MATH 235: Modern Markov Chains

Lecturer: Professor Persi Diaconis

Notes by: Andrew Lin

Winter 2024

1 January 9, 2024

Markov chains are a big subject, and it's impossible to cover very much of it in ten weeks. What we'll be focusing on this quarter is a specialization to **random walks on groups and the mathematics of shuffling cards**, based on a recent book by Professor Diaconis and Jason Fulman. We'll do some introductory material on Markov chains and L^2 theory, and then we'll use noncommutative Fourier analysis to study simple random walks on groups. We'll then specialize to actual card-shuffling, where we'll find that there will be interesting (and sometimes exotic) math.

Remark 1. *Professor Diaconis's office is in room 383D – we should visit in person instead of sending an email.*

We'll start with an overview: let $\mathfrak{X}$ be a finite set, and let $K(x, y)$ be a **stochastic kernel** such that $\sum_y K(x, y) = 1$ (and here x, y are elements of $\mathfrak{X}$). Thinking of K as a matrix indexed by the elements of $\mathfrak{X}$ (where $K(x, y)$ is the probability of going from x to y in a single step), we can define

$$K^2(x, y) = \sum_z K(x, z)K(z, y),$$

and similarly K^n to be the matrix multiplication generalization, which we can think of as the "chance of going from x to y in n steps." Essentially all of the chains we work with will be **ergodic**, meaning that there is some N such that $K^n(x, y) > 0$ for all x, y and all $n \geq N$, so we can assume there aren't any problems with parity or connectivity. In such a situation, there will be some **stationary distribution** $\pi(x)$ such that $\sum_x \pi(x)K(x, y) = \pi(y)$ (meaning π is a left eigenvector of K with eigenvalue 1); probabilistically, if we start at a point x with probability $\pi(x)$ and take one step, we still have the same probabilities of being at various points in $\mathfrak{X}$.

The key is that $K^n(x, y)$ will converge to $\pi(y)$ for all x as $n \to \infty$; lots of this course will be about **how fast this convergence occurs**. For now, though, we can define the **total variation**

$$||K_x^n - \pi||_{\text{T.V.}} = \max_{A \subseteq \mathfrak{X}} |K^n(x, A) - \pi(A)|.$$

Our question is then (mathematically) to ask how large n needs to be so that $||K_x^n - \pi||_{\text{T.V.}} < \varepsilon$, given some starting point x and some $\varepsilon > 0$.

Example 2

One special case that comes up often in this class is as follows: let G be a finite group, and let $Q(s)$ be a probability distribution on G. Then we can define

$$Q * Q(s) = \sum_t Q(t)Q(st^{-1})$$

(that is, the probability of being at s after two steps is to choose t, then multiply it on the left by st^{-1}) and then define Q^{*n} inductively in a similar way.

This is a special case of Markov chains with $K(s,t) = Q(ts^{-1})$, where we start from the identity and we repeatedly multiply by elements of the group. And under mild assumptions, namely that the support of Q is not contained in the coset of some proper subgroup, we will have $Q^{*k}(s)$ converging to the **uniform distribution** with $u(s) = \frac{1}{|G|}$ for all $s \in G$.

The next three examples are key ones to keep in mind for the rest of the class:

Example 3

Let $G = C_n = \mathbb{Z}/n\mathbb{Z}$ be the integers mod n for some odd integer n. Suppose we perform gambler's ruin, meaning that $Q(1) = Q(-1) = \frac{1}{2}$ and $Q(s) = 0$ for all other s.

After performing this walk for many steps, we approach the uniform distribution U, and in fact we'll prove later in the class that

$$\frac{1}{2}e^{-2\pi^2 k/n^2} \leq \left|\left|Q^{*k} - U\right|\right| \leq e^{-2\pi^2 k/n^2}.$$

So this tells us how many steps we need to take because of randomness – it'll take a multiple of n^2 steps before we can get below some threshold of ε, and in fact n^2 is necessary and sufficient because we have both inequalities. And this isn't special to simple random walk or having the integers mod n – much of probability involves these types of random walks on abelian groups.

Example 4 (Ehrenfest urn)

Suppose we have two urns, where initially one of them is filled with n balls and the other is empty. At each step, pick a ball at random and move it to the other urn.

The motivation for this problem is the following: around 1890, Boltzmann introduced statistical mechanics, and there were controversies at the time about the theory because it wasn't known that there are atoms. Poincaré had proved the **recurrence theorem** at the time, which says that a dynamical system (like gas molecules in a box all starting on the left side) will eventually return to the original state, while Boltzmann had described that entropy always increases. This seemed like a contradiction, but Ehrenfest introduced this model as a toy example (where the gas particles are either in the left or right urn) as an explanation.

The idea is that for any finite number of balls n, we **will** have all the balls in the left urn infinitely often, but the entropy of the probability distribution $-\sum_j P_n^k(j) \log P_n^k(j)$ still does increase as k increases (where $P_n^k(j)$ is the number of balls in the left urn if we start with n balls and take n steps). And in this class, we'll prove that if $k = \frac{1}{4}n \log n + cn$ for some $c > 0$, then

$$\frac{1}{2}e^{-c} \leq ||P_n^k(j) - B_n(j)|| \leq e^{-c},$$

where $B_n(j)$ is binomial with parameters $(n, 1/2)$. And on the other hand, if we started off with half and half in the two urns instead of all n on the left, we would converge in just n steps instead of $n \log n$, so the starting point does matter.

This example turns out to secretly be an example of a random walk on a group, too: instead of coding the system in terms of which balls are in the left urn, we can code by a binary vector $(x_1, \cdots, x_n)$ where $x_i = 1$ if ball i is in the left urn and $x_i = 0$ otherwise. Then the Ehrenfest urn is actually the **nearest-neighbor random walk on the hypercube** $\{0, 1\}^n$, where at each step we move to an adjacent vertex (take a random coordinate and flip it). And one question we may want to ask is when we can lift a Markov chain to a walk on a group or even an abelian group.

Remark 5. *There's a parity problem if we always move to an adjacent vertex, so secretly we want to be slightly lazy and stay where we are with probability* $\frac{1}{n+1}$ *and move to one of the neighbors with probability* $\frac{1}{n+1}$ *instead, and then the logic actually goes through.*

The bounds on total variation distance we've described above are quite sharp – we're saying that once we get to $\frac{1}{4} n \log n$, we get a transition from order to chaos very suddenly over a lower-order amount of time. This is the **cutoff phenomenon**, where the total variation distance is flat up until a certain point and then goes down to 0 very quickly over a short amount of time, and this seems to happen in a lot of Markov chains (in fact conjectured "almost always"). But some pretty refined analysis is required for this to actually be proven.

Example 6 (Random transpositions)
Next, consider a Markov chain on S_n where at each step we stay at our current transposition with probability $\frac{1}{n}$ and multiply our transposition by (i, j) with probability $\frac{2}{n^2}$.

The motivation for this problem came from card-guessing games: while Professor Diaconis was at Bell Labs, computer simulations were giving funny results, and the fundamental problem came from how the algorithm was generating random permutations. The **Fisher-Yates** algorithm does this by picking $1 \le i \le n$ and swapping i with 1, then picking $2 \le j \le n$ and swapping j with 2, and so on. But what was being done was instead swapping two random cards, and it turns out 100 of these is not enough. What was proved is that after $k = \frac{1}{2} n \log n + cn$ steps, we have

$$||Q^{*k} - U|| \le 2e^{-c},$$

and in particular if we want this right-hand side to be at most 0.001, we actually need $k = 480$ transpositions. (And again, the TV distance has a sharp cutoff in this problem.)

Remark 7. *All of the examples we've shown so far (with sharp bounds) come from* **Fourier analysis** *on groups, and we'll develop the theory for this as we go on.*

After we develop the tools for these results, we'll then move into **comparison theory**, which allows us to transfer nice results from one walk on a group to other walks on a group. (For example, the walk where we either transpose the top two cards or put the top one on the bottom – a transposition and an n-cycle generate S_n – takes $n^3 \log n$ steps to mix.) And then the remaining part of the course will focus more on actual cards:

Example 8
There are three main ways people shuffle cards: riffle shuffle, overhand shuffle, and smushing them on a table.

We'll make these techniques more mathematically rigorous: suppose we're working on S_n. **In a riffle shuffle**, we cut off c cards with probability $\frac{\binom{n}{c}}{2^n}$ and then recombine the deck. The rule for that is as follows: if we have a cards in

the left hand and b cards in the right hand, we drop the next card from the left with probability $\frac{a}{a+b}$ and from the right with probability $\frac{b}{a+b}$. And this makes sense, both physically because larger piles are more springy and also because it is pretty consistent with how people actually riffle shuffle. It turns out that if $k = \frac{3}{2}\log_2 n + c$, then

$$||Q^{*k} - U|| = 1 - 2\Phi\left(-\frac{2^{-c}}{4\sqrt{3}}\right) O\left(\frac{1}{\sqrt{n}}\right),$$

where Φ is the cumulative normal distribution function. This is a sharp result related to the descent algebra in the symmetric group, and we'll spend some time building up to this. However, in some we don't care about some aspects of the deck (like in blackjack), so sometimes we just need to study certain **features**. In particular, there are nice formulas related to the cycle structure of permutations.

Remark 9. *When we add two numbers together, we get a* **carry structure** *corresponding to which places have a "+1", and the carry structure turns out to have the same structure as shuffling (if we think about carries as* **cocycles***). And it turns out that what we know about arithmetic has revealed some information about shuffling.*

Next, we'll make math out of **overhand shuffles**: one way to do so is to flip a θ-coin between any two cards in the deck, and cut off cards into clumps based on where the coins show up as heads. Then overhand shuffling reverses the clumps while keeping the order within each clump the same. For this one, $n^2 \log n$ turns out to be necessary and sufficient, meaning that it takes about 10000 shuffles to mix up 52 cards. But both riffle shuffling and overhand shuffles have "order n amount of randomness" per steps, so there's a clear sense of which one is more efficient. This proof comes from **coupling machinery** that will be used in this course a few times, rather than Fourier analysis.

Finally, there are reasonable models for **smushing cards together** – that model is sort of related to fluid mechanics, and the math required is stochastic calculus, but we'll talk about that more when we get to it near the end of the course.

Fact 10

We'll go through the course syllabus in more detail now, talking about what will happen during each week of this quarter.

In week 1 we'll set up the introduction (today) and L^2 theory, week 2 will cover path arguments, Cheeger inequalities, and walks on C_n and C_2^n, and week 3 will be comparison theory (with applications to shuffling). Fourier analysis and intro to representation theory will begin on week 4 (we can read a free book on Professor Diaconis' website for more on this), which will allow us to study the random transpositions problem. Week 5 will cover riffle shuffling and the "seven shuffles theorem," and week 6 will talk about features. Week 7 will talk about carries when adding numbers (and how they're connected to determinantal point processes), week 8 about hyperplane walks, week 9 about overhand shuffling and coupling, and finally week 10 about smushing.

We'll have two or three homework assignments – the first homework assignment was handed out to us today and is due in two weeks. We'll also have a final project where we pick one from a list of papers and submit a 10 to 15 page paper making some progress towards a real research problem. And if we want a sense of how difficult this course will be, taking a look at the books mentioned will give us a good idea.

2 January 11, 2024

Today's topic is the L^2 **theory of Markov chains** – we'll do everything in finite spaces, but if we're interested in a general kernel of the form $K(x)dy$, everything will go through. Like last time, let $\mathfrak{X}$ be a finite set, and let $K(x, y) \geq 0$

be a Markov kernel (meaning that $\sum_y K(x,y) = 1$).

Definition 11

A probability measure π is **reversible** if for all $x, y \in \mathfrak{X}$, we have

$$\pi(x)K(x,y) = \pi(y)K(y,x).$$

Example 12

Let Γ be a simple (undirected) graph with vertex set $\mathfrak{X}$ and edges E. For each edge $e \in E$, fix some positive weight $w(e) > 0$, and make a Markov chain on $\mathfrak{X}$ where at each step, we choose a neighbor of our current vertex x with probability proportional to $w((x,y))$ and move to y.

In other words, the Markov kernel is given by

$$K(x,y) = \begin{cases} \frac{w(x,y)}{W(x)}, & W(x)\sum_{z\sim x} w(x,z) \quad x \sim y \\ 0 & \text{otherwise,} \end{cases}$$

and the stationary distribution of this Markov chain will be $\pi(x) = \frac{W(x)}{W}$, where W is a normalizing constant. Indeed,

$$\pi(x)K(x,y) = \frac{W(x)}{W}\frac{W(x,y)}{W(x)} = \pi(y)K(y,x),$$

so we have a reversible Markov chain. Thus

$$\sum_x \pi(x)K(x,y) = \sum_x \pi(y)K(y,x) = \pi(y)\sum_x K(y,x) = \pi(y),$$

so a reversing measure is automatically a stationary distribution. (And essentially all reversible chains are of this type.)

Example 13

For a random walk on a group G, we have $\pi(x) = \frac{1}{|G|}$, and reversibility is the same as saying that the Markov matrix K is symmetric. But not all random walks on a group are symmetric – for example, if $G = C_n$ and $Q(1) = q$ and $(Q-1) = 1-q$ for some $q \neq \frac{1}{2}$, then this biased random walk has a uniform stationary distribution but is not reversible.

We'll treat nonreversible chains by comparison later on, but for now we'll just focus on the reversible case and develop the theory there.

Definition 14

Define $\ell^2(\pi)$ to be the set of functions $f : \mathfrak{X} \to \mathbb{R}$ with inner product

$$\langle f, g\rangle = \sum_x f(x)g(x)\pi(x).$$

Then K acts on ℓ^2 via

$$Kf(x) = \sum_y f(y)K(x,y)$$

(so Kf averages the value of f over all possibilities one step later), and we have by Cauchy-Schwarz that

$$\left(\sum_y K(x,y)f(y)\right)^2 \leq \sum_y K(x,y)f(y)^2.$$

Multiplying both sides by $\pi(x)$ and summing, we find that $||Kf||_2^2 \leq ||f||_2^2$, and thus K sends $\ell^2 \to \ell^2$ and in fact $||K||_{2\to 2} = 1$ (because the function which is identically 1 is sent to itself under K).

Proposition 15

Reversibility is equivalent to saying that

$$\langle Kf, g\rangle = \langle f, Kg\rangle;$$

that is, the operator is self-adjoint.

Proof. If we plug in the functions $f = \delta_x$ and $g = \delta_y$, then this relation is the same as the reversibility condition, and these delta functions form a basis for all functions in $\ell^2(\pi)$. □

We can then get bounds on total variation (ℓ^1) in terms of bounds in ℓ^2: after ℓ steps, we have by definition that

$$||K_x^\ell - \pi||_{\text{TV}} = \frac{1}{2}\sum_y |K^\ell(x,y) - \pi(y)|,$$

which means we can square this and simplify

$$4||K_x^\ell - \pi||_{\text{TV}}^2 = \left(\sum_y \left|\frac{K^\ell(x,y)}{\pi(y)} - 1\right|\pi(y)\right)^2 \leq \sum_y \left|\frac{K^\ell(x,y)}{\pi(y)} - 1\right|^2 \pi(y)$$

using Cauchy-Schwarz. But now $\left|\frac{K^\ell(x,y)}{\pi(y)} - 1\right|^2$ is exactly the chi-square distribution after ℓ steps, and the point is that the expression on the right is expressible via **eigenvalues**. So the strategy is to bound ℓ^1 by ℓ^2 and then use eigenvalues to bound the latter.

Fact 16

Since K is self-adjoint, the spectral theorem says that we have eigenfunctions $\phi_i(x)$ and eigenvalues $\beta_i \in \mathbb{R}$ such that $K\phi_i(x) = \beta_i\phi_i(x)$ for all $0 \leq i \leq |\mathfrak{X}| - 1$, and the ϕ_i are orthonormal in ℓ^2.

(A good reference for this material is Horn and Johnson's Matrix Analysis.) We'll use the convention that $\beta_0 \geq \beta_1 \geq \cdots \beta_{|\mathfrak{X}|-1}$; notice that $\beta_0 = 1$ with $\phi_0(x) = 1$ identically. Write

$$\beta_* = \max(\beta_1, |\beta_{|\mathfrak{X}|-1}|)$$

to be the eigenvalue closest to 1 in absolute value.

Proposition 17

Suppose $\mathfrak{X}$ is finite and (π, K) is a reversible Markov chain. Then we have the following:

1. $|\beta_i| \leq 1$ for all i,
2. If the chain is **connected** (meaning that for all x, y there is some $n(x,y)$ with $K^N(x,y) > 0$ for all $N > n(x,y)$), then $\beta_i < \beta_0 = 1$ for all $i \neq 0$,
3. If the graph of K is not **bipartite**, then $\beta_i > -1$ for all i,
4. For all $x \in \mathfrak{X}$, we have
$$\sum_{i=0}^{|\mathfrak{X}|-1} \phi_i^2(x) = \frac{1}{\pi(x)}.$$
5. For all $x \in \mathfrak{X}$, we have
$$\left|\left|\frac{K_x^\ell(y)}{\pi(y)} - 1\right|\right|_2^2 = \sum_{i=1}^{|\mathfrak{X}|-1} \phi_i(x)^2 \beta_i^{2\ell} \leq \frac{1-\pi(x)}{\pi(x)} \beta_*^{2\ell} \leq \frac{\beta_*^{2\ell}}{\pi(x)}.$$

In particular, statement (5) tells us how to use eigenvalues to bound the ℓ^2 norm (and thus the ℓ^1 norm).

Proof of (4) and (5). Let $d_x(y)$ be the function which is $\frac{1}{\pi(x)}$ if $x = y$ and 0 otherwise. Expanding this function in the eigenfunction basis, we have coefficients

$$\langle d_x, \phi_i \rangle \sum_y \phi_i(y) \delta_x(y) \pi(y) = \phi_i(x),$$

which means that

$$d_x(x) = \frac{1}{\pi(x)} = \sum_y \phi_i(x) \langle d_x, \phi_i \rangle = \sum_i \phi_i(x)^2$$

as desired. So now if we expand $\frac{K^\ell(x,y)}{\pi(y)}$ as a function of y, we want to find the coefficients in

$$\frac{K^\ell(x,y)}{\pi(y)} = \sum_i \phi_i(y) \langle \frac{K_x}{\pi}, \phi_i \rangle.$$

But by definition,

$$\left\langle \frac{K_x^\ell}{\pi}, \phi_i \right\rangle = \sum_y \frac{K^\ell(x,y)}{\pi(y)} \phi_i(y) \pi(y) = \sum_y K^\ell(x,y) \phi_i(y) = \beta_i^\ell \phi_i(x)$$

by definition of the eigenfunction. Since ϕ_0 is identically 1, "subtracting off 1" removes the term from the top eigenvalue and we have

$$\left|\left|\frac{K_x^\ell}{\pi} - 1\right|\right|_2^2 = \sum_{i=1}^{|\mathfrak{X}|-1} \beta_i^{2\ell} \phi_i^2(x),$$

as desired. Therefore, we have the useful bounds

$$4||K_x^\ell - \pi||_{\mathrm{TV}}^2 \leq \left|\left|\frac{K_x^\ell}{\pi} - 1\right|\right|_2^2 = \sum_{i=1}^{|\mathfrak{X}|-1} \beta_i^{2\ell} \phi_i^2(x),$$

and now bounding all β_i by β_* simplifies this to

$$\leq \frac{1-\pi(x)}{\pi(x)} \beta_*^{2\ell} = \frac{\beta_*^{2\ell}}{\pi(x)},$$

completing the proof. □

This bound is usually pretty sharp because we're applying it once we're close to stationarity and thus Cauchy-Schwarz is pretty close to equality, but the last step sometimes loses us a factor of n. And this is the first step in the L^2 theory; we now want to talk about how we get bounds on eigenvalues. The idea is that we use the matrix as a quadratic form and take the minimum or maximum over row and column vectors, and here's a coordinate-free way to do that:

Definition 18

The **Dirichlet form** is defined by

$$\mathcal{E}(f,g) = \langle (I-K)f, g\rangle.$$

Proposition 19

The Dirichlet form can also be written more explicitly as

$$\mathcal{E}(f,g) = \frac{1}{2}\sum_{x,y}(f(x)-f(y))(g(x)-g(y))\pi(x)K(x,y).$$

Proof. Expanding out the inner products on the left-hand side, we have

$$\langle (I-K)f, g\rangle = \sum_x f(x)g(x)\pi(x) - \sum_{x,y} f(y)K(x,y)g(x)\pi(x).$$

Meanwhile, expanding out the right-hand side yields

$$\text{RHS} = \frac{1}{2}\left(\sum_{x,y} f(x)g(x)\pi(x)K(x,y) + f(y)g(y)\pi(x)K(x,y) - f(y)g(x)\pi(x)K(x,y) - f(x)g(y)\pi(x)K(x,y)\right).$$

These two expressions are now equal, because the first two terms we can sum over one of the two variables and use that π is the stationary distribution, and the last two terms are the same after reindexing and by reversibility. □

The main fact that we'll use is that we have the positive quantity

$$\mathcal{E}(f,f) = \frac{1}{2}\sum_{x,y}(f(x)-f(y))^2\pi(x)K(x,y),$$

and this object can be useful in various settings. In particular, it leads to the classical method of bounding eigenvalues:

Proposition 20

Again let $\mathfrak{X}$ be finite and (π, K) a reversible chain. Then

$$1-\beta_1 = \min \frac{\mathcal{E}(f,f)}{\text{Var}(f)}, \quad 1-\beta_{|\mathfrak{X}|-1} = \max \frac{\mathcal{E}(f,f)}{\text{Var}(f)},$$

where we take the min and max over all nonconstant functions and where

$$\text{Var}(f) = \sum_x (f(x)-\overline{f})^2\pi(x) = \frac{1}{2}\sum_{x,y}(f(x)-f(y))^2\pi(x)\pi(y).$$

Proof. Let $W = \{f : \langle f, 1\rangle = 0\}$ be the set of functions orthogonal to the constant functions. For any $f \in W$, we can normalize it so that $||f||_2^2 = 1$ (everything is homogeneous), and now we can expand it as

$$f(x) = \sum_{i=1}^{|\mathfrak{X}|-1} \phi_i(x)\langle f, \phi_i\rangle.$$

Then expanding out in the eigenfunction basis yields

$$(I - K)f(x) = \sum_i (1-\beta_i)\phi_i(x)\langle f, \phi_i\rangle,$$

which means that by orthonormality of the eigenfunctions we have

$$\mathcal{E}(f,f) = \langle (I-K)f, f\rangle = \sum_{i=1}^{|\mathfrak{X}|-1} (1-\beta_i)\langle f, \phi_i\rangle^2.$$

This quantity is now bounded from below by $1-\beta_1$ because the sum of these squared Fourier coefficients is 1, and equality holds by plugging in $f = \phi_1$. Bounding in the other direction gives the other fact. □

Thus, if we can get a bound of the form

$$\boxed{\mathrm{Var}(f) \le A\mathcal{E}(f,f)}$$

for some fixed constant A (this is called a **Poincaré inequality**), then this tells us that

$$\frac{1}{A} \le \min \frac{\mathcal{E}(f,f)}{\mathrm{Var}(f)} = 1-\beta_1 \implies \beta_1 \le 1 - \frac{1}{A}.$$

The method for proving such Poincaré inequalities is very useful, and in particular we can use what's called the **path bound**. Given a reversible chain (π, K), we can associate to it a graph Γ where (x,y) is an edge in Γ if and only if $K(x,y) > 0$ (reversibility means this is equivalent to $K(y,x) > 0$). A **path** from x to y in Γ is then a sequence of vertices $\gamma_{xy} = \{x_0, x_1, \cdots, x_n\}$, where $x_0 = x$, $x_n = y$, and $K(x_i, x_{i+1}) > 0$ for all i; we say that such a path has length n. **Fix such a path** for each x, y in $\mathfrak{X}$. The idea now is that

$$f(x) - f(y) = (f(x_0) - f(x_1)) + (f(x_1) - f(x_2)) + \cdots + (f(x_{n-1}) - f(x_n)) = \sum_{e \in \gamma_{xy}} (f(e^-) - f(e^+))$$

where now the edges e are directed from e^- to e^+. We then have

$$\begin{aligned}\mathrm{Var}(f) &= \frac{1}{2}\sum_{x,y}(f(x)-f(y))^2\pi(x)\pi(y) \\ &= \frac{1}{2}\sum_{x,y}\left\{\sum_{e\in\gamma_{xy}}(f(e^-)-f(e^+)\right\}^2 \pi(x)\pi(y);\end{aligned}$$

using Cauchy-Schwarz on the curly brace part (no weights here, but in some settings using weights is useful) simplifies this to

$$\mathrm{Var}(f) \le \frac{1}{2}\sum_{x,y}|\gamma_{xy}| \sum_{e\in\gamma_{xy}} (f(e^-)-f(e^+))^2\pi(x)\pi(y).$$

Changing the order of summation simplifies this to

$$\mathrm{Var}(f) \le \frac{1}{2}\sum_e (f(e^-)-f(e^+))^2 \sum_{\text{paths } \gamma_{xy} \ni e} |\gamma_{xy}|\pi(x)\pi(y).$$

If $e = (z, w)$ is an edge, we can then multiply and divide by $Q(e) = \pi(z)K(z, w)$ so that the Dirichlet form shows up inside, and we find that

$$\mathrm{Var}(f) = A\mathcal{E}(f, f), \qquad \boxed{A = \max_e \frac{1}{Q(e)} \sum_{\gamma_{xy} \ni e} |\gamma_{xy}|\pi(x)\pi(y)}.$$

It may seem like A is much harder to compute, since we have to sum over all x, y whose path contains a given edge, but it turns out that this does actually give us reasonable bounds in practice.

Example 21

Consider nearest-neighbor (unweighted) random walk on a connected simple graph $G = (V, E)$. Since G is connected, we can fix paths γ_{xy} between any two vertices, and let $\gamma_* = \max |\gamma_{xy}|$ and $d_* = \max_x \deg(x)$.

For such a walk, the stationary distribution is $\pi(x) = \frac{\deg(x)}{2|E|}$, and the Markov kernel is $K(x, y) = \frac{1}{\deg(x)}$ if y is adjacent to x and 0 otherwise. Now $\pi(x)K(x, y) = \frac{1}{2|E|}$ for any adjacent x, y, so we can bound

$$A = 2|E|\frac{d_*^2}{|E|^2}\gamma_* b_*,$$

where we have a "bottleneck" situation

$$b_* = \max_e \sum_{\gamma_{xy} \ni e} 1$$

where we want to know which edge has the most traffic over it. In other words, this means that

$$\beta_1 = 1 - \frac{2|E|}{\gamma_* d_*^2 b_*},$$

and intuitively this means b_* is small if we can not use any particular edge too much. Next time, we'll see how this bound can be good in various particular examples.

Remark 22. *It turns out that using weights in Cauchy-Schwarz is equivalent to randomly choosing our paths $\gamma_{x,y}$, and it is a fact that we can choose some choice of paths or weights to try and minimize b_*. But it's a difficult problem for graphs in general.*

All of this works for $\mathbb{R}^n$ and even more general abstract spaces. That's in fact why Poincaré got his name on this inequality – he bounded eigenvalues of certain operators using paths. But doing this in continuous spaces hasn't been explored too much yet, so there are good research problems involving path arguments in that direction.

3 January 16, 2024

Last time, we discussed the L^2 theory of reversible Markov chains: if $L^2(\pi)$ is the set of functions $\mathfrak{X} \to \mathbb{R}$ with inner product $\langle f, g\rangle = \sum f(x)g(x)\pi(x)$, and K is self-adjoint (meaning that $\langle f, Kg\rangle = \langle Kf, g\rangle$, then we have eigenvalues and eigenvectors β_i, ϕ_i such that $K\phi_i = \beta_i\phi_i$, and we can order them so that $1 = \beta_0 \geq \beta_1 \geq \cdots \geq \beta_{|\mathfrak{X}|-1} \geq -1$. Introducing the Dirichlet form $\mathcal{E}(f, f) = \langle (I - K)f, f\rangle = \frac{1}{2}\sum_{x,y}(f(x) - f(y))^2\pi(x)K(x, y)$, we found the variational characterization

$$1 - \beta_1 = \max_{f \text{ nonconstant}, \bar{f}=0} \frac{\mathcal{E}(f, f)}{\mathrm{Var}(f)}.$$

We then mentioned that this gives us a bound on the spectral gap whenever we can prove a Poincaré inequality of the form $\mathrm{Var}(f) \leq A\mathcal{E}(f, f)$ (since this implies $\beta_1 \leq 1 - \frac{1}{A}$). In particular, the path argument (assuming the chain is

ergodic) gives us such a bound: fixing a path γ_{xy} between any $x, y \in \mathfrak{X}$, we have

$$A \le \max_{e=(z,w) \text{ edge}} \frac{1}{Q(e)} \sum_{\gamma_{xy} \ni e} |\gamma_{xy}| \pi(x)\pi(y), \quad Q(e) = \pi(z)K(z,w).$$

Remark 23. *If we'd like some additional references for the material we're covering, we can look at the paper "Geometric Bounds for Eigenvalues of Markov Chains" (by Diaconis and Stroock) or the book "Markov Chains and Mixing Times" (by Levin and Peres).*

Today we're going to explain why this expression actually makes useful estimates with some examples.

Example 24

Consider nearest-neighbor random walk on a path with **holding**, meaning that we have a sequence of vertices $1, 2, \cdots, N$ and move to one of the two neighbors with probability $\frac{1}{2}$ each – if we're at 1 or N, there's a probability $\frac{1}{2}$ of staying where we are instead.

