The random-to-random shuffles and their q-deformations

Darij Grinberg (Drexel University) joint work with
Sarah Brauner, Patricia Commins, Franco Saliola

Kungliga Tekniska högskolan, Stockholm, 2025-03-19;
Rutgers University, 2025-04-30;
CAGE seminar, 2025-05-08

slides: http://www.cip.ifi.lmu.de/~grinberg/algebra/kth2025b.pdf

paper (draft): https://www.cip.ifi.lmu.de/~grinberg/algebra/r2r2.pdf

Finite group algebras: Basics

* Let $\mathbf{k}$ be any commutative ring. (Usually $\mathbb{Z}$, $\mathbb{Q}$ or a polynomial ring.)
* Let G be a finite group. (We will only use symmetric groups.)
* 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.

- Let $\mathbf{k}$ be any commutative ring. (Usually $\mathbb{Z}$, $\mathbb{Q}$ or a polynomial ring.)
- Let G be a finite group. (We will only use symmetric groups.)
- 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

$$(1 + s_1)(1 - s_1) = 1 + s_1 - s_1 - s_1^2 = 0$$

(since $s_1^2 = 1$);

- Let **k** be any commutative ring. (Usually $\mathbb{Z}$, $\mathbb{Q}$ or a polynomial ring.)
- Let G be a finite group. (We will only use symmetric groups.)
- Let $\mathbf{k}[G]$ be the group algebra of G over **k**. Its elements are formal **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

$$(1 + s_1)(1 - s_1) = 1 + s_1 - s_1 - s_1^2 = 0$$

(since $s_1^2 = 1$);

$$(1 + s_2)(1 + s_1 + s_1 s_2) = 1 + s_2 + s_1 + s_2 s_1 + s_1 s_2 + s_2 s_1 s_2$$
$$= \sum_{w \in S_3} w.$$

Finite group algebras: $L(a)$ and $R(a)$

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

$$L(a) : \mathbf{k}[G] \to \mathbf{k}[G], \qquad x \mapsto ax \qquad (\text{"left multiplication by } a\text{"})$$

and

$$R(a) : \mathbf{k}[G] \to \mathbf{k}[G], \qquad x \mapsto xa \qquad (\text{"right multiplication by } a\text{"}).$$

(So $L(a)(x) = ax$ and $R(a)(x) = xa$.)

Note: The symbol * denotes important points.

Finite group algebras: $L(a)$ and $R(a)$

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

$$L(a) : \mathbf{k}[G] \to \mathbf{k}[G], \quad x \mapsto ax \qquad (\text{"left multiplication by } a\text{"})$$

and

$$R(a) : \mathbf{k}[G] \to \mathbf{k}[G], \quad x \mapsto xa \qquad (\text{"right multiplication by } a\text{"}).$$

(So $L(a)(x) = ax$ and $R(a)(x) = xa$.)

- Both $L(a)$ and $R(a)$ 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, $L(a)$ and $R(a)$ can be viewed as $|G| \times |G|$-matrices.

Finite group algebras: $L(a)$ and $R(a)$

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

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

and

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

(So $L(a)(x) = ax$ and $R(a)(x) = xa$.)

* Studying a, $L(a)$ and $R(a)$ 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).

- ∗ Each $a \in \mathbf{k}[G]$ has a *minimal polynomial*, i.e., a minimum-degree monic polynomial $P \in \mathbf{k}[X]$ such that $P(a) = 0$. It is unique when $\mathbf{k}$ is a field.
  The minimal polynomial of a is also the minimal polynomial of the endomorphisms $L(a)$ and $R(a)$.
- When $\mathbf{k}$ is a field, we can also study the eigenvectors and eigenvalues of $L(a)$ and $R(a)$.

- ∗ Each $a \in \mathbf{k}[G]$ has a *minimal polynomial*, i.e., a minimum-degree monic polynomial $P \in \mathbf{k}[X]$ such that $P(a) = 0$. It is unique when $\mathbf{k}$ is a field.
  The minimal polynomial of a is also the minimal polynomial of the endomorphisms $L(a)$ and $R(a)$.
- When $\mathbf{k}$ is a field, we can also study the eigenvectors and eigenvalues of $L(a)$ and $R(a)$.
- **Theorem 1.1.** Assume that $\mathbf{k}$ is a field. Let $a \in \mathbf{k}[G]$. Then, the two linear endomorphisms $L(a)$ and $R(a)$ are conjugate in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$ (that is, similar as matrices).
  (Thus, they have the same eigenstructure.)
- This is surprisingly nontrivial!

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

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

We shall write a^* for $S(a)$.

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

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

  We shall write a^* for $S(a)$.

- **Proposition 1.2.** The antipode S is an involution:

$$a^{**} = a \qquad \text{for all } a \in \mathbf{k}[G],$$

  and a $\mathbf{k}$-algebra anti-automorphism:

$$(ab)^* = b^* a^* \qquad \text{for all } a, b \in \mathbf{k}[G].$$

- **Lemma 1.3.** Assume that $\mathbf{k}$ is a field. Let $a \in \mathbf{k}[G]$. Then, $L(a) \sim L(a^*)$ in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$.
- *Proof:* Consider the standard basis $(g)_{g \in G}$ of $\mathbf{k}[G]$. The matrices representing the endomorphisms $L(a)$ and $L(a^*)$ in this basis are mutual transposes. But the Taussky–Zassenhaus theorem says that over a field, each matrix A is similar to its transpose A^T.

- **Lemma 1.3.** Assume that $\mathbf{k}$ is a field. Let $a \in \mathbf{k}[G]$. Then, $L(a) \sim L(a^*)$ in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$.
- *Proof:* Consider the standard basis $(g)_{g \in G}$ of $\mathbf{k}[G]$. The matrices representing the endomorphisms $L(a)$ and $L(a^*)$ in this basis are mutual transposes. But the Taussky–Zassenhaus theorem says that over a field, each matrix A is similar to its transpose A^T.
- **Lemma 1.4.** Let $a \in \mathbf{k}[G]$. Then, $L(a^*) \sim R(a)$ in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$.
- *Proof:* We have $R(a) = S \circ L(a^*) \circ S$ and $S = S^{-1}$.

- **Lemma 1.3.** Assume that $\mathbf{k}$ is a field. Let $a \in \mathbf{k}[G]$. Then, $L(a) \sim L(a^*)$ in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$.
- *Proof:* Consider the standard basis $(g)_{g \in G}$ of $\mathbf{k}[G]$. The matrices representing the endomorphisms $L(a)$ and $L(a^*)$ in this basis are mutual transposes. But the Taussky–Zassenhaus theorem says that over a field, each matrix A is similar to its transpose A^T.
- **Lemma 1.4.** Let $a \in \mathbf{k}[G]$. Then, $L(a^*) \sim R(a)$ in $\operatorname{End}_{\mathbf{k}}(\mathbf{k}[G])$.
- *Proof:* We have $R(a) = S \circ L(a^*) \circ S$ and $S = S^{-1}$.
- *Proof of Theorem 1.1:* Combine Lemma 1.3 with Lemma 1.4.
- **Remark (Martin Lorenz).** Theorem 1.1 generalizes to arbitrary finite-dimensional Frobenius algebras.

Symmetric groups: Notations

* Let $\mathbb{N} := \{0, 1, 2, \ldots\}$.
* Let $[k] := \{1, 2, \ldots, k\}$ for each $k \in \mathbb{N}$.

* 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. See:
  - Murray Bremner, Sara Madariaga, Luiz A. Peresi, *Structure theory for the group algebra of the symmetric group, ...*, Commentationes Mathematicae Universitatis Carolinae, 2016. (Quick and to the point.)
  - Daniel Edwin Rutherford, *Substitutional Analysis*, Edinburgh 1948. (Dated but careful and quite readable; perhaps the best treatment.)
  - Adriano M. Garsia, Ömer Egecioglu, *Lectures in Algebraic Combinatorics*, Springer 2020. (Messy but full of interesting things.)

