i} = (i_1, i_2, \ldots, i_k) \in \mathbb{N}^k$ satisfying $i_1 + i_2 + \cdots + i_k = n$, the **i-intervals** are the intervals of lengths $i_1, i_2, \ldots, i_k$ into which the set $[n]$ is subdivided (i.e., the intervals $[i_1 + i_2 + \cdots + i_{j-1} + 1,\ i_1 + i_2 + \cdots + i_j]$ for all $0 < j \leq k$). (Recall that $0 \in \mathbb{N}$, so that these intervals may be empty.)

  This $\mathbf{S}_k$ is called the ***k*-riffle shuffle**. Roughly speaking, it corresponds to cutting the deck into k piles of sizes $i_1, i_2, \ldots, i_k$ and shuffling them back together arbitrarily. (This description is a bit imprecise, as it ignores probabilities.)

- **Theorem 18.1 (e.g., Gerstenhaber/Schack 1991).** The elements $\mathbf{S}_0, \mathbf{S}_1, \mathbf{S}_2, \ldots$ commute. Moreover,

$$\mathbf{S}_i \mathbf{S}_j = \mathbf{S}_{ij} \qquad \text{for all } i, j \in \mathbb{N}.$$

- *Proof using Hopf algebras:* It suffices to show that $S(\mathbf{S}_i) \cdot S(\mathbf{S}_j) = S(\mathbf{S}_{ij})$ for all $i, j \in \mathbb{N}$ (where S is the antipode, sending each $\sigma \in S_n$ to σ^{-1}).

  The symmetric group algebra $\mathbf{k}[S_n]$ acts faithfully on the tensor power $V^{\otimes n}$ of any free $\mathbf{k}$-module V of rank $\geq n$ (by permuting the tensorands). This tensor power $V^{\otimes n}$ is the n-th degree part of the tensor algebra $T(V)$, which is a cocommutative connected graded Hopf algebra (Δ = unshuffle coproduct). Now, the action of $S(\mathbf{S}_i)$ on $V^{\otimes i}$ is just the convolution $\mathrm{id}^{\star i} = \underbrace{\mathrm{id} \star \mathrm{id} \star \cdots \star \mathrm{id}}_{i \text{ times}} : T(V) \to T(V)$ (restricted to $V^{\otimes i}$). So it remains to prove that $\mathrm{id}^{\star i} \circ \mathrm{id}^{\star j} = \mathrm{id}^{\star (ij)}$. But this can be done easily using cocommutativity.

- *Remark:* These $\mathrm{id}^{\star i}$ are known as **Adams operations**, and are defined on any bialgebra. The equality $\mathrm{id}^{\star i} \circ \mathrm{id}^{\star j} = \mathrm{id}^{\star (ij)}$ holds for any commutative or cocommutative bialgebra.

- **Theorem 18.2.** The minimal polynomial of $\mathbf{S}_i$ is a divisor of

$$\left(X - i^1\right)\left(X - i^2\right)\cdots\left(X - i^n\right).$$

- **Theorem 18.3.** If $\mathbf{k}$ is a field of characteristic 0, the subalgebra of $\mathbf{k}[S_n]$ generated (= spanned) by $\mathbf{S}_0, \mathbf{S}_1, \mathbf{S}_2, \ldots$ is n-dimensional as a $\mathbf{k}$-vector space, and is isomorphic to a product of n copies of $\mathbf{k}$. It is called the **Eulerian subalgebra** of $\mathbf{k}[S_n]$, and its decomposing idempotents are the famous **Eulerian idempotents**.

- Reference: Loday, *Cyclic homology*, 2nd edition 1998, §4.5.

- **Question.** How does the Eulerian subalgebra look like for general $\mathbf{k}$?

19. Row-to-row sums

- **Definition.** A **set composition** of $[n]$ is defined to mean a tuple $\mathbf{U} = (U_1, U_2, \ldots, U_k)$ of disjoint nonempty subsets of $[n]$ such that $U_1 \cup U_2 \cup \cdots \cup U_k = [n]$. We set $\ell(\mathbf{U}) = k$ and call k the **length** of $\mathbf{U}$.

- **Definition.** Let $\operatorname{SC}(n)$ be the set of all set compositions of $[n]$.

- **Definition.** If $\mathbf{A} = (A_1, A_2, \ldots, A_k)$ and $\mathbf{B} = (B_1, B_2, \ldots, B_k)$ are two set compositions of $[n]$ having the same length, then we define the **row-to-row sum**

$$\nabla_{\mathbf{B},\mathbf{A}} := \sum_{\substack{w \in S_n; \\ w(A_i) = B_i \text{ for all } i}} w \qquad \text{in } \mathbf{k}[S_n].$$

- **Easy properties:**
  - We have $\nabla_{\mathbf{B},\mathbf{A}} = 0$ unless $|A_i| = |B_i|$ for all i.
  - We have $\nabla_{\mathbf{B},\mathbf{A}} = \nabla_{\mathbf{B}\sigma,\mathbf{A}\sigma}$ for any $\sigma \in S_k$ (acting on set compositions by permuting the blocks).
  - We have $S(\nabla_{\mathbf{B},\mathbf{A}}) = \nabla_{\mathbf{A},\mathbf{B}}$.