In this case, the most sensible way to choose paths is to not double back and take the shortest path γ_{xy} from x to y. The stationary distribution is $\pi(x) = \frac{1}{N}$ for all x, and $Q(i, i+1) = \frac{1}{2N}$ for any edge $(i, i+1)$. If we just make the bound $|\gamma_{xy}| \le N$ for all x, y, we find that (substituting everything in)

$$A \le \frac{1}{1/2N} \cdot N \cdot \frac{1}{N^2} \cdot \sum_{\gamma_{xy} \ni e} 1;$$

now the number of paths is certainly less than the total number of paths N^2, so this means $\boxed{A \le 2N^2}$ and thus we have the bound $\beta_1 \le 1 - \frac{1}{2N^2}$. But for this problem, we know exactly what the eigenvalues actually are – it turns out that $\beta_j = \cos\left(\frac{\pi j}{N}\right)$ by the reflection principle, and thus we in fact have

$$\beta_1 = \cos\frac{\pi}{N} = 1 - \frac{\pi^2}{2N^2} + O\left(\frac{1}{N^4}\right).$$

In other words, our bound is of the right order of magnitude but missing a π^2 constant factor, which is pretty good for the level of care we put into the bound. For a more careful bound, we know the edge that is used the most is the one in the middle, so we can in fact bound $\sum_{\gamma_{xy} \ni e} 1$ by $\frac{N^2}{4}$ instead of N^2 and gain a factor of 4 (remember that edges are directed, so we only need to consider paths from left to right or vice versa). And notice that this argument is pretty robust – it works even if we had slightly different weights or did the walk on a higher-dimensional grid.

We can also show that $\beta_{|\mathfrak{X}|-1} \ge -1 + \frac{2}{N^2}$ (see the end of this lecture for a slightly worse bound), which means that $\beta_* \le 1 - \frac{2}{N^2}$; thus we have the total variation bound

$$4\left|\left|K_x^\ell - \pi\right|\right|_{\text{TV}}^2 \le \frac{1}{\pi(x)}\beta_*^{2\ell} = N\left(1 - \frac{2}{N^2}\right)^{2\ell} = e^{\log N - 4\ell/N^2},$$

where we use that $1 - x \le e^{-x}$. So this tells us that $\ell = \frac{1}{4}N^2(\log N + c)$, then $4\left|\left|K_x^\ell - \pi\right|\right|_{\text{TV}}^2 \le e^{-c}$; it turns out that if we're more careful and use all of the eigenvalues and eigenvectors, we see that it actually only requires cN^2 steps.

Example 25

Let C_2^d be the hypercube, meaning that $\mathfrak{X} = \{(x_1, \cdots, x_d) : x_i \in \{0, 1\}\}$. We perform nearest-neighbor random walk on the hypercube with holding at each point, meaning that $K(x, y) = \frac{1}{d+1}$ if $x = y$ or $y = x + e_i \pmod 2$ for some $1 \le i \le d$.

Again the stationary distribution is uniform with $\pi(x) = \frac{1}{2^d}$ for all d; we get a reversible Markov chain, and the way to make a path γ_{xy} is to go left to right and change bits until x matches y. (For example, the path from $x = 01001$ to $y = 11110$ is given by $01001, 11001, 11101, 11111, 11110$.) With this construction, we have $|\gamma_{xy}| \le d$ uniformly and $Q(z, y) = \frac{1}{2^d(d+1)}$ along any edge (z, y). Thus

$$A \le \max_e \frac{1}{Q(e)} \sum_{\gamma_{xy} \ni e} |\gamma_{xy}| \pi(x)\pi(y) = 2^d(d+1) \cdot \frac{1}{2^{2d}} d \sum_{\gamma_{xy} \ni e} 1.$$

To evaluate this "bottleneck number," notice that each edge is some (z, w) differing at the ith coordinate. Then an edge from x to y passes through (z, w) if x is one of the 2^{i-1} possible strings with the same ending and y is one of the 2^{d-i} strings with the same beginning, and thus

$$A \le d(d+1)\frac{2^d \cdot 2^{d-1}}{2^{2d}} = \frac{d(d+1)}{2} \implies \beta_1 \le 1 - \frac{2}{d(d+1)}.$$

But again we know the actual eigenvalues of the matrix; in reality $\beta_1 = 1 - \frac{2}{d+1}$, so we're off by a factor of d. Feeding our bound into the machine, we find that

$$4\left|\left|K_x^\ell - \pi\right|\right|_{\text{TV}}^2 \le 2^d \left(1 - \frac{2}{d(d+1)}\right)^{2\ell} \le \exp\left(d \log 2 - 4\ell/(d(d+1))\right),$$

so we're saying that we need $\ell = O(d^3)$ steps; the correct eigenvalue bound would have given $O(d^2)$, but in fact $\frac{1}{4}d(\log d + c)$ is necessary and sufficient. So using the second eigenvalue gives us something but not always the best answer.

We'll now do a "real" example – there are references where we can see the details, but we'll just talk through the most important points for the sake of time.

Example 26

Let M be an $n \times n$ matrix. The **permanent** of M is defined to be

$$\text{perm}(M) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} M_{\sigma(i)}.$$

The permanent of M is like the determinant but without the signs; it has various applications, but it turns out (due to work by Valiant) that computing the permanent is #-P complete and thus we can't do it efficiently in general. And even if M_{ij} are all $\{0, 1\}$-valued (for example, if we have a bipartite graph with n vertices on each side, and $M_{ij} = 1$ if there is an edge (i, j) between the ith vertex on the left and the jth vertex on the right – in this case the permanent counts the number of **perfect matchings**) we still have a #-P complete problem.

However, Broder, Jerrum, and Valiant showed that if we can sample random matchings uniformly to a good approximation, then we get an approximation of perm(M). This led to the **random switch** algorithm, which goes as follows: given a perfect matching, pick pairs (i_1, j_1) and (i_2, j_2) in the matching and try to swap to (i_1, j_2) and (i_2, j_1) (with some holding). Then under weak conditions, this Markov chain is connected, ergodic, and reversible, and it will converge to a uniform perfect matching. Jerrum and Sinclair then studied this using the path argument: it turns out that in the **dense** case where each vertex had degree at least $\frac{N}{2}$, if we expand the state space to the almost-perfect matchings and only report if we're actually at a perfect matching, we don't lose that much. Then we can use the covering number $\beta_* = \sum_{\gamma_{xy} \ni e} 1$ to bound the **Cheeger constant** using **Cheeger's inequality**. This turns out to be bad because it roughly introduces an extra square in the mixing time – they found that this chain requires $O(n^{12})$, but Poincaré yields $O(n^6)$. And later on, the denseness assumption was also removed (through work by Jerrum, Sinclair,

and Vigoda).

Remark 27. *What Diaconis and Stroock did was to take six of the examples that Jerrum and Sinclair worked on and plugged them into Poincaré instead of Cheeger to get much better bounds. If we'd like to learn more about Cheeger's inequality, we can read that paper, but we'll be just using Poincaré for this purpose in this class.*

There are problems where there are lots of paths, though (like in our example above for the hypercube); in these settings it's common to choose random paths instead. The same argument but now writing the variance with that extra randomness yields the following:

Proposition 28

Let (π, K) be a reversible Markov chain, and for each x, y, let $\mu_{x,y}$ be a probability measure on the set of all paths from x to y. Then we have the Poincaré estimate

$$A \le \max_e \frac{1}{Q(e)} \sum_{\gamma_{xy} \ni e} \mu_{x,y}(\gamma_{xy}) |\gamma_{xy}| \pi(x)\pi(y).$$

For a quick sketch of the calculation, notice that

$$\mathrm{Var}(f) = \frac{1}{2} \sum_{x,y} \pi(x)\pi(y) \sum_{\text{possible } \gamma_{xy}} \mu_{x,y}(\gamma_{x,y}) \sum_e (f(e^+) - f(e^-))^2),$$

and then using Cauchy-Schwarz in the same way as before gives us the correct bound.

Example 29

Consider the complete bipartite graph $K_{n,n}$ (with all n^2 edges drawn between the two sides), and suppose we perform simple random walk on this graph, meaning that we go to one of the N vertices on the other side uniformly at random (no holding, but we'll just worry about bounding the second eigenvalue).

The stationary distribution here is again uniform with $\pi(x) = \frac{1}{2N}$ for all x. A naive choice of paths is to say that from i on the left-hand side to j on the right-hand side, we just use the edge between those vertices, and from i to i' on the left-hand side, suppose we pass through vertex i on the right-hand side. So all paths are of length 1 or 2; plugging into the path bound, we have

$$A \le \frac{1}{1/2N^2} \cdot 2 \cdot \frac{1}{(2N)^2} \cdot \max_e \sum_{\gamma_{xy} \ni e} 1.$$

But each edge (i, i) has $(n-1)$ edges passing through it, so this tells us that $A \le n-1$ and thus $\beta \le 1 - \frac{1}{n-1}$. But for this graph, the eigenvalues are actually 1 and -1, each with multiplicity 1, and 0 with multiplicity $2n-2$, so this isn't a great bound. If we instead use **random** paths where j is chosen uniformly in the path $i \to j \to i'$, we'll instead get $A \le 2$ and thus $\beta_1 \le \frac{1}{2}$.

Fact 30

As we briefly mentioned last time, we've been using Cauchy-Schwarz with uniform weights, but we can use weights that depend on the edge (and this is sometimes important – we can see the Diaconis and Stroock paper to see this written out). It turns out that with random paths and arbitrary Cauchy-Schwarz weights, the path bound is sharp up to a $\log N$ factor. For a more precise statement, we can see "A Semidefinite Bound for Mixing Rates of Markov Chains" by Kahale.

We'll finish today by talking about **lower bounds for negative eigenvalues**: if $\mathfrak{X}, \pi, K$ are as above (aperiodic, connected, reversible), then for each $x \in \mathfrak{X}$ we can choose a path σ_x of **odd length** from x to x. (This is always possible for any connected nonbipartite graph.)

Proposition 31

We have the bound

$$\beta_{|\mathfrak{X}|-1} \geq -1 + \frac{2}{B}, \quad B = \max_e \frac{1}{Q(e)} \sum_{\sigma_x \ni e} |\sigma_x| \pi(x),$$

where we must now allow loops as edges.

Proof. Define a different quadratic form

$$\mathcal{F}(f, f) = \langle (I + K)f, f \rangle = \frac{1}{2} \sum_{x,y} (f(x) + f(y))^2 \pi(x) K(x, y).$$

Like above, we can show that

$$1 + \beta_{|X|-1} = \min_{f \text{ nonconstant}, \bar{f}=0} \frac{\mathcal{F}(f, f)}{||f||_2^2},$$

which means that $||f||_2^2 \leq B\mathcal{F}(f, f)$ implies a bound of the form $1 + \beta_{|\mathfrak{X}|-1} \geq \frac{1}{B}$. □

The idea is that if we have a path of length 3 from x to y to z to x, we can write

$$f(x) = \frac{1}{2} \left(f(x) + f(y) - (f(y) + f(z)) + (f(z) + f(x)) \right),$$

and this type of expression works for any odd length. We then find that

$$||f||_2^2 = \sum_x |f(x)|^2 \pi(x) = \sum_x \frac{1}{2} \left(\sum_{e \text{ } i\text{th edge} \in \sigma_x} (-1)^i (f(e^+) + f(e^-) \right)^2 \pi(x);$$

using Cauchy-Schwarz and changing the order of summation like in the previous proof then gives us an analogous result. Often in probability, people make their chains lazy to avoid any issues with the negative eigenvalues, but in a real-world algorithm we may not always want to slow our chain down by a factor of 2 and thus we might actually care about parity effects.

Example 32

Suppose $K(x, x) > \varepsilon > 0$ for all x, meaning that we have some holding. Choosing σ_x to be a loop of length 1 for all x, we have

$$\frac{1}{Q(e)} \sum_{\sigma_x \ni e} |\gamma_{xy}| \pi(x) = \frac{1}{K(x, x)} \leq \frac{1}{\varepsilon},$$

which means that $\beta_{|\mathfrak{X}|-1} \geq -1 + 2\varepsilon$.

Example 33

Going back to the nearest-neighbor random walk on a path with holding from the beginning of the lecture, we pick σ_x to be the path that goes from x to the closest endpoint, makes a loop for one step, and then goes back to x (this is the shortest path of odd length). For this walk we have $Q(e) = \frac{1}{2N}$ and $|\sigma_x| \leq N+1$, and we end up getting the bound

$$B \leq \frac{N(N+1)}{N} \max_e \sum_{\sigma_x \ni e} 1,$$

meaning that $B \leq N(N+1)$ and thus $\beta_{|\mathfrak{X}|-1} \geq -1 + \frac{2}{N(N+1)}$ as promised.

4 January 18, 2024

Today will be a discussion of **comparison theory** – it's a big subject, so we'll start with random walks on finite groups (which is an area where the techniques work particularly well) and only eventually get to shuffling. Basically comparison theory tells us how to translate results over from a "nice" probability distribution (where we know everything) to another distribution.

Example 34

Suppose G is a finite group like C_n (the integers mod n) or C_2^n (the n-dimensional hypercube) or S_n (the set of permutations of size n). Let Q be a probability distribution on G. This generates a random walk as follows: pick $s_1, s_2, \cdots$ iid from Q and consider the walk which starts at the identity and repeatedly multiplies on the left by elements s_i, so we have $\text{id} \to s_1 \to s_2 s_1 \to \cdots$.

Symbolically, we have $Q * Q(s) = \sum_{t \in G} Q(t)Q(st^{-1})$, and similarly Q^{*k} is a sum over all possible intermediate steps that we could have taken. In our Markov chain notation, this means $K(t,s) = Q(st^{-1})$ for all $s, t \in G$.

Under mild conditions, such a walk always converges to the uniform distribution U on G, and in this lecture we'll be taking **symmetric** walks in which $Q(s) = Q(s^{-1})$. For such a walk, the Markov chain is reversible and thus we have a self-adjoint operator (we'll talk about the nonreversible case later on). Like in a previous lecture, we'll let ℓ^2 be the set of functions $f : G \to \mathbb{R}$ with inner product

$$\langle f, g \rangle = \sum_{s \in G} f(s)g(s)U(s),$$

and we think of K as a map $\ell^2 \to \ell^2$ given by

$$Kf(s) = \sum_{t \in G} K(s,t)f(t).$$

Self-adjointness yields eigenvalues and eigenvectors – our goal is to estimate how large k needs to be before we have $||Q^{*k} - U||_{\text{TV}} < \varepsilon$, and as usual we'll bound ℓ^1 by ℓ^2. We have by Cauchy-Schwarz that

$$\left|\left|Q^{*k} - U\right|\right|_{\text{TV}} = \frac{1}{2}\sum_s |Q^{*(k)}(s) - U(s)| \implies 4||Q^{*k} - u||_{\text{TV}}^2 \leq \left(\sum |Q^{*k}(s) - U(s)|\right)^2$$
$$\leq |G| \sum_s \left|(Q^{*k}(s) - U(s)\right|^2$$
$$= |G|^2 ||Q^{*k} - U||_2^2.$$

So far in this class, we've been bounding the last term on the right-hand side by bounding the eigenvalues.

Remark 35. *Notice that for this problem, where we start doesn't matter, we because*

$$\sum_s \left|Q^*(sx^{-1}) - U(s)\right| = \sum_s \left|Q^*(sx^{-1}) - U(sx^{-1})\right|$$

because our distribution is uniform and we're summing over all elements of the group.

There are two quadratic forms that we've introduced in this class so far, namely the Dirichlet form

$$\mathcal{E}(f,f) = \langle (I-K)f, f\rangle = \frac{1}{2|G|}\sum_{x,y}(f(x)-f(xy))^2 Q(y)$$

(here we're specializing to the form of $\pi(x)$ that we have for our random walk) and

$$\mathcal{F}(f,f) = \langle (I+K)f, f\rangle = \frac{1}{2|G|}\sum_{x,y}(f(x)+f(xy))^2 Q(y).$$

We've only described how to analyze the second and the smallest eigenvalues so far, but we can say more as well:

Theorem 36 (Minimax characterization)
Let V be a real vector space and $S : V \to V$ be a symmetric linear map. Suppose $q_0 \le q_1 \le q_2 \le \cdots$ are the eigenvalues of S. For a subspace $W \subseteq V$, let $m(W) = \min_{f\in W} \frac{\langle Sf,f\rangle}{\langle f,f\rangle}$ and $M(W) = \max_{f\in W} \frac{\langle Sf,f\rangle}{\langle f,f\rangle}$. Then

$$q_i = \max\left(m(W) : \dim(W^\perp) = i\right) = \min\left(M(W) : \dim(W) = i+1\right).$$

(For a reference, we can see Horn and Johnson's Matrix Analysis book.) **Throughout this lecture**, we'll have two different probability distributions: Q will be a distribution on G that we care about, and $\tilde{Q}$ will be a "nice" distribution where we already know all the results. The minimax characterization directly implies the following fact:

Theorem 37
Let $\mathcal{E}, \tilde{\mathcal{E}}$ be the Dirichlet forms corresponding to the distributions $Q, \tilde{Q}$ respectively. If $\tilde{\mathcal{E}} \le A\mathcal{E}$ for some A, then $\beta_i \le 1 - \frac{1-\tilde{\beta}_i}{A}$. On the other hand, if $\tilde{\mathcal{F}} \le A\mathcal{F}$, then $\beta_i \ge -1 + \frac{1+\tilde{\beta}_i}{A}$.

Proposition 38
Suppose we have the comparison $\tilde{\mathcal{E}} \le A\mathcal{E}$. Then

$$|G|\,||Q^{*n} - U||_2^2 \le \beta_{|G|-1}^{2n} + \exp(-n/A) + |G| \cdot \left|\left|\tilde{Q}^{*\lfloor n/2A\rfloor} - U\right|\right|_2^2.$$

If we additionally also have $\tilde{\mathcal{F}} \le A\mathcal{F}$, then

$$|G|\,||Q^{*n} - U||_2^2 \le \exp(-n/A) + |G| \cdot \left|\left|\tilde{Q}^{*\lfloor n/2A\rfloor} - U\right|\right|_2^2.$$

In other words, knowing how many steps it takes to make the $\tilde{Q}$ chain small tells us how many steps it takes to make the Q chain small – if it takes k steps in the former, it takes kA steps in the latter.

Proof sketch. We just need to work through lots of calculations and use the identities $1 - x \le e^{-x}$ for all x and $1 - x \ge e^{-2x}$ for $0 \le x \le \frac{1}{2}$. (For the details, see Diaconis and Saloff-Coste's paper "Comparison theory for random

walks on finite groups.") First, we have by definition that

$$\boxed{|G| \cdot ||Q^{*n} - U||_2^2} = \sum_{s \in S} |Q^{*n}(s) - U(s)|^2 = \sum_{s \in S} (Q^{*n}(s))^2 - \frac{1}{|G|} = Q^{*2n}(\mathrm{id}) - \frac{1}{|G|},$$

where in the last step we used the fact that the chain is reversible, so the sum of all possible ways of getting to the identity after $2n$ steps is to multiply by s after n steps and then multiply by s^{-1}. And this last quantity is equal to $\boxed{\frac{1}{|G|} \sum_{i=1}^{|G|-1} \beta_i^{2n}}$, since $Q^{*2n}(\mathrm{id}) = K^{2n}(x,x)$ for **any** x and thus

$$\sum_{i=0}^{|G|-1} \beta_i^{2n} = \mathrm{tr}(K^{2n}) = |G| \cdot Q^{*2n}(\mathrm{id}),$$

and subtracting off the first eigenvalue is where the $-\frac{1}{|G|}$ contribution comes from. But now we can separate out only the positive eigenvalues and the most negative one:

$$\frac{1}{|G|} \sum_{i=1}^{|G|-1} \beta_i^{2n} \leq \beta_{|G|-1}^{2n} + \frac{1}{|G|} \sum_{\beta_i > 0} \beta_i^{2n},$$

and now we use inequalities like $0 < \beta_i \leq 1 - \frac{1-\tilde{\beta}_i}{A} \leq \exp\left(-(1-\tilde{\beta}_i)/A\right)$ to conclude that

$$\frac{1}{|G|} \sum_{i=1}^{|G|-1} \beta_i^{2n} \leq \beta_{|G|-1}^{2n} + \frac{1}{|G|} \sum_{\beta_i > 0} \exp\left(-2(1-\tilde{\beta}_i)n/A\right) \leq \beta_{|G|-1}^{2n} + e^{-n/A} + |G| \cdot \left|\left|\tilde{Q}^{*\lfloor n/2A \rfloor} - U\right|\right|_2^2.$$

(The point is that the calculations are rather annoying to check, but we can read about it on our own if we want to check the details.) □

What we'll instead focus on for now is how to actually bound forms – we'll do this with a "path argument." Let $S = \{z_1, z_2, \cdots, z_{|S|}\}$ be a set of generators for G, meaning that we can write each y as a product of the form $z_{i_1} z_{i_2} \cdots z_{i_\ell}$. We **fix such a product** for each y and say that its length is $|y| = \ell$, and we let $N(z,y)$ be the number of times that a generator z appears in y.

Proposition 39

Let $\tilde{Q}$ and Q be symmetric probability distributions on a finite group G. Let S be a symmetric generating set for G with $\mathrm{supp}(Q) \supseteq S$. Then $\hat{\mathcal{E}} \leq A\mathcal{E}$ with

$$A = \max_{z \in S} \frac{1}{Q(z)} \sum_{y \in G} |y| N(z,y) \tilde{Q}(y).$$

As we'll see in some examples, this quantity A will actually be manageable to calculate in some complicated settings.

Proof. Suppose that $y = z_1 z_2 \cdots z_k$ with $z_i \in S$. Then we can write

$$f(x) - f(xy) = ([f(x) - f(xz_1)] + [f(xz_1) - f(xz_1 z_2)] + \cdots + [f(xz_1 \cdots z_{k-1}) - f(xy)])$$

like in our other path arguments. Squaring both sides and using Cauchy-Schwarz (without weights), we find that

$$(f(x) - f(xy))^2 \leq |y| \left([f(x) - f(xz_1)]^2 + \cdots + [f(xz_1 \cdots z_{k-1}) - f(xy)]^2\right).$$

Summing both sides in x, we have

$$\sum_x (f(x) - f(xy))^2 \leq |y| \sum_{x \in G, z \in S} (f(x) - f(xz))^2 N(z, y)$$

(this is the part where we use that we're summing over a group, because we can group based on the "jump" that the edge has made), and now multiply both sides by $\frac{\tilde{Q}(y)}{2|G|}$ and sum over y to get the Dirichlet form $\mathcal{E}(f, f)$ on the left-hand side. What's left on the right-hand side after changing the order of summation is

$$\frac{1}{2|G|} \sum_{x \in G, z \in S} (f(x) - f(xz))^2 Q(z) \cdot \boxed{\frac{1}{Q(z)} \sum_y |y| N(z, y) \tilde{Q}(y)},$$

and the boxed thing is what we need to maximize over all possible values of z. □

Corollary 40

Let $\tilde{Q}$ be the uniform distribution on G. Then $\hat{\mathcal{E}}(f, f)$ is just the variance of f, and we have $\beta_1(Q) \leq 1 - \frac{\eta}{\gamma^2}$, where $\eta = \min_{z \in S} Q(z), \quad \gamma = \operatorname{diam}(G)$.

Proof. In the expression $A \leq \min_z \frac{1}{Q(z)} \sum_{y \in G} |y| N(z, y)$, we can bound $N(z, y)$ by $|y|$ and bound $|y|$ by the diameter of G. Then $\sum_y \tilde{Q}(y) = 1$ and thus the whole boxed expression above simplifies to $\frac{\gamma^2}{\eta}$. Additionally, $\beta_1(\tilde{Q}) = 0$, since our matrix has $\frac{1}{|G|}$ in all entries and thus has top eigenvalue 1 and all other eigenvalues 0 (for example by Proposition 20). □

Example 41

Consider $G = S_n$ and let S consist of the generators $(1, 2)$, $(n, n-1, \cdots, 1)$, $(1, 2, \cdots, n)$, and (1). Let $Q(s) = \frac{1}{4}$ if $s \in S$ and 0 otherwise (so at each step, either do nothing, swap the top two cards, move the top card to the bottom, or move the bottom card to the top, all with equal probability).

We claim that $\gamma \leq 3n^2$ with this set of generators, and we show this in the following way: bring card n to the bottom in at most n moves. Now, inductively if cards i through n are in order, cycle card $i - 1$ to the top, and now repeatedly switch the top two, then cycle, then switch until $i - 1$ is in the right place; finally, re-cycle so that cards $i - 1$ through n are back in the right place. Since $\eta = \frac{1}{4}$, we have $\boxed{\beta_1 \leq 1 - \frac{1}{36n^4}}$ for this shuffle. The answer turns out to be $1 - \frac{c}{n^3}$, but this is a pretty good answer for how crude our estimate was!

We'll now improve that bound to the correct order by using **comparison**. Now let $\tilde{Q}(s)$ be $\frac{1}{n}$ if s is the identity or $\frac{2}{n^2}$ if $s = (i, j)$ for some transposition (i, j). With a bit of character theory (which we'll discuss later in the course), we find that $\beta_1 = 1 - \frac{2}{n}$ for the $\tilde{Q}$ walk. We now claim that

$$A \leq 4 \sum_y |y|^2 \tilde{Q}(n) \leq 36n^2.$$

The difference now is that $\tilde{Q}$ is **only supported on transpositions**, so we can bound $|y|$ only for those transpositions. And we can write any transposition using $3n$ generators from the S walk, giving us that inequality above. Now since the gap for the original chain is $\frac{2}{n}$, the gap for the compared chain is $\frac{2}{n \cdot 36n^2} = \frac{1}{18n^3}$ and thus $\boxed{\beta_1 \leq \frac{1}{18n^3}}$.

Therefore, if we try to study the random walk driven by Q and use the naive bound from the second eigenvalue, we find that

$$4 \left|\left| Q^{*k} - U \right|\right|_{\mathrm{TV}}^2 \leq n! \left(1 - \frac{1}{18n^3}\right)^{2k} \leq \exp\left(n \log n - \frac{k}{9n^3}\right),$$

meaning that we need k to be $9n^4(\log n + c)$ to make the total variation small. But the right answer is instead $n^3 \log n$, and we'll get there now again using comparison. In work by Diaconis and Shahshahani, it was shown that **for random transpositions**, if $k = \frac{1}{2}n(\log n + c)$, then $|G|^2 \left|\left|\tilde{Q}^{*k} - U\right|\right|_2^2 \leq 2e^{-c}$. But our comparison theorem above says that this means

$$|G|^2 \left|\left|Q^{*k} - U\right|\right|_2^2 \leq |G|\beta_{|G|-1}^{2k} + |G|e^{-k/A} + |G|^2 \left|\left|\tilde{Q}^{\lfloor k/2A \rfloor} - U\right|\right|_2^2,$$

where $A \sim n^2$. The last two terms are small if k/A is on the order of $n(\log n + c)$, and thus we require $k \sim n^3(\log n + c)$; this also makes the first term small enough.

We'll do a few more examples next time – Borel mentioned a few examples of "future work" in his book "The Mathematical Theory of Bridge," but "the future is now!"

5 January 23, 2024

We'll see some strengths and weaknesses of comparison theory through examples today, stating some open problems that can be interesting research directions too. Recall from last time that if we have a symmetric probability distribution Q on a finite group G (which generates G), and $\tilde{Q}$ is another "known" symmetric probability distribution, then

$$\tilde{\mathcal{E}} \leq A\mathcal{E} \implies |G| \cdot ||Q^{*k} - U||_2^2 \leq \beta_{|G|-1}^{2k} + \exp(-n/A) + ||G|| \cdot \left|\left|\tilde{Q}^{*\lfloor n/2A \rfloor} - U\right|\right|_2^2.$$

So being able to compare quadratic forms gives us a bound in terms of the smallest eigenvalue and the convergence rate of the $\tilde{Q}$ chain. We also discussed one way to find A: if S is a symmetric generating set for G with $\text{supp}(Q) \supseteq S$, and we choose a representation for every element of G as a product of generators $z_1 z_2 \cdots$, then $\tilde{\mathcal{E}} \leq A\mathcal{E}$ with $A = \max_{z \in S} \frac{1}{\tilde{Q}(z)} \sum_{y \in G} |y| N(z, y) \tilde{Q}(y)$, where $N(z, y)$ is the number of times z occurs in y.

Last time, we saw an example of this when S consisted of $(1, 2), (1, \cdots, n), (n, \cdots, 1)$, *and* id, and we compared the walk Q (which takes one of those four steps with probability $\frac{1}{4}$) to the walk $\tilde{Q}$ using random transpositions. (This told us that because we need $\frac{1}{2}n(\log n + c)$ steps for random transpositions, we need $36n^3(\log n + c)$ steps for this walk – our bound on total variation is $e^{-36n^2} + 3e^{-c}$ in this case.)

Conjecture 42

There is some universal constant $C > 0$ such that for every symmetric generating set $S \subseteq S_n$, $Cn^3(\log n + c)$ steps suffice. (So in particular, the chain we described above is the "slowest one.")

This conjecture has been verified for a lot of chains, and Helfgott, Seress, and Zuk have shown that $n^3(\log n)^2$ steps suffice for the generating set $S = (x, x^{-1}, y, y^{-1}, \text{id})$ for almost every pair $x, y \in S_n$ (using the same strategy of comparison to random transpositions). But reading that paper in more detail is one of the possible final projects for us to do.

Example 43 (A quantum mechanics conjecture of Feynman)

Let Γ be an undirected, connected graph on $\{1, 2, \cdots, n\}$ with edge set E. Let Q be defined on S_n as follows:

$$Q(s) = \begin{cases} \frac{1}{n} & s = \text{id}, \\ \left(1 - \frac{1}{n}\right) \frac{1}{|E|} & s = (i, j) \in E. \end{cases}$$

Basically, we can think of picking a random edge from the graph and flipping the cards corresponding to the edge's two neighbors. So if Γ is the complete graph, we get random transpositions, while if Γ is a path on n vertices, we get

random **adjacent** transpositions – Lacoin has shown that $\frac{n^3(\log n+c)}{\pi^2}$ is necessary and sufficient for this case. Finally, a star graph Γ can be thought of as random transposition with the top card, and that turns out to be twice as slow as random transpositions – Flatto, Odlyzko and Wales showed that $n(\log n + c)$ is necessary and sufficient.