- What can we say about the group algebra $\mathbf{k}[S_n]$ that doesn't hold for arbitrary $\mathbf{k}[G]$?
- **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.
  Or, for a different proof, see my *introduction to the symmetric group algebra* (§5.14).

- What can we say about the group algebra $\mathbf{k}[S_n]$ that doesn't hold for arbitrary $\mathbf{k}[G]$?
- **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.
- The structure of $\mathbf{k}[S_n]$ for $0 < \operatorname{char} \mathbf{k} \leq n$ is far less straightforward. See, e.g.,
  - Matthias Künzer, *Ties for the integral group ring of the symmetric group*, thesis 1998.

- What can we say about the group algebra $\mathbf{k}[S_n]$ that doesn't hold for arbitrary $\mathbf{k}[G]$?
- **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.
- The structure of $\mathbf{k}[S_n]$ for $0 < \operatorname{char} \mathbf{k} \leq n$ is far less straightforward. See, e.g.,
  - Matthias Künzer, *Ties for the integral group ring of the symmetric group*, thesis 1998.
- **Remark.** If $\mathbf{k}$ is a field of characteristic 0, then each $a \in \mathbf{k}[S_n]$ satisfies $a \sim a^*$ in $\mathbf{k}[S_n]$.
  But not for general $\mathbf{k}$.
- From now on, we shall focus on 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 $\operatorname{cyc}_i = \operatorname{id}$, whereas $\operatorname{cyc}_{i,j}$ is the transposition $t_{i,j}$.

* 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 $\operatorname{cyc}_i = \operatorname{id}$, whereas $\operatorname{cyc}_{i,j}$ is the transposition $t_{i,j}$.
* For each $k \in [n]$, we define the *k-th Young–Jucys–Murphy (YJM) element*

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

  - **Note.** We have $J_1 = 0$. Also, $J_k^* = J_k$ for each $k \in [n]$.

- 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 $\operatorname{cyc}_i = \operatorname{id}$, whereas $\operatorname{cyc}_{i,j}$ is the transposition $t_{i,j}$.
- For each $k \in [n]$, we define the *k-th Young–Jucys–Murphy (YJM) element*

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

  - **Note.** We have $J_1 = 0$. Also, $J_k^* = J_k$ for each $k \in [n]$.
- **Theorem 3.1.** The YJM elements $J_1, J_2, \ldots, J_n$ commute: We have $J_i J_j = J_j J_i$ for all i, j.
  - *Proof:* Easy computational exercise.

* **Theorem 3.2.** The minimal polynomial of J_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.)

Theorem 3.2. The minimal polynomial of J_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 J_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 J_k and J_{k+1} are simultaneously diagonalizable over $\mathbb{C}$ (since they are symmetric as real matrices and commute) and satisfy $s_k J_{k+1} = J_k s_k + 1$, where $s_k := \text{cyc}_{k,k+1}$. See https://mathoverflow.net/a/83493/ for details.

* **Theorem 3.2.** The minimal polynomial of J_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.)

- Thus, the eigenvalues of J_k are $-k+1, -k+2, \ldots, k-1$ (except for 0 when $k \leq 3$). Their multiplicities can be computed in terms of standard Young tableaux. Even better:

- **Theorem 3.2.** The minimal polynomial of J_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.)

- Thus, the eigenvalues of J_k are $-k+1, -k+2, \ldots, k-1$ (except for 0 when $k \leq 3$). Their multiplicities can be computed in terms of standard Young tableaux. Even better:
- **Theorem 3.3.** Assume that $\mathbf{k}$ is a field of characteristic 0. Then, there exists a basis $(e_{S,T})$ of $\mathbf{k}[S_n]$ indexed by pairs of standard Young tableaux of the same (partition) shape called the *seminormal basis*. This basis has the property that

$$J_k e_{S,T} = c_S(k) \cdot e_{S,T},$$

where $c_S(k) = j - i$ if the number k lies in cell (i, j) of S.

- **Theorem 3.2.** The minimal polynomial of J_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.)

- Thus, the eigenvalues of J_k are $-k+1, -k+2, \ldots, k-1$ (except for 0 when $k \leq 3$). Their multiplicities can be computed in terms of standard Young tableaux. Even better:
- **Theorem 3.3.** Assume that $\mathbf{k}$ is a field of characteristic 0. Then, there exists a basis $(e_{S,T})$ of $\mathbf{k}[S_n]$ indexed by pairs of standard Young tableaux of the same (partition) shape called the *seminormal basis*. This basis has the property that

$$J_k e_{S,T} = c_S(k) \cdot e_{S,T},$$

where $c_S(k) = j - i$ if the number k lies in cell (i, j) of S.
- Moreover, each Specht module $\mathcal{S}^\lambda$ (= irreducible representation of S_n) is spanned by part of the seminormal basis, and thus we find the eigenvalues of J_k on that $\mathcal{S}^\lambda$.

- **Theorem 3.2.** The minimal polynomial of J_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.)

- Thus, the eigenvalues of J_k are $-k+1, -k+2, \ldots, k-1$ (except for 0 when $k \leq 3$). Their multiplicities can be computed in terms of standard Young tableaux. Even better:
- The seminormal basis exists only for char $\mathbf{k} = 0$ (or, more generally, when $n!$ is invertible in $\mathbf{k}$).
But Theorem 3.2 and the algebraic multiplicities transfer automatically to all rings $\mathbf{k}$.
- **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 3.4.** For each $k \in \mathbb{N}$, we can evaluate the k-th elementary symmetric polynomial e_k at the YJM elements $J_1, J_2, \ldots, J_n$ to obtain

$$e_k(J_1, J_2, \ldots, J_n) = \sum_{\substack{\sigma \in S_n; \\ \sigma \text{ has exactly } n-k \text{ cycles}}} \sigma.$$

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

Symmetric polynomials in the YJM elements, 1

- **Theorem 3.4.** For each $k \in \mathbb{N}$, we can evaluate the k-th elementary symmetric polynomial e_k at the YJM elements $J_1, J_2, \ldots, J_n$ to obtain

$$e_k\left(J_1, J_2, \ldots, J_n\right) = \sum_{\substack{\sigma \in S_n; \\ \sigma \text{ has exactly } n-k \text{ cycles}}} \sigma.$$

- *Proof:* Nice homework exercise (once stripped of the algebra).
- There are formulas for other symmetric polynomials applied to $J_1, J_2, \ldots, J_n$ (see Garsia/Egecioglu).
  There is also a general fact:

- **Theorem 3.5 (Murphy).**

$$\{f(J_1, J_2, \ldots, J_n) \mid f \in \mathbf{k}[X_1, X_2, \ldots, X_n] \text{ symmetric}\}$$
$$= (\text{center of the group algebra } \mathbf{k}[S_n]).$$

- **Theorem 3.5 (Murphy).**

  $$\{f(J_1, J_2, \ldots, J_n) \mid f \in \mathbf{k}[X_1, X_2, \ldots, X_n] \text{ symmetric}\}$$
  $$= (\text{center of the group algebra } \mathbf{k}[S_n]).$$

- *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).
  - Ceccherini-Silberstein/Scarabotti/Tolli, *Representation Theory of the Symmetric Groups*, 2010, Theorem 4.4.5 (for the case $\mathbf{k} = \mathbb{Q}$, but the proof is easily adjusted to all $\mathbf{k}$).
    This book also has more on the $J_1, J_2, \ldots, J_n$ (but mind the errata).

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.

- 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 $\sum_{\sigma \in S_n} a_\sigma \sigma$ 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.

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 $\sum\limits_{\sigma \in S_n} a_\sigma$.

- 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, $1 + \text{cyc}_{1,2,3}$ 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 $\frac{1}{2}$.

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 $\sum_{\sigma \in S_n} a_\sigma \sigma$ 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.
- An $\mathbb{R}$-vector space endomorphism of $\mathbb{R}[S_n]$, such as $L(a)$ or $R(a)$ for some $a \in \mathbb{R}[S_n]$, 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.