- **Theorem 19.1.** Let $\mathcal{A} = \mathbf{k}[S_n]$. Let $k \in \mathbb{N}$. We define two $\mathbf{k}$-submodules $\mathcal{I}_k$ and $\mathcal{J}_k$ of $\mathcal{A}$ by

$$\mathcal{I}_k := \operatorname{span}\{\nabla_{\mathbf{B},\mathbf{A}} \mid \mathbf{A}, \mathbf{B} \in \operatorname{SC}(n) \text{ with } \ell(\mathbf{A}) = \ell(\mathbf{B}) \leq k\}$$

and

$$\mathcal{J}_k := \mathcal{A} \cdot \operatorname{span}\{\boldsymbol{\alpha}_U^- \mid U \text{ is a } (k+1)\text{-element subset of } [n]\} \cdot \mathcal{A},$$

where

$$\boldsymbol{\alpha}_U^- := \sum_{\sigma \in S_U} (-1)^\sigma \sigma \in \mathbf{k}[S_n].$$

Then:

  - Both $\mathcal{I}_k$ and $\mathcal{J}_k$ are ideals of $\mathcal{A}$, and are preserved under S.
  - We have

$$\mathcal{I}_k = \mathcal{J}_k^\perp = \operatorname{LAnn} \mathcal{J}_k = \operatorname{RAnn} \mathcal{J}_k \qquad \text{and}$$
$$\mathcal{J}_k = \mathcal{I}_k^\perp = \operatorname{LAnn} \mathcal{I}_k = \operatorname{RAnn} \mathcal{I}_k.$$

  Here, $\mathcal{U}^\perp$ means orthogonal complement wrt the standard bilinear form on $\mathcal{A}$, whereas LAnn and RAnn mean left and right annihilators.

  - The **k**-module $\mathcal{I}_k$ is free of rank = # of $(1, 2, \ldots, k+1)$-avoiding permutations in S_n.
  - The **k**-module $\mathcal{J}_k$ is free of rank = # of $(1, 2, \ldots, k+1)$-nonavoiding permutations in S_n.
  - The quotients $\mathcal{A}/\mathcal{J}_k$ and $\mathcal{A}/\mathcal{I}_k$ are also free, with the same ranks as $\mathcal{I}_k$ and $\mathcal{J}_k$ (respectively), and with bases consisting of (residue classes of) the relevant permutations.
  - If $n!$ is invertible in **k**, then $\mathcal{A} = \mathcal{I}_k \oplus \mathcal{J}_k$ (internal direct sum) as **k**-modules, and $\mathcal{A} \cong \mathcal{I}_k \times \mathcal{J}_k$ as **k**-algebras.

- This is not hard to show using representation theory if $\mathbf{k} = \mathbb{C}$ (or $\mathbb{Q}$), but the characteristic-free case needs to be done from scratch.

- **Remark.** The **Murphy basis** of $\mathcal{A}$ consists of the elements $\nabla_{\mathbf{B},\mathbf{A}}$ for the **standard** set compositions **A** and **B** of $[n]$. Here, "standard" means that the blocks are the rows of a standard Young tableau (in particular, they must be of partition shape).

  This is a cellular basis of $\mathcal{A}$. Thus, the Specht modules are quotients of spans of certain subfamilies of this basis.

  (This was done for Hecke algebras in: G. E. Murphy, *On the Representation Theory of the Symmetric Groups and Associated Hecke Algebras*, 1991. Our $\nabla_{\mathbf{B},\mathbf{A}}$ correspond to his $x_{s,t}$ for $q = 1$.)

- **Question.** How far can we develop the representation theory of S_n using this approach? (e.g., prove the LR rule?)

20. Row-to-row sums of length 2

- The elements $\nabla_{\mathbf{B},\mathbf{A}}$ are fairly general, and in fact each $w \in S_n$ can be written as $\nabla_{\mathbf{B},\mathbf{A}}$ for some $\mathbf{A}$ and $\mathbf{B}$. But some things can be said when $\ell(\mathbf{A}) = \ell(\mathbf{B}) \leq 2$.

* **Definition.** If A and B are two subsets of $[n]$, then we set

$$\nabla_{B,A} := \sum_{\substack{w \in S_n; \\ w(A)=B}} w \qquad \text{in } \mathbf{k}[S_n].$$

This is $\nabla_{\mathbf{B},\mathbf{A}}$ for $\mathbf{A} = (A, [n] \setminus A)$ and $\mathbf{B} = (B, [n] \setminus B)$.

* **Theorem 20.1.** The minimal polynomial of each $\nabla_{B,A}$ over $\mathbb{Q}$ is a product of linear factors.