The conjecture of Feynman is to consider an $N \times \cdots \times N$ **grid** graph (so $n = N^d$); we know some things about the two-dimensional case but less about dimensions three and higher. What we'll do is bound the mixing time using the **geometry** of the graph.

Theorem 44

Choose paths γ_{xy} in a general graph Γ, and let $\gamma = \max|\gamma_{xy}|$ and $b = \max_e \#\{\gamma_{xy} \ni e\}$. Then if $k = \left(\frac{8|E|\gamma b}{n} + n\right)(\log n + c)$ for some $c > 0$, then $||Q^{*k} - U||_{\text{TV}} \le \alpha e^{-c}$ for some explicit α.

Proof. Let $\tilde{Q}$ be the walk with random transpositions. We have $\tilde{\mathcal{E}} \le A\mathcal{E}$ with

$$A = \max_e \frac{1}{Q(e)} \sum_{y \in S_n} |y| N(e, y) \tilde{Q}(y),$$

but we only need to sum over transpositions y since those are the only cases with $\tilde{Q}$ nonzero. Notice that any transposition that switches i and j can be done by taking the path forward from i to j, then backwards from j to i (for example, if $1, 2, 3, 4, 5$ are in a line, we switch adjacent pairs to get 23451, then switch all adjacent pairs except the last one to get 52341); thus, $|(i, j)| \le 2|\gamma_{ij}| \le 2\gamma$. Any fixed edge is used at most twice in any path, so $|N(e, (i, j)| \le 2$, and there are only b paths that can use any fixed edge overall in this contribution. Finally, we have $Q(e) = \frac{n-1}{n}\frac{1}{|E|}$ uniformly for all edges. Then substituting everything back in gives the result. □

Feynman was less interested in the mixing time question and more in the following: there are discrete quantum Hamiltonians (finite Hermitian matrices) in which the Hamiltonian is unitarily equivalent to the transition matrix of a random walk on a graph. To state his question, we need a bit of background: any permutation $\sigma \in S_n$ can be written as a product of cycles. If we pick a uniform permutation at random, the length of the longest cycle turns out to be longer than we might think:

Theorem 45 (Lloyd–Shepp)

The expected length of the longest cycle is $\mathbb{E}[L(\sigma)] \approx 0.62n$ (where the 0.62 is actually some known, transcendental number).

So Feynman wanted the value of k such that under Q^{*k}, we have $L(\sigma) \asymp n$ (since when we start off at the identity permutation we have $L(\sigma) = 1$). He conjectured that **on a grid graph**, $L(\sigma)$ actually gets to the right order of magnitude faster than the mixing time (which has some physical significance) in dimensions 3 and higher. For example, the mixing time on the 2D grid is $N^{5/2} \log N$, and Feynman thinks this is still right for $L(\sigma)$. But in higher dimensions, he's claiming that we don't need the analogous log factor.

This is still a question of interest today, and Schramm did it for the complete graph – there it turns out it takes $\frac{1}{2}n \log n$ to mix everything but βn (where $\beta \approx 0.71$) for long cycles; other than the number of fixed points, the distribution of cycles are all correct faster than $n \log n$. And a paper by Berestycki, Schramm, and Zeitouni (called "Mixing times for random k-cycles and coalescence-fragmentation chains") goes into more detail along these lines.

Remark 46. *The research community on random graphs knows a lot about the model where we start with an empty graph on n vertices and add edges gradually at random. It turns out that it takes $\frac{1}{2}n \log n$ steps to make the graph connected, and this is connected to the $\frac{1}{2}n \log n$ from random transpositions if we think about "adding (i, j) as "swapping*

i and j." But it turns out representation theory gives a much shorter proof than what's required from bringing together work across the random graph literature. A similar story where representation theory can do a lot of work is the "coagulation-fragmentation" physics model related to Markov chains on cycles.

We'll now return closer to actual card shuffling, using the machinery we've introduced here.

Example 47

In the **neat overhand shuffle** (which is what we use if we're trying to cheat in a card game and only draw one card down at a time), we use the following operations: let t_j reverse the top j cards, which we can think of as the permutation $(1,j)(2,j-1)(3,j-2),\cdots$ (and let t_1 be the identity). Let $Q(\sigma)=\frac{1}{n}$ for $\sigma=t_j$ for some $1\le j\le n$ and 0 otherwise.

Theorem 48

For the chain above, let $k=48n(\log n+c)$. Then $||Q^{*k}-U||_{\text{TV}}\le \alpha e^{-c}$.

Proof. Again compare with random transpositions. Notice that applying $t_{j-1}t_j$ is the same as swapping the top card with the jth card, and $t_{i-1}t_{i-2}t_{i-1}t_i$ is the same as swapping two adjacent cards. Therefore, we can compare with the "adjacent transpositions" chain. The length of any generator is 4. Furthermore, for any fixed t_i, $N(t_i,(1,j))$ is constant, and we have a finite sum because each t_i only appears in finitely many of the $(1,j)$s. Thus we end up finding that A is constant in this case. □

Example 49

Similarly, consider the shuffle where we cut a deck in two spots, and instead of grouping them as "bottom, middle, then top", we swap the order as "top, middle, then bottom" while keeping the order within each group the same. Then we can show $607n(\log n+c)$ shuffles is enough, though the constant can probably be improved.

Looking at the bigger picture, there are other groups besides S_n where random walks are interesting, such as the finite almost simple groups of Lie type (like $\text{GL}_n(\mathbb{F}_q)$, $\text{SL}_{2n}(\mathbb{F}_q)$, or $O_n(\mathbb{F}_q)$). And we can carry out the same project on these groups – if $S\subseteq G$ is a symmetric generating set, we can have Q be the identity with probability θ and each of the generators of S with probability $(1-\theta)\frac{1}{|S|}$. And what's nice is that the group theory community has figured out the equivalent of the "random transposition" question for these other groups – they've done the work of understanding random walks constant on conjugacy classes. Here's an example of a result that they've proved:

Theorem 50

Let G be a finite almost simple group and $S\subseteq G$ a conjugacy class that generates G, and let $Q(s)$ be as above. Then there are universal constants $c,C>0$ independent of G such that

$$\frac{c\log|G|}{\log|S|}\le\tau\le\frac{C\log|G|}{\log|S|},$$

where τ is the mixing time (the smallest k such that $||Q^{*k}-U||_{\text{TV}}\le\frac{1}{e}$).

Example 51

Let $G=O_{2n}(\mathbb{F}_q)$ for q odd, and let S be the set of all reflections of the form $I-2UU^T$ where $U^TU=1$. Then $|G|=2q^{n^2}\prod_j(q^{2j}-1)$ and $|S|=(q^n-1)/2$, so τ is of order n.

So what remains to be done is to take natural generating sets for these groups and do this process where we write generators in terms of these conjugacy classes to get comparison theory results.

Example 52

Let $G = \mathrm{SL}_n(\mathbb{F}_q)$, and let S be the set of transvections of the form $I + b^T a$, where $a, b \in \mathbb{F}_q^n$ (basically row operations). It's been shown that $n + c$ steps are necessary and sufficient for this S (using character theory). If we then compare to $S = \{I + aE_{ij}\}$ (meaning that we multiply row i by a and add it to row j), we can solve an interesting problem understanding how long it takes for row reduction operations to mix.

Remark 53. *Tikhomirov and Youssef have shown how to generalize comparison theory to Markov chains on different spaces, though we do need a way of studying the mapping between the spaces. Interestingly, this technique doesn't require similar stationary distributions – everything we've been doing has implicitly been using that the walks are uniform, because otherwise we lose some factors in various places in our argument.*

We'll start representation theory and Fourier analysis on finite groups next time, finally proving the $\frac{1}{2} n \log n$ fact that we've been using as comparison.

6 January 25, 2024

We'll start today with an introduction to representation theory on finite groups, since this is the main way that we can compute exact results about certain Markov chains (and thus use them for comparison theory). For more details, we can read chapter 2 of Professor Diaconis' free book "Group Representations in Probability and Statistics" or Serre's "Linear Representations of Finite Groups."

Throughout this discussion, G will be a finite group.

Definition 54

A **representation** of G is a map $s \mapsto \rho(s) \in \mathrm{GL}_k(\mathbb{C})$ such that $\rho(st) = \rho(s)\rho(t)$.

In other words, we assign a matrix $\rho(s)$ to each group element s in a way that respects multiplication – the representation of permutations as permutation matrices is a valid example. We can think of having some vector space V and having each $\rho(s)$ as being a map on V.

Definition 55

A representation ρ is **reducible** if there is some nonzero proper subspace W of V with $\rho(s)W \subseteq W$ for all s, and it is **irreducible** otherwise.

Definition 56

Let $Q(s)$ be a probability distribution on G. The **Fourier transform** of Q is defined as

$$\hat{Q}(\rho) = \sum_{s \in G} Q(s)\rho(s).$$

We can check by a direct computation that

$$\widehat{Q * Q}(\ell) = \hat{Q}(\ell)^2$$

(this is the usual "Fourier transform takes convolution to products" fact), and thus more generally $\widehat{Q^{*k}}(\ell) = \hat{Q}(\ell)^k$. And given the Fourier transform, we can also recover the original function using Fourier inversion: in particular, we have that (letting $\hat{G}$ denote the **dual space** of all such representations)

$$Q^{*k}(s) = \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_\rho \mathrm{Tr}(\hat{Q}(\ell)^k \rho(s^{-1})),$$

where d_ρ is the dimension of the representation (that is, the dimension of the vector space).

Fact 57

Let U be the uniform distribution on G. If ρ is irreducible, then $\hat{U}(\rho) = 1$ if ρ is the one-dimensional trivial representation (denoted 1) and $\hat{U}(\rho) = 0$ otherwise.

The idea will be to show that $Q^{*k} \to U$ by instead showing that $\hat{Q}(\rho)^k \to 0$ for all nontrivial $\rho \in \hat{G} - \{1\}$.

Lemma 58 (Upper bound lemma)

Let G be a finite group and $Q(s)$ a probability distribution on G. Then

$$4 \left|\left|Q^{*k} - U\right|\right|_{\mathrm{TV}}^2 \leq \sum_{\rho \in \hat{G} - \{1\}} d_\rho ||\hat{Q}(\rho)||^{2k},$$

where the norm of a matrix is defined via $||M||^2 = \mathrm{Tr}(MM^*)$.

Proof. We have

$$4 \left|\left|Q^{*k} - U\right|\right|_{\mathrm{TV}}^2 = \left(\sum |Q^{*k}(s) - U(s)|\right)^2 \leq |G| \sum \left|Q^{*k}(s) - U(s)\right|^2$$

by Cauchy-Schwarz, and now by the Plancherel theorem (which says that the L^2 norm between two functions is the same as the L^2 norm between their Fourier transforms)we can also write this as

$$= \sum_{\rho \in \hat{G} - \{1\}} d_\rho \mathrm{Tr}\left(\hat{Q}(\rho)^k (\hat{Q}(\rho)^k)^*\right),$$

and now we use that the norm of a product is at most the product of the norms. □

Remark 59. *The above was the bound stated in class, but notice that the final step loses a factor of* $(\dim \rho)^{k-1}$ *in the calculation – if we have eigenvalue estimates for* $\hat{Q}$*, it is more efficient to apply them to* $\hat{Q}(\rho)^k$ *and* $(\hat{Q}(\rho)^k)^*$ *directly.*

Example 60

Suppose that $G = \mathbb{Z}/m\mathbb{Z}$ is the cyclic group on m elements. This is an abelian group, and for all abelian groups all irreducible representations are one-dimensional.

In this case, we can write the representations as

$$\rho_j(k) = e^{2\pi i j k/n}, \quad 0 \leq j \leq m-1;$$

that is, there are m irreducible representations indexed by the complex roots of unity. We then have the relations

$$\hat{Q}(j) = \sum_{k=0}^{m-1} Q(k) e^{2\pi i j k/m},$$

$$Q(k) = \frac{1}{m}\sum_{j=0}^{m-1} \hat{Q}(j) e^{-2\pi i j k/m},$$

and this is what the engineers use as the "finite Fourier transform." So the upper bound lemma then tells us that

$$4||Q^{*k} - U||_{\text{TV}}^2 \leq \sum_{j=1}^{m-1} |\hat{Q}(j)|^{2k},$$

and we can bound convergence if we can understand how the Fourier transforms tend to zero. In the simplest case, suppose $Q(1) = Q(-1) = \frac{1}{2}$ (so we have a simple random walk). Then

$$\hat{Q}(j) = \frac{1}{2}e^{2\pi i j/n} + \frac{1}{2}e^{-2\pi i j/n} = \cos\left(\frac{2\pi j}{n}\right),$$

which means that

$$4||Q^{*k} - U||_{\text{TV}}^2 \leq \sum_{j=1}^{m-1} \cos\left(\frac{2\pi j}{n}\right)^{2k},$$

and now to bound the right-hand side we have to do some calculus – first at the heuristic level, we have $\cos(x) = 1 - \frac{x^2}{2} + O(x^4)$, so

$$\cos\left(\frac{2\pi}{m}\right)^{2k} \approx \left(1 - \frac{2\pi^2}{m^2}\right)^{2k} \approx \exp\left(-\frac{2\pi^2}{m^2}2k\right),$$

which is small if $k = cm^2$. So now we're ready to be more careful:

Theorem 61

With everything as above (simple random walk $Q(1) = Q(-1) = \frac{1}{2}$) on a cycle of size m), if $k \geq m^2$ and m is odd to avoid parity issues, then $||Q^{*k} - U||_{\text{TV}} \leq e^{-\frac{\pi^2}{2}k/m^2}$ (so in particular cm^2 steps gets a TV of $e^{-c\pi^2/2}$).

Proof. There's a few main tricks we use for these kinds of bounds, and we'll see them as we continue on through the class (like $1 - x \leq e^{-x}$). We have from above that

$$||Q^{*k} - U||_{\text{TV}}^2 \leq \frac{1}{4}\sum_{j=1}^{m-1} \cos\left(\frac{2\pi j}{m}\right)^{2k},$$

and now if we "fold the sum over" in half (using the symmetry of cosine), this simplifies to $\frac{1}{2}\sum_{j=1}^{(m-1)/2} \cos\left(\frac{\pi j}{m}\right)^{2k}$ (here we're using that $\cos x = -\cos(\pi - x)$). We can now use that $\cos x \leq e^{-x^2/2}$ for all $x \in [0, \pi/2]$ (see the following inequalities cheat sheet for more useful stuff like this), so we can bound this by

$$||Q^{*k} - U||_{\text{TV}}^2 \leq \frac{1}{2}\sum_{j=1}^{(m-1)/2} \exp\left(-\frac{\pi^2 j^2 k}{m^2}\right) \leq \frac{1}{2}\exp\left(-\frac{\pi^2}{m^2}\right)\sum_{j=1}^{\infty} \exp\left(-\frac{\pi^2(j^2-1)k}{m^2}\right),$$

and now we can turn this into a geometric series by bounding from above by something with a smaller exponent:

$$||Q^{*k} - U||_{\text{TV}}^2 \leq \frac{1}{2}\exp\left(-\frac{\pi^2 k}{m^2}\right)\sum_{j=1}^{\infty} \exp\left(-\frac{3\pi^2 j k}{m^2}\right) = \frac{\frac{1}{2}e^{-\pi^2 k/m^2}}{1 - e^{-3\pi^2 k/m^2}},$$

and now as long as $k \geq m^2$ the denominator is at least $\frac{1}{2}$. Finally taking square roots yields the result. □

We've done the simple case where we have a simple random walk, but there are lots of research questions we can

ask even from this point. For example, suppose S is a symmetric generating set for C_m, and consider the walk

$$Q(s) = \begin{cases} \frac{1}{|S|} & s \in S, \\ 0 & \text{otherwise.} \end{cases}$$

For example, we could consider the the set where S is uniform on the integers between $-j$ and j – in such cases, the same reasoning shows that $O(m^2)$ steps are necessary and sufficient. If $|S| = 2$ (even if we don't have a symmetric set), we always have the same situation as ± 1, since we can solve the equations $ax + b = 1, ay + b = -1$ and thus we have an affinely transformed walk from the usual one. However, when $|S| = 3$, almost all sets (as a proportion of the possibly sets) end up converging in $O(m)$ steps. Interestingly, it was open for a while to find an example where $O(m)$ is actually achieved – Greenhalgh was able to find a result.

On a cycle, most of these walks here take cm^2 steps, where we need c large to get small TV distance. So there was a question for a while which asked whether there was a set of generators so that the walk has cutoff (convergence happening in terms of a lower order term); Hough showed that when $S = \{\pm 1, \pm 2, \pm 4, \cdots, \pm 2^{\lfloor \log p \rfloor}\}$ in fact has a cutoff when we're on $\mathbb{Z}/p\mathbb{Z}$. But we'll explain more precisely what we mean by cutoff now:

Definition 62

Let G_n be a sequence of groups, and let $(K_n(x, y), \pi_n(y))$ be a sequence of Markov chains and stationary distributions on G_n and x_0^n a sequence of starting states. Then we say that G_n has a **cutoff at ℓ_n** if for all $\varepsilon > 0$,

$$\left|\left| K_{x_0^n}^{\ell_n(1+\varepsilon)} - \pi_n \right|\right|_{\text{TV}} \to 0, \quad \left|\left| K_{x_0^n}^{\ell_n(1-\varepsilon)} - \pi_n \right|\right|_{\text{TV}} \to 1.$$

In other words, we need to get from TV distance 1 to 0 in a "lower-order" amount of time than the leading term.

Conjecture 63 (Peres conjecture)

A reversible sequence (K_n, π_n) has a cutoff if and only if the product of the **mixing time** (the smallest k so that $||K^\ell - \pi|| < \frac{1}{e}$) and **spectral gap** (distance between 1 and the second eigenvalue) tends to infinity.

Example 64

We know that C_m with the $\{\pm 1\}$ walk has mixing time of order m^2 but spectral gap of order $\frac{1}{m^2}$, so the product is bounded (and indeed there is no cutoff).

By the way, this behavior where "getting away from the trivial representation causes the eigenvalues to decrease" in the $\{\pm 1\}$ walk is similar to the **Riemann-Lebesgue lemma**, and it's true often enough that there should be a way of proving that. And we'll comment on this in various examples, but it's hard to formulate such a result and prove it (especially since the eigenvalues do "come back around" on the other side).

Example 65

Meanwhile, for the hypercube C_2^d, the mixing time is of order $d \log d$ and the spectral gap is of order $\frac{1}{d}$, and indeed we do have cutoff for the hypercube.

We have the tools to calculate the spectral gap now: labeling the vertices of the hypercube with binary d-tuples, we have

$$\rho_x(y) = (-1)^{x \cdot y}.$$

If we now think about the Ehrenfest urn example, where $Q(0) = Q(e_j) = \frac{1}{d+1}$ is the nearest-neighbor random walk with holding, then

$$\hat{Q}(x) = \sum_y Q(y)(-1)^{x\cdot y} = \frac{1}{d+1}\left(1 + \sum_{j=1}^{d}(-1)^{x_j}\right) = 1 - \frac{2|x|}{d+1},$$

where $|x|$ is the number of nonzero elements in the vector x. Therefore,

$$4\left|\left|Q^{*k} - U\right|\right|_{\text{TV}}^2 \le \sum_{j=1}^{d}\binom{d}{j}\left(1 - \frac{2j}{d+1}\right)^{2k}.$$

To compute the right-hand side, we can again fold in half and write this as

$$2\sum_{j=1}^{\lfloor d/2\rfloor}\binom{d}{j}\left(1 - \frac{2j}{d+1}\right)^{2k},$$

and now we use the bounds $\binom{d}{j} \le \frac{d^j}{j!}$ and $1 - x \le e^{-x}$ to find that

$$4\left|\left|Q^{*k} - U\right|\right|_{\text{TV}}^2 \le 2\sum_{j=1}^{\infty}\frac{d^j}{j!}\exp\left(-\frac{4jk}{d+1}\right).$$

In particular, if $\boxed{k = \frac{d+1}{4}(\log d + c)}$, then we can cancel out the $d^j = e^{j\log d}$ term and we're left with

$$4\left|\left|Q^{*k} - U\right|\right|_{\text{TV}}^2 \le 2\sum_{j=1}^{\infty}\frac{1}{j!}e^{-jc} = 2\left(e^{e^{-c}} - 1\right),$$

and this right-hand side is exponentially small as c grows (because $e^{e^{-c}} \approx 1 + e^{-c}$). So the analysis is pretty straightforward again (just using simple inequalities), and we're able to get pretty sharp results. (All of these results have matching lower bounds as well.)

We'll close with a few remarks and questions (and next time we'll start on the symmetric group).

Example 66

Professor Diaconis was interested in the problem of "cooking potatoes evenly," and he thought about this with the following simple model. Suppose we have n potato slices on the boundary of a pan, and we have a spatula of radius d. Then our mixing of the potatoes involves putting the spatula into the pan randomly and flipping d consecutive potatoes around (including wrap-around). Our question is then to imagine all potatoes starting on the "down" side and seeing how long it takes for the up-down pattern to get random.

When we try doing this, we need mathematically for d to be relatively prime to n, but thinking of this as a random walk on the hypercube, we end up doing the same kinds of inequalities and bounds – the mixing time doesn't end up depending on the size of our spatula d. We can even use differently-shaped "spatulas" and we get the same answer! But after a while, Professor Diaconis realized that this walk is given by $S = \{v_1, v_2, \cdots, v_n\}$ for $v_i \in C_2^n$, and we need the v_i to be a basis for C_2^n. And any basis is linearly equivalent to the standard basis, so it's equivalent to just consider flipping one potato at a time.

On the other hand, it's interesting to ask the question of how to make the walk mix faster if we have more than n generators in S – we know that for most sets of size $2n$ we end up with $n^{3/4}$ instead of $n\log n$, but we haven't been able to find an explicit example yet!

7 January 30, 2024

Today's first topic is random transpositions – we're working on S_n, and we consider the walk where $Q(\text{id}) = \frac{1}{n}$ and $Q(\tau) = \frac{2}{n^2}$ for any transposition τ. (This is the walk that we've been doing comparison theory with, but we haven't actually proven any results with it yet.) Then we want to show the following:

Theorem 67

For the random-transpositions walk, after $\left\lfloor \frac{1}{2} n(\log n + c) \right\rfloor$ steps, we have

$$\begin{cases} ||Q^{*k} - U||_{\text{TV}} \leq 2e^{-c} & c > 0, \\ ||Q^{*k} - U||_{\text{TV}} \geq \frac{1}{e} - e^{-e^{-2c}} & c < 0. \end{cases}$$

The proof uses representation theory of S_n, and we'll do it in stages. First, notice that we all already know three representations of the symmetric group:

- the **trivial representation**, which assigns $\rho_n(\sigma) = 1$ to all permutations σ,
- the **sign representation**, which is defined by $\rho_n(\sigma) = \text{sgn}(\sigma)$, and
- the **permutation representation**, where $\rho(\sigma)$ is an n-dimensional representation whose (i,j)th entry is $\delta_{i,\sigma(j)}$.

This last one is not irreducible: if e_i denotes the ith basis vector, then $\rho(s)e_i = e_{\rho(i)}$, which means that the subspace

$$W = \left\{ v \in \mathbb{R}^n : \sum v_i = 0 \right\}$$

is an invariant subspace of $\mathbb{R}^n$, and its complement $W^\perp$ (the linear span of $\{1, 1, \cdots\}$) is invariant as well. But the restriction of the permutation representation to W **is** in fact irreducible, and we denote it with $\rho_{n,n-1}$. We can now build a fourth representation:

- Let S_n act on $\mathbb{R}^{\binom{n}{2}}$, labeling a basis with the set of 2-element sets of $[n]$. Then we can define $\rho(s)$ via

$$\rho(s)e_{\{i,j\}} = e_{\{s(i),s(j)\}}.$$

Like before, this representation is not irreducible – it turns out there are two copies of the $(n-1)$-dimensional representation and one of the trivial representation, so we have the decomposition

$$\mathbb{R}^{\binom{n}{2}} = W + V_1 + V_2 + \text{trivial},$$

where W is a representation of dimension $\binom{n}{2} - 2(n-1) - 1 = \frac{n(n-3)}{2}$. And in general, if we look at an indexing not by pairs but by k-tuples, we can build all of the irreducible representations by doing this kind of construction and subtracting off smaller parts.

Recall that in a general group, two elements s, t are **conjugate** if we have $s = u^{-1}tu$ for some other group element u. Conjugacy is an equivalence relation, so we can break up a group into conjugacy classes; it's a fact that the **number of irreducible representations of G is equal to the number of conjugacy classes**.

Example 68

Every permutation can be written as a sum of disjoint cycles (for example the permutation sending $1,2,3,4,5,6$ to $3,2,1,4,6,5$ has the cycles $(13)(2)(4)(56)$), and then conjugating by some other permutation τ is the same as "applying τ inside each cycle" (in this case it would give us $(\tau(1)\tau(3))(\tau(2))(\tau(4))(\tau(5)\tau(6))$).

So the conjugacy classes in S_n are indexed by **partitions** of n – all that matters is the number of cycles of each type. We write that $\lambda \vdash n$ (λ is a partition of n) if we have $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq 0)$ with $\sum_i \lambda_i = n$; we can also think of this as being represented with a diagram with λ_1 boxes in the first row, λ_2 in the next, and so on. Alternatively, we can denote a partition $1^{a_1}2^{a_2}\cdots n^{a_n}$, where a_i is the number of parts of λ of size i. So we'll index the irreducible representations of S_n using partitions λ and write them as $\rho_\lambda(\sigma)$.

What's nice is that the random-transpositions measure Q is **constant on conjugacy classes** (because all transpositions are conjugate):

Lemma 69

Let G be a finite group, and let Q be constant on conjugacy classes (meaning that $Q(s) = Q(t^{-1}st)$ for all s,t). Let ρ be an irreducible representation. Then the Fourier transform satisfies $\hat{Q}(\rho) = cI$, where

$$c = \frac{1}{d_\rho}\sum_{s\in G} Q(s)\chi_\rho(s).$$

Here $\chi_\rho(s)$ is the trace of the matrix $\rho(s)$, and it's called the **character** of ρ at s.

Proof. We have that

$$\rho(s^{-1})\hat{Q}(\rho)\rho(s) = \sum_{t\in G} Q(t)\rho(s^{-1}ts) = \hat{Q}(\rho),$$

so $\rho(s)\hat{Q}(\rho) = \hat{Q}(\rho)\rho(s)$. Now **Schur's lemma** says that if ρ is irreducible and M is a matrix that commutes with the action of the group, then M is a constant times the identity; thus, $\hat{Q}(\rho) = cI$ and taking traces on both sides yields the formula for c. □

So now if Q is the random transpositions walk, then

$$\hat{Q}(\rho) = cI, \quad c = \frac{1}{d_\rho}\left(d_\rho + \binom{n}{2}\cdot\frac{1}{n^2}\cdot\chi_\rho((1,2)\right)$$

(the character of any transposition is the same), and therefore

$$\hat{Q}(\rho) = 1 + \frac{n-1}{n}\frac{\chi_\rho(1,2)}{d_\rho}.$$

Plugging this into the upper bound lemma, we thus find that

$$\begin{aligned} 4||Q^{*k} - U||_{\mathrm{TV}}^2 &\leq \sum_{\lambda\vdash n, \lambda\neq(n)} d_\lambda \mathrm{Tr}(\hat{Q}(\rho)^k\hat{Q}(\ell)^{*k}) \\ &= \sum_{\lambda\perp n} d_\lambda^2\left(\frac{1}{n} + \frac{n-1}{n}\cdot\frac{\chi_\lambda(1,2)}{\chi_\lambda(1)}\right)^{2k}. \end{aligned}$$

But now we need to understand what the values of $\frac{\chi_\lambda((1,2))}{d_\lambda}$ look like, and this is where we need to do work. If we look up a table of all 42 partitions of 10, for example, we see that the dimensions vary a lot (for example $(5,3,2)$ has dimension 450), but in general $\chi_\rho(\tau)$ will be significantly smaller (for example $\chi_($(5,3,2)) for a transposition is 70).

So the rough argument is that this whole quantity can be approximately bounded by $\left(\frac{1}{2}\right)^{2k} \sum_\lambda d_\lambda^2$, and now we can use the fact that the sum of the irreducible representations' dimensions is always the size of the group (this comes from the decomposition of the regular representation). Thus we find heuristically that

$$4||Q^{*k} - U||_{\text{TV}}^2 \le \left(\frac{1}{2}\right)^{2k} n! \approx \exp\left(-2k \log 2 + n \log n\right)$$

and therefore we need k needs to be of order $n \log n$ to get something small.

However, we'll notice that there are terms in the sum like $\lambda = (n-1, 1)$ in which $d_\lambda = n-1$ but $\chi_\lambda((1,2)) = n-3$. (Indeed, if we make a transposition, that puts i, j off the diagonal so we lose 2 from the trace, and we lose another 1 from subtracting off the multiples of the all-1s vector.) So one of the terms in our sum above will have the base of its exponential be $\left(\frac{1}{n} + \frac{n-1}{n}\left(\frac{n-3}{n-1}\right)\right) = 1 - \frac{2}{n}$, which is not close to $\frac{1}{2}$. But the total contribution of this term to the sum is $(n-1)^2\left(1-\frac{2}{n}\right)^{2k} \le e^{2\log n - \frac{4k}{n}}$, so in fact again we just need k around $\frac{1}{2} n \log n$ to kill that individual term. It turns out this is the biggest term – all other terms are smaller, so $\frac{1}{2} n \log n$ does end up being the right answer.

Fact 70

Now that we've established the heuristics, we'll be a bit more precise. One comment is that we have a **sum over partitions** in this problem, where the analysis ends up different from ordinary Fourier analysis but some of the computations still end up being relatively similar.

Recall that our goal is to get some nice bounds on $\frac{\chi_\lambda(\tau)}{d_\lambda}$ that we can do calculations with, and it turns out Frobenius has the following result (which we can prove by induction or symmetric function theory):

Proposition 71 (Frobenius)

We have

$$\frac{\chi_\lambda(\tau)}{d_\lambda} = \frac{1}{n(n-1)} \sum_{j=1}^{\ell} (\lambda_j^2 - (2j-1)\lambda_j) = \frac{1}{\binom{n}{2}} \left(\sum_i \binom{\lambda_i}{2} - \sum_j \binom{\lambda_j'}{2} \right),$$

where λ' is the transpose of the permutation λ.