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 $\sum_{\sigma \in S_n} a_\sigma \sigma$ 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.
- An $\mathbb{R}$-vector space endomorphism of $\mathbb{R}[S_n]$, such as $L(a)$ or $R(a)$ for some $a \in \mathbb{R}[S_n]$, 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 $R(J_k)$ by the YJM element J_k corresponds to swapping the k-th card with some card above it (chosen uniformly at random).

- 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.
- An $\mathbb{R}$-vector space endomorphism of $\mathbb{R}[S_n]$, such as $L(a)$ or $R(a)$ for some $a \in \mathbb{R}[S_n]$, 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 $R(J_k)$ by the YJM element J_k corresponds to swapping the k-th card with some card above it (chosen uniformly at random).
- Transposing such a matrix means time-reversing the random shuffle.

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

$$\mathcal{B}_{n,k} := \sum_{\substack{\sigma \in S_n; \\ \sigma^{-1}(1) < \sigma^{-1}(2) < \cdots < \sigma^{-1}(n-k)}} \sigma$$

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

$$\mathcal{B}_{n,n} = \mathcal{B}_{n,n-1} = \sum_{\sigma \in S_n} \sigma;$$

$$\mathcal{B}_{n,1} = \sum_{i=1}^{n} \operatorname{cyc}_{n,n-1,\ldots,i};$$

$$\mathcal{B}_{n,0} = \operatorname{id}.$$

We set $\mathcal{B}_n := \mathcal{B}_{n,1}$.

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

$$\mathcal{B}_{n,k} := \sum_{\substack{\sigma \in S_n; \\ \sigma^{-1}(1) < \sigma^{-1}(2) < \cdots < \sigma^{-1}(n-k)}} \sigma$$

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

$$\mathcal{B}_{n,n} = \mathcal{B}_{n,n-1} = \sum_{\sigma \in S_n} \sigma;$$

$$\mathcal{B}_{n,1} = \sum_{i=1}^{n} \operatorname{cyc}_{n,n-1,\ldots,i};$$

$$\mathcal{B}_{n,0} = \operatorname{id}.$$

We set $\mathcal{B}_n := \mathcal{B}_{n,1}$.

- As a random shuffle, $\mathcal{B}_{n,k}$ (to be precise, $R(\mathcal{B}_{n,k})$) takes the bottom k cards and moves them to random positions.
  Its antipode $\mathcal{B}_{n,k}^*$ takes k random cards and moves them to the bottom positions.

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

$$\mathcal{B}_{n,k} := \sum_{\substack{\sigma \in S_n; \\ \sigma^{-1}(1) < \sigma^{-1}(2) < \cdots < \sigma^{-1}(n-k)}} \sigma$$

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

$$\mathcal{B}_{n,n} = \mathcal{B}_{n,n-1} = \sum_{\sigma \in S_n} \sigma;$$

$$\mathcal{B}_{n,1} = \sum_{i=1}^{n} \mathrm{cyc}_{n,n-1,\ldots,i};$$

$$\mathcal{B}_{n,0} = \mathrm{id}\,.$$

We set $\mathcal{B}_n := \mathcal{B}_{n,1}$.

- $\mathcal{B}_n := \mathcal{B}_{n,1}$ is known as the *bottom-to-random shuffle* or the *Tsetlin library*.

Bottom-to-random and random-to-bottom shuffles: facts

- **Theorem 5.1 (Diaconis, Fill, Pitman).** We have

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

- **Theorem 5.1 (Diaconis, Fill, Pitman).** We have

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

- **Corollary 5.2.** The $n+1$ elements $\mathcal{B}_{n,0}, \mathcal{B}_{n,1}, \ldots, \mathcal{B}_{n,n}$ commute and are polynomials in $\mathcal{B}_n$, namely

$$\mathcal{B}_{n,k} = \prod_{i=0}^{k-1} (\mathcal{B}_n - i) \qquad \text{for each } k \in \{0, 1, \ldots, n\}.$$

Bottom-to-random and random-to-bottom shuffles: facts

- **Theorem 5.1 (Diaconis, Fill, Pitman).** We have

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

- **Corollary 5.2.** The $n+1$ elements $\mathcal{B}_{n,0}, \mathcal{B}_{n,1}, \ldots, \mathcal{B}_{n,n}$ commute and are polynomials in $\mathcal{B}_n$, namely

$$\mathcal{B}_{n,k} = \prod_{i=0}^{k-1} (\mathcal{B}_n - i) \qquad \text{for each } k \in \{0, 1, \ldots, n\}\,.$$

- **Theorem 5.3 (Wallach).** The minimal polynomial of $\mathcal{B}_n$ over $\mathbb{Q}$ is

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

- **Theorem 5.1 (Diaconis, Fill, Pitman).** We have

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

- **Corollary 5.2.** The $n+1$ elements $\mathcal{B}_{n,0}, \mathcal{B}_{n,1}, \ldots, \mathcal{B}_{n,n}$ commute and are polynomials in $\mathcal{B}_n$, namely

$$\mathcal{B}_{n,k} = \prod_{i=0}^{k-1} (\mathcal{B}_n - i) \qquad \text{for each } k \in \{0, 1, \ldots, n\}.$$

- **Theorem 5.3 (Wallach).** The minimal polynomial of $\mathcal{B}_n$ 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.

Bottom-to-random and random-to-bottom shuffles: more

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

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

$$\mathcal{B}^*_{n,k} := \sum_{\substack{\sigma \in S_n; \\ \sigma(1) < \sigma(2) < \cdots < \sigma(n-k)}} \sigma$$

of $\mathcal{B}_{n,k}$ are known as the *k-random-to-bottom shuffles* and have the same properties (since S is an algebra anti-automorphism).

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

$$\mathcal{B}^*_{n,k} := \sum_{\substack{\sigma \in S_n; \\ \sigma(1)<\sigma(2)<\cdots<\sigma(n-k)}} \sigma$$

  of $\mathcal{B}_{n,k}$ are known as the *k-random-to-bottom shuffles* and have the same properties (since S is an algebra anti-automorphism).
- Moreover, there are *top-to-random* and *random-to-top* shuffles defined in the same way but with renaming $1, 2, \ldots, n$ as $n, n-1, \ldots, 1$. They are just images of the $\mathcal{B}_{n,k}$ and $\mathcal{B}^*_{n,k}$ under the automorphism $a \mapsto w_0 a w_0^{-1}$ of $\mathbf{k}[S_n]$, where w_0 is the permutation with one-line notation $(n, n-1, \ldots, 1)$. Thus, top vs. bottom is mainly a matter of notation.

- 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.

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

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

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

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

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

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

- **Example:** Writing permutations in one-line notation,

$$\begin{aligned}\mathcal{R}_{4,2} = 6[1,2,3,4] + 5[1,2,4,3] + 5[1,3,2,4] + 4[1,3,4,2] \\ + 4[1,4,2,3] + 3[1,4,3,2] + 5[2,1,3,4] + 4[2,1,4,3] \\ + 4[2,3,1,4] + 3[2,3,4,1] + 3[2,4,1,3] + 2[2,4,3,1] \\ + 4[3,1,2,4] + 3[3,1,4,2] + 3[3,2,1,4] + 2[3,2,4,1] \\ + 2[3,4,1,2] + [3,4,2,1] + 3[4,1,2,3] + 2[4,1,3,2] \\ + 2[4,2,1,3] + [4,2,3,1] + [4,3,1,2].\end{aligned}$$

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

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

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

- **Note:** $\mathcal{R}_{n,0} = \mathrm{id}$ and $\mathcal{R}_{n,n-1} = n \sum_{\sigma \in S_n} \sigma$ and $\mathcal{R}_{n,n} = \sum_{\sigma \in S_n} \sigma$.

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

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

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

- **Note:** $\mathcal{R}_{n,0} = \mathrm{id}$ and $\mathcal{R}_{n,n-1} = n \sum_{\sigma \in S_n} \sigma$ and $\mathcal{R}_{n,n} = \sum_{\sigma \in S_n} \sigma$.
- The card-shuffling interpretation of $\mathcal{R}_{n,k}$ is "pick any k cards from the deck and move them to k randomly chosen positions".