- **Example.** For $n = 5$, the minimal polynomial of $\nabla_{\{1,2\},\{2,3\}}$ is $(x-12)(x-2)x(x+4)$.

- More generally:

* **Theorem 20.2.** Fix any $A \subseteq [n]$. Then, the minimal polynomial of any $\mathbb{Q}$-linear combination of $\nabla_{B,A}$ with B ranging over the subsets of $[n]$ is a product of linear factors.

- This can be proved using a filtration (albeit not of $\mathcal{A}$).

- **Questions.** What are the linear factors (i.e., the eigenvalues)? (I have a complicated sum formula.)

  What is the characteristic polynomial? (i.e., what are the multiplicities of the eigenvalues?)

- The proofs of Theorems 20.1 and 20.2 rely on the following fact:

- **Proposition 20.3 (product formula).** Let A, B, C, D be four subsets of $[n]$ such that $|A| = |B|$ and $|C| = |D|$. Then,

$$\nabla_{D,C}\nabla_{B,A} = \omega_{B,C} \sum_{\substack{U \subseteq D, \\ V \subseteq A; \\ |U|=|V|}} (-1)^{|U|-|B\cap C|} \binom{|U|}{|B \cap C|} \nabla_{U,V},$$

where

$$\omega_{B,C} := |B \cap C|! \cdot |B \setminus C|! \cdot |C \setminus B|! \cdot |[n] \setminus (B \cup C)|! \in \mathbb{Z}.$$

- *Proof.* Nice exercise in enumeration!
- **Digression.** Define a free **k**-module with basis $(\Delta_{B,A})_{A,B\subseteq[n] \text{ with } |A|=|B|}$, where the $\Delta_{B,A}$ are formal symbols. Define a multiplication on $\mathcal{D}$ by

$$\Delta_{D,C}\Delta_{B,A} := \omega_{B,C} \sum_{\substack{U\subseteq D, \\ V\subseteq A; \\ |U|=|V|}} (-1)^{|U|-|B\cap C|} \binom{|U|}{|B\cap C|} \Delta_{U,V}.$$

- **Theorem 20.4.** This $\mathcal{D}$ is a nonunital algebra (i.e., associative).
- **Question.** Is this algebra unital when $n!$ is invertible in **k** ?
- **Question.** What is this algebra really? (It is a free **k**-module of rank $\binom{2n}{n}$, so it might be a diagram algebra – e.g., a nonunital $\mathbb{Z}$-form of the planar rook algebra?)

21. Philosophical questions

- Why is so much happening in $\mathbf{k}[S_n]$? In particular:
- **Why do so many elements commute?** Are there any general methods for proving commutativity?
- **Why do so many elements have integer eigenvalues** (i.e., factoring minimal polynomials)?
- Methods I have seen so far:
  - Explicit multiplication rules: proves commutativity for $\mathbf{B}_k$, eigenvalues for $\nabla_{B,A}$, and various properties for elements in the descent algebra (Solomon Mackey rule).
  - Faithful action on $V^{\otimes n}$: proves commutativity for $\mathbf{S}_i$, $\mathbf{R}_i$ (Lafrenière's approach).
  - Preserved filtration: proves eigenvalues and simultaneous trigonalizability for $\mathbf{t}_i$; can theoretically be used for commutativity as well when the elements generate an S-invariant subalgebra (via Okounkov-Vershik involution trick), but haven't seen that happen.
  - Bijective brute-force: proves commutativity for $\mathbf{m}_k$, $\boldsymbol{\beta}_k^{\varphi}$.
  - Action on irreps (= Specht modules): proves eigenvalues for $\mathbf{m}_k$, $\mathbf{R}_i$.
  - Diagonalization: proves eigenvalues for $\mathbf{m}_k$ (Young seminormal basis), $\mathbf{R}_i$.
  - Faithful action on something else (e.g., Gelfand model, polynomial ring via divided symmetrization, etc.): would be nice to see a use, but have not encountered yet.
  - Transfer principles (e.g., §3.1 in Mukhin/Tarasov/Varchenko arXiv:0906.5185v1): would be really great to see.
  - Recognition as polynomials in simpler commuting elements: would be nice to see.
  - Okounkov–Vershik lemma (centralizer of multiplicity-free branching): would be nice to see.
  - Categorization (replacing $S_n = \operatorname{Bij}([n], [n])$ by $\operatorname{Inj}([n], [m])$ or $\operatorname{Surj}([n], [m])$, just like square matrices are a particular case of rectangular matrices): would be great to see!

Any additions to this list are welcome!

22. I thank

- **Nadia Lafrenière** for obvious reasons.
- **Martin Lorenz, Franco Saliola, Marcelo Aguiar, Vic Reiner, Travis Scrimshaw**, **Theo Douvropoulos**, **Volkmar Welker** for helpful conversations recent and not so recent.
- **Vasily Dolgushev** for the invitation (Temple).
- **Joel Brewster Lewis** for the invitation (GW).
- **Walter Mazorchuk** for the invitation (Uppsala).
- **you** for your patience.