Example 72

Suppose $\lambda = (n-1, 1)$. Then the first formula yields the correct answer of

$$\frac{\chi_\lambda(\tau)}{d_\lambda} = \frac{1}{n(n-1)}([(n-1)^2 - (n-1)] + [1^2 - 3]) = \frac{1}{n(n-1)}(n^2 - 3n) = \frac{n-3}{n-1},$$

and similarly the second formula yields $\frac{2}{n(n-1)}\left(\binom{n-1}{2} - 1\right) = \frac{2}{n(n-1)}\left(\frac{n^2-3n}{2}\right) = \frac{n-3}{n-1}$ as well (since the transpose of our partition is $(2, 1, 1, \cdots)$).

Proposition 73 (Young)

For any λ, d_λ is the number of standard **Young tableaux** of shape λ, meaning that we fill in the boxes of the permutation with 1 through n so that the entries are increasing to the right and downward.

For example, here is a valid Young tableau of size $(4, 2, 2)$:

1	2	5	7
3	4		
6	8		

In particular, we will just need the inequality

$$d_\lambda \le \binom{n}{\lambda_1} d_{\lambda^*},$$

where $\lambda^* = (\lambda_2, \lambda_3, \cdots, \lambda_\ell)$, since we can choose λ_1 of the numbers to be in the first row and then arrange the remaining numbers in the remaining boxes to be monotone in the remaining shape (we just have an upper bound because there are additional constraints coming from that first row). We can then bound d_{λ^*} by $\sqrt{(n-\lambda_1)!}$ and that's often good enough for general estimates.

Proposition 74

Let $r(\lambda) = \frac{\chi_\lambda(\tau)}{d_\lambda}$. Then r is monotone in the usual partial ordering on partitions (**Schur convexity** or the **majorization order**), where two partitions of n satisfy $\lambda \ge \lambda'$ if

$$\lambda_1 \ge \lambda_1', \quad \lambda_1 + \lambda_2 \ge \lambda_1' + \lambda_2', \quad \lambda_1 + \lambda_2 + \lambda_3 \ge \lambda_1' + \lambda_2' + \lambda_3', \cdots$$

Another way to describe this majorization order is by saying that we can get from λ' to λ by moving up boxes (and having legitimate partitions along the way) – under this partial order, the partition (n) is the largest, and $(1, 1, \cdots, 1)$ is the smallest.

Proof. It suffices to consider just moving up one box and proving that $r(\lambda)$ increases. If we have $\lambda_a = \lambda_a' + 1$ and $\lambda_b = \lambda_b' - 1$ (so we move the box from the bth row to the ath row), then we can write down from Proposition 71 that

$$r(\lambda) - r(\lambda') = \frac{1}{n(n-1)} (\lambda_a' - \lambda_b' + (b-a) + 1) \ge \frac{4}{n(n-1)} > 0,$$

so we do increase the character ratio. □

So the idea is that we can always move boxes up until the partitions are nice and where we have nicer formulas for these character ratios:

Corollary 75

If λ is a partition of n, then $r(\lambda) \le \frac{\lambda_1 - 1}{n-1}$ for all λ. Additionally, if $\lambda_1 \ge \frac{n}{2}$, we have $r(\lambda) \le 1 - \frac{2(n-\lambda_1)(\lambda_1+1)}{n(n-1)}$.

We find that the main contributions to the sum mostly come from terms where λ_1 is large, so those are the ones we'll have to bound carefully. And the rest is just computation – we need to do some more involved bounding involving geometric series and inequalities. We can see the book on group representations (pages 42 to 43) for more details; here we'll just do the lower bound:

Proof of the lower bound in Theorem 67. Recall that the total variation distance is defined by

$$\left|\left|Q^{*k} - U\right|\right| = \sup_{A \subseteq S_n} \left|Q^{*k}(A) - U(A)\right|,$$

and so getting a lower bound just comes from finding a set A where explicit formulas are easier to find. Intuitively, not doing enough switches means that there are some cards we haven't touched, so we can define

$$A = \{\sigma \in S_n : \text{fixed points}(\sigma) \ge 1\}.$$

The number of fixed points of a permutation are approximately Poisson with parameter 1, and in fact $U(A) = 1 - \frac{1}{e} + O\left(\frac{1}{n!}\right)$. But if we want to estimate $Q^{*k}(A)$, suppose $(L_1, R_1), \cdots, (L_k, R_k)$ are the pairs we've switched along the way. Then we can think about whether the set $\{L_1, R_1, \cdots, L_k, R_k\}$ has hit all of $\{1, 2, \cdots, n\}$; this is the coupon collector's problem, and when the dust settles we see that $Q^{*k}(A) \geq 1 - e^{-e^{-c}} + o(1)$ if $k = \frac{1}{2}n(\log n + c)$. Putting these together yields the result. □

Remark 76. *It turns out that this example above is the "only way" in which random transpositions fails to mix: if $k > 0.7n$ and we have L fixed points, then we can compare Q^{*k} to the uniform distribution on permutations with L fixed points, and we have exponential convergence. (This is work by Berestycki, Schramm, and Zeitouni.) So the only obstacle past this point is mixing between the number of fixed points!*

A natural generalization of this idea is to try other conjugacy classes (for example); the character theory all goes through and we just need to do the computation. The following is the state-of-the-art theorem:

Theorem 77 (Muller-Schlage-Puchta, 2007)
Let C be a conjugacy class in S_n with $F(C) > 0$ fixed points. Then $k = \frac{\log n}{\log(n/F(C))}$ steps are necessary and sufficient.

For example, if C is the set of transpositions, then $F(C) = n - 2$ and the denominator is

$$\log \frac{n}{n-2} = -\log\left(1 - \frac{2}{n}\right) = \frac{2}{n} + O\left(\frac{1}{n^2}\right),$$

so we do indeed get the bound $\frac{n}{2}\log n$. But it's interesting that in all of the problems that have been solved, comparison theory has never been applied to anything besides random transpositions!

8 February 1, 2024

Today's goal is to be a little more rigorous with the representation theory that we motivated in the last few lectures – again, everything is in Professor Diaconis' book (chapter 2) written for statisticians. We'll do everything with finite-dimensional vector spaces over $\mathbb{C}$ (for something like S_n we only needed $\mathbb{R}$, but in general it's good to have complex numbers to account for non-real eigenvalues). Recall that a representation ρ is a map $G \to \mathrm{GL}(V)$ satisfying $\rho(s)\rho(t) = \rho(st)$, and we say that ρ is irreducible if there is no invariant nontrivial subspace W with $\rho(s)W \subseteq W$ for all s.

Theorem 78
Suppose $W \subseteq V$ is a nontrivial invariant subspace. Then W has an invariant complement W_0 (with $\rho(s)W_0 \subseteq W_0$ for all s) such that $V = W + W_0$ and $W \cap W_0 = \{0\}$; we write this as $V = W \oplus W_0$.

Proof. Let $\langle \cdot, \cdot \rangle_0$ be any nontrivial inner product on V. Then define a new inner product via

$$\langle v, w \rangle_1 = \sum_{s \in G} \langle \rho(s)v, \rho(s)w \rangle_0;$$

this is now an **invariant** inner product (meaning $\langle v, w \rangle_1 = \langle \rho(s)v, \rho(s)w \rangle_1$ for any ρ) and thus we can let W_0 be the orthogonal complement of W under $\langle \cdot, \cdot \rangle_1$. Then we can check that all properties do indeed hold. □

Remark 79. *In particular, this construction shows that we can always assume that $\rho(s)$ are unitary matrices (since they preserve the inner product of the "averaged" inner product). The same argument works for a general compact group, but it fails if we work with noncompact groups or if we work over a field like $\overline{F_q}$.*

This theorem also easily yields the following consequence, since we can think of ρ as being a representation restricted to W and to W_0 and repeatedly decompose:

Theorem 80

Let (ρ, V) be a representation. Then we can write $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$, where (ρ, W_i) is an irreducible representation for all i.

There are more general ways we can construct new representations from old ones as well:

Definition 81

Let (ρ_1, V_1) and (ρ_2, V_2) be two representations. Then the **direct sum representation** $\rho_1 \oplus \rho_2$ is a representation on $V_1 \oplus V_2 = \{(v_1, v_2) : v_1 \in V_1, v_2 \in V_2\}$ defined by

$$(\rho_1 \oplus \rho_2)(s)(v_1, v_2) = (\rho_1(s)(v_1), \rho_2(s)(v_2)).$$

Similarly, the **tensor product representation** $\rho_1 \otimes \rho_2$ is a representation on $V_1 \otimes V_2 = \{v_1 \otimes v_2 : av_1 + bv_1' \otimes v_2 = av_1 \otimes v_2 + bv_1' \otimes v_2, v_1 \otimes av_2 + bv_2' = av_1 \otimes v_2 + bv_1 \otimes v_2'\}$ (we mod out by linear combination relations) defined by

$$\rho_1 \otimes \rho_2(s)(v_1 \otimes v_2) = \rho_1(s)(v_1) \otimes \rho_2(s)(v_2).$$

(The tensor product of two representations can be thought of in terms of the usual matrix tensor product.) We already run into trouble here, though: the decomposition of $\rho_1 \otimes \rho_2$ into irreducible representations is difficult even for simple cases like the symmetric group S_n (this is called the **Kronecker problem**). And in fact, one way to find representations is to take tensor products of ones we already know and decompose them to see if we get anything new:

Definition 82

Let ρ be a representation of G. The **character** of ρ is a function $G \to \mathbb{C}$ defined by

$$\chi_\rho(s) = \mathrm{Tr}(\rho(s)).$$

Theorem 83 (Burnside-Brauer)

Let G be a finite group, and say $\rho : G \to \mathrm{GL}(V)$ is a **faithful** representation (meaning that we don't collapse group elements – if $\rho(s) = \rho(t)$, then $s = t$). Then every irreducible representation of G occurs in some tensor power $\rho^{\otimes k}$ of ρ, and in fact we only need to check up to the number of distinct values $\chi_\rho(s)$ takes on.

Characters will play a big role in our work, and we can extract a few properties of them here:

Proposition 84

The following hold for a representation ρ:

1. $\chi_\rho(\mathrm{id}) = d_V$ (where d_V is the dimension of the vector space),
2. $\chi_\rho(s^{-1}) = \chi_\rho(s)^*$ for all $s \in G$,
3. $\chi_\rho(s) = \chi_\rho(t^{-1}st)$ for all $s, t \in G$; that is, χ is constant on conjugacy classes.

Proof. For (1), since ρ is a homomorphism, it must take the identity group element to the $d_V \times d_V$ identity matrix, which has trace d_V. For (2), because we have a finite group, there is some positive integer A such that $s^A = \mathrm{id}$ for all s. This means that $\rho(s)^A = I$, so in particular the eigenvalues of $\rho(s)$ are roots of unity and thus each corresponding eigenvalue of $\rho(s^{-1}) = \rho(s)^{-1}$ is its complex conjugate. Summing this over all eigenvalues (to get the trace) yields the result. Finally, (3) follows because trace satisfies $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for any A, B. □

Proposition 85

Let (ρ_1, V_1) and (ρ_2, V_2) be two representations of G. Then

$$\chi_{\rho_1 \oplus \rho_2}(s) = \chi_{\rho_1}(s) + \chi_{\rho_2}(s), \quad \chi_{\rho_1 \otimes \rho_2}(s) = \chi_{\rho_1}(s)\chi_{\rho_2}(s).$$

Proof. For (1), we can choose a basis for each of V_1 and V_2, and then the matrices for $\rho_1 \oplus \rho_2$ are block diagonal coming from the matrices for ρ_1 and ρ_2 (and thus the traces just add). Similarly for (2), the matrix for $(\rho_1 \otimes \rho_2)(s)$ is the tensor product of the matrices $\rho_1(s)$ and $\rho_2(s)$; this has diagonal entries which are products of the diagonal entires of the individual matrices. □

Theorem 86 (Schur's lemma)

Say that (ρ_1, V_1) and (ρ_2, V_2) are **equivalent** if there is some linear isomorphism $f : V_1 \to V_2$ such that $\rho_2(s) \circ f = f \circ \rho_1(s)$ (that is, the diagram formed by f and the maps ρ_1, ρ_2 commute). Let $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ be irreducible, and suppose $f : V_1 \to V_2$ is any linear map with $\rho_2(s) \circ f = f \circ \rho_1(s)$. If ρ_1, ρ_2 are not equivalent, then $f = 0$, and if $V_1 = V_2$ and $\rho_1 = \rho_2$, then $f = cI$ for some constant c.

Proof. First, we claim that $\ker(f)$ and $\mathrm{Im}(f)$ are invariant subspaces. Indeed, if $f(v) = 0$ for some v, then $f(\rho_1(v)) = \rho_2(f(v)) = 0$, and if $v = f(w)$ for some w, then $\rho_2(f(v)) = f(\rho_1(v))$ is also in the image of f.

So now to prove the theorem, one case is where $\ker(f)$ is nonempty. Then $\ker f = V_1$ (since by irreducibility the kernel must be everything), meaning that $f = 0$. In the other case, if $\ker f = 0$, then $\mathrm{Im}(f) = V_2$ and we have an isomorphism (meaning that ρ_1 and ρ_2 are equivalent).

For the other statement, because we're working over $\mathbb{C}$, we have $fv = \lambda v$ for some nonzero vector v. Then $f_1 = f - \lambda I$ also satisfies $\rho_2 \circ f_1 = f_1 \circ \rho_1$, so by the previous reasoning (because f_1 has nontrivial kernel) it must be zero. That must mean $f = \lambda I$ as desired. □

Corollary 87

For an application of this, now suppose U is the uniform distribution on G (with $U(s) = \frac{1}{|G|}$). Then $\hat{U}(1) = 1$ and $\hat{U}(\rho) = 0$ for all other nontrivial irreducible representations ρ.

Proof. By definition, the trivial representation just multiplies everything by the constant 1, so we have $\hat{U}(1) = \sum \frac{1}{|G|} = 1$. Now

$$\rho(s)^{-1}\hat{U}(\rho)\rho(s) = \sum_{t\in G} \frac{1}{|G|}\rho(s)^{-1}\rho(t)\rho(s) = \sum_{t\in G} \frac{1}{|G|}\rho(t) = \hat{U}(\rho),$$

meaning that U commutes with the action of the group. Thus by Schur's lemma $\hat{U}(\rho) = cI$, and furthermore $U*U = U$ and thus $c^2 = c$. But if $Q(s) = \delta_{ts}$ is a point mass fixed at t, then $U * Q = U$, and for any nontrivial representation there is some t with $\rho(t) \neq I$, yielding a contradiction (since we can apply both sides of $\hat{U}\hat{Q} = \hat{U}$ to ρ). □

We can also rewrite Schur's lemma in the following two ways:

Corollary 88

Let h be any linear map from $V_1 \to V_2$, and define

$$h_0 = \frac{1}{|G|}\sum_{s\in G} \rho_2(s^{-1})h\rho_1(s).$$

(Think of ρ_2 as a $d_2 \times d_2$ matrix, h as a $d_2 \times d_1$ matrix, and ρ_1 as a $d_1 \times d_1$ matrix.) Then if ρ_1, ρ_2 are not equivalent, $h_0 = 0$, and if $V_1 = V_2, \rho_1 = \rho_2$, $h_0 = cI$ for $c = \frac{\mathrm{Tr}(h)}{d_{\rho_1}}$.

Proof. For any $s \in G$, we can write out

$$\rho^2(s^{-1})h^0\rho_1(s) = \frac{1}{|G|}\sum_{s\in G} \rho_2(s^{-1}t^{-1})h\rho_1(ts) = h^0,$$

so h^0 is indeed an equivalent map in the notation of Schur's lemma and we can apply it directly to get this result. □

Now we can try choosing bases and seeing how the statement carries over:

Corollary 89

Suppose we write the representations as matrices

$$\rho_1(t) = \Lambda_{i_1,j_1}(t), \quad \rho_2(t) = \Lambda_{i_2,j_2}(t).$$

Suppose the linear maps h (any map) and h^0 (the symmetrized version) are given in coordinates by x_{i_2,i_1}, $x^0_{i_2,i_1}$. Then in coordinates we have

$$x^0_{i_2,i_1} = \frac{1}{|G|}\sum_{t,j_1,j_2} \Lambda_{i_2,j_2}(t^{-1})x_{j_2,j_1}\Lambda_{j_1,i_1}(t).$$

Then either we have (case 1) $\sum_t \Lambda_{i_2,j_2}(t^{-1})\Lambda_{j_1,i_1}(t) = 0$ for all i_1, i_2, j_1, j_2, **or** (case 2) $\frac{1}{|G|}\sum_t \Lambda_{i_2,j_2}(t^{-1})\Lambda_{j_1,i_1}(t) = \frac{1}{d_\ell}$ if $i_1 = i_2, j_1 = j_2$ and 0 otherwise.

So Schur's lemma is actually giving us the following **orthogonality relations** which are essential for computing characters:

Corollary 90

Let $L^2(G)$ be the set of functions $f : G \to \mathbb{C}$ with inner product $\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_s f_1(s)\overline{f_2(s)}$. Let ρ_1, ρ_2 be unitary (in particular meaning that $\rho(t^{-1}) = \rho(t)^*$). Then the matrix entries Λ_{i_2,j_2}, Λ_{i_1,j_1} of the irreducible representations are orthogonal in L^2.

That is, the matrix entries of different representations are orthogonal, and even for the same representation the matrix entries of different coordinates are orthogonal. For compact groups, this is called the **Peter-Weyl theorem**.

Theorem 91
The characters of the irreducible representations are orthonormal in $L^2(G)$.

Proof. Let ρ be an irreducible representation with matrix entries $\rho(t)_{i,j}$. Then

$$\chi_\rho(t) = \sum_i \rho(t)_{i,i},$$

and therefore

$$\langle \chi_\rho, \chi_\rho \rangle = \sum_{i,j} \langle \Lambda_{i,i}, \Lambda_{j,j} \rangle = \sum_{i=1}^{d_\rho} \langle \Lambda_{i,i}, \Lambda_{j,j} \rangle = 1.$$

On the other hand, if we do this inner product with two different irreducible representations, all inner products in the sum are zero. □

Theorem 92
Let (ρ, V) be a representation of G with character ϕ, and suppose that V decomposes as the direct sum $\bigoplus_i W_i$ with W_i irreducible. Then for any irreducible representation with character χ, $\langle \phi, \chi \rangle$ is the number of times that χ appears in the decomposition.

In particular, this means (1) the number of W_i isomorphic to a given W doesn't depend on the way in which we decompose V or on the basis that we choose, and (2) ϕ determines ρ because ϕ determines the number of direct summands isomorphic to each irreducible representation; we write $V = \bigoplus m_i W_i$.

Corollary 93
The norm of any character $\langle \phi, \phi \rangle = \sum m_i^2$ is a nonnegative integer which is 1 if and only if ϕ is irreducible.

9 February 6, 2024

Last time, we discussed some simple properties of characters from Schur's lemma. We'll continue our introduction of representation theory today, with today's topics being the **decomposition of the regular representation** and **Fourier inversion**.

Fixing notation, we'll let G be a finite group and $L(G)$ be the set of all functions $f : G \to \mathbb{C}$. $L(G)$ has a basis consisting the functions $e_s(t) = \delta_s(t)$ for all $s \in G$. Then the group G acts on $L(G)$ by left multiplication on the basis elements: if we define

$$R(s)e_t = e_{st},$$

then R is the **regular representation** of the group G.

Proposition 94
The character χ_R of the regular representation is given by

$$\chi_R(\mathrm{id}) = |G|, \quad \chi_R(s) = 0 \text{ otherwise.}$$

(This is clear if we think about writing out the matrix of R in the basis $\{e_s\}$ – if s is the identity, then we have the identity matrix, and otherwise all diagonal entries are zero.) This turns out to have lots of implications:

Corollary 95

Each irreducible representation occurs in the regular representation, with multiplicity given by its degree. In other words, we have $R = \bigoplus_i d_i \rho_i$.

Proof. Let ρ be any irreducible representation with character χ. Then

$$\langle \chi_R, \chi \rangle = \frac{1}{|G|} \sum_{s \in G} \chi_R(s) \chi^*(s) = \frac{1}{|G|} |G| \chi^*(\text{id}) = \chi(\text{id}),$$

which is just the degree of the representation. □

Corollary 96

Any group G has only finitely many irreducible representations. Furthermore, if d_i is the sum of the ith irreducible representation, then

$$\sum_i d_i^2 = |G|, \quad \sum d_i \chi_i(s) = 0 \text{ for all } s \neq \text{id}.$$

Proof. The above result tells us that $\chi_R(s) = \sum d_i \chi_i(s)$, so plugging in $s = \text{id}$ yields $|G|$ on the left-hand side and $\sum d_i^2$ on the right, and plugging in anything else for s yields the other result. □

Corollary 97

The matrix entries of the irreducible representations (as functions on G) form an orthogonal basis for $L(G)$ in the usual inner product.

Proof. We showed orthogonality of the entries last time from Schur's lemma; furthermore, we have $\sum_i d_i^2$ total matrix entries across all irreducible representations, so in total we indeed have $|G|$ of them. □

Theorem 98

We have the following:

1. (Fourier inversion) For any $f \in L(G)$, let $\hat{f}(\rho) = \sum_{s \in G} f(s) \rho(s)$ be its Fourier transform. Then

$$f(s) = \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_\rho \text{Tr}\left(\rho(s^{-1}) \hat{f}(\rho)\right),$$

   where we're summing over all irreducible representations.

2. (Plancherel) For any $f_1, f_2 \in L(G)$, we have

$$\sum_{s \in G} f_1(s^{-1}) f_2(s) = \frac{1}{|G|} \sum_{\rho \in \hat{G}} d_\rho \text{Tr}\left(\hat{f}_1(\rho) \hat{f}_2(\rho)\right).$$

   (In other words, we can relate the inner products of the functions and the transforms.)

Proof. For (1), both sides are linear, so it suffices to just consider the function $f(s) = \delta_t(s)$ for some fixed $t \in G$. Then $\hat{f}(\rho) = \sum_s f(s)\rho(s) = \rho(t)$, so the right-hand side is

$$\frac{1}{|G|}\sum_{\rho\in\hat{G}} \mathrm{Tr}(\rho(s^{-1})\rho(t)) = \frac{1}{|G|}\sum_{\rho\in\hat{G}} \rho(s^{-1}t),$$

but now by our corollary above if $t \neq s$ then this is zero, and otherwise it is $\frac{1}{|G|}\cdot|G| = 1$, so Fourier inversion does indeed hold.

For (2), again both sides are linear in the functions, so we can choose $f_1(s) = \delta_{t^{-1}}(s)$. Then the left-hand side is just $f_2(t)$ (because all terms vanish except when $s = t$), and the right-hand side is now

$$\frac{1}{|G|}\sum_{\rho\in\hat{G}} d_\rho \mathrm{Tr}\left(\rho(t^{-1})\hat{f}_2(\rho)\right),$$

which is indeed f_2 by Fourier inversion (which we just proved). □

Example 99

Let's relate this to the usual abelian case with $G = C_n$. Then our characters (which are just the representations because everything is one-dimensional) are given by

$$\chi_j(k) = \exp\left(\frac{2\pi ijk}{n}\right).$$

In this case, the Fourier transform becomes the usual finite Fourier transform $\hat{f}(j) = \sum_{k=0}^{n-1} f(k)e^{2\pi ijk/n}$, and the inverse Fourier transform can be computed as usual.

Fact 100

It turns out that just like in the abelian case, there is a fast Fourier transform for general groups too – we can see Diaconis and Rockmore's JAMS paper for more on this.

Recall that two elements s, t in a group are **conjugate** if $s = \eta^{-1}t\eta$ for some $\eta \in G$; this is an equivalence relation that yields equivalence classes called **conjugacy classes**. We can then define the set of functions constant on all conjugacy classes

$$Z_G = \{f : G \to \mathbb{C} : s \sim t \implies f(s) = f(t)\} = \{f : G \to \mathbb{C} : f(st) = f(ts) \quad \forall s, t\}.$$

We call this set the **center** (of the group algebra), and a basis for Z_G is given by the functions of the form

$$\delta_C(g) = 1\{g \in C\}$$

where C ranges over all conjugacy classes. But we know that characters are elements of Z_G, and we know that the irreducible ones are orthogonal. Furthermore, if $f \in Z_G$, then $\hat{f}(\rho) = cI$ for $c = \frac{1}{d_\rho}\sum f(s)\chi_\rho(s)$, so by Fourier inversion we see that any class function is a sum of irreducible characters (since we can pull the cI out of the trace). So the characters also form a basis for the center:

Proposition 101

The number of irreducible representations of a group G is the same as the number of conjugacy classes in G.

Unfortunately, this is not a constructive statement, so it's hard to make a natural bijection between the irreducible representations and the conjugacy classes (even when we can describe them explicitly). And this is "worst" in the case $G = C_n$ (at least in the functorial sense).

Corollary 102

If G is abelian, then all irreducible representations are 1-dimensional (since all conjugacy classes have size 1 and this is the only way to have $\sum d_i^2 = |G|$).

We'll do some (more) applications to probability now. Recall the discussion after Example 6, which explains how Fisher-Yates is the standard way to generate a random permutation. We can think of that process as a big convolution: if we define

$$Q_j = \frac{1}{n-j+1} \sum_{k \geq j} (j, k),$$

though of as an element of the group algebra but also as a probability distribution, then we have $U = Q_1 * Q_2 * \cdots * Q_{n-1}$. This motivates the following question about "factoring" U:

Problem 103

If G is some general finite group and U is the uniform distribution on G, when do we have a nontrivial (non-uniform) square root Q such that $U = Q * Q$?

It turns out that if G is abelian, then passing to the Fourier transform yields $0 = \hat{Q}(\chi)^2$, so this only works if $\hat{Q}(\chi) = 0$ for all $\chi \in \hat{G} \setminus \{1\}$, meaning we only have the trivial case $Q = U$. But we **can** sometimes do this for a nonabelian group – suppose $\rho^* \in \hat{G}$ is a **real** matrix (in $GL_d(\mathbb{R})$), and choose a nilpotent matrix N with $N^2 = 0$ (such as the matrix with only a 1 in the top right corner). Then we can define a function f via Fourier inversion satisfing $\hat{f}(\rho^*) = N$ and $\hat{f}(\rho) = 0$ for all other $\rho \neq \rho^*$: we then have

$$f(s) = \sum_{\rho \in \hat{G}} d_\rho \mathrm{Tr}(\hat{f}(\rho)\rho(s^{-1})) = \frac{d_\rho^*}{|G|} \mathrm{Tr}(N\rho^*(s^{-1})).$$

Now $f * f$ is a constant (because $N^2 = 0$ and convolution becomes multiplication under the Fourier transform), and if we choose $\varepsilon > 0$ so that $1 + \varepsilon f(s) > 0$ for all s, then $Q(s) = \frac{1+\varepsilon f(s)}{Z}$ is a probability distribution. The Fourier transform of 1 at any nontrivial representation is zero, so we do indeed have $Q * Q = U$ for a probability distribution Q, as desired. So we can just do this **as long as the group has a real representation**. This motivates the general question of "when we can factor Haar measure on a finite or compact group:"

Fact 104

The eight-element group of quarternions $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ has four real representations and one two-dimensional representations, the last of which isn't real no matter how we choose our basis.

Theorem 105 (Diaconis–Shahshahani)

We can factor the uniform distribution U on a finite or compact group if and only if G is not $Q_8 \times C_2^n$ for some $0 \leq n \leq \infty$. (For more, see "Factoring Probabilities on Compact Groups."

One problem we could try along these lines is the following:

Problem 106

Let $G = S_n$ and let ρ^* be the $(n-1,1)$ irreducible representation. Using this recipe and the "upper-right corner" N, figure out what the corresponding Q is.

Our next application is in a research area where there is still lots to be done, which is the **tensor product of Markov chains**:

Example 107

Let $\hat{G}$ be the set of irreducible representations of a group G. Pick a faithful representation (not necessarily irreducible) and let its character be α. Then Brauer-Burnside showed that every χ occurs in $\alpha^{\otimes k}$ for some $1 \leq k \leq$ (number of distinct values of α).

We can thus form a Markov chain on $\hat{G}$ as follows: starting with some $\chi \in \hat{G}$, we can tensor with α to get $\alpha\chi = \sum m_i \chi_i$, and then choose the next representation to be χ_i with probability proportional to the "size" $m_i \chi_i(1)$. In other words, we have (remembering that for characters the tensor product just becomes the normal product)

$$K(\chi, \chi') = \frac{\langle \alpha\chi, \chi' \rangle \chi'(1)}{\alpha(1)\chi(1)}$$

Theorem 108

For any kernel K of the form above, we have the following:

- The stationary distribution π is the **Plancherel measure** $\pi(\chi) = \frac{\chi^2(1)}{|G|}$.
- If $\alpha(s) = \alpha(s^{-1})$, then (π, K) is reversible.
- The eigenvalues of the matrix K are $\{\alpha(C)\}$, where C ranges over the conjugacy classes of G. The corresponding right and left eigenfunctions are, respectively,

$$r_c(\chi) = \frac{\chi(c)}{\chi(1)}, \quad \ell_c(\chi) = \frac{\chi(1)\overline{\chi(c)}}{|C_G(C)|},$$

  where $C_G(C)$ is the **centralizer** of the conjugacy class C (the set of group elements that commute with all elements in C).

Proof of reversibility. We have

$$\sum_\chi \pi(\chi) K(\chi, \chi') = \sum_\chi \frac{d_\chi^2}{|G|} \langle \alpha\chi, \chi' \rangle \chi'(1)\alpha(1)\chi(1);$$

now bringing one copy of d_χ into the inner product gives us the regular representation and thus this all simplifies to $\pi(\chi')$. □

For some motivation for all of this, note that the decomposition of α^n takes on the form

$$\alpha^n = \sum_i m_i^{(n)} \chi_i,$$

with $\frac{m_i^{(n)}}{\alpha(1)^n}$ approaching the Plancherel measure $\frac{\chi_i^2(1)}{|G|}$ as $n \to \infty$. Brauer's refinement of Burnside's result was that you only need to take n as large as the number of values of α, but that bound can be very far off in some examples.