* **Theorem 6.1 (Reiner, Saliola, Welker).** The $n+1$ elements $\mathcal{R}_{n,0}, \mathcal{R}_{n,1}, \ldots, \mathcal{R}_{n,n}$ commute (but are not polynomials in $\mathcal{R}_{n,1}$ in general).

- **Theorem 6.1 (Reiner, Saliola, Welker).** The $n+1$ elements $\mathcal{R}_{n,0}, \mathcal{R}_{n,1}, \ldots, \mathcal{R}_{n,n}$ commute (but are not polynomials in $\mathcal{R}_{n,1}$ in general).
- **Theorem 6.2 (Dieker, Saliola, Lafrenière).** The minimal polynomial of each $\mathcal{R}_{n,k}$ over $\mathbb{Q}$ is a product of $X - i$'s for distinct integers i. For example, the one of $\mathcal{R}_{n,1}$ divides

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

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

Random-to-random shuffles: References

- Main references: the "classics"
  - 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.

  and the two recent preprints
  - Ilani Axelrod-Freed, Sarah Brauner, Judy Hsin-Hui Chiang, Patricia Commins, Veronica Lang, *Spectrum of random-to-random shuffling in the Hecke algebra*, arXiv:2407.08644.
  - Sarah Brauner, Patricia Commins, Darij Grinberg, Franco Saliola, *The q-deformed random-to-random family in the Hecke algebra*, arXiv:2503.17580.

- The "classical" proofs are complicated, technical and long. In this talk, I will outline some parts of the two recent preprints, including a simpler proof of Theorem 6.1 and most of Theorem 6.2. (The full proof of Theorem 6.2 is still long and hard.)
  Moreover, I will show how all these results can be generalized to the **(Iwahori–)Hecke algebra** $\mathcal{H}_n = \mathcal{H}_n(q)$, a q-deformation of $\mathbf{k}[S_n]$.

- The first step is a formula that is easy to prove combinatorially:

Proposition 6.3. For each $k \in \{0, 1, \ldots, n\}$, we have

$$\mathcal{R}_{n,k} = \frac{1}{k!} \cdot \mathcal{B}^*_{n,k} \, \mathcal{B}_{n,k}.$$

- The first step is a formula that is easy to prove combinatorially:

* **Proposition 6.3.** For each $k \in \{0, 1, \ldots, n\}$, we have

$$\mathcal{R}_{n,k} = \frac{1}{k!} \cdot \mathcal{B}_{n,k}^{*} \, \mathcal{B}_{n,k}.$$

- However, the $\mathcal{B}_{n,k}$ do not commute with the $\mathcal{B}_{n,k}^{*}$, so this is not by itself an answer.

- Let $q \in \mathbf{k}$ be a parameter.
  The n-th *Hecke algebra* (or *Iwahori–Hecke algebra* to be more historically correct) is a q-deformation of the group algebra $\mathbf{k}[S_n]$. It has generators $T_1, T_2, \ldots, T_{n-1}$ and relations

$$\begin{aligned} T_i^2 &= (q-1) T_i + q && \text{for all } i \in [n-1]; \\ T_i T_j &= T_j T_i && \text{whenever } |i-j| > 1; \\ T_i T_{i+1} T_i &= T_{i+1} T_i T_{i+1} && \text{for all } i \in [n-2]. \end{aligned}$$

  We call this algebra $\mathcal{H}_n$.

The Hecke algebra: Definition

- Let $q \in \mathbf{k}$ be a parameter.
  The n-th *Hecke algebra* (or *Iwahori–Hecke algebra* to be more historically correct) is a q-deformation of the group algebra $\mathbf{k}[S_n]$. It has generators $T_1, T_2, \ldots, T_{n-1}$ and relations

$$\begin{aligned} T_i^2 &= (q-1) T_i + q && \text{for all } i \in [n-1]; \\ T_i T_j &= T_j T_i && \text{whenever } |i-j| > 1; \\ T_i T_{i+1} T_i &= T_{i+1} T_i T_{i+1} && \text{for all } i \in [n-2]. \end{aligned}$$

  We call this algebra $\mathcal{H}_n$.
- For $q = 1$, this is the group algebra $\mathbf{k}[S_n]$ (and the generator T_i is the simple transposition $s_i = \mathrm{cyc}_{i,i+1}$).

- Let $q \in \mathbf{k}$ be a parameter.
  The n-th *Hecke algebra* (or *Iwahori–Hecke algebra* to be more historically correct) is a q-deformation of the group algebra $\mathbf{k}[S_n]$. It has generators $T_1, T_2, \ldots, T_{n-1}$ and relations

$$\begin{aligned} T_i^2 &= (q-1)\,T_i + q && \text{for all } i \in [n-1]\,; \\ T_i T_j &= T_j T_i && \text{whenever } |i-j| > 1; \\ T_i T_{i+1} T_i &= T_{i+1} T_i T_{i+1} && \text{for all } i \in [n-2]\,. \end{aligned}$$

  We call this algebra $\mathcal{H}_n$.
- For $q = 1$, this is the group algebra $\mathbf{k}[S_n]$ (and the generator T_i is the simple transposition $s_i = \operatorname{cyc}_{i,i+1}$).
- For general q, it still is a free $\mathbf{k}$-module of rank $n!$, with a basis $(T_w)_{w \in S_n}$ indexed by permutations $w \in S_n$. The basis vectors are defined by $T_w := T_{i_1} T_{i_2} \cdots T_{i_k}$, where $s_{i_1} s_{i_2} \cdots s_{i_k}$ is a reduced expression for w. For $q = 1$, this T_w is just w.

* Much of the theory of $\mathbf{k}[S_n]$ exists in a subtler form for $\mathcal{H}_n$. Sometimes, the added difficulty brings the best proofs to light.

* Much of the theory of $\mathbf{k}[S_n]$ exists in a subtler form for $\mathcal{H}_n$. Sometimes, the added difficulty brings the best proofs to light.
* $\mathcal{H}_n$ shows up in many places: as a better-behaved model for the modular representation theory of S_n; as a nonunital subalgebra of $\mathbf{k}[\mathrm{GL}_n(\mathbb{F}_q)]$ (when q is a prime power); as an algebraic model for some random walks (when $q \in [0, 1]$), ...
  It also can be defined for other types of groups.
  Cf. Taylor–Wiles, *Ring-Theoretic Properties of Certain Hecke Algebras*, 1995.

- $*$ Much of the theory of $\mathbf{k}[S_n]$ exists in a subtler form for $\mathcal{H}_n$. Sometimes, the added difficulty brings the best proofs to light.
- $\mathcal{H}_n$ shows up in many places: as a better-behaved model for the modular representation theory of S_n; as a nonunital subalgebra of $\mathbf{k}[\mathrm{GL}_n(\mathbb{F}_q)]$ (when q is a prime power); as an algebraic model for some random walks (when $q \in [0,1]$), ...
  It also can be defined for other types of groups.
  Cf. Taylor–Wiles, *Ring-Theoretic Properties of Certain Hecke Algebras*, 1995.
- I think of $\mathcal{H}_n$ as a "biased" version of $\mathbf{k}[S_n]$, which breaks the symmetry in favor of "entropy".

* **Theorem 7.1 (Dipper–James).** Assume that $\mathbf{k}$ is a field, and that $q \neq 0$ and $q^{n!} \neq 1$. Then, the Hecke algebra $\mathcal{H}_n$ is semisimple and in fact isomorphic to $\mathbf{k}[S_n]$ (in a nontrivial way).
  Thus, its irreducible representations are again some kind of Specht modules $\mathcal{S}^\lambda$, deforming the ones for $\mathbf{k}[S_n]$.
* This was proved for generic q by Dipper/James (*Representations of Hecke algebras of general linear groups*, 1984), and in the general case by Murphy (*The Representations of Hecke algebras of type A_n*, 1995), modulo the semisimplicity, which can be found in most texts now (e.g., Mathas, *Iwahori-Hecke Algebras and Schur Algebras of the Symmetric Group*, 1999).
* In the following, unless I say otherwise, I am working in $\mathcal{H}_n$.

* The antipode $S : \mathbf{k}[S_n] \to \mathbf{k}[S_n]$ can be generalized to the Hecke algebra. The generalization is the **k**-linear map

$$S : \mathcal{H}_n \to \mathcal{H}_n, \qquad T_w \mapsto T_{w^{-1}} \qquad (\text{thus } T_i \mapsto T_i).$$

* Again, this is a **k**-algebra anti-automorphism and an involution.
* Again, we write a^* for $S(a)$.

* When $q \in \mathbf{k}$ is invertible, we can define the *Young–Jucys–Murphy (YJM) elements in the Hecke algebra* $\mathcal{H}_n$. These are the elements $J_1, J_2, \ldots, J_n \in \mathcal{H}_n$ defined by

$$J_k := \sum_{i=1}^{k-1} q^{i-k} T_{\mathrm{cyc}_{i,k}} \in \mathcal{H}_n.$$

Setting $q = 1$ recovers the YJM elements of $\mathbf{k}[S_n]$.

The Hecke algebra: The YJM elements

- When $q \in \mathbf{k}$ is invertible, we can define the *Young–Jucys–Murphy (YJM) elements in the Hecke algebra* $\mathcal{H}_n$. These are the elements $J_1, J_2, \ldots, J_n \in \mathcal{H}_n$ defined by

$$J_k := \sum_{i=1}^{k-1} q^{i-k} T_{\mathrm{cyc}_{i,k}} \in \mathcal{H}_n.$$

  Setting $q = 1$ recovers the YJM elements of $\mathbf{k}[S_n]$.
- Again, $J_1 = 0$. Also, $J_k^* = J_k$ for each $k \in [n]$.
- The elements $J_1, J_2, \ldots, J_n$ commute.
- The eigenvalues of each J_k are

$$[-k+1]_q, \ [-k+2]_q, \ \ldots, \ [k-1]_q,$$

  where we are using the *q-integers*

$$[m]_q := \frac{1-q^m}{1-q} = \begin{cases} 1 + q + q^2 + \cdots + q^{m-1}, & \text{if } m \geq 0; \\ -q^{-1} - q^{-2} - \cdots - q^m, & \text{if } m \leq 0. \end{cases}$$

  Their multiplicities are as in the $\mathbf{k}[S_n]$ case.

- We define the *q-deformed k-bottom-to-random shuffles* $\mathcal{B}_{n,k}$ and the *q-deformed k-random-to-bottom shuffles* $\mathcal{B}^*_{n,k}$ for $k \in \{0, 1, \ldots, n\}$ by

$$\mathcal{B}_{n,k} := \sum_{\substack{\sigma \in S_n; \\ \sigma^{-1}(1) < \sigma^{-1}(2) < \cdots < \sigma^{-1}(n-k)}} T_\sigma \in \mathcal{H}_n$$

and

$$\mathcal{B}^*_{n,k} := \sum_{\substack{\sigma \in S_n; \\ \sigma(1) < \sigma(2) < \cdots < \sigma(n-k)}} T_\sigma \in \mathcal{H}_n.$$

Note that $\mathcal{B}_{n,0} = \mathcal{B}^*_{n,0} = 1$. We also set $\mathcal{B}_{n,k} = \mathcal{B}^*_{n,k} = 0$ for $k > n$.

* **Theorem 7.2 (Axelrod-Freed–Brauner–Chiang–Commins–Lang 2024).** We have

$$\mathcal{B}_{n,k} = \mathcal{B}_{n-k+1}\mathcal{B}_{n-k+2}\cdots\mathcal{B}_n,$$

where we arrange the Hecke algebras in a chain of inclusions:

$$\mathbf{k} = \mathcal{H}_0 \subseteq \mathcal{H}_1 \subseteq \mathcal{H}_2 \subseteq \cdots .$$

- **Theorem 7.3 (essentially Brauner–Commins–Reiner 2023, to be made explicit in Grinberg 2025+ on q-deformed somewhere-to-below shuffles).** The $n+1$ elements $\mathcal{B}_{n,0}, \mathcal{B}_{n,1}, \ldots, \mathcal{B}_{n,n}$ commute and are polynomials in $\mathcal{B}_n$, namely

$$\mathcal{B}_{n,k} = \prod_{i=0}^{k-1} \left(\mathcal{B}_n - [i]_q \right) \qquad \text{for each } k \in \{0, 1, \ldots, n\} .$$

* **Theorem 7.3 (essentially Brauner–Commins–Reiner 2023, to be made explicit in Grinberg 2025+ on q-deformed somewhere-to-below shuffles).** The $n+1$ elements $\mathcal{B}_{n,0}, \mathcal{B}_{n,1}, \ldots, \mathcal{B}_{n,n}$ commute and are polynomials in $\mathcal{B}_n$, namely

$$\mathcal{B}_{n,k} = \prod_{i=0}^{k-1} \left(\mathcal{B}_n - [i]_q\right) \qquad \text{for each } k \in \{0, 1, \ldots, n\}.$$

* **Theorem 7.4 (same).** The minimal polynomial of $\mathcal{B}_n$ over $\mathbf{k}$ (when $\mathbf{k}$ is a field) divides

$$\prod_{i \in \{0,1,\ldots,n-2,n\}} \left(X - [i]_q\right).$$

The Hecke algebra: Bottom-to-random and back, 4

- The proofs here are similar to the $q = 1$ case, but attention needs to be paid to the lengths of the permutations as they get multiplied.

- The proofs here are similar to the $q = 1$ case, but attention needs to be paid to the lengths of the permutations as they get multiplied.
- There is a bespoke interpretation of $\mathcal{B}_n$ as a "q-Tsetlin library", where decks of cards are replaced by flags of vector subspaces of $\mathbb{F}_q^n$. (See arXiv:2407.08644 for details.)

* We can also generalize the k-random-to-random shuffles $\mathcal{R}_{n,k}$:
For each $k \geq 0$, we set

$$\mathcal{R}_{n,k} := \frac{1}{[k]!_q} \mathcal{B}_{n,k}^* \mathcal{B}_{n,k} \in \mathcal{H}_n,$$

where we use the q-factorial $[k]!_q = [1]_q [2]_q \cdots [k]_q$.

- We can also generalize the k-random-to-random shuffles $\mathcal{R}_{n,k}$: For each $k \geq 0$, we set

$$\mathcal{R}_{n,k} := \frac{1}{[k]!_q} \mathcal{B}^*_{n,k} \mathcal{B}_{n,k} \in \mathcal{H}_n,$$

  where we use the q-factorial $[k]!_q = [1]_q [2]_q \cdots [k]_q$.
- The coefficients of $\mathcal{R}_{n,k}$ are actually in $\mathbb{Z}[q]$, since the denominator can be cancelled.

The Hecke algebra: Random-to-random, example

- **Example:** Again using one-line notation,

$$
\begin{aligned}
\mathcal{R}_{4,2} = {} & (q^4 + q^3 + 2q^2 + q + 1)\ T_{[1,2,3,4]} + (q^3 + 2q^2 + q + 1)\ T_{[1,2,4,3]} \\
& + (q^4 + q^3 + q^2 + q + 1)\ T_{[1,3,2,4]} + (q^3 + q^2 + q + 1)\ T_{[1,3,4,2]} \\
& + (q^3 + q^2 + q + 1)\ T_{[1,4,2,3]} + (q^3 + q + 1)\ T_{[1,4,3,2]} \\
& + (q^4 + q^3 + 2q^2 + q)\ T_{[2,1,3,4]} + (q^3 + 2q^2 + q)\ T_{[2,1,4,3]} \\
& + (q^4 + q^3 + q^2 + q)\ T_{[2,3,1,4]} + (q^3 + q^2 + q)\ T_{[2,3,4,1]} \\
& + (q^3 + q^2 + q)\ T_{[2,4,1,3]} + (q^3 + q)\ T_{[2,4,3,1]} \\
& + (q^4 + q^3 + q^2 + q)\ T_{[3,1,2,4]} + (q^3 + q^2 + q)\ T_{[3,1,4,2]} \\
& + (q^4 + q^3 + q^2 + q - 1)\ T_{[3,2,1,4]} + (q^3 + q^2 + q - 1)\ T_{[3,2,4,1]} \\
& + (q^3 + q)\ T_{[3,4,1,2]} + (q^3 + q - 1)\ T_{[3,4,2,1]} \\
& + (q^3 + q^2 + q)\ T_{[4,1,2,3]} + (q^3 + q)\ T_{[4,1,3,2]} \\
& + (q^3 + q^2 + q - 1)\ T_{[4,2,1,3]} + (q^3 + q - 1)\ T_{[4,2,3,1]} \\
& + (q^3 + q - 1)\ T_{[4,3,1,2]} + (q^3 + q - 2)\ T_{[4,3,2,1]}.
\end{aligned}
$$

Note: The last coefficient becomes 0 in the $q = 1$ case!