Example 109

Professor Diaconis studied this for the projective linear group $G = PGL_n(q)$ for some fixed q and large n, considering the case where α is the permutation character of G acting on lines of $\mathbb{F}_q^n$. Then α takes on order $\frac{n^{q!}}{(q-1)!^2}$ values, but the walk itself is random after just n steps. Thus Burnside-Brauer is just an upper bound – how long it takes may be very different.

Another reason we might care is that sometimes $K(\chi, \chi')$ is itself an interesting chain:

Example 110

Let $G = SU_2(\mathbb{C})$. Then $\hat{G}$ is indexed by the nonnegative integers; if we think of the matrices as acting on polynomials of degree n, then the corresponding walk is given by

$$K(i, i-1) = \frac{1}{2}\left(1 - \frac{1}{i+1}\right) \quad \forall i \geq 0, \quad K(i, i+1) = \frac{1}{2}\left(1 + \frac{1}{i}\right) \quad \forall i \geq 1.$$

This walk has a drift to ∞ (since it's a little more likely to go right than left) and thus doesn't have a stationary distribution. Instead we might want to ask how long it takes to go to infinity, and we can answer quite accurately. In particular, if X_n is the position of the walk after n steps starting at 0 (the trivial representation), then

$$\mathbb{P}\left(\frac{X_n}{\sqrt{cn}} \leq x\right) \sim \sqrt{\frac{2}{\pi}} \int_0^x y^2 e^{-y^2/2} dy.$$

for some explicit constant c. And this kind of accurate study only exists because this walk is connected to the study of SU_2, where we know all of the eigenvalues and can do careful Fourier analysis! This particular Markov chain is actually a famous chain related to **Pitman's 2M − X theorem** – if we have simple random walk **conditioned to stay nonnegative**, that's actually the same as this chain K.

10 February 8, 2024

Card-shuffling will return more explicitly next week – today, we're going to discuss **features** in Markov chains in the context of random walks on groups. We'll fix the notation where we have a Markov chain on a finite set $\mathfrak{X}$ and a Markov chain $K(x, y)$ with stationary distribution π. If $X_0, X_1, X_2, \cdots$ is a realization of the chain and T is some function $\mathfrak{X} \to \mathcal{Y}$, then we can look at the "features" of the chain $Y_i = T(X_i)$. Unfortunately, $Y_0, Y_1, Y_2, \cdots$ is not generally a Markov chain:

Example 111

Let $\mathfrak{X} = C_n$ and $K(i, i \pm 1) = \frac{1}{2}$ (meaning that we have the usual symmetric random walk on a circle), and define the feature $T(j) = 1\{0 \leq j \leq \lfloor \frac{n}{2} \rfloor\}$ (which keeps track of whether we're on one half of the circle). Then $Y_i = T(X_i)$ violates the Markov property, since if the last two values of Y were $0, 1$, then the chance of the next step being 1 is very different than if the last two values were $1, 1$.

However, some features do turn out to be okay: in the example above, if $T(j) = 1\{j \text{ is even}\}$, then $Y_i = T(X_i)$ is a Markov chain. But notice that features converge at very different rates from the original chain: $T(j)$ gets random in a bounded amount of steps, while the original chain needs n^2 time to mix.

Theorem 112 (Dynkin's criterion)

Take the above notation, and suppose we partition our state space as $\mathfrak{X} = \bigsqcup_j \mathfrak{X}_j$, and $Y_a = j$ if $X_a \in \mathfrak{X}_j$. Then the **lumped chain** $Y_0, Y_1, Y_2, \cdots$ is Markov **for all** starting distributions if and only if for any two lumps $i \neq j$, $K(x, \mathfrak{X}_j)$ is the same for all $x \in \mathfrak{X}_i$.

Note that there **are** processes (like riffle shuffling) where the lumped chain is Markov for some distributions but not others. If we want further references on this, we can see Kemeny and Snell's "Finite Markov Chains" or Amy Pang's "Lumpings of Algebraic Markov Chains arise from Subquotients."

There's a field of probability dealing with **integrable models** (ASEP, TASEP, some models related to KPZ), in which some calculations are exactly solvable using methods from algebraic combinatorics or analysis. The idea is that certain features of those processes can be studied exactly, which yields useful predictions or results for related models as well. Our analogous example here is random walks constant on conjugacy classes, and specifically we're going to consider **double coset Markov chains**:

Definition 113

Let G be a finite group and $Q(s)$ a probability distribution on G. Let H, K be two subgroups of G, and define an equivalence relation such that $s \sim t$ if $s = htk$ for some $h \in H, k \in K$. This equivalence relation partitions G into equivalence classes which we call **double cosets**, denoted $H\backslash G/K$.

In the special case where H is just the identity, we get the space of coset representatives G/K. And if $K = S_{n-1}$ is the set of permutations σ with $\sigma(1) = 1$, then $G/K = \{1, 2, \cdots, n\}$ keeps track of the positions of $\sigma(1)$. (This is the case that we're considering on our homework.) Remember that cosets of a group always have the same size, but double cosets can have very different sizes.

Theorem 114

Let $Q(s)$ be a **class function**, meaning that $Q(s) = Q(t^{-1}st)$ for all $s, t \in G$. Let H, K be any subgroups of G. Then the process induced by Q on the double cosets $H\backslash G/K$ (that is, run the random walk given by Q and report the double coset we're in) is a Markov chain with transition matrix $K(x, y) = Q(HyKx^{-1})$. If $Q(s^{-1}) = Q(s)$, then K is reversible with stationary distribution $\pi(x) = \frac{|HxK|}{|G|}$.

Theorem 115

Continuing with the notation from above, suppose C is a conjugacy class of G and $Q(s) = \frac{1}{|C|}\{s \in C\}$. Then the eigenvalues β_i are among the numbers $\beta_\lambda = \frac{\chi_\lambda(C)}{d_\lambda}$, where $\lambda \in \hat{G}$, and β_λ occurs with multiplicity $m_\lambda = \langle \chi_\lambda|_H, 1\rangle \langle \chi_\lambda|_K, 1\rangle$. Then we can get the bound on TV distance

$$\sum_{x \in H\backslash G/K} \pi(x) ||K_x^\ell - \pi||_{\text{TV}}^2 \leq \frac{1}{4} \sum_{\lambda \neq 1} m_\lambda \left| \frac{\chi_\lambda(C)}{\chi_\lambda(1)} \right|^{2\ell}.$$

(If we restrict a representation χ_λ to H, it's still a representation but might split up; the quantity $\langle \chi_\lambda|_H, 1\rangle$ counts the number of copies of the trivial representations in that split.) So if we have a group and we know the characters of it, then we automatically have a bunch of rates of convergence for other Markov chains coming from these double cosets.

Example 116

Let $G = S_n$, let $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k)$ be a partition of n, and let S_λ be the **Young subgroup** (or **parabolic subgroup**) of permutations which can permute things among the first λ_1 entries, among the next λ_2, and so on. (So S_λ is isomorphic to $\prod_{i=1}^k S_{\lambda_i}$.) Also, let $\mu = (\mu_1 \geq \cdots \mu_\ell)$ be another partition of μ with associated subgroup S_μ.

There's a nice description of the double cosets in this case:

Proposition 117

$S_\lambda \backslash S_n / S_\mu$ is the set of **contingency tables** T, which are $k \times \ell$ arrays of nonnegative integers with row sums λ and column sums μ.

We may imagine having four levels of undergraduate students and seven levels of age, and we might write down a table keeping track of how many people are of each level and each age. Statistics gives motivations for why given row and column sums matter (for instance, we may want to test for independence).

Proof sketch. Suppose we color the first λ_1 numbers with color 1, the next λ_2 numbers with color 2, and so on. Then for any permutation $\sigma \in S_n$, we can define T_{ij} to be the number of numbers colored i in the jth μ-block. We can check that this all works, and if we want a more careful check of this we can read James' "The Representation Theory of Symmetric Groups." □

So the double cosets have nice descriptions, but computing the number of double cosets $|S_\lambda \backslash S_n / S_\mu|$ is #-P complete. (We might be running this random walk to get an estimate on the size.) If we take Q to be the random-transpositions walk on S_n and consider the corresponding Markov chain on double cosets (which has a nice description in terms of the contingency tables), then we can count the number of tables of a given size to be

$$\pi(T) = \frac{1}{n!} \prod_{i,j} \frac{\lambda_i! \mu_j!}{T_{ij}!}$$

This is the **Fisher-Yates** distribution, and if the independence model holds so that the chance of being in a row is θ_i and the chance of being in a column is η_i, then the conditional distribution on tables given the sufficient statistics (row and column sums) is exactly this table. (For more on this model, we can see Simper's paper "Random Transpositions on Contingency Tables," or we can look at her thesis for more details on the topic.)

Example 118

Coagulation-fragmentation processes are studied by physicists and chemists to think about the size of oil blobs in water. (We can see Diaconis, Wolf, Zeitouni, and Zerner's paper for some survey references). The base model is the following: let $\mathfrak{X}$ be the set of partitions of n (the parts of the partitions thought of as the "blobs"). At each step, pick i, j uniformly at random. If $i = j$, do nothing. Otherwise, if i, j are in the same piece of the partition, then break the piece into two nonempty pieces uniformly (over the options $(1, n-1), (2, n-2), \cdots$), and otherwise join the two pieces together into one.

Notice that this is exactly how the cycle structure behaves under random transpositions! If i and j are in the same piece of the cycle and we transpose them, we break the cycle in two; otherwise, we end up combining the two cycles

into one. So we may be curious about questions like the stationary distribution or rates of convergence to stationarity. The former is easy, since

$$\pi(\lambda) = \prod_{i=1}^{n} \frac{1}{i^{a_i} a_i!},$$

where we write λ as a decomposition of a_1 fixed points, a_2 transpositions, a_3 3-cycles, and so on. And we can think about starting from the identity permutation and seeing how the process evolves – this corresponds to the Erdös-Renyi random graph where we start with an empty graph and start drawing edges together. Convergence to stationarity is then guaranteed after $\frac{1}{2} n \log n$ steps, because that's how long it takes for random transpositions to mix.

It turns out that in general for a measure on the group which is constant on conjugacy classes, we induce a Markov chain. But that follows from the following:

Example 119

Let M be a finite group, $G = M \times M$, and let $H = K$ be the diagonal subgroup $\{(m, m) : m \in M\}$. Then the conjugacy classes of G are products of conjugacy classes of M.

Notice that in our double coset equivalence relation, we have

$$(s, t) \sim (\mathrm{id}, s^{-1}t) \sim (\mathrm{id}, h^{-1}s^{-1}th),$$

so in fact **double cosets in G are indexed by conjugacy classes in M**, meaning anything we can say about conjugacy classes can be phrased in the language of double cosets as well.

Theorem 120 (Bruhat decomposition)

Let $G = \mathrm{GL}_n(\mathbb{F}_q)$, and let $H = K$ be the **Borel subgroup** of upper-triangular invertible matrices. Then we can write

$$\mathrm{GL}_n(\mathbb{F}_q) = \bigsqcup_{w \in S_n} BwB,$$

where w is interpreted as an $n \times n$ permutation matrix.

In other words, the double cosets of the Borel subgroup of GL_n (in fact over any field) are indexed by permutations, and the permutation corresponds to **row reduction**. In the row reduction process, sometimes there's a zero on the diagonal that we want to use to subtract off, so we need to do some pivoting to get our matrix to be upper-triangular. That permutation turns out to be the w here.

So random walks on GL_n lead us to random walks on permutations – in this case over $\mathbb{F}_q$, the uniform distribution on $\mathrm{GL}_n(\mathbb{F}_q)$ leads us to the **Mallows measure** on $B\backslash G/B$

$$\pi(w) = \frac{q^{l(w)}}{[n]_q!} = \frac{q^{l(w)}}{(1+q)(1+q+q^2)\cdots(1+\cdots+q^{n-1})}.$$

A natural conjugacy-invariant random walk on GL_n is **random transvections**, which is the analog of random transpositions for permutations. A **transvection** is a non-identity linear transformation $T \in \mathrm{GL}_n(\mathbb{F}_q)$ in the set of row operations (up to change of basis), meaning that T fixes some hyperplane. So this is a conjugacy class containing elements of the form $I + \theta E_{ij}$, and the transvection walk is where we repeatedly multiply by such elements T starting from the identity. For a reference, we can see Diaconis, Ram, and Simper's paper "Double Coset Markov Chains" – there are lots of examples, and it turns out that it does matter where we start for this particular random walk. For $q > 1$, this Mallows measure is maximized at the reversed permutation $(n, n-1, \cdots, 1)$ and minimized at the identity;

it turns out that it takes $O(n)$ steps if we start at the identity and $O(\log n)$ steps if we start the reversed chain. The proof makes use of the mathematics of Hecke algebras, and there's a lot of interesting concepts there!

Example 121

In the 1780s, Bernoulli and Laplace were studying diffusion and the model of air molecules passing through a porous membrane. They studied this by considering n red balls in one urn and n black balls in the other urn and repeatedly swapping random balls from the two.

The stationary distribution for the number of red balls in one of the urns is the hypergeometric distribution $\pi(x)$, but we can also think about this as just being random transpositions: let $G = S_n$, $H = \mathrm{id}$, and $K = S_k \times S_{n-k}$. Then $H\backslash S_n/K = S_n/(S_k \times S_{n-k})$, and the size of this double coset is $\binom{n}{k}$. Random transpositions lumped to these double cosets exactly become this urn problem, and because we have representation theory now we can make more progress than Bernoulli and Laplace could hundreds of years ago!

11 February 13, 2024

We're finally returning to the "mathematics of shuffling" now – the content we'll be discussing is now of a different flavor.

Definition 122

The **Gilbert–Shannon–Reeds** shuffle on S_n (for our purposes we can imagine $n = 52$) is defined by letting $Q(\sigma)$ define the following process: cut off c cards with probability $\frac{\binom{n}{c}}{2^n}$ for $0 \le c \le n$ (which is a discrete "bell curve" concentrated near $\frac{n}{2}$), forming two piles of cards. Then if we have a cards in the left pile and b cards in the right pile, drop the next card from the left with probability $\frac{a}{a+b}$ and from the right with probability $\frac{b}{a+b}$; repeat this until all n cards have dropped, forming a permutation of the cards.

Theorem 123

For this shuffling, $\frac{3}{2}\log_2 n + c$ shuffles are necessary and sufficient for mixing.

The motivation for studying this walk is that people do actually shuffle cards (and this is a pretty good model of how people do so); Las Vegas actually had to change some of its rules because of this theorem! And shuffling is "basic math" in the sense that we may have the shuffling of two words (here are all the ways to "shuffle" AB into XYZ)

$$AB\omega XYZ = ABXYZ + AXBYZ + AXYBZ + \cdots + XYZAB$$

when we compute the wedge product of differential forms (where instead of AB we now write $A \wedge B$, and we also introduce the correct factors of $(-1)^\sigma$). We can then prove various facts about multiplying wedge products and studying the exterior algebra, and in particular in algebraic topology knowing the homology or homotopy of two spaces and their intersection can tell us about that of the union – any such results like this do involve some amount of shuffling. (And this comes up when we study descent algebras or Hopf algebras as well.)

Remark 124. *The reason we know the eigenvalues of the Gilbert–Shannon–Reeds chain is that they're given by a "Hodge decomposition of Hochschild homology" – these aren't words we need to know now, but it's interesting that we can study a* **realistic** *Markov chain model and get such explicit results. And we'll see that the mathematics actually works out nicely too!*

This shuffle actually has four equivalent descriptions for Q, which we'll describe now:

1. The **sequential description** – this is the one we gave above in the definition.
2. The **inverse description** – instead of thinking about shuffling in the ordinary way, we can imagine taking out cards and putting them on top. It turns out that if we pick cards iid $\{0,1\}$ with probability $\frac{1}{2}$ and put the ones labeled 1 on top, keeping the order within each group, then we can call this inverse measure $\tilde{Q}$.

   Notice that there are $(n+1)$ sequences out of the 2^n total ones which yield the identity permutation, so $\tilde{Q} = \frac{n+1}{2^n}$. It then turns out that
   $$\left|\left|\tilde{Q}^{*k} - U\right|\right| = \left|\left|Q^{*k} - U\right|\right|$$
   on any group (since we're summing over the whole group, so we can sum over inverses and get the same answer), so we can study inverse shuffling if it's easier to do.
3. The **max entropy description**: notice that all 2^n ways of cutting the deck and doing the inverse shuffling process are equally likely, and this is the distribution with the maximum value of $-p \log p$.
4. The **geometric description**: let $U_1, \cdots, U_n$ be iid uniform on $[0,1]$, and label them as $U_{(1)}, \cdots, U_{(N)}$ from left to right (in increasing order). Now do the **baker's transformation**, $T(x) = 2x \bmod 1$ (which takes the left and right halves of the interval and overlays them – this is the process that we might do with bread dough).

There are extensions of this as well – we may think of doing the Baker's map but with $T(x) = ax \bmod 1$ instead of $2x \bmod 1$, which would lead us to an "a-shuffle." In terms of the original card shuffling formulation, we can cut the deck into three piles by a trinomial distribution, and then we can drop cards from "three hands" with probability proportional to deck size:

Definition 125
An ***a*-shuffle** is given by dividing the n cards into a (possibly empty) packets via $\frac{\binom{n}{n_1, \cdots, n_a}}{a^n}$ and then shuffle a dropped card from the bottom with probability proportional to the packet size.

We can check that the sequential sampling here is equivalent to a Gilbert–Shannon–Reels shuffle where we mix two at a time. And in the inverse description, we label each card uniformly on $\{1, 2, \cdots, a\}$ iid, and then keeping the order within each label, we put the cards labeled 1 on the top, then the cards labeled 2 next, and so on. And the maximum entropy description is the one induced by the inverse description, where all choices of "cuts followed by shuffles" are equally likely.

Remark 126. *We can try to describe $\frac{3}{2}$-shuffles in the same way, but we'll see that it doesn't work – a does need to be an integer for the math way to work out.*

Proposition 127
The four descriptions of a-shuffles above are all equivalent.

Proof. We can first check that all four descriptions lead to multinomial descriptions on the cuts. For the sequential definition, this comes directly from the specification of how we group, and for the inverse definition this comes from the number of ways to pick n_i cards to be in pile i for all i; the maximum entropy description follows from this. And finally for the geometric description, we can break up the unit interval into a equally spaced intervals; the number of points landing in each one exactly follows the multinomial distribution.

From here, the idea is to show that **given** the cut distribution $n_1, n_2, \cdots, n_a$, all ways of interleaving the cards have equal probability. We'll start with the sequential definition, and we'll do $a = 2$ to make notation easier. If we cut off j cards into the left pile, then we drop a card with probability proportional to the packet size, so the interleaving probability in any situation will always be

$$\frac{j(j-1)\cdots(1)(n-j)(n-j-1)\cdots\cdots 1}{n(n-1)(n-2)\cdots\cdots 1} = \frac{1}{\binom{n}{j}},$$

since the probability of the first drop is either $\frac{j}{n}$ or $\frac{n-j}{n}$, and then the next one after that is the number of cards left in a pile divided by the total number of cards – this means that the numbers 1 through j will show up in the numerator at some point (coming from the left pile), and so will the numbers 1 through $n-j$ (coming from the right pile). Thus we are uniform on interleaving. And similarly in the inverse description, conditioned on the n_is the set of cards which are put on the top are uniform (because of independence of the "coin tosses"). The maximum entropy description is also immediate because a uniform distribution is what gives us the maximum entropy.

Finally, for the geometric description (this is where non-integer a breaks down), use the fact that if X is uniform on $[0,1]$ then writing $x = \sum_{j=0}^{\infty} \frac{\varepsilon_j}{a^j}$ (where $\varepsilon_j \in \{0, 1, \cdots, a-1\}$) we have all ε_j iid uniform. (This is just a property of Lebesgue measure.) So now out of the n_1 points in $[0, \frac{1}{a})$ which get put into the first pile, if we're told that we have n_1 points then they'll be uniform on $[0, \frac{1}{a})$ and thus multiplying by a makes them uniform on $[0,1]$. So then all interleavings across points in different groups are equally likely. □

For more details on some of these points, we can see the course textbook, or we can see the paper by Bayer and Diaconis titled "Trailing the Dovetail Shuffle to its Lair."

Fact 128

Even if "everybody knows" that cards are random after three, four, or five shuffles, it turns out to be incorrect. Bridge is a card game where four players are each given 13 random cards and try to "take tricks." One of the things that's crucial is the breakdown of a hand into suits – knowing your own cards and your partner's cards, we know how many cards the other team has, but the breakdown should be uniform between them. And in the "bridge encyclopedia," probabilities were carefully calculated, but experts turn out to play differently from the theoretical breakdown.

It turns out what's wrong was that cards in bridge were shuffled by hand, and in Berger's article "On the distribution of hand patterns in bridge: man versus computer," the distribution of suits was recorded, and it was found that the hand-shuffled frequencies differed significantly from the theoretical ones by chi-square tests (the chi-square was 10.3 on 10 degrees of freedom for the computer-generated ones, but the one against the hand-shuffled ones was 31.1.)

So what this means is that cards tend to get clumped in groups of four because of how tricks are taken, and when we deal in groups of four we tend to spread those out across the players. Indeed, we end up finding too many flat hands (like $4,4,3,2$ or $4,3,3,3$) from data.

Remark 129. *Professor Diaconis got many emails from blackjack players who like to do shuffle tracking and count cards after showing up in the New York Times. (There are "shuffle journals" who describe the algorithm publicly, so it's something that computer calculations can help do predictions.)*

Example 130

There's also an interesting "card trick" that we can try doing: Professor Diaconis could mail us a deck of cards, suggest that we try cutting and shuffling a deck of cards twice and doing a couple of cuts, then remember the top card and stick it somewhere in the middle of the deck. Then even after another shuffle, if we give the deck back to Professor Diaconis, he'll be able to tell which card was moved.

The "magic police" may be annoyed that the trick here is being revealed, but it turns out to be related to the physics of shuffling. Suppose the deck is in order $1, 2, \cdots, n$ (from the point of view of the magician). After one shuffle, the relative order of the top and bottom halves of the cards form two chains, so after two shuffles there will be four distinct chains. Taking a card and creates its own chain, so even if we shuffle the deck again we'll see eight chains and one funny card. (Cuts don't do anything – they just change the cyclic order of the chains.) If we then "play solitaire" with the resulting cards, placing down cards in piles based on the correct chains, we'll see eight chains and a single lone card. And in fact five riffle shuffles will not be enough, because we still have at most 32 rising sequences and that will miss a big proportion of possible arrangements of the deck.

Definition 131

The **rising sequence** of a permutation σ is defined by grouping σ as follows: start from 1 and group it with 2 if it comes after 1, then 3 if it comes after 2, and so on. Once we get to the end, start the next group of the sequence from the next smallest number, and repeat until we finish going through all n numbers. Let $R(\sigma)$ be the number of rising sequences of σ.

For example, $9, 1, 3, 7, 8, 4, 2, 6, 5, 10$ would be decomposed into $(1, 2)$, then $(3, 4, 5)$, then (6), then $(7, 8)$, then $(9, 10)$.

Definition 132

We say that a permutation σ has a **descent** at i if $\sigma(i)$ (the label of the card at position i) is greater than $\sigma(i+1)$; let $D(\sigma)$ be the number of descents of σ.

So in the example above, we would have descents at positions $1, 5, 6, 8$. Notice that the number of rising sequences ranges from 1 to n, and the number of descents ranges from 0 to $n-1$.

Proposition 133

We have $R(\sigma) = D(\sigma^{-1}) + 1$ for any permutation σ.

In terms of these statistics, we can write down a nice expression for the measure of riffle shuffling:

Theorem 134 (Bayer)

Let Q_a be the a-shuffle measure on S_n. Then

$$Q_a(\sigma) = \frac{\binom{n+a-R(\sigma)}{n}}{a^n}.$$

Proposition 135 (IOU lemma)

With the notation as above, we have $Q_a * Q_b = Q_{ab}$ for any integers a, b.

Proof. This is easily seen through the inverse description (where we label the cards iid 1 through a and then group). If we label twice with an b-shuffle and then an a-shuffle, then each card has an equal probability of getting each of the labels (x, y) for $x \in [a]$ and $y \in [b]$, but that's the same as labeling with all ab options from the beginning (since the $(1, 1)$ cards go at the top, then the $(2, 1)$ cards next, and so on). □

This is great, because we care about studying the shuffle $(Q_2)^{*k}$ and thus can just think about the shuffle Q_{2^k}; this means that Bayer's theorem can tell us everything we need to know about the measure! The first proof of Bayer's theorem involved some complicated arguments from high-dimensional geometry, but here is a nicer proof:

Proof of Theorem 134. Start with the numbers $(1, 2, \cdots, n)$ and use the sequential description. We know that each of the a piles stays in the same relative order, so each pile is part of a rising sequence – the pile $(1, 2, \cdots, n_1)$ forms a rising sequence, and then it may be even longer if every card from this pile drops before every card from the second pile of n_2 cards (meaning we combine the two rising sequences from the two piles).

But all shuffles leading to some fixed σ have the same probability, and each rising sequence in σ is a union of packets. If we're told the cuts and we're told σ, there's a unique way for the cards to yield σ (since we know which cards must drop at each point), so we need to count how many cut sequences lead to σ. Some cuts are forced – if we see two consecutive rising sequences like $(1, 2, \cdots, 17)$ and $(18, 19, \cdots)$, then the cards **must** have been cut between 17 and 18. This forces $R(\sigma) - 1$ cuts, and the remaining $a - R(\sigma) + 1$ cuts can be made anywhere, so we have a stars and bars problem to count the number of ways to make these extra cuts. □

12 February 15, 2024

Last time, we considered riffle shuffles on S_n, letting $Q(\sigma)$ be the Gilbert–Shannon–Reeds a-shuffle measure. Specifically, we showed that Q takes the form

$$Q_a(\sigma) = \frac{1}{a^n}\binom{n + a - R(\sigma)}{n},$$

and then the convolution of an a-shuffle and a b-shuffle is just an ab-shuffle, making the study of TV distance much easier.

Theorem 136

We have

$$\left|\left|Q_2^{*k} - U\right|\right|_{\text{TV}} = \frac{1}{2}\sum_{j=0}^{n-1} a(n, j)\left(\frac{\binom{n+2^k-j-1}{n}}{2^{nk}} - \frac{1}{n!}\right),$$

where $a(n, j)$ is the number of permutations in S_n with j descents (also called the **Eulerian numbers**).

We can think of the form of $Q_a(\sigma)$ as telling us that all permutations of the same rising sequence number $R(\sigma) = D(\sigma^{-1}) + 1$ are equally likely, so the TV distance comes from summing over possible values for D. The Eulerian numbers satisfy a simple recurrence

$$a(n, j) = (n - j)a(n - 1, j - 1) = (j + 1)a(n - 1, j),$$

meaning that they're easy to calculate.

Fact 137

For $n = 52$ (a deck of cards), we can compute $||Q_2^{*k} - U||$ explicitly with a computer, and we'll see the following data (to a few decimal places):

k	1	2	3	4	5	6	7	8
$\|\|Q^{*k} - U\|\|$	1.000	1.000	1.000	1.000	.924	.64	.32	.16

In particular, we might notice that the TV distance starts going down by a factor of 2, and that's indeed what happens forever.

Professor Diaconis calls this the "seven shuffles theorem," because in general the cutoff happens at $\frac{3}{2}\log_2 n$ and that's around 7 for $n = 52$. Here's the more precise result:

Theorem 138

If $k = \frac{3}{2}\log_2 n + c$ for some fixed constant c and n large, then

$$||Q^{*k} - U||_{\text{TV}} = 1 - 2\Phi\left(-\frac{2^{-c}}{4\sqrt{3}}\right) + O\left(\frac{1}{\sqrt{n}}\right),$$

where $\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt$ is the cumulative distribution function for the standard normal.

Indeed, this is where we see the powers of 2 – since $\Phi(x)$ is approximately $\frac{1}{2} + \frac{1}{\sqrt{2\pi}}x$ for small x, this quantity decays exponentially. And in fact for negative c, this quantity will go to 1 "exponentially fast."

Proof idea. We won't go through the full proof because it's a lot of calculations with binomial coefficients and factorials, but there's a part of it which is instructive. The important fact is that if u_i are iid uniform on $[0, 1]$, then we have

$$\frac{a(n, j)}{n!} = \mathbb{P}\left(j - 1 \le u_1 + \cdots + u_n < j\right).$$

Laplace found a formula on the right-hand side, and combinatorialists got a formula for the left-hand side, and it turned out these formulas were the same. We can read the book if we want an "a-ha" reasoning for why it's true, though.

This is not a reversible Markov chain, so eigenvalue bounds don't immediately give us rates of convergence (we'd need to know some things about the singular values instead). So instead this shape-type result needs the full distribution of the measure so that we can establish a local central limit theorem. □

This is a result on the symmetric group ("type A"), so people may be interested in generalizing this to Coxeter groups such as the symmetry groups of the hypercube or the hyperoctahedral group $C_2^n \rtimes S_n$ ("type B"). There are some things we can indeed do there, and we also have an analog of riffle shuffling for something like the hyperoctahedral group where we turn one of the piles upside down. But things do go through.

Fact 139

After Professor Diaconis worked on this problem he got a letter from a company ("Shuffle Master") who makes shuffling machines. It turns out that casinos have complicated machines which "riffle shuffle" automatically, and this was the only company that sold such machines to Las Vegas and Atlantic City.