The Hecke algebra: The main theorems

- We have been able to extend the main properties of k-random-to-random shuffles from $\mathbf{k}[S_n]$ to $\mathcal{H}_n$:

- We have been able to extend the main properties of k-random-to-random shuffles from $\mathbf{k}[S_n]$ to $\mathcal{H}_n$:

* **Theorem 7.5 (Brauner–Commins–G.–Saliola 2025).** The $n+1$ elements $\mathcal{R}_{n,0}, \mathcal{R}_{n,1}, \ldots, \mathcal{R}_{n,n}$ of $\mathcal{H}_n$ commute (but are not polynomials in $\mathcal{R}_{n,1}$ in general).

- We have been able to extend the main properties of k-random-to-random shuffles from $\mathbf{k}[S_n]$ to $\mathcal{H}_n$:

* **Theorem 7.5 (Brauner–Commins–G.–Saliola 2025).** The $n+1$ elements $\mathcal{R}_{n,0}, \mathcal{R}_{n,1}, \ldots, \mathcal{R}_{n,n}$ of $\mathcal{H}_n$ commute (but are not polynomials in $\mathcal{R}_{n,1}$ in general).
* **Theorem 7.6 (Brauner–Commins–G.–Saliola 2025).** All eigenvalues of each $\mathcal{R}_{n,k}$ over a field $\mathbf{k}$ can be written as polynomials in q with coefficients in $\mathbb{N}$.

- We have been able to extend the main properties of k-random-to-random shuffles from $\mathbf{k}[S_n]$ to $\mathcal{H}_n$:

* **Theorem 7.5 (Brauner–Commins–G.–Saliola 2025).** The $n+1$ elements $\mathcal{R}_{n,0}, \mathcal{R}_{n,1}, \ldots, \mathcal{R}_{n,n}$ of $\mathcal{H}_n$ commute (but are not polynomials in $\mathcal{R}_{n,1}$ in general).
* **Theorem 7.6 (Brauner–Commins–G.–Saliola 2025).** All eigenvalues of each $\mathcal{R}_{n,k}$ over a field $\mathbf{k}$ can be written as polynomials in q with coefficients in $\mathbb{N}$.
* **Theorem 7.7 (Brauner–Commins–G.–Saliola 2025).** If $\mathbf{k}$ is a field and q is generic, then there is a basis of $\mathcal{H}_n$ in which all the $\mathcal{R}_{n,k}$ (that is, all the $R(\mathcal{R}_{n,k})$) are diagonal.

The Hecke algebra: The main theorems

- We have been able to extend the main properties of k-random-to-random shuffles from $\mathbf{k}[S_n]$ to $\mathcal{H}_n$:

* **Theorem 7.5 (Brauner–Commins–G.–Saliola 2025).** The $n+1$ elements $\mathcal{R}_{n,0}, \mathcal{R}_{n,1}, \ldots, \mathcal{R}_{n,n}$ of $\mathcal{H}_n$ commute (but are not polynomials in $\mathcal{R}_{n,1}$ in general).
* **Theorem 7.6 (Brauner–Commins–G.–Saliola 2025).** All eigenvalues of each $\mathcal{R}_{n,k}$ over a field $\mathbf{k}$ can be written as polynomials in q with coefficients in $\mathbb{N}$.
* **Theorem 7.7 (Brauner–Commins–G.–Saliola 2025).** If $\mathbf{k}$ is a field and q is generic, then there is a basis of $\mathcal{H}_n$ in which all the $\mathcal{R}_{n,k}$ (that is, all the $R(\mathcal{R}_{n,k})$) are diagonal.

- We also have complicated formulas for the eigenvalues and their multiplicities; more on that later.

- We have been able to extend the main properties of k-random-to-random shuffles from $\mathbf{k}[S_n]$ to $\mathcal{H}_n$:
- **Theorem 7.5 (Brauner–Commins–G.–Saliola 2025).** The $n+1$ elements $\mathcal{R}_{n,0}, \mathcal{R}_{n,1}, \ldots, \mathcal{R}_{n,n}$ of $\mathcal{H}_n$ commute (but are not polynomials in $\mathcal{R}_{n,1}$ in general).
- **Theorem 7.6 (Brauner–Commins–G.–Saliola 2025).** All eigenvalues of each $\mathcal{R}_{n,k}$ over a field $\mathbf{k}$ can be written as polynomials in q with coefficients in $\mathbb{N}$.
- **Theorem 7.7 (Brauner–Commins–G.–Saliola 2025).** If $\mathbf{k}$ is a field and q is generic, then there is a basis of $\mathcal{H}_n$ in which all the $\mathcal{R}_{n,k}$ (that is, all the $R(\mathcal{R}_{n,k})$) are diagonal.
- For $k=1$, the above was done in:
  - Ilani Axelrod-Freed, Sarah Brauner, Judy Hsin-Hui Chiang, Patricia Commins, Veronica Lang, *Spectrum of random-to-random shuffling in the Hecke algebra*, arXiv:2407.08644.

We use this work in our proofs (mostly for computing the eigenvalues).

* **Theorem 8.1 (Brauner–Commins–G.–Saliola 2025, based on Axelrod-Freed–Brauner–Chiang–Commins–Lang 2024).** For any $1 \leq k \leq n$, we have

$$\mathcal{B}_n \, \mathcal{R}_{n,k} = \underbrace{\left(q^k \, \mathcal{R}_{n-1,k} + \left([n+1-k]_q + q^{n+1-k} J_n \right) \, \mathcal{R}_{n-1,k-1} \right)}_{=:\mathcal{W}_{n,k}} \mathcal{B}_n .$$

* **Theorem 8.1 (Brauner–Commins–G.–Saliola 2025, based on Axelrod-Freed–Brauner–Chiang–Commins–Lang 2024).** For any $1 \leq k \leq n$, we have

$$\mathcal{B}_n \, \mathcal{R}_{n,k} = \underbrace{\left(q^k \, \mathcal{R}_{n-1,k} + \left([n+1-k]_q + q^{n+1-k} J_n \right) \, \mathcal{R}_{n-1,k-1} \right)}_{=:\mathcal{W}_{n,k}} \mathcal{B}_n .$$

- The proof takes about 5 pages, relying on some more elementary computations from prior work (ca. 10–15 pages in total).

* **Theorem 8.1 (Brauner–Commins–G.–Saliola 2025, based on Axelrod-Freed–Brauner–Chiang–Commins–Lang 2024).** For any $1 \leq k \leq n$, we have

$$\mathcal{B}_n \, \mathcal{R}_{n,k} = \underbrace{\left(q^k \, \mathcal{R}_{n-1,k} + \left([n+1-k]_q + q^{n+1-k} J_n \right) \mathcal{R}_{n-1,k-1} \right)}_{=: \mathcal{W}_{n,k}} \mathcal{B}_n.$$

- The proof takes about 5 pages, relying on some more elementary computations from prior work (ca. 10–15 pages in total).
- This recursion does not actually compute $\mathcal{R}_{n,k}$. But it says enough about $\mathcal{R}_{n,k}$ to be the key to our proofs.
- Note also that $\mathcal{R}_{n,k} \in \mathcal{B}_n^* \, \mathcal{H}_n$ by its definition (when $k \geq 1$). This makes the recursion so useful.

The Hecke algebra: Commutativity of random-to-random

- Theorem 8.1 leads fairly easily to a proof of commutativity (Theorem 7.5).
  Indeed, inducting on n, we observe that the $\mathcal{W}_{n,k}$s all commute by the induction hypothesis (and the easy fact that J_n commutes with everything in $\mathcal{H}_{n-1}$). Thus, using $\mathcal{B}_n \mathcal{R}_{n,k} = \mathcal{W}_{n,k} \mathcal{B}_n$, we find

  $$\begin{aligned} \mathcal{B}_n \mathcal{R}_{n,i} \mathcal{R}_{n,j} &= \mathcal{W}_{n,i} \mathcal{B}_n \mathcal{R}_{n,j} = \mathcal{W}_{n,i} \mathcal{W}_{n,j} \mathcal{B}_n \\ &= \mathcal{W}_{n,j} \mathcal{W}_{n,i} \mathcal{B}_n = \mathcal{W}_{n,j} \mathcal{B}_n \mathcal{R}_{n,i} = \mathcal{B}_n \mathcal{R}_{n,j} \mathcal{R}_{n,i}. \end{aligned}$$

  Remains to get rid of the $\mathcal{B}_n$ factor at the front. Recall that all $\mathcal{R}_{n,i}$ (except for the trivial $\mathcal{R}_{n,0}$) lie in $\mathcal{B}_n^* \mathcal{H}_n$. But it can be shown that when q is a positive real, $\mathcal{B}_n \mathcal{B}_n^* a = 0$ entails $\mathcal{B}_n^* a = 0$ (positivity trick! cf. linear algebra: $\operatorname{Ker}\left(A^T A\right) = \operatorname{Ker} A$ for real matrix A).
  Now extend back to arbitrary q using polynomial identity trick.
- Alternatively, the tricks can also be avoided (see our preprint).

The Hecke algebra: The approach to eigenvalues, 1

- Now to Theorem 7.6: Why are all eigenvalues of $\mathcal{R}_{n,k}$ integer polynomials in q ? (Let's drop the nonnegativity for now.)

- Now to Theorem 7.6: Why are all eigenvalues of $\mathcal{R}_{n,k}$ integer polynomials in q ? (Let's drop the nonnegativity for now.)
- We have a theory of "split elements" that can help answer such questions in general. Here is an outline:

- Now to Theorem 7.6: Why are all eigenvalues of $\mathcal{R}_{n,k}$ integer polynomials in q ? (Let's drop the nonnegativity for now.)
- We have a theory of "split elements" that can help answer such questions in general. Here is an outline:

* An element a of a $\mathbf{k}$-algebra A is said to be *split* (over $\mathbf{k}$) if there exist some scalars $u_1, u_2, \ldots, u_n \in \mathbf{k}$ (not necessarily distinct) such that $\prod_{i=1}^{n} (a - u_i) = 0$.

- Now to Theorem 7.6: Why are all eigenvalues of $\mathcal{R}_{n,k}$ integer polynomials in q ? (Let's drop the nonnegativity for now.)
- We have a theory of "split elements" that can help answer such questions in general. Here is an outline:

* An element a of a $\mathbf{k}$-algebra A is said to be *split* (over $\mathbf{k}$) if there exist some scalars $u_1, u_2, \ldots, u_n \in \mathbf{k}$ (not necessarily distinct) such that $\prod_{i=1}^{n} (a - u_i) = 0$.
* When $\mathbf{k}$ is an integral domain and A is a free $\mathbf{k}$-module of finite rank, this is the same as saying that $R(a)$ has all eigenvalues in $\mathbf{k}$.

The Hecke algebra: The approach to eigenvalues, 1

- Now to Theorem 7.6: Why are all eigenvalues of $\mathcal{R}_{n,k}$ integer polynomials in q ? (Let's drop the nonnegativity for now.)
- We have a theory of "split elements" that can help answer such questions in general. Here is an outline:
- ∗ An element a of a $\mathbf{k}$-algebra A is said to be *split* (over $\mathbf{k}$) if there exist some scalars $u_1, u_2, \ldots, u_n \in \mathbf{k}$ (not necessarily distinct) such that $\prod_{i=1}^{n} (a - u_i) = 0$.
- ∗ When $\mathbf{k}$ is an integral domain and A is a free $\mathbf{k}$-module of finite rank, this is the same as saying that $R(a)$ has all eigenvalues in $\mathbf{k}$.
- In particular, for $\mathbf{k} = \mathbb{Z}[q]$ and $A = \mathcal{H}_n$, this means that all eigenvalues of a are $\in \mathbb{Z}[q]$. This is what we want to show for $a = \mathcal{R}_{n,k}$.

- Now to Theorem 7.6: Why are all eigenvalues of $\mathcal{R}_{n,k}$ integer polynomials in q ? (Let's drop the nonnegativity for now.)
- We have a theory of "split elements" that can help answer such questions in general. Here is an outline:
- ∗ An element a of a $\mathbf{k}$-algebra A is said to be *split* (over $\mathbf{k}$) if there exist some scalars $u_1, u_2, \ldots, u_n \in \mathbf{k}$ (not necessarily distinct) such that $\prod_{i=1}^{n} (a - u_i) = 0$.
- ∗ When $\mathbf{k}$ is an integral domain and A is a free $\mathbf{k}$-module of finite rank, this is the same as saying that $R(a)$ has all eigenvalues in $\mathbf{k}$.
- In particular, for $\mathbf{k} = \mathbb{Z}[q]$ and $A = \mathcal{H}_n$, this means that all eigenvalues of a are $\in \mathbb{Z}[q]$. This is what we want to show for $a = \mathcal{R}_{n,k}$.
- So we must show that $\mathcal{R}_{n,k}$ is split over $\mathbb{Z}[q]$.

- So we must show that $\mathcal{R}_{n,k}$ is split over $\mathbb{Z}[q]$.

- So we must show that $\mathcal{R}_{n,k}$ is split over $\mathbb{Z}[q]$.
- It suffices to show that $\mathcal{R}_{n,k}$ is split over $\mathbb{Z}\left[q, q^{-1}\right]$ (Laurent polynomials), since then an integral closure argument will yield that the eigenvalues are in fact $\in \mathbb{Z}[q]$. This is easier because we have YJM elements over $\mathbb{Z}\left[q, q^{-1}\right]$.

General theory of split elements, 1

- We prove several general properties of split elements (nice exercises on commutative algebra!):

- We prove several general properties of split elements (nice exercises on commutative algebra!):

* **Theorem 9.1.** If two commuting elements $a, b \in A$ are split, then both $a + b$ and ab are split.
* **Corollary 9.2.** A commutative subalgebra of A generated by split elements consists entirely of split elements.

General theory of split elements, 1

- We prove several general properties of split elements (nice exercises on commutative algebra!):

* **Theorem 9.1.** If two commuting elements $a, b \in A$ are split, then both $a + b$ and ab are split.
* **Corollary 9.2.** A commutative subalgebra of A generated by split elements consists entirely of split elements.
* **Theorem 9.3.** If b, c, f are elements of A such that f is split and such that $bc = fb$ and $c \in Ab$, then c is split.

General theory of split elements, 1

- We prove several general properties of split elements (nice exercises on commutative algebra!):

* **Theorem 9.1.** If two commuting elements $a, b \in A$ are split, then both $a + b$ and ab are split.
* **Corollary 9.2.** A commutative subalgebra of A generated by split elements consists entirely of split elements.
* **Theorem 9.3.** If b, c, f are elements of A such that f is split and such that $bc = fb$ and $c \in Ab$, then c is split.

- Theorem 9.3 is tailored to our use:

$bc = fb$	$c \in Ab$
$\mathcal{B}_n \mathcal{R}_{n,k} = \mathcal{W}_{n,k} \mathcal{B}_n$	$\mathcal{R}_{n,k} \in \mathcal{H}_n \, \mathcal{B}_n$

.