So Professor Diaconis took a look at their new "shelf shuffler" machine to see if it was actually getting random enough, and it turned out to exactly be type B shuffling and one pass through really wasn't good. The way to explain this without needing to use the phrase "total variation" is by playing a "card-guesser game" where you try to sequentially guess the cards – you expect to guess $\frac{1}{n} + \frac{1}{n-1} + \cdots + \frac{1}{2} + 1 \approx 4.5$ of them correctly if it's shuffled correctly, but instead it was possible to guess 9.5 cards on average! We can read the chapter in the textbook about this, and for further reading we can see Mark Sellke's paper about a related riffle shuffle where we have a bias on how we cut the cards.

Example 140

We can buy cheap 10 dollar card riffle shuffling machines at Target or on Amazon, and when Professor Diaconis tried to sample a bunch of permutations from one of them (which has a different mechanism), it seemed to fit a drop probability of $\frac{a^\theta}{a^\theta + b^\theta}$ with θ some other number than 1. So it might be interesting to try to do the math in that case too!

Example 141

We can now think about a generalization of our inverse shuffling process with **Markovian drops** – suppose we have a symmetric two-state Markov chain with diagonal entries θ (not necessarily $\frac{1}{2}$), and then we choose a binary pattern of our cards according to that Markov chain and then take the 0s and put them on top. Again, there hasn't been much work done here, but it could be a way to study how people tend to shuffle "more neatly" than random.

That's all we'll say about this exact problem for now, and we'll now continue our discussion of **features**. (Recall that the idea here is that we don't care about the total variation distance, just the convergence of some **specific** function that we want to integrate or sum over.) Some examples include the original top card on our deck (it turns out $\log_2 n$ riffle shuffles is necessary and sufficient for this), the red/black pattern (again we can get upper and lower bounds that show $\log_2 n$), the label of the card on top (this is the inverse permutation – this turns out to be $\frac{1}{2}\log_2 n$), or the card distribution except for all of the face cards, which matters in blackjack (this is also $\log_2 n$), or the longest increasing subsequence ($\frac{5}{6}\log_2 n$). We'll do one of the stories of this type, looking at the **cycle structure**.

We'll write $\sigma \sim 1^{a_1(\sigma)} \cdots n^{a_n(\sigma)}$, where $a_i(\sigma)$ is the number of cycles of length i in σ. There are various features of permutations that only depend on the cycle structure, such as the number of fixed points, number of cycles, the order of σ as a group element of S_n (this is the lcm of the cycle lengths), or the length of the longest cycle. For reference, a uniform permutation has $O(1)$ fixed points (it's Poisson(1)), $O(\log n)$ cycles (more precisely, it's normal with mean $\log n$ and standard deviation $\sqrt{\log n}$), and longest cycle of length roughly $0.62n$. Furthermore, we can write the logarithmic asymptotics as

$$\mathbb{P}\left(\frac{\log(\text{order}(\sigma)) - \left(\frac{\log n}{2}\right)^2}{\sqrt{\left(\frac{\log n}{3}\right)^3}}\right) \to \Phi(x),$$

Before we dive into proving convergence of features under shuffling, we'll first understand how we get these kinds of results (because they can be useful). In other words, today's theme will be **proving theorems about cycle statistics for a uniform permutation**, and next time we'll show how this deforms.

We can write down the generating function for the number of cycles

$$C_n(x_1, \cdots, x_n) = \frac{1}{n!}\sum_{\sigma \in S_n}\prod_{i=1}^{n} x_i^{a_i(\sigma)},$$

and we get a power series in infinitely many variables

$$C(t) = \sum_{n=0}^{\infty} C_n(x_1, \cdots, x_n) t^n.$$

Theorem 142 (Polya)

We can write the power series as

$$C(t) = \prod_{i=1}^{\infty} \exp\left(\frac{t^i x_i}{i}\right).$$

The meta-idea here is that we can think of products as corresponding to independence. The first step is to use a result of Cauchy:

Theorem 143 (Cauchy)

We have

$$\frac{1}{n!}\left|\{\sigma \in S_n \text{ of cycle type } \prod i^{a_i}\}\right| = \prod_{i=1}^{n} \frac{1}{i^{a_i} a_i!} \cdot 1\left\{\sum_{i=1}^{n} i a_i = n\right\}.$$

(Indeed, if $\sigma = \mathrm{id}$ has cycle type 1^n, then this quantity is exactly $\frac{1}{1^n n!}$, and if σ is an n-cycle of cycle type n^1, then this quantity is exactly $\frac{1}{n}$, and there are indeed $(n-1)!$ possible n-cycles.)

Proof. We use that S_n acts transitively on the set of permutations σ of a particular cycle via conjugation (conjugation replaces each symbol j by $\eta(j)$ without changing the cycle structure). So the size of the set is the size of the group divided by the subgroup fixing a point, meaning the left-hand side here is $\frac{1}{|\{\sigma \text{ fixing anything in the conjugacy class}\}|}$, which is indeed exactly $\prod_{i=1}^{n} \frac{1}{i^{a_i} a_i!}$. So by randomizing a parmeter we have managed to make things independent! □

Proof of Theorem 142. We expand out the exponentials

$$\prod_{i=1}^{\infty} \exp\left(\frac{x_i t^i}{i}\right) = \prod_{i=1}^{\infty} \left(\sum_{j=0}^{\infty} \frac{(x_i t^i / i)^j}{j!}\right)$$

and then regroup the terms by powers of t to get

$$= \sum t^n \left(\text{sum of } \frac{x_i^{j_i}}{i^{j_i} j_i!} \text{ over all } \sum i j_i = n\right),$$

and now we can rewrite this with Cauchy's result to indeed get this coefficient to simplify to $\frac{1}{n!} \sum_{\sigma \in S_n} \prod x_i^{a_i}$, as desired. □

Recall that the Poisson(λ) distribution is defined via the probability mass function $p_\lambda(j) = \frac{e^{-\lambda}\lambda^j}{j!}$ and this has generating function $e^{-\lambda(x-1)}$. Computing the expected value of this is easiest with falling factorials: we have for a Poisson(λ) distribution Y that

$$\mathbb{E}[Y(Y-1)\cdots(Y-\ell)] = \lambda^\ell$$

for any ℓ, so in particular $\mathbb{E}[Y] = \lambda$ and $\mathrm{Var}(Y) = \lambda$.

Example 144

We'll do a quick refresher on the **moment method** – suppose μ is a probability measure on $\mathbb{R}$. Then we say that μ is **determined** if μ is the only measure on $\mathbb{R}$ with the kth moments

$$\mu_k = \int_{-\infty}^{\infty} x^k \mu(dx),$$

If the Laplace transform or the generating function of our measure μ is analytic, then μ is indeed determined (we can read Billingsley) for the details. Similarly, normal and Poisson distributions are also determined, and so is the chi-square distribution (for example a squared standard normal Z^2) or the fourth power of a standard normal. But something like Z^3 or Z^n for $n \geq 5$ are not determined.

Fact 145

A sufficient (but not necessary) condition for being determined is that $\sum_{k=0}^{\infty} \frac{1}{\mu_{2k}^{1/2k}} = \infty$.

It turns out that if μ is not determined, then it is "really not determined" in the following sense:

Proposition 146

Suppose μ is not deteremined. THen there exists some μ^* with an atom at x and all moments the same as μ (so in particular, there is a continuous spectrum of measures all with the same moments.)

If we'd like to read more, we can see the survey book "Moments in Mathematics," in which Professor Diaconis has a chapter about its applications to probability and statistics (but there are applications to many other fields as well).

What we'll do is "go from Polya to Poisson:" multiply both sides of the equation

$$\sum t^n C_n(x_1, \cdots, x_n) = \prod_{i=1}^{\infty} \exp\left(\frac{t^i x_i}{i}\right)$$

by $1-t$ to get (use that $e^{\log(1-t)} = e^{-\sum_i \frac{t^i}{i}}$)

$$\boxed{\sum_{n=0}^{\infty} (1-t) t^n C_n(x_1, \cdots, x_n) = \exp\left(\sum_{i=1}^{\infty} \frac{t^i}{i}(x_i - 1)\right)}$$

(this of this as flipping a coin until we get the first head on the left-hand side, and that's the number of variables that we have a permutation on). But now notice that the right-hand side is the generating function of $Y_1, Y_2, \cdots$, where the Y_i are **independent** Poisson random variables of parameter $\frac{t^i}{n}$. So randomizing n can be thought of as making the cycles independent!

This means that if we want to think about the law of a_1 (the number of fixed points) on S_1, we can substitute 1 for all of $x_2, \cdots, x_n$. Then we have

$$C_n(x, 1, 1, \cdots, 1) = \frac{1}{n!} \sum_{\sigma \in S_n} x^{a_1(\sigma)} = \mathbb{E}_{S_n}[x_1^{a_1}],$$

and the right-hand side simplifies to just $e^{t(x_1 - 1)}$. Now we can substitute everything into the boxed equation, differen-

tiate both sides k times in t, and plug in $x_1 = 1$, to find that

$$\mathbb{E}_{S_n}[x_1^k] = \begin{cases} 1 & n \geq k, \\ 0 & \text{otherwise.} \end{cases}$$

But this means that for all n, this means that the first k moments of a_1 in S_n equal the first k moment of a Poisson(1) random variable for $n \geq k$. This is the same argument that we can use for transpositions and other joint mixed moments $\mathbb{E}[a_1^{n_1} \cdots a_k^{n_k}]$ – we'll always find that the moments are exactly equal!

13 February 20, 2024

We're headed towards understanding questions about cycles in riffle shuffling – last time, we studied what typical permutations look like for **uniform** permutations (that is, we studied the cycle indicator function

$$C_n(x_1, \cdots, x_n) = \frac{1}{n!} \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_i^{a_1(\sigma)} = \mathbb{E}_{S_n}\left[\prod x_i^{a_i(\sigma)}\right]$$

along with the corresponding generating function $C(t) = \sum_{n=0}^{\infty} t^n C_n$, for which Polya's theorem gives us a nice factorization (and thus after some work we can find basically any statistic we care about).

Example 147

We'll do one more example of the type we did last week now, since we'll see a similar formula after riffle shuffling as well. Suppose we want to study the number of cycles $\mathcal{C}(\sigma) = \sum_{i=1}^{n} a_i$ in a uniform permutation.

Setting all $x_i = x$, we find that

$$C_n(x, x, \cdots, x) = \mathbb{E}_{S_n}\left[x^{\mathcal{C}(\sigma)}\right] \implies C(t) = \exp\left(x \sum_{i=1}^{\infty} \frac{t^i}{i}\right) = \frac{1}{(1-t)^x}$$

by using the power series for $\log(1-t)$. And now by Newton's formula, we can expand this out as

$$C(t) = \sum_{n=0}^{\infty} \binom{-x}{n} (-t)^n, \quad \binom{-x}{n} = \frac{-x(-x-1)\cdots(-x-n+1)}{n!} = (-1)^n \frac{x(x+1)\cdots(x+n-1)}{n!},$$

so if we plug in the binomial coefficient expression here and cancel out the factors of $(-1)^n$ we find that

$$C(t) = \sum_{n=0}^{\infty} \frac{x(x+1)\cdots(x+n-1)}{n!} t^n.$$

So now we can equate coefficients of powers of t on both sides and get the **Stirling numbers of the first kind**

$$\mathbb{E}_{S_n}[x^{\mathcal{C}(\sigma)}] = \frac{x(x+1)\cdots(x+n-1)}{n!} = x\left(\frac{x+1}{2}\right)\left(\frac{x+2}{3}\right)\cdots\left(\frac{x+n-1}{n}\right).$$

Since we have an expectation that we can write as a product, we may ask where independence comes up. And in fact, $\frac{x+j}{j+1}$ is the generating function of a random variable X_j which takes value 0 with probability $\frac{j}{j+1}$ and 1 with probability $\frac{1}{j+1}$; then $\mathcal{C}(\sigma)$ is equal in distribution to $X_0 + X_1 + X_2 + \cdots + X_{n-1}$ with X_i independent and with distribution as above. Thus we can calculate

$$\mu_n = \mathbb{E}_{S_n}[\mathcal{C}(\sigma)] = 1 + \frac{1}{2} + \cdots + \frac{1}{n} = \log n + \gamma + O\left(\frac{1}{n}\right)$$

and (because the variances also add for independent variables)

$$\sigma_n^2 = \mathrm{Var}(\mathcal{C}(\sigma)) = \sum_{i=1}^{n} \frac{1}{i} - \frac{1}{i^2} = \log n + \gamma - \frac{\pi^2}{6} + O\left(\frac{1}{n}\right).$$

So by the central limit theorem for the X_is, we have

$$\mathbb{P}\left(\frac{\mathcal{C}(\sigma) - \mu_n}{\sigma_n} \leq x\right) \to \Phi(x),$$

and we can get correction terms if we really need to.

Fact 148

There are many more statistics we can get out of this – for example, the average length of the shortest cycle is $e^{-\gamma} \log n$. And for more, we can see Shepp and Lloyd's "Ordered cycle lengths in a random permutation" or Fulman's "Random matrix theory over finite fields." Sometimes singularity analysis helps with picking off constants, and sometimes we have to use Tauberian theorems if things are not analytic.

Returning now to shuffling cards, we'll go back to the setting in which we consider a-shuffles on S_n, governed by the measure on S_n

$$Q_a(\sigma) = \frac{1}{a^n}\binom{n + a - D(\sigma^{-1}) - 1}{n}.$$

(This is a one-parameter family of measures on S_n, in fact a semigroup.) We then might be curious to see what a random a-shuffle looks like, and today we're going to look at it from the point of view of shuffles. We'll code up the result in three equivalent theorems in which a certain number appears:

Definition 149

For $j \in \mathbb{N}$, let the **necklace numbers** $f_{j,a}$ be the number of aperiodic cyclic necklaces of length j with alphabet $\mathcal{A} = \{0, 1, \cdots, a-1\}$. (In other words, place a symbol on j places around a circle, with two equivalent if we can get from one to the other by rotation, and we get an aperiodic arrangement if there is no smaller period than j.)

Fact 150

We have the formula

$$f_{j,a} = \frac{1}{j}\sum_{d|j} \mu(d) a^{j/d},$$

where $\mu(n)$ is the **Mobius function** (0 if not squarefree, otherwise $(-1)^k$ if n is the product of k different

For example, we have $f_{1,a} = a$ (we choose one of the symbols) and $f_{2,a} = \frac{1}{2}(a^2 - a) = \binom{a}{2}$ (we must choose distinct symbols, and $(1,2)$ is the same necklace as $(2,1)$).

Theorem 151

On S_n, under the a-shuffle measure Q_a, we have (as long as $\sum_i i n_i = n$)

$$\mathbb{P}(\sigma \text{ has } n_i \ i\text{-cycles}) = \frac{1}{a^n}\prod_{j=1}^{n}\binom{f_{j,a} + n_j - 1}{n_j}.$$

Theorem 152

Let $a = q = p^b$ be a prime power. Let $b(x) = \sum_{j=0}^{n} a_j x^j$ be a random polynomial with coefficients $a_j \in \mathbb{F}_q$ such that it's monic ($a_n = 1$), and factor it into irreducibles over $\mathbb{F}_q$. Then we get the same result as above:

$$\mathbb{P}(b \text{ factors into } n_i \text{ factors of degree } i) = \frac{1}{a^n} \prod_{j=1}^{n} \binom{f_{j,a} + n_j - 1}{n_j}$$

We can now get an analogous version of Polya's theorem for shuffles (where the right-hand side was originally an exponential of sums, or equivalently a product of exponentials):

Theorem 153

With all notation as above (and letting $Q_{n,a}$ be the a-measure on S_n), we have

$$\sum_{n=0}^{\infty} t^n \sum_{\sigma \in S_n} Q_{n,a}(\sigma) \prod x_i^{a_i(\sigma)} = \prod_{j=1}^{\infty} \left(1 - \left(\frac{t}{a}\right)^j x_j\right)^{-f_{j,a}}.$$

In particular, this gives specific formulas that look like

$$\mathbb{E}_{Q_{n,a}(\sigma)}[a_1] = 1 + \frac{1}{a} + \frac{1}{a^2} + \cdots + \frac{1}{a^{n-1}},$$

which gives a sense of why it takes longer for the fixed points to mix than the larger cycles.

To get to the proof, we'll describe the Gessell-Reutenauer bijection, and we'll do that by first describing the **records-to-cycles bijection**.

Example 154

The idea is as follows: n people go in order and try to run a race as fast as possible, and suppose everyone's times are iid drawn from the same continuous distribution. Then we sample $X_1, X_2, \cdots, X_n$, and we keep track of the **record values**, which are the values which are smaller than anything that came before them. We can then let R_n be the number of record values.

(We can see Glick's "Breaking records and breaking boards" if we want to read more about this with real data, and there are many books written about the topic as well.) Since this is basically a question about order statistics, this is the same as drawing a uniform random permutation $\sigma \in S_n$ and keeping track of the points i at which $\sigma(i) < \sigma(1), \sigma(2), \cdots, \sigma(i-1)$.

Then the **cycle-to-records map** can be described via the following example: suppose we start with the permutation $\sigma = (3, 4, 6, 2, 5, 1, 7, 8)$. Rewriting this in cycle notation, we get $(136)(24)(5)(7)(8)$ – the decomposition is non-unique since we can rearrange the cycles or choose any starting point, and this time we choose the convention to **begin each cycle with its smallest element and order in decreasing order of the first element**, which would be $(8)(7)(5)(24)(136)$ in this case. Now erase the brackets, **treating this as if it were a one-line permutation** (we can reconstruct the parentheses because they occur at the record values), so we end up with the permutation $R(\sigma) = (8, 7, 5, 2, 4, 1, 3, 6)$.

It turns out this complicated operation has amazing properties:

Theorem 155

The cycle-to-records map R above is a bijection from S_n to itself, and it takes permutations σ with n_i cycles of length i to $R(\sigma)$ with n_i records of length i (where the length of a record is "how long it is a record for").

Corollary 156

The number of records in σ satisfies the same statistics and central limit theorem as the one for cycles – for example, the number of consecutive records is Poisson(1).

Example 157

The Gessell-Reutenauer bijection is described as follows. Let $\mathcal{A} = \{0, 1, \cdots, a-1\}$ and let $\mathcal{A}^n$ be the set of all n-letter words from this alphabet $\mathcal{A}$. Then we have a bijective map from $\mathcal{A}^n$ into sentences of "words" in $\mathcal{A}$, which we'll explain by example.

For this example, let $n = 14$ and $a = 2$, so we are working with binary sequences of length 14. Start with the sequence

$$\boxed{x = (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)},$$

which has **weakly increasing rearrangement** $x^{\uparrow} = (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$. We can then define the inverse shuffle which tells us which position in x each point in $x^{\uparrow}$ came from (if we kept the same relative order within each value in $\mathcal{A}$):

$$\pi_x = (1, 5, 6, 8, 10, 11, 12, 13, 14, 2, 3, 4, 7, 9).$$

Now we can write this as a product of cycles (in increasing order, with smallest element first within each cycle)

$$(1)(2, 5, 10)(3, 6, 11)(4, 8, 13, 7, 12)(9, 14),$$

and replace symbol i by the ith coordinate of $x^{\uparrow}$:

$$\boxed{s_x = (0)(0, 0, 1)(0, 0, 1)(0, 0, 1, 0, 1)(0, 1)}.$$

This map $x \mapsto s_x$ has amazing properties, and to describe them we'll need to know about **Lyndon words**:

Definition 158

A word $(w_1, w_2, \cdots, w_\ell) \in \mathcal{A}^\ell$ is **Lyndon** if it is uniquely smallest among all cyclic rearrangements of the word (for example, $(0, 0, 1)$ is Lyndon, but $(0, 1, 0)$ and $(0, 1, 0, 1)$ are not). Let $\mathcal{L}$ denote the set of all Lyndon words, and order $\mathcal{L}$ by repeated lexicographic order (that is, $x < y$ if and only if $x^* < y^*$, where x^* is the word x repeated infinitely often).

This definition turns out to be fundamental to parts of Lie theory and also in much of this current theory:

Theorem 159

The map $x \mapsto s_x$ described above is a bijection between $\mathcal{A}^n$ and the set of sentences of Lyndon words which are weakly monotone in the ordering described above.

For example, we indeed have $0, 001, 001, 00101, 01$ in weakly increasing order in our example above. This is a complicated result, but it actually encodes all of the three theorems we described above about cycle structure! We'll talk about this a bit more next time. (And the point of today's lecture is broadly that there are lots of connections to other fields of math if we take the study seriously.)

Remark 160. *It's possible to enumerate permutations via descents instead of cycle structures, keeping track of the distribution of the descent set. There's a huge literature in that direction as well, but there's almost none on the joint distribution betwen cycle structure and descent set. That's what Gessell does, and he has a "formula" for the number of such permutations. Lots of people have used this formula to do other things as well (in combinatorics and group theory)!*

14 February 22, 2024

Last time, we stated three equivalent theorems involving cycles of permutations after riffle shuffling (one of them being Theorem 153, a version of Polya's theorem). We'll do two examples where we can see that we do get nice information about shuffles out of this complicated equation:

Example 161
Under the measure Q_a on S_n, let's see how we get the equation $\mathbb{E}[a_1] = 1 + \frac{1}{a} + \cdots + \frac{1}{a^{n-1}}$ for the number of fixed points.

Indeed, take Theorem 153 and plug in $_1 = x$ and $x_j = 1$ for all other j. Then we have

$$\begin{aligned}\sum_{n=0}^{\infty} t^n \mathbb{E}_{Q_a}[x^{a_1}] &= \left(1 - \frac{t}{a}\right)^{-f_{1,a}} \prod_{j=2}^{\infty} \left(1 - \left(\frac{t}{a}\right)^j\right)^{-f_{j,a}} \\ &= \left(\frac{1 - t/a}{1 - tx/a}\right)^a \prod_{j=1}^{\infty} \left(1 - \left(\frac{t}{a}\right)^j\right)^{-f_{j,a}} \\ &= \frac{1}{1-t} \left(\frac{1 - t/a}{1 - tx/a}\right)^a,\end{aligned}$$

where the last line is because if we set all x_is equal to 1 then we just have exactly a geometric series $\sum_{n=0}^{\infty} t^n$. Since we want the mean, we differentiate both sides in t n times and look at the constant coefficients, and we'll exactly get the formula above.

A natural follow-up question is to ask about the distribution of the fixed points (not just the mean). Recall that a **negative binomial** random variable with parameters (f, p) is a nonnegative-integer valued variable with distribution

$$\mathbb{P}(X = m) = \binom{f + m - 1}{m} p^m (1 - p)^f$$

where X can be thought of as the number of heads before the fth tail if we're flipping a p-coin (since we need f tails and m heads, and $\binom{f+m-1}{m}$ is the number of ways to arrange everything before the last tail).

Theorem 162
Fix a. As $n \to \infty$, the distribution of the number of j-cycles under the measure Q_a on S_n is independent for different js, and it is negative binomial with parameters $f_{j,a}$, $\frac{1}{a^j}$ (instead of Poisson).

It's an elementary fact that such a negative binomial distribution converges to the Poisson distribution of mean $\frac{1}{j}$ as $a \to \infty$, so we do indeed get that "the more we shuffle, the closer we get to uniform." (For example, we can write down the moment generating functions and see that they do converge.)

Fact 163

We can check that under just a single shuffle (the measure Q_2), large cycles have the **right stick-breaking distribution**. Specifically, imagine taking a long stick of length 1, breaking it in half, and then repeating the process repeatedly on the right piece. Sorting the lengths longest to shortest, the resulting partition is given by the **Poisson-Dirichlet distribution**.

Fact 164

It turns out that as $n \to \infty$, as long as we have $a \to \infty$ (no matter how slowly), all features of our cycles will have the right limiting distribution. (For example, the expression $1 + \frac{1}{a} + \cdots + \frac{1}{a^{n-1}}$ indeed goes to 1.) There's likely more analytic work that can be done though (for example studying different ways that a and n go to infinity together).

One example of an interesting statistic is the length of the longest increasing subsequence L – it turns out we have thee expression

$$\mathbb{E}\left[\frac{L}{n}\right] \to \int_0^\infty e^{-x - \int_x^\infty \frac{e^{-y}}{y} dy} dx \approx 0.62113.$$

We can do this with the generating functions we mentioned above or with "softer" analysis that's now available, and if we're curious for more details about cycle lengths we can see the book by Arratia, Barbour, and Tavaré, and it turns out that these types of calculations also come up in number theory (distributions of large prime divisors matching those with long cycles, for example).

We'll return to the "three equivalent theorems" later so that we can move on to something else for now (but we can read the paper with McGrath and Pitman if we're curious in the meantime).

Example 165

We've been working with this distribution $Q_a(\sigma) = \frac{1}{a^n}\binom{n+a-R(\sigma)}{n}$ where $Q_a * Q_b = Q_{ab}$, and we may ask why such a "miracle" happened where this structure worked out so nicely. It turns out there is some algebraic reason, and that will bring us to **descent theory**. If we'd like a reference here, we can see Kyle Peterson's paper or Graham, Knuth, and Patashnik's book "Concrete mathematics."

Recall the definition of descents from Definition 132 – for example for $\sigma = 534162$, we have $D(\sigma) = 3$ and descent set $\{1, 3, 5\}$.

Definition 166

The **Eulerian polynomial** is defined by

$$A_n(t) = \sum_{\sigma \in S_n} t^{D(\sigma)} = \sum_{j=0}^{n-1} t^j A(n, j),$$

where $A(n, j)$ (the number of permutations of size n with j descents) are called the **Eulerian numbers**.

The first few examples are given by $A_0(t) = 1$, $A_1(t) = 1$, $A_2(t) = 1 + t$, $A_3(t) = 1 + 4t + t^2$. The reason for the naming was that Euler discovered the identity

$$\sum_{k=0}^{\infty} k^n t^k = \frac{A_n(t)}{(1-t)^{n+1}}.$$

(In the special case when $n = 0$ this gives us $\sum t^k = \frac{1}{1-t}$ and $n = 1$ yields $\sum k t^k = \frac{t}{(1-t)^2}$, so these are familiar formulas and we just have one of them for general n. And it wasn't until the 1950s that the connection to permutations as made.)

One natural question we may ask is what the distribution of $D(\sigma)$ looks like (if we sample σ uniformly from S_n). It makes sense that each position kind of has a $\frac{1}{2}$ probability of being a descent, and we have the following:

Theorem 167

We have

$$\sup_x \left| \mathbb{P}_{S_n} \left(\frac{d(\sigma) - \frac{n-1}{2}}{\sqrt{(n+1)/12}} \le x \right) - \Phi(x) \right| \le \frac{12}{\sqrt{n+1}}.$$

It's hard to do this in an elementary way because the generating function is a bit messy, but there are at least six different proofs. And if we're curious about the descent set, we can define a point process

$$X_i(\sigma) = 1\{\sigma \text{ descends at } i\}$$

and ask whether this converges to a Poisson process or something else:

Theorem 168

The process X_i defined above is a **1-dependent determinantal point process**. Specifically, for any subset $A \subseteq [n-1]$, we have

$$\mathbb{P}(X_i = 1 \text{ for all } i \in A) = \det\left(K(i,j)\right)_{i,j \in A},$$

where K is a matrix of the form $K(i,j) = k(j-i)$ and where k has generating function $\sum_{j \in \mathbb{Z}} k(j) z^j = \frac{1}{1-e^z}$ (up to rescaling, these ks are basically the Bernoulli numbers).

Here we say that a point process is determinantal if the probabilities take a determinant form for a fixed kernel K as above, and "1-dependent" means that X_is separated by more than 1 are independent. (We can use inclusion-exclusion from here to get the probability of X_i being 1 exactly at A.) If we want some other examples of this type of behavior, we can see Borodin, Diaconis, and Fulman's paper "On adding a list of numbers (and other one-dependent determinantal processes)."

To see connections with shuffling, we can now look at **Solomon's descent algebra**. We'll work in the **group algebra**

$$\mathbb{Q}[S_n] = \sum_{\sigma} a_\sigma \sigma,$$

which is the list of all formal $\mathbb{Q}$-linear combinations of permutations or equivalently the set of all functions $S_n \to \mathbb{Q}$. This has both an addition structure (via coordinate-wise summation) and a multiplication one (from the group law). Now for any set $S \subseteq [n-1]$ we can define

$$A_S = \sum_{\text{descent set}(\sigma) = S} \sigma$$

(for typical sets S there are a lot of different permutations with that descent set).

Theorem 169

Linear combinations of $\{A_S\}_{S\subseteq[n-1]}$ form an **algebra**, meaning that $A_S A_T = \sum_{U\subseteq[n-1]} c_{ST}^U A_U$ for some positive integer coefficients c_{ST}^U (which are reasonably explicit). We call this subalgebra of $\mathbb{Q}[S_n]$ the **descent algebra**.

We can finally connect this all back to card shuffling now by phrasing some of these quantities in those terms:

Fact 170

Consider the inverse shuffling process where we take out some i cards from our deck and put them at the top. This creates a permutation with only a single descent at position i, as long as we don't remove exactly the top i cards.

We can write this down in more formal mathematical language too:

Proposition 171

Let B_i be the sum of all permutations whose inverse has $(i-1)$ descents, and let Q_2 be the usual riffle shuffle measure. Then

$$\sum_{\sigma\in S_n} Q_2(\sigma)\sigma = \frac{n+1}{2^n}\mathrm{id} + \frac{1}{2^n}B_2.$$

In other words, 2-riffle shuffles yield something in the descent algebra. And similarly if we do an inverse 3-shuffle, we usually get two descents (at positions i and $i+j$ if the first and second group have i and j cards, respectively). So there's something more general we can say:

Theorem 172

With the notation above, linear combinations of the $\{B_i\}_{i=1}^n$ span a semisimple **commutative** algebra, meaning that $B_iB_j = \sum_k c_{ij}^k B_k$ with B_i and B_j commuting. This algebra has dimension n, and it has primary idempotents

$$\sigma_\ell = \frac{1}{n!}\sum_{r=1}^{n} e_\ell(n-r, n-1-r, \cdots, 1-r)B_r,$$

where e_ℓ is the ℓth elementary symmetric function (so e_1 is the sum of all arguments, e_2 is the sum of pairs of the arguments, and so on).