The splitness of $\mathcal{W}_{n,k}$ follows from the splitness of the commuting elements J_n, $\mathcal{R}_{n-1,k-1}$ and $\mathcal{R}_{n-1,k}$ (induction!) by Corollary 9.2. We need the splitness of the YJM elements, which was proved (e.g.) by Murphy.

- Theorem 9.3 looks baroque, but in fact it easily decomposes into two particular cases:
  Corollary 9.4. If ba is split, then ab is also split.
  Corollary 9.5. If a is split and $b^2 = ab$, then b is split.
  (Both times, $a, b \in A$ are arbitrary.)

The Hecke algebra: Formulas for eigenvalues, 1

- The splitness theory proves easily that all eigenvalues of $\mathcal{R}_{n,k}$ belong to $\mathbb{Z}[q]$, but it fails to show that they belong to $\mathbb{N}[q]$. Indeed, it produces "phantom eigenvalues" which do not actually appear; some of them have negative coefficients. It also does not compute the multiplicities.

The Hecke algebra: Formulas for eigenvalues, 1

- The splitness theory proves easily that all eigenvalues of $\mathcal{R}_{n,k}$ belong to $\mathbb{Z}[q]$, but it fails to show that they belong to $\mathbb{N}[q]$. Indeed, it produces "phantom eigenvalues" which do not actually appear; some of them have negative coefficients. It also does not compute the multiplicities.
- With a lot more work (Specht modules, seminormal basis for $\mathcal{H}_n$, Pieri rule, etc.), we have been able to compute the eigenvalues with their multiplicities fully.
- I only have time to state the main result.

- **Theorem 10.1.** Let $n, k \geq 0$. The eigenvalues of $R(\mathcal{R}_{n,k})$ on $\mathcal{H}_n$ are the elements

$$\mathcal{E}_{\lambda\setminus\mu}(k) := q^{nk-\binom{k}{2}} \sum_{j<(\ell_1<\ell_2<\cdots<\ell_k)\leq n} \prod_{m=1}^{k} q^{-\ell_m}[\ell_m+1-m+c_{\mathfrak{t}^{\lambda\setminus\mu}}(\ell_m)]_q$$

for all horizontal strips $\lambda \setminus \mu$ that satisfy $\lambda \vdash n$ and $d^{\mu} \neq 0$. Here,
  - d^{μ} denotes the number of *desarrangement tableaux* of shape μ (that is, standard tableaux of shape μ whose smallest non-descent is even);
  - j is the size of μ;
  - $\mathfrak{t}^{\lambda\setminus\mu}$ is the skew tableau of shape $\lambda \setminus \mu$ obtained by filling in the boxes of $\lambda \setminus \mu$ with $j+1, j+2, \ldots, n$ from top to bottom;
  - $c_{\mathfrak{t}^{\lambda\setminus\mu}}(p) = y - x$ if the cell of $\mathfrak{t}^{\lambda\setminus\mu}$ containing the entry p is (x, y).

Moreover, the multiplicity of each such eigenvalue $\mathcal{E}_{\lambda\setminus\mu}(k)$ is $d^{\mu} f^{\lambda}$, where f^{λ} is the number of standard tableaux of shape λ (unless there are collisions).

- **Theorem 10.1.** Let $n, k \geq 0$. The eigenvalues of $R(\mathcal{R}_{n,k})$ on $\mathcal{H}_n$ are the elements

$$\mathcal{E}_{\lambda\setminus\mu}(k) := q^{nk-\binom{k}{2}} \sum_{j<(\ell_1<\ell_2<\cdots<\ell_k)\leq n} \prod_{m=1}^{k} q^{-\ell_m}[\ell_m+1-m+\mathrm{c}_{\mathrm{t}^{\lambda\setminus\mu}}(\ell_m)]_q$$

for all horizontal strips $\lambda \setminus \mu$ that satisfy $\lambda \vdash n$ and $d^\mu \neq 0$. Here,
  - d^μ denotes the number of *desarrangement tableaux* of shape μ (that is, standard tableaux of shape μ whose smallest non-descent is even);
  - j is the size of μ;
  - $\mathrm{t}^{\lambda\setminus\mu}$ is the skew tableau of shape $\lambda \setminus \mu$ obtained by filling in the boxes of $\lambda \setminus \mu$ with $j+1, j+2, \ldots, n$ from top to bottom;
  - $\mathrm{c}_{\mathrm{t}^{\lambda\setminus\mu}}(p) = y - x$ if the cell of $\mathrm{t}^{\lambda\setminus\mu}$ containing the entry p is (x, y).

  Moreover, the multiplicity of each such eigenvalue $\mathcal{E}_{\lambda\setminus\mu}(k)$ is $d^\mu f^\lambda$, where f^λ is the number of standard tableaux of shape λ (unless there are collisions).
- The right hand side can be rewritten as an evaluation of a factorial h-polynomial, but this may not be much of a simplification.

- We have explicit formulas for specific shapes and strips:

$$\mathcal{E}_{(n)\setminus\varnothing}(k) = [k]!_q \begin{bmatrix} n \\ k \end{bmatrix}_q^2;$$

$$\mathcal{E}_{(n-1,1)\setminus(j,1)}(k) = [k]!_q \begin{bmatrix} n-j-1 \\ k \end{bmatrix}_q \begin{bmatrix} n+j \\ k \end{bmatrix}_q \qquad \text{for all } j \in [n-1].$$

But $\mathcal{E}_{(4,1,1)\setminus(1,1)}(1)$ is not a quotient of products of q-integers.

The Hecke algebra: Open questions

- **Question:** Any nicer formulas for the eigenvalues $\mathcal{E}_{\lambda\backslash\mu}(k)$?
- **Question:** As polynomials in q, are the eigenvalues $\mathcal{E}_{\lambda\backslash\mu}(k)$ unimodal?
- **Question (Reiner):** How big is the subalgebra of $\mathbb{Q}[S_n]$ generated by $\mathcal{R}_{n,0}, \mathcal{R}_{n,1}, \ldots, \mathcal{R}_{n,n}$? Some small values:

n	1	2	3	4	5	6	7	8	9	10	11	12
dim (subalgebra)	1	2	4	7	15	30	54	95	159	257	400	613

(sequence not in the OEIS as of 2025-03-17).

The same numbers hold for the q-deformation!

The affine Hecke algebra: Open questions

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

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

  in the *twisted group algebra*

$$\mathcal{T} := \mathbf{k}[S_n] \otimes \mathbf{k}[x_1, x_2, \ldots, x_n]$$

  with multiplication $(\sigma \otimes f)(\tau \otimes g) = \sigma\tau \otimes \tau^{-1}(f)\, g$.

  Then, the $\widetilde{\mathcal{R}}_{n,0}, \widetilde{\mathcal{R}}_{n,1}, \ldots, \widetilde{\mathcal{R}}_{n,n}$ commute.
- This twisted group algebra $\mathcal{T}$ acts on $\mathbf{k}[x_1, x_2, \ldots, x_n]$ in two ways: by multiplication ($(\sigma \otimes f)(p) = \sigma(fp)$) or by differentiation ($(f \otimes \sigma)(p) = \sigma(f(\partial)(p))$). (In either case, the S_n part permutes the variables.)
- **Question:** Simpler proof for this generalization? q-deformation? (The obvious one in the affine Hecke algebra does not work!)

I thank

- **Sarah Brauner, Patricia Commins** and **Franco Saliola** for obvious reasons.
- the **Mathematisches Forschungsinstitut Oberwolfach** for the Research in Pairs program during which most of this was found.
- **Nadia Lafrenière, Martin Lorenz, Franco Saliola, Marcelo Aguiar, Vic Reiner, Travis Scrimshaw, Theo Douvropoulos, Volkmar Welker** for various ideas shared over the years.
- **Lorenzo Vecchi** for the invitation (KTH).
- **Swee Hong Chan** for the invitation (Rutgers).
- **you** for your patience.