It turns out that having such explicit descriptions makes a dent in certain parts of algebra (Hodge decompositions for Hochshield homology), and this all comes from the fact that an a-shuffle followed by a b-shuffle is an ab-shuffle! Just about anything in descent theory can be phrased in terms of shuffling in some way, as can the theory of the free Lie algebra, P-partitions (a unified theory on enumeration of features of posets) and the studies of quasi-symmetric functions. And what's nice is that the concreteness of shuffling sometimes allows probabilists and combinatorialists to write down more abstract results than algebraists can.

Remark 173. *We'll close today with a little about the* **history** *of shuffling, starting with the history of cards. They're not so ancient – they're first dated to around 1280. (There were edicts against gambling in those days; in 1286 there was a list of games not including cards, but in 1287 the updated list also included cards.) Cards can be used for fortune-telling or games, but for any such use we do need to shuffle them. But it's hard to find any description of shuffling in the literature before Cardano (from around 1560). At the time there was no notion of probability, and*

Cardano wrote that usually cards were just gathered together for the next hand unless someone didn't trust someone else. It wasn't until around 1860 where documentation of actually riffle shuffling cards can be referenced!

15 February 27, 2024

Today's topic will be completely different from what we've been doing in the last few lectures – we'll discuss **adding numbers**. Specifically, we'll think about doing ordinary arithmetic in the way we may have learned in elementary school, where we go one column at a time from right to left, and we keep track of where carries occur. It's natural to ask various questions about this process, such as "how many carries are there" or "how correlated are the different carries" or "does the behavior depend on the base" or "what happens if we add more than two numbers at once."

Example 174

To set this up as a math problem, work in base b, so that we have digits $\{0, 1, \cdots, b-1\}$. Suppose we add n numbers, and suppose they are made up of iid uniform random digits X_{ij} (where X_{ij} is the digit in the b^ith place for the jth number). Let $\kappa_0 = 0, \kappa_1, \kappa_2, \cdots$ be the (random) carries in the b^ith places – notice that $0 \leq \kappa_i \leq n-1$ for all i.

Professor Diaconis discovered this topic from the article "Carries, Combinatorics, and An Amazing Matrix" by John Holte in the AMM. (Holte was interested in thinking about fractal geometry – for example, Pascal's triangle has a fractal pattern mod 2, and knowing about carries helps with studying those kinds of objects.) Professor Diaconis and Jason Fulman then subsequently talked about "Carries, Shuffling, and an Amazing Matrix" in their own paper.

Fact 175

The carries $\kappa_0, \kappa_1, \kappa_2, \cdots$ form a Markov chain – that is, $\mathbb{P}(\kappa_\ell = j | \kappa_0, \kappa_1, \cdots, \kappa_{\ell-1}) = \mathbb{P}(\kappa_\ell = j | \kappa_{\ell-1})$.

This is true because if we look at the carry at stage ℓ, we only need to know the carry at stage $\ell - 1$ and the values of the iid variables in that column. And this therefore tells us that there is some matrix which encodes the transition probabilities

$$P(i,j) = \mathbb{P}(\kappa_1 = j | \kappa_0 = i).$$

For example, we can do this in the case where $b = 10$ and $n = 2$: if there was no carry in the previous step, we know that the probability of a carry is $\frac{\binom{b}{2}}{b^2} = \frac{1}{2} - \frac{1}{2b} = 45\%$, and if there was a carry in the previous step, the probability is now $\frac{1}{2} + \frac{1}{2b} = 55\%$. Thus when $n = 2$ we have

$$P = \frac{1}{2b} \begin{bmatrix} b+1 & b-1 \\ b-1 & b+1 \end{bmatrix},$$

and when $n = 3$ we have

$$P = \frac{1}{6b^2} \begin{bmatrix} b^2+3b+2 & 4b^2-4 & b^2-3b+2 \\ b^2-1 & 4b^2+2 & b^2-1 \\ b^2-3b+2 & 4b^2-4 & b^2+3b+2 \end{bmatrix}.$$

In particular, notice that this matrix is not symmetric or self-adjoint (reversible) in any inner product, so when $n > 2$ this is not a reversible chain.

Fact 176

The general expression for the entries of P looks like

$$P(i,j) = \frac{1}{b^n} \sum_{r=0}^{j-\lfloor i/b \rfloor} (-1)^r \binom{n+1}{r} \binom{n-1-i+(j+1-r)b}{n}$$

Indeed, we're just asking for the probability of n uniform random variables to be between certain values – this is easy to prove using generating functions. For example, for $b = 2$ this expression is $P(i,j) + \frac{1}{2^n}\binom{n+1}{2j-i+1}$ for all $0 \le i, j \le n-1$.

We may not see yet why this is an "amazing matrix," and a good starting point is to calculate the stationary distribution. (With 2 numbers, it makes sense that we'll get half and half between 0 and 1 carry, but it's harder to see what happens with more numbers.)

Fact 177

The stationary distribution for P is given by $\pi(j) = \frac{A(n,j)}{n!}$, where $A(n,j)$ is the Eulerian number (the number of permutations $\sigma \in S_n$ with j descents).

In particular, this number doesn't depend on b (even though the transition matrix depends on b), and it's interesting to ask where the symmetric group is even coming up in this! In the small cases above, we have the stationary distribution $(1/2, 1/2)$ for $n = 2$ and $(1/6, 2/3, 1/6)$ for $n = 3$.

Fact 178

Let P_a, P_b be the transition matrices in base a and base b. Then $P_b P_a = P_{ab}$.

Fact 179

The eigenvalues of this Markov chain are $1, \frac{1}{b}, \frac{1}{b^2}, \cdots, \frac{1}{b^{n-1}}$, just like in the riffle shuffling chain.

But we've seen these facts before, and so we see now that this is secretly also a problem about riffle shuffling.

Theorem 180

Let $\kappa_0 = 0, \kappa_1, \kappa_2, \cdots$ be the carries when we add n numbers mod b, and let $\delta_0 = 0, \delta_1, \delta_2, \cdots$ be the number of descents when n cards are repeatedly b-shuffled. Then $\mathbb{P}(\kappa_1 = a_1, \cdots, \kappa_\ell = a_\ell) = \mathbb{P}(\delta_1 = a_1, \cdots, \delta_\ell = a_\ell)$ for all $n, b, \ell, a_1, \cdots, a_\ell$ – that is, they have the same distribution.

In particular, since b-shuffling approaches the uniform distribution on S_n, the stationary distribution of descents is $\frac{A(n,j)}{n!}$, and that explains one reason for Fact 177. But the connection gives us some other applications to carries:

Theorem 181

We have

$$\mathbb{E}[\kappa_j] = \frac{n-1}{2}\left(1 - \frac{1}{b^j}\right), \quad \mathrm{Var}(\kappa_j) = \frac{n+1}{12}\left(1 - \frac{1}{b^{2r}}\right), \mathrm{Cov}(\kappa_r, \kappa_{s+r}) = \frac{1}{b^s} \cdot \frac{n+1}{72}\left(1 - \frac{1}{b^{2r}}\right),$$

and for b and j fixed and n large, we have $\mathbb{P}\left(\frac{\kappa_j - \mu_j}{\sigma_j} \le x\right) \to \Phi(x)$.

Theorem 182

Let $S_m = \kappa_0 + \cdots + \kappa_{m-1}$ be the total number of carries in the first m places. Fixing n and letting $m \to \infty$, we have $\mathbb{P}\left(\frac{S_n - \mathbb{E}[S_n]}{\mathrm{SD}(S_n)} \le x\right) \to \Phi(x)$.

Theorem 183

We have the TV bound for the carries process

$$||P^\ell - \pi|| \le 1 - e^{-1/2c} \text{ if } \ell = \log_b n + c.$$

In particular, the descents get to their stationary distribution faster than the full permutation (which takes $\frac{3}{2}\log_b n$). And it turns out that all of this relates to some work that can be done in areas of combinatorics:

Example 184

Sometimes we can write the generating function of a sequence (a_n) in the form

$$\sum a_n x^n = \frac{h(x)}{(1-x)^{d+1}}$$

for some polynomial h of degree at most $d+1$.

For reference, recall that the generating function for a_n is rational if and only if it satisfies a recurrence relation with constant coefficients. For some examples of this specific setting, Euler showed that

$$\sum n^d x^n = \frac{A(d,x)}{(1-x)^{d+1}}$$

where $A(d,x)$ is the Eulerian polynomial of degree d, and if V is a coordinate ring of some projective variety, its Hilbert series (where a_j is the dimension of the jth graded piece) also takes this form. Then we may be curious about the generating series of "every kth term" $\sum a_{2n}x^n$ or $\sum a_{jn}x^n$:

Theorem 185 (Brenti–Welker)

If $\sum a_n x^n = \frac{h(x)}{(1-x)^{d+1}}$, then $\sum a_{jn}x^n = \frac{h^{\langle j\rangle}(x)}{(1-x)^{d+1}}$, where $h^{\langle j\rangle}$ are polynomials of degrees at least $d+1$.

We can see the paper "The Veronese Construction for Formal Power Series and Graded Algebras" for more details. In particular, they show that if $h(x) = \sum_{i=0}^{d-1} h_i x^i$, then

$$h^{\langle j\rangle}(x) = \sum h_i^{\langle j\rangle} x^i, \quad h_i^{\langle j\rangle} = \sum c(i,j) h_i,$$

where $c(i,j)$ is exactly the same as the "amazing matrix" we've been talking about!

Fact 186

Returning now to carries and shuffling, Holte found the left and right eigenvectors of $P(i,j)$. In particular, if $u_j^n(i)$ is the value of the jth right eigenvector (with eigenvalue $\frac{1}{b^j}$) evaluated at i , then

$$u_j^n(i) = \sum_{k=n-j}^{n} s(n,k)\binom{k}{n-j}(n-1-i)^{k-(n-j)},$$

where $s(n,k)$ are the Stirling numbers.

Since carries and descents go into each other, we can lift this result to the random walk given by the b-shuffle on the symmetric group:

Theorem 187

The vector $f_j(\sigma) = u_j^n(d(\sigma))$ is an eigenvector of $K(\sigma,\tau) = Q_b(\tau\sigma^{-1})$ with eigenvalue $\frac{1}{b^j}$.

For example, we know that $f_1^n(\sigma) = d(\sigma) - \frac{n-1}{2}$ is an eigenvector of $K(\sigma,\tau)$ with eigenvalue $\frac{1}{b}$. So for example if $X_0 = \mathrm{id}, X_1, X_2, \cdots$ is a chain on S_n given by repeated b-riffle shuffles, then the number of descents is given by

$$\mathbb{E}[d(X_k)] = \frac{n-1}{2}\left(1 - \frac{1}{2^k}\right).$$

Fact 188

If we make a matrix out of the **left** eigenvectors instead (so the first row is the stationary distribution, the next one is the left eigenvector of eigenvalue $\frac{1}{b}$, and so on), we get the **Foulkes character table** of S_n.

We'll go through some of this in more detail next time, explaining why some of this is true and writing out more proofs. Specifically, the ideas of determinantal point processes and 1-dependent point processes will explain why shuffling and carries are really the same idea! (And it turns out that signed digits have their own shuffling analog as well – we can read the book with more details.)

16 February 29, 2024

Today, we'll take some of the facts we claimed last lecture and explain why they're actually true. We'll explain why carries and shuffling are related, and we'll start with something very basic:

Example 189

Suppose we want to add just a **single column of numbers** like $3,7,7,5,8,9,1,6$ (which add to 46). A standard bookkeeping device here (used by accountants) is to mark dots to indicate the carries; see the **Trachtenberg system** of speed arithmetic for more details.

The first questions we would ask in this setting are "how many dots appear" and "where do they appear." Suppose our digits are each iid among $\{0,1,2,\cdots,b-1\}$; notice that if we keep track of the set of remainders (in this case $3,0,7,2,0,9,0,6$), we get a corresponding carry if and only if we have a strict descent on remainders. Furthermore, the

set of remainders will be iid uniform if the increments are (because adding iid uniform to anything gives us iid uniform). Thus the joint distribution of the carries process is the same as the **up-down pattern of a random sequence**. (Usually probabilists would study such a process for a continuous random variable, though.)

Thus, we already see that there is a connection between carries and descents. We can do all of this with vectors as well – in general we find that the carries and descents are the same as shuffles – but the details are a bit more annoying combinatorially. (We can read the paper mentioned last time if we want to understand it more carefully.)

So now we can let $X_1, X_2, \dots, X_{n-1}$ each be 1 or 0, indicating whether we get a carry or descent at (0-indexed) position i. This yields a point process $\{X_i\}_{i=1}^{n-1}$ – point processes are a big area of applied probability, and we can read Daley and Vere-Jones' "An Introduction to the Theory of Point Processes " for a comprehensive study of such objects. But we'll just list off a few useful observations here:

Fact 190

We have $\mathbb{P}(X_i = 1) = \frac{1}{b^2}\binom{b}{2} = \frac{1}{2} - \frac{1}{2b}$ (since if we have two iid digits, there are $\binom{b}{2}$ ways to have a descent). Similarly, the probability that we have $X_1 = X_2 = \cdots = X_j = 1$ (j carries in a row) is $\frac{1}{b^{j+1}}\binom{b}{j+1}$; in particular we can't have more than $b-1$ carries in a row.

From this, we can calculate

$$\mathrm{Cov}(X_i, X_{i+1}) = \mathbb{P}(X_i = X_{i+1} = 1) - \left(\frac{1}{b^2}\binom{b}{2}\right)^2 = -\frac{1}{12}\left(1 - \frac{1}{b^2}\right).$$

We also have **stationary** 1-**dependence** of the process $\{X_i\}$. Being **stationary** means that if we take any k places (like $X_1, X_7, X_{15}, \cdots$) and look at the probabilities of having 1s in those positions, this is translation-invariant (so it's the same as the probability for $X_2, X_8, X_{16}, \cdots$), and being 1-**dependent** means that

$$\{X_i\}_{i=1}^{j-1} \perp \{X_i\}_{i=j+1}^{n-1} \text{ for all } j$$

(this is clear if we phrase it in terms of descents). So that means we know the full correlation structure of this process, and what's useful is that **1-dependence yields a central limit theorem** (this is a more precise version of Theorem 182):

Theorem 191

Consider an infinite sequence of the X_is generated in the same way as our finite one. Then

$$\left|\mathbb{P}\left(\frac{S_n - \mu_n}{\sigma_n} \le x\right) - \Phi(x)\right| \le \frac{C}{\sqrt{n}},$$

where $\mu_n = n\left(\frac{1}{2} - \frac{1}{2b}\right)$ and $\sigma_n = \sqrt{\frac{n+1}{12}\left(1 - \frac{1}{b^2}\right)}$.

A reference for this is Hoeffding and Robbins' "The Central Limit Theorem for Dependent Random Variables" or Chen and Shao's "On some approximations for sums of m-dependent random variables." But the point is that we have a central limit theorem and the mean and variance are what we expect them to be. Furthermore, physicists often care about the k-point correlations of processes like this, and that follows from 1-dependence and Fact 190:

Corollary 192

Let $A \subseteq [n-1]$ be a subset of size k. Then

$$\mathbb{P}(X_i = 1 \text{ for all } i \in A) = \prod_{i=1}^{m} \frac{1}{b^{a_i+1}} \binom{b}{a_i+1},$$

where a_i are the sizes of the largest consecutive increasing blocks. (For example, if $A = \{2, 3, 5, 6, 7, 11\}$, then $a_1 = 2, a_2 = 3, a_3 = 1$.)

From this, we can get the probability of a given string of 1s and 0s by inclusion-exclusion, and that relates to **determinantal formulas** (which we'll discuss next).

Fact 193

Note that there **are** stationary binary pairwise independent (even k-wise independent) point processes for which the central limit theorem fails – we need that the correlations decay fast enough. Richard Bradley has a variety of counterexamples that we can read about, but they're not very "realistic" examples.

Definition 194

Let $\{X_x\}$ be binary random variables indexed by a finite set $|\mathfrak{X}|$. We say that the X_i form a **determinantal point process** if there exists a **kernel** $K(x, y)$ such that for all $A \subseteq \mathfrak{X}$, we have

$$\rho(A) = \mathbb{P}(X_x = 1 \text{ for all } x \in A) = \det\left(K(x, y)_{x,y \in A}\right).$$

(Everything works for a general index set too – we're just doing a finite set for simplicity.) We can read Alexei Borodin's short survey on determinantal point processes for some proofs and examples, and there's also a long survey by Svechnikov and a short book by Hough and other authors for the case where $\mathfrak{X}$ is continuous.

Remark 195. *Most of the literature mentioned above assume that our kernels $K(x, y)$ are symmetric, but carries are a determinantal point process where K isn't symmetric (and our examples in general won't be).*

Example 196

In particle physics, particles are smashed together and the resulting energy that comes out of the collision is measured. Then it turns out there are gaps in the energy that can occur, and Wigner claimed that while the low energy levels are informative, the high energy levels are given by eigenvalues of random matrices. And then Dyson and Macchi found that the point process indexed by the line of energies can be described, and in random matrix theory it really is given by a particular kernel K. (Dyson wrote down the determinants and Macchi generalized this to general processes.)

One concrete example is to consider a uniform (from the Haar measure) unitary matrix $M \in U_n$ (meaning that $MM^* = I$) and consider the eigenvalues, which will all lie on S^1. It turns out that those eigenvalues form a point process on the circle with a kernel of the form $K(x, y) = \frac{\sin(x-y)}{x-y}$; similar statements can be made about symmetric matrices or other ensembles, and knowing the representation allows us to prove lots of things about them.

Example 197

Let G be some fixed connected simple graph, and let T be a uniformly chosen spanning tree of G. We can then form a point process where X_e is the indicator of an edge e appearing in the tree, and this will also be a determinantal point process.

Example 198

Let $f(z) = \sum_{j=0}^{\infty} X_j z^j$, where X_j are independent normal with parameters (μ_j, σ_j). Then as long as the parameters are "not too wild," this will be a random analytic function on the unit disk $D_1 = \{z : |z| < 1\}$, and it'll have a discrete set of zeros which also form a determinantal point process for very general sets of means and variances (and that's what the book by Hough et al. is about).

About thirty more "natural" processes which are determinantal are given in the book by Borodin, Diaconis, and Fulman – the reason people often care about them is that it's easier to specify a kernel $K(x, y)$ than to specify a full distribution of X_xs. (And in fields like machine learning, people like Emily Fox use determinantal structure to query data.) In particular, it means the expectation of X_x is just $K(x, x)$ and the covariance is $\begin{bmatrix} K(x,x) & K(x,y) \\ K(y,x) & K(y,y) \end{bmatrix}$. In particular if K is symmetric and the covariance is negative, then the points repel each other.

Fact 199

If $K(x, y)$ (as an operator) has real eigenvalues $\{\lambda_x\}_{x \in \mathfrak{X}}$, then for any subset A, we have equality in law

$$\sum_{x \in A} X_x = \sum_{x \in A} Y_x$$

with Y_x independent Bernoulli of parameter λ_x. So the central limit theorem is easy in this case, even if the process is rather complicated!

Fact 200

If $K_n(x, y)$ is a sequence of kernels with $K_n \to K$ in some sense, then the processes $\{X_x\}$ also converge to $\{Y_x\}$ with Y_x given by the kernel K.

The field of integrable probability is all about determinantal point processes, and the idea is to determine the kernel (often as a contour integral) and then show that as $n \to \infty$ these converge to something like $\frac{\sin(x-y)}{x-y}$ so that the processes converge. And Borodin and Svechnikov's surveys are good for learning more about this!

Theorem 201

The process of carries we've described forms a determinantal point process with

$$K(i, j) = k(j - i), \quad \sum_{j \in \mathbb{Z}} k(j) z^j = \frac{1}{1 - (1 - z)^b}.$$

For example, when $b = 2$, we have

$$\frac{1}{1 - (1 - z)^2} = \frac{1}{2z(1 - z/2)},$$

and now if we change $z \mapsto z$ in this type of calculation we get $k(j) \mapsto c^j k(j)$, meaning $K_c(i,j) = c^{-i}K(i,j)c^j$. Thus we are just conjugating the kernel by a diagonal matrix, which **doesn't change determinants**. So if we let $t = \frac{z}{2}$, our generating function is of the form

$$\frac{1}{4}\left(\frac{1}{t} + 1 + t + t^2 + \cdots\right),$$

which means our kernel looks something like

$$K = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

In particular, this means $\rho(A) = 0$ if A has two consecutive positions and $\rho(A) = \left(\frac{1}{4}\right)^{|A|}$ otherwise (indeed, when we add binary digits, we can't have consecutive carries, and the probability of an isolated carry is $\frac{1}{4}$). And note that the number of ways to get binary sequences with no two consecutive ones is given by the Fibonacci series.

The next result we'll discuss is how **any** 1-**dependent process is determinantal**, and more is coming next time!

17 March 5, 2024

We've been discussing the theory of determinantal point processes in the context of the carries process in the last few lectures, and today we'll give an introduction to the theory of 1-dependent processes.

Definition 202

Let $\Gamma = (V, E)$ be an undirected simple graph, and let $(X_v)_{v\in V}$ be a collection of random variables. We say that (X_v) are 1-**dependent** if for any disjoint sets of vertices S, T with no edge in Γ from a vertex in S to a vertex in T, we have $\{X_s\}_{s\in S} \perp \{X_t\}_{t\in T}$.

Example 203

Suppose Γ is a path on $\{1, 2, \cdots, n-1\}$, and $(X_1, \cdots, X_{n-1})$ are the carries (of single-digit numbers) that we've been studying so far in the last few lectures. Then $(X_1, \cdots, X_{j-1})$ is independent from $(X_{j+1}, \cdots, X_{n-1})$, and in fact the carries process is 1-dependent.

Here's a strategy for constructing 1-dependent processes (which works in more general settings than paths): let U_i be iid uniform on $[0, 1]$, and say we have a function $h(x, y) : [0, 1] \to \{0, 1\}$. Then we can define $X_i = h(u_i, u_{i+1})$, which is clearly a 1-dependent process – we think of this as being made up of "2-block factors." For a long time, it was unknown if there are any stationary 1-dependent processes which **aren't** 2-block factors – it turns out there are, but they're not very easy to create. If we want to see what's needed for such a construction, we can take a look at Holroyd's paper "One-dependent coloring by finitary factors."

But we'll stick to processes on $\{1, 2, \cdots, n\}$ for now, and we'll consider stationary 1-dependent processes (meaning that if we take a finite block and look at the random variables on that block, then the law is translation-invariant while we stay within the interval). We can then define $a_1 = 0$ and $a_i = \mathbb{P}(X_1 = 1, X_2 = 1, \cdots, X_i = 1)$ for all $i > 0$.

Theorem 204

In the setting of stationary 1-dependent processes, the law of $\{X_i\}_{i=1}^n$ is determined by the sequence $\{a_i\}$.

Proof. We can actually write $\mathbb{P}(X_1 = \varepsilon_1, \cdots, X_n = \varepsilon_n)$ as a polymonimal in the a_is. Indeed, for strings e and f, let $e0f$ be the concatenation of e, then 0, then f, and similarly define $e1f$. Then we have

$$\mathbb{P}(e0f) + \mathbb{P}(e1f) = \mathbb{P}(e)\mathbb{P}(f)$$

by 1-dependence, meaning that if we know the right-hand side (by induction), we can replace 0s by 1s in our string and thus calculate the probability of any string of length i for any i. For example, we have $\mathbb{P}(000) = 1 - 3a_2 + a_2^2 + 2a_3 - a_4$. □

It turns out this polynomial is actually "nice" in the following way (see the paper by Borodin, Diaconis, and Fulman):

Theorem 205

In the notation above, we have

$$\mathbb{P}(\varepsilon_1, \cdots, \varepsilon_{n-1}) = \det\left(a_{s_{j+1}-s_i}\right)_{i,j=0}^{k},$$

where we look at our string and let $s_1, s_2, \cdots$ be the lengths of the blocks when we decompose the string into pieces ending in 1. Furthermore, this function is a Schur function in the a_is.

Corollary 206

Any stationary 1-dependent point process on a path is determinantal with kernel $K(i,j) = k(j-i)$ such that $\sum_{j\in\mathbb{Z}} k(j)z^j = -\frac{1}{\sum_{j=1}^{\infty} a_j z^j}$; in fact, the stationarity assumption isn't needed to have a determinantal process.

There are some interesting open problems we can think about as well:

1. Consider a 1-dependent stationary process on an $n \times n$ grid. Is there a nice analog of the $\{a_i\}$s (that is, how many parameters do we need to describe the law)??
2. Now consider a 1-dependent stationary process on a finite tree (whatever being stationary means). Then how much do we need to specify to describe the process?

It turns out there are some surprising connections of what we've been talking about to algebra, and we'll describe them here now.

Definition 207

A **graded algebra** is an algebra $\mathcal{A} = A_0 \oplus A_1 \oplus A_2 \cdots$ where we can add and multiply, such that each A_i is a subspace, $A_i A_j \subseteq A_{i+j}$ for all i, j, and $A_0 = k$ is often the field that the spaces are defined over.

For example, the ring of polynomials $k[x_1, \cdots, x_n]$ is graded by degree.

Definition 208

An algebra is **quadratic** if it is generated by elements of degree 1, meaning that $\mathcal{A} = \langle A_1 \rangle$, and all relations are in A_2.

For example, since $x_1, \cdots, x_n$ are polynomials and we have the commutativity relations $x_i x_j - x_j x_i = 0$ (which are quadratic), we do have a quadratic algebra here.

Fact 209

We call a quadratic algebra **Koszul** if there is some condition on the growth of the dimensions $\dim A_i$. It turns out that if A is a Koszul algebra and we define $a_i = \frac{\dim(A_i)}{(\dim A_1)^i}$, then a_is form a 1-dependent stationary point process in the sense of Theorem 204 (in particular, the resulting determinants are all positive).

This result is due to Positselski and Polishchuk (we can see their book "Quadratic Algebras")

Example 210

Consider the polynomial ring $k[x_1, \cdots, x_b]$ with the additional conditions that $x_i x_j = x_j x_i$ and $x_i^2 = 1$ for all i. Then A_i are generated by the squarefree monomials of degree i, meaning that $\dim A_i = \binom{b}{i}$. But this means that $a_i = \frac{1}{b^i}\binom{b}{i}$, and those are exactly the numbers coming from carries! And in general, it's likely that many "nice" Koszul algebras lead to nice determinantal point point processes. So there are lots of research problems in this direction as well.

So we've seen that there's some interesting math in the carries process, and specifically **carries are cocycles**:

Example 211

Let G be a finite group and N be a normal subgroup of G. Further assume that N is a subset of the center of G (for example if G is abelian). Let G/N be the quotient group, and choose coset representatives $T = \{t_1, \cdots, t_{G/N}\}$ such that $t_1 = \mathrm{id}$. Then we can uniquely write $s = tn$ for some $t \in T$ and $n \in N$.

Note that the product of coset representatives isn't always a coset representative – for example, if $G = C_{100}$ is the integers mod 100 and $N = C_{10} = \{0, 10, 20, \cdots, 90\}$ is a central subgroup, then we might choose coset representatives $T = \{0, 1, \cdots, 9\}$. Then any number can be written as a multiple of 10 plus a remainder, but $5 + 7 = 12$ is not in T. So in **extension theory**, we fix this by noting that

$$t_1 + t_2 = t^* f(t_1, t_2),$$

where t^* is the representative in the coset of $t_1 t_2$ and $f(t_1, t_2) \in N$. We then call the values $f(t_1, t_2)$ **cocycles**, and it turns out using homological algebras we can say much more (the second cohomology group is the set of all possible cocycles, and so on). So we might ask how to do carries in this setting:

Example 212

Let $s_1, s_2, \cdots$ be iid uniform on G, and write $s_i = t_i n_i$ for all i. Because N commutes with everything, we have

$$s_1 \cdots s_k = (t_1 n_1) \cdots (t_k n_k) = t_1 \cdots t_k (n_1 \cdots n_k),$$

and we can make a carries processes by writing down $t_1, t_2, \cdots$, and then writing down cocycles if they appear, yielding $X_i \in N$ for all N.

Then the same argument as above shows that this carries process is stationary and 1-dependent with values in N. And if we want a binary process, we can just record whether we have a carry (a non-identity X_i) or not; this still gives us a stationary 1-dependent point process. And we can try different examples ourselves and see whether we get a broadly interesting result!

Example 213

Everything above we've described works for locally compact groups where G/N is compact, for example if $G = \mathbb{R}$ and $N = \mathbb{Z}$, so that $G/N = S^1$.

For comparison, recall from shuffling that if we let σ be uniform in S_n and let $D(\sigma)$ be the number of descents of σ, then $\mathbb{P}_{S_n}(D(\sigma) = j) = \mathbb{P}(j \leq u_1 + \cdots u_n \leq j + 1)$, where u_is are iid uniform. We mentioned previously that the formulas were discovered independently, but it turns out their connections comes through what we're talking about here!

Proof that descents are related to sums of uniform random variables. Consider the carries process on $\mathbb{R}/\mathbb{Z} = S^1$, where $u_1, \cdots, u_n$ are iid uniform. Then we get a carry going from u_1 to $u_1 + u_2$ if and only if there is a descent in the value. But we get j carries if and only if $j \leq u_1 + \cdots + u_n \leq j + 1$, and we also get this if and only if the relative permutation of the remainders (which is uniform over all permutations) has j descents. □

It's natural to ask whether there's a generalization of this beyond $\mathbb{R}/\mathbb{Z}$, and there's indeed a lot left to be done in this area if we're curious.

Example 214

We'll move back to shuffling regular cards soon, but first we may ask whether there are similar "miracles" in which things work out as nicely as shuffling does. One such area is the study of **random walks and hyperplane arrangements**.

Definition 215

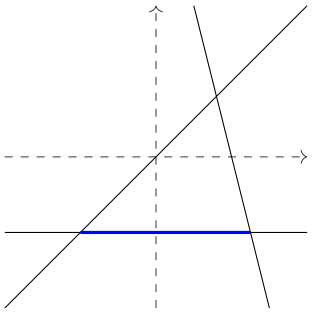
A **hyperplane** is a codimension-1 subspace of $\mathbb{R}^d$, and an **affine hyperplane** is a translation of a hyperplane.

We'll consider the following setting: let $\mathcal{A} = \{H_1, \cdots, H_k\}$ be a collection (**arrangement**) of distinct affine hyperplanes (for example, if $d = 2$, we can imagine having a bunch of lines in the xy-plane in various directions). Each hyperplane divides $\mathbb{R}^d$ into two sides, and for each H_i choose some "positive" and "negative" side so that $\mathbb{R}^d = H_i^+ \cup H_i^- \cup H$.

Definition 216

In any hyperplane arrangement $\mathcal{A}$, the points in $\mathbb{R}^d$ not on any hyperplane are divided into **chambers**; let $\mathcal{C}$ be the set of chambers. A **face** is a nonempty set of points on some of the hyperplanes that are all on a particular side of each other hyperplane – we also consider chambers to be faces.

For example, in the diagram below, there are seven chambers, and the part marked in blue is a face:



The key operation we'll need is the **Tits projection operator**, which works as follows: for any chamber $c \in \mathcal{C}$ and any face $f \in \mathcal{F}$, there is a **unique chamber** adjacent to f that is closest to c in the sense of crossing the fewer number of hyperplanes. (For example, the three chambers on the bottom would project to the chamber below the blue line, and the four on the top would project to the chamber above it.) An alternative definition is as follows: instead of an arrangement of k hyperplanes, consider a vector of length k with all entries in $\{-1, 0, 1\}$, and say that the ith entry is zero if we're on the ith hyperplane H_i, 1 if we're in H_i^+, and -1 if we're in H_i^-; the geometry of the arrangement is then contained in the **set of possible vectors that can occur**. Then the Tits projection is described as follows: if a face is represented as $f = (f_1, f_2, \cdots, f_k)$, with all $f_i \in \{-1, 0, 1\}$, and a chamber is represented as $c = (c_1, c_2, \cdots, c_k)$, with all $c_i \in \{-1, 1\}$, then we can define

$$(f * c)_i = \begin{cases} f_i & f_i \neq 0 \\ c_i & f_i = 0 \end{cases},$$

and the result is the chamber that we project onto. This yields an associative product, and in fact we can use this to define the product of two faces. Then the linear combinations of the faces with this product is called the **face algebra** – it makes the faces into a semigroup. We'll talk more about this next time, seeing how shuffling relates to this, and we'll prove some interesting results!

18 March 7, 2024

We'll continue our discussion of **random walks and hyperplane arrangements** today; a good reference for this material is Richard Stanley's lectures on hyperplane arrangements. Like yesterday, we let $(H_1, \cdots, H_k)$ be a set of k affine hyperplanes in $\mathbb{R}^d$, which divide the space into chambers and faces; recall that we fix half-spaces H_i^+ and H_i^- for each hyperplane by "picking a side," and then faces are subsets of a hyperplane that are on a certain side of each of the others – recall that we count chambers as faces too. (And there's already an interesting question to determine the number of chambers and faces given some set of hyperplanes.)

Last time, we defined the projection operator, where for any chamber $c \in \mathcal{C}$ and face $f \in \mathfrak{F}$ we can define the projection $\text{Proj}_{c \to f}$, which is the chamber c' adjacent to f closest to c in terms of the number of hyperplanes that must be crossed. (Alternatively, you can pick any point in c and any point in f, draw the straight line connecting them, and look at the first chamber adjacent to the point in f.) If we now define a probability distribution $(w_f)_{f \in \mathcal{F}}$ on faces (where the w_f are nonnegative and sum to 1), we can define a Markov chain on $\mathcal{C}$ in the following manner: if we're currently at $c \in C$, pick a face f with probability w_f and move to $\text{Proj}_{c \to f}$. The kernel of the Markov chain is then

$$K(c, c') = \sum_{f : \text{Proj}_{c \to f} c = c'} w_f$$

(in general there can be many faces which project to the same chamber). We also gave the following alternate characterization of this process last time: represent each chamber c as $(x_1, \cdots, x_k)$, where $x_i = 1$ if $c \in H_i^+$ and -1 otherwise, and similarly represent each face but potentially with $x_i = 0$ if the face is a subset of H_i. Then the projection $\text{Proj}_{c \to f}$ matches with f at all coordinates where $f_i \neq 0$, and otherwise it matches with c. (We call this configuration the **oriented matroid** associated with the hyperplane arrangement – we can check the sign patterns we get here satisfy the necessary axioms if we define multiplication of two faces in a similar way, where the left one takes priority. And that's essentially what all oriented matroids are, except that we can have "wiggly hyperplanes" instead of affine ones.)

Remark 217. *Semigroups that comes from this construction have special properties that normal oriented matroids don't, so there is in fact some appeal to the geometric structure of this walk we're doing. But it's not so relevant for the study that we're doing here.*

Example 218 (Boolean arrangement)
Consider the arrangement in $\mathbb{R}^d$ where we have the usual coordinate hyperplanes $H_i = \{\vec{x} : x_i = 0\}$ for $1 \leq i \leq d$. Then the chambers are the usual orthants, so we have 2^d chambers, and we have 3^d total faces because any vector in $(-1, 0, 1)^d$ is valid. The projection operator is then described most easily by the formula for $\text{Proj}_{c \to f}$ given above: we copy the signs of f onto c but leave everything else unchanged. For example, if f is described by $(0, 0, +, -, 0)$ in the five coordinates, then the projection of c onto f is given by replacing the third and fourth coordinates with $+$ and $-$ respectively, keeping everything else fixed.

So our random walk on chambers will be a walk on the hypercube, and we can define the face weights

$$w_f = \begin{cases} 1/2d & f = (0, \cdots, \pm 1, \cdots, 0) \\ 0 & \text{otherwise.} \end{cases}$$

This means that if we're in the chamber $(\varepsilon_1, \cdots, \varepsilon_d)$, then the next step is given by picking a random coordinate and then flipping it to $+1$ or -1 at random. So this is actually the Ehrenfest urn with holding probability $\frac{1}{2}$.

Example 219
For our next example, we'll describe the walk in ordinary probabilistic terms first. On a path of length $d + 1$ (though we can do this on any graph in general), put a random ± 1 sign on each vertex, so that our state space is $\{\pm 1\}^{d+1}$. Then the dynamics are as follows: pick an edge of our graph uniformly at random with probability $\frac{1}{d}$, and change the signs there to both $++$ or both $--$.

Remark 220. *This is very closely related to the* **graphical arrangement**, *where on $\mathbb{R}^d$ we have a hyperplane $H_e = \{\vec{x} : x_i = x_j\}$ for any $e = (i, j)$.*

The stationary distribution of this chain is very far from uniform – if we're at the state with all $+$s, then there's a $\frac{1}{2}$ probability we stay at that state, but if we're at the state which alternates $+$s and $-$s, then there's zero probability we're there at the next step. So it makes sense that states with a lot of alternations are less likely, but that's still open! And with a bit of work, we can see that this becomes another Boolean chain like the one above with different face weights. The point is that any kind of Markov chain where we choose a chunk at random and change it to something with a fixed configuration, we'll get a Boolean chain.

Example 221 (Braid arrangement)
Again working on $\mathbb{R}^d$, consider the set of hyperplanes $H_{ij} = \{\vec{x} : x_i = x_j\}$ for all $i < j$. We then have $\binom{d}{2}$ hyperplanes, and the chambers are specified by the **relative ordering** of points within that chamber – thus we can index the $d!$ chambers via permutations.

Proposition 222
The faces of the braid arrangement are indexed by block ordered set partitions of $\{1, \cdots, d\}$.

A set partition looks something like $\{\{1,3\},\{2,4\},\{5\}$, and block ordered means we order the blocks in some particular order. The correspondence is as follows: being on certain hyperplanes tells us that some set of the coordinates are equal, and we put all of those sets into a single block. Then because we're on a fixed side of each hyperplane, we have a relative ordering of the coordinates among the blocks. The number of set partitions of $\{1,\cdots,d\}$ is the Bell number, and the number of ordered ones is also well-studied, but it's not so important for our purposes here.

The projection operator can then be described as follows: say we have a chamber c and a face f. We can associate c to some permutation $\sigma \in S_d$, and we can associate f to some block-ordered set partition. Then $\text{Proj}_{c\to f}$ is described similarly to the inverse shuffling process we've described: we put the cards in the locations given by the first block (in the same relative order) and put them on the top, then put the cards in the locations given by the second block and put them directly underneath, and so on.

Example 223 (Tsetlin library)
Set $w_f = \theta_i$ if f corresponds to the set-partition with first block $\{i\}$ and second block $[d]\setminus\{i\}$, and set $w_f = 0$ otherwise (where θ_i are nonnegative and sum to 1). This corresponds to picking the card labeled i and putting it on the top of our deck.

The motivation for this problem is imagining that there is a pile of books in a library, and people grab the books they like and put them back on top when they're done. And this is actually similar to how disks in deep storage are allocated.

Example 224 (Shuffling)
Set $w_f = \frac{1}{2^d}$ if f corresponds to the set partition $(S,[d]\setminus S)$ for some subset S, and 0 otherwise. This means we flip a fair coin for each card, and we put the cards with heads on top of the ones with tails. So inverse shuffling, and in general a-shuffling, is in the general framework of hyperplane random walks!

The point of the lecture is that there's actually basically a complete theory of these chains, despite how general they are – we know the eigenvalues and good rates of convergence for them, and there's a description of the stationary distribution as well. But the first thing we want to discuss is ergodicity:

Definition 225
A collection of weights $(w_f)_{f\in\mathcal{F}}$ is **separating** if not all f with nonzero w_f are in the same hyperplane (that is, there is a face contained in either H_i^+ or H_i^-).

Theorem 226
A collection of weights is separating if and only if there exists a unique stationary distribution (meaning that $\sum_c \pi(c)K(c,c') = \pi(c')$).

To find the eigenvalues of the chain, we need to make use of the **intersection lattice** $\mathcal{L}$, which is the lattice (in fact a geometric lattice) consisting of all possible intersections of hyperplanes. This is a partially ordered set under inclusion (or reverse inclusion, depending on convention).

Theorem 227

We have the following for any hyperplane walk:

1. The kernel $K(c, c')$ is diagonalizable (even though it's not reversible).
2. For each $\ell \in \mathcal{L}$, there is an eigenvalue $\beta_\ell = \sum_{f \subseteq \ell} w_f$ (in particular, they are real and nonnegative – this isn't clear from matrix analysis methods!)
3. The multiplicity of β_ℓ is the absolute value of the Möbius function $\mu(\ell, \mathbb{R}^d)$.

Here, the Möbius function is defined in the spirit of inclusion-exclusion: we have $\mu(v, v) = 1$, and $\mu(w, v) = -\sum_{w \le u \le v} \mu(u, v)$. For example, if we have three parallel lines ℓ_1, ℓ_2, ℓ_3 in $\mathbb{R}^2$, then $\mu(\mathbb{R}^2, \mathbb{R}^2) = 1$, $\mu(\ell, \mathbb{R}^2) = -1$ for each line ℓ, and $\mu(\varnothing, \ell) = 2$.

Theorem 228

Suppose $(w_f)_{f \in \mathcal{F}}$ is separated, so we have a stationary distribution π. Then

$$\left|\left|K_c^\ell - \pi\right|\right|_{\text{TV}} \le \sum_{i=1}^{k} \beta_{H_i}^\ell, \quad \beta_{H_i} = \sum_{f \subseteq H_i} w_f.$$

If we're curious about interesting research problems in this direction, the general idea is to find interesting (interpretable) arrangements. For example, taking the union of the braid arrangement with $x_i = x_j + 1$ yields the **Shi arrangement**, which has $(n+1)^{n-1}$ chambers. Then what's necessary is to find a natural set of weights w_f and describe the resulting stationary distribution.

Proposition 229

Suppose the set of hyperplanes $\mathcal{A}$ and the weights w_f are invariant under the action of a transitive group. Then $\pi(c)$ is uniform (like in the cases of the Ehrenfest urn or riffle shuffling).

On the other hand, for the Tsetlin library, the stationary distribution for weights $(\theta_1, \cdots, \theta_n)$ is given by the **Luce measure**, where $\pi(\sigma)$ is given by sampling the numbers $1, 2, \cdots, n$ without replacement repeatedly with probabilities proportional to $\theta_1, \cdots, \theta_n$ until no numbers are left. In particular, this means

$$\pi(\sigma) = \theta_{\sigma_1} \cdot \frac{\theta_{\sigma_2}}{1 - \theta_{\sigma_1}} \cdots \frac{\theta_{\sigma_3}}{1 - \theta_{\sigma_1} - \theta_{\sigma_2}} \cdots,$$

and there are indeed lots of interesting statistics we can extract about the distribution of permutations under the Luce measure! Here's the general theorem:

Theorem 230

Let $(w_f)_{f \in \mathcal{F}}$ be separating weights. Then we can sample from the stationary distribution π as follows: put all weights w_f in an urn and sample without replacement like in the Tstelin library; suppose this yields the sequence of faces $(f_{i_1}, f_{i_2}, \cdots, f_{i_{|\mathcal{F}|}})$. Then starting from **any** chamber c, if we project onto $f_{i_{|\mathcal{F}|}}$, then onto $f_{i_{|\mathcal{F}|-1}}$, and so on, until we project onto f_{i_1}, then the end result is distributed as π.

Example 231

Consider the Markov chain on $+/-$ labelings on a path of length $n+1$ from before, where we change two adjacent vertices to $++$ or $--$ at random. Then it turns out that the least likely configurations with many alternations have measure around $\frac{c}{n!}$, while the most likely ones have measure around $\frac{1}{n}$ (this is a paper by Fan Chung and Ron Graham).

To put this in the framework of shuffling cards, start with n cards, and on card i write $i+$ on one side and $i-$ on the other. Now shuffle the deck (including $+/-$ sides) and process the cards from top to bottom as follows: if we see $i+$, we take the ith edge $(i, i+1)$ and make the two adjacent vertices both $+$, and if we see $i-$ we make the two adjacent vertices both $-$. And this holds for any graph as well if we have a card for each of the graph's edges.

From this description, we can gather that π is actually 1-dependent (because if two vertices are separated by more than 1 vertex in between, the cards $i+$ or $i-$ can only affect one of them at a time), hence a determinantal point process. So there are some things to say about this distribution – the number of $+$s obeys a central limit theorem and even a local central limit theorem for general graphs – but we don't know everything about it yet!

Remark 232. *Sometimes the bounds we get on mixing times with this are off by a small constant factor. For the Ehrenfest urn, the right answer with holding* $\frac{1}{2}$ *is* $\frac{1}{2} n \log n$ *but this setup gives us* $n \log n$*, and for riffle shuffling we get a constant* 2 *instead of* $\frac{3}{2}$.

If we want to learn more, we can see the corresponding chapter in the textbook, Bidigare, Hanlon, and Rockmore's paper which introduced the topic, Brown and Diaconis' "Random walks and hyperplane arrangements," or Brown's "Semigroups, rings, and Markov chains." And it turns out that using hyperplanes, lots of standard constructions in algebra can be generalized, and this has been done in a series of books by Aguiar and Mahajan. It's possible that some of the examples and theory there can be studied in an interesting context in probability too!

19 March 12, 2024

Today is another change of topic – we'll study the **overhand shuffle** and the general strategy of **coupling**.

Definition 233

An overhand shuffle goes as follows: we pick up a deck of cards, and then we drop a few at a time into a new pile from the top. (Other than riffle shuffling, this is the most popular method for shuffling cards.) Equivalently, we can repeatedly take a small packet of cards from the top of the deck and put it on the bottom.

We'll introduce three different models for overhand shuffles:

Example 234

In the p-coin toss model, we imagine a deck of N cards, and between each adjacent pair of cards we flip a p-coin. We then cut the deck into packets at the locations of the 1s. For example if $N = 8$ and our deck reads 1 through 8 from top to bottom, and our coins flip $0, 1, 0, 0, 1, 0, 0$ from top to bottom, then our new card ordering is $6, 7, 8, 3, 4, 5, 1, 2$.

We call the resulting measure $Q_p(S_n)$, and it generates a Markov chain. This chain turns out to be reversible (because the same set of packets gets us back the original cards). In practice for $N = 52$, people tend to break into 5 to 10 packets, so it makes sense to choose p somewhere in the range $[0.1, 0.2]$.

A slight variation of this model is that we can let the 0s and 1s between the cards be governed by a Markov chain with stationary distribution $\begin{bmatrix} \theta & 1-\theta \\ 1-\theta & \theta \end{bmatrix}$, where the first number is uniform between 0 and 1.

Example 235

In a second model, we can fix the number of total packets that we form in overhand shuffling – for example, fix some $1 \leq k \leq n$, and choose $k-1$ break points uniformly at random among all possibilities. The particular case $k = 3$ was suggested as a problem by Borel and Levy.

Example 236

In the final "neat overhand shuffle" model, we pick $1 \leq k \leq n$ from a distribution (for example uniformly) and reverse the top k cards and place them on the bottom (equivalently, deal the first k cards and then put the rest of the pile on the top).

It may seem like the first of these three models is the most natural one to consider, but it turns out there's interesting mathematics that can be discovered in all cases. We'll first state the results "in words:"

Fact 237

For $p \in (0,1)$ fixed and n large, the three models of overhand shuffling above have $n^2 \log n$, $n \log n$, and $n \log n$ necessary and sufficient, respectively.

In particular, notice that the "silly" model is better than the more "natural" model – $n^2 \log n$ is around 11000 and $n \log n$ around 200 for a standard deck of cards. And furthermore in the $p = \frac{1}{2}$ case, remember that both the riffle shuffle and overhand shuffle use the same amount of randomness (n coin flips per shuffle) but take $\log n$ and $n^2 \log n$ steps to mix, respectively! Here's the more careful statement for what "necessary and sufficient" means for our first model:

Theorem 238 (Pemantle)

Fix some $p \in (0,1)$ in the shuffle given by Example 234. Then there is some $\mathbb{N}_+$-valued function $\theta(p)$ and some positive r, n such that for a deck of n cards and $k = \theta(p) n^2 \lceil \log n + r \log 2 \rceil$ shuffles, we have

$$||Q^{*k} - U||_{\text{TV}} \leq 2^{-r-1}$$

Theorem 239 (Jonasson)

Fix $p \in (0,1)$ in the same setting as above. Then

$$k \leq \frac{p^2(2-p)}{8\pi^2(1-p^2)} n^2 \log n \implies ||Q^{*k} - U|| \geq 1 - \frac{1}{\log n}.$$

In particular, this is 0.75 when $n = 52$.

For example, if $p = \frac{1}{2}$, we have $\frac{p^2(2-p)}{8\pi^2(1-p^2)} \approx 0.0063$, so for $n = 52$ the bound is around 70 – this means that "70 shuffles are required at least," which is nowhere near as bad at 10000. And in Pemantle's theorem, the best bound we have for $\theta(p)$ shows that 1.2×10^9 shuffles suffices for $p = \frac{1}{2}$ and 3.7×10^{11} for $p = \frac{1}{4}$. So **constants actually matter** and we should keep track of them whenever possible.

Theorem 240 (Diaconis–Saloff-Coste)
If $\ell = 672n(\log n + c)$ in our second model Example 235, then $||Q_3^{*\ell} - U|| \leq \alpha e^{-c}$ for some (not bad) constant α. On the other hand, if $\ell = \frac{n}{2}(\log n - c)$, then $||Q_3^{*\ell} - U|| \geq \frac{1}{e^2} - e^{-e^c} + o(1)$. The neat overhand shuffle yields similar results with similar constants. (The constants here yield bounds of $102 \leq \ell \leq 138072$.)

Intuitively, the idea is that overhand shuffles keep big clumps of cards together, so we might expect that the number of **adjacencies** $A(\pi)$ (that is, the number of i such that $\pi(i+1) = \pi(i)+1$) stays large for a long time, even though in a uniformly random permutation it should be Poisson(1).

Fact 241
However, from simulation, we can graph the number of average adjacencies for 52 cards and various values of p – we can see that by around 40 the averages are already close to their correct value. So this isn't the "limiting statistic" preventing us from mixing quickly.

Instead, we can think about the statistic which keeps track of whether card 1 is in the top half or the bottom half of the deck – we expect that after an even number of shuffles it'll be near the top, and after an odd number it'll be near the bottom. And the simulation here shows that 500 shuffles are needed at least, but that's the best bound from simple-looking statistics that Professor Diaconis knows. Instead, our strategies from here will involve **coupling**, which is one of the most powerful techniques for proving rates of convergence. (A good reference for coupling arguments is given by the textbook by Levin, Peres, and Wilmer)

Example 242
In the **top-to-random** shuffle, we repeatedly take the top card and put it randomly into the deck in a uniform location (meaning that $Q(\sigma) = \frac{1}{n}$ if σ is the k-cycle $(1, k, k-1, \cdots, 2)$) and 0 otherwise.

We'll study this shuffle, and we'll do so by studying the inverse **random-to-top shuffle** instead – it turns out we can do a coupling in this setting. Consider two decks, where the first deck starts in order $1, 2, \cdots, n$ and the second deck is uniformly shuffled. Then from each deck, we can repeatedly pick a named card at random (such as the 7 of hearts), and we put that same card on the top of both decks. From the perspective of each deck individually, this is doing the random-to-top shuffle.

When we do this, the two decks begin to match better and better – the number of matches at the top weakly increases (it can stay the same if we pick a card that we've already picked). Then by the first time T we've chosen every card, the two decks will be in the same order, but one deck was random to start with (hence still random) and thus both of our decks are random at that point. We call T the **coupling time**, and we have the following result:

Theorem 243 (Coupling inequality)
Let T be a coupling time. Then for all k, we have $||Q^{*k} - U||_{\text{TV}} \leq \mathbb{P}(T > k)$.

In particular, this is the coupon collector's problem and thus it's elementary to bound T: it turns out that if $k = n(\log n + c)$, then $\mathbb{P}(T > k) \leq e^{-c}$. So indeed $n(\log n + c)$ steps are enough to mix using random-to-top, and there's a matching sharp lower bound (in fact we can show cutoff in this setting).

This may seem like an isolated argument, but in fact there are some interesting things to be said here in general:

Theorem 244 (Pitman, Griffiths)

For any Markov chain $K(x,y)$ with stationary distribution π, there exists a perfect coupling such that $||Q^{*k} - U||_{\text{TV}} = \mathbb{P}(T > k)$ for all k (where in general, T is the time it takes for the two copies of the chain to become equal).

Unfortunately, we can't find the coupling explicitly – the proof here isn't constructive – but the point is that we can hope to find okay couplings in general on Polish spaces. (If we like these types of "nice but useless" theorems, we can see Lindvall's book – it also explains how to couple various stochastic processes.)

Example 245

Next, let's consider the Tsetlin library (recall this from Example 223) and study the rates of convergence for this chain. This is very similar to random-to-top, except we now have non-uniform weights and the stationary distribution is given by the Luce model.

The same reasoning works – we start with one deck sorted in order and the other randomly distributed from the stationary distribution, and then we match up the cards at random again. The main difference is that we now have the coupon collector problem with unequal probabilities, which is slightly more complicated – the asymptotics are hard, but just doing a union bound yields

$$||K^\ell - \pi||_{\text{TV}} = \sum_{1 \le i \le j \le n} (1 - \theta_i - \theta_j)^\ell.$$

There are some interesting families of examples here (see Professor Diaconis's "The cutoff phenomenon in finite Markov chains"):

Theorem 246

Suppose $\theta_i = \frac{1}{Z}(n+1-i)^{-t}$ for all $1 \le i \le n$. If $t = 0$, this is the uniform distribution and $k = n(\log n + c)$ steps are sufficient. For $0 < t < 1$, $\frac{n}{1-t}(\log n - \log\log n + c)$ steps are now necessary and sufficient. Similarly for $t = 1$ we have $n \log n(\log n - \log\log n + c)$ required, and for $t > 1$ we have $k = \frac{n^t}{\zeta(t)}(\log n - \log\log n + c)$ required. (And all of these chains have cutoffs in c, meaning the cutoff behavior can be interesting just by varying c.)

Fact 247

Suppose now we consider the process where we alternate putting cards on top and bottom, and also consider (possibly different) weights. This is a model of voting, in which people have preferences for candidates but also vote against them. Then one open question is to study the stationary distribution of this new walk (for example, whether it has a simple description similar to "sampling without replacement" in the Luce model).

We'll close today by describing Pemantle's coupling for overhand shuffles. Recall that between any pair of cards, we have iid Bernoulli random variables $\varepsilon_1, \cdots, \varepsilon_{n-1}$ with parameter p. Just like in our earlier example, we start with two decks (one random, one deterministic), and the coupling goes as follows: say we're currently in order σ and σ', and the two decks match at some set of positions S, such as $\{8, 17\}$. Then sequentially for each $i \in S$ (here $i = 8$, then $i = 17$) couple by using the same coin flips above and below i until we get a 1 (so around some neighborhood of each position, we use the same coin flips – if we run into previously assigned flips, that's fine); now for the remaining unflipped coins, do them independently for the two decks.

The key point is that no matter what happens with the remaining coins, previously matching things in S will continue to match, because the clusters around the points in S will get cut off at the same time and of the same size! So the number of matches continues to increase, and that's how we can get bounds on how long it takes for $|S|$ to reach n (though it does take some hard combinatorics).

Remark 248. *To get a sense of how long this coupling time takes, we can do some simulations – we see that it takes around* 15000 *shuffles for* $p \approx 0.1$ *and around* 10000 *shuffles for* $p \approx 0.2$. *So the advantage of coupling is that even if we can't prove bounds, we can still get a sense of how long it takes, and this does give us something close to* 10000 *shuffles.*

Finally, the two other overhand shuffle bounds come from comparison to random transposition – they're proved in the comparison theory paper. And there's a nice connection to interval exchange maps in ergodic theory as well!

20 March 14, 2024

We'll talk today about a useful technique for bounding rates of convergence, called **strong stationary times**, that we haven't covered in the class so far. For further references here, we can read Aldous and Diaconis' paper "Strong uniform times and finite random walks" in the American Mathematical Monthly or Diaconis and Fill's "Strong Stationary Times Via a New Form of Duality" in the Annals of Probability. And this is all still a viable area of research – there's a two-week conference this July on this exact subject.

The best way to understand this all is through an example:

Example 249

Consider top-to-random shuffle – we've studied it before in various ways, but we'll describe another way to study it here. We start with an ordered deck and repeatedly put the top card somewhere back in the deck. Call the bottom card the ace of spades. Then there's some time T_1 until the top card goes underneath the ace of spades, which is a geometric random variable of parameter $\frac{1}{n}$. After that, there's some time T_2 until the top card goes underneath the ace of spades again, which is T_1 plus an independent geometric random variable of parameter $\frac{2}{n}$. We can repeat this until the ace of spades reaches the top of the deck, and then finally the ace of spades gets put somewhere random.

Inductively, the idea is that even if we know all values T_i, the relative ordering of the cards underneath the ace of spades will always be uniform. And so conditioned on the final time, we know that our deck will be shuffled.

More formally, let $Q(\sigma)$ be the top-to-random measure (like last time, it's $\frac{1}{n}$ for any permutation $(j, j-1, \cdots, 1)$ and 0 otherwise), and let $T_1, T_2, T_3, \cdots$ be the times that a card goes below the original bottom card. Then $T_j - T_{j-1}$ are independent geometric random variables of parameter $\frac{j}{n}$, and then T_n is the time that the original bottom card is at the top. Therefore

$$\mathbb{E}[T_n] = n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n} = n \log n + \gamma n + O(1),$$

and from this we can match to the fact that $k = n(\log n + c)$ implies $||Q^{*k} - U||_{\mathrm{TV}} \leq^{-c}$, since $\mathbb{P}(T_n > k) \leq n\left(1 - \frac{1}{n}\right)^k$. The key fact here is that if X_t is the position of the chain at time t, then **given** that we've already stopped at or before t we're uniform:

$$\mathbb{P}(X_t = \sigma | T \leq t) = \frac{1}{n!}.$$

So the idea of having "strong" stationary times is that X_T is uniform even when given the time that we stop. Here's a

way to see that there is a difference between a stationary time (that is, the time at which we become stationary) and a strong stationary time:

Example 250

Consider simple random walk on a cycle C_n of odd length n, and color each point the first time it is visited. Let T be the first time that all points on the cycle are colored. Then X_T is uniform over $C_n \setminus \{0\}$ (we're equally likely to end at any of the other points). However, if we condition on $T = n-1$, then $(X_T | T = n-1)$ is now only supported on ± 1. So this is a uniform time but not a strong uniform time.

Definition 251

Let $\mathfrak{X}$ be a finite state space, and let $K(x,y)$ be a Markov chain on $\mathfrak{X}$ with stationary distribution $\pi(x)$. A **stopping time** is a map $T : \mathfrak{X}^\infty \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ such that if $T(x) = j$, then $T(y) = j$ for all y agreeing with x in the first j coordinates. (In other words, the stopping rule can only be determined by what has happened so far.) A stopping time T is a **strong stationary time** if $\mathbb{P}(X_t = x | T = t) = \pi(x)$ for all t (equivalently by the definition of stationarity, $\mathbb{P}(X_t = x | T \leq t) = \pi(x)$); in particular this means $X_T \perp T$.

Strong stationary times are naturally associated to **separation distance**, which is defined by

$$\text{sep}(k) = \max_{x \in \mathfrak{X}} 1 - \frac{K^k(x_0, x)}{\pi(x)}.$$

In particular, $\text{sep}(k)$ is bounded between 0 and 1, and it's equal to 0 if and only if $K^k(x_0, x$ is stationary and 1 if and only if $K^k(x_0, x) = 0$ (for example, there are many permutations of 52 cards that we can't get to after 5 steps of top-to-random, so $\text{sep}(5) = 0$). Then we can write

$$||K^\ell - \pi||_{\text{TV}} = \sum_{y : \pi(y) - K^\ell(x,y)} (\pi(y) - K^\ell(x,y)) \leq \sum_{y \in \mathfrak{X}} \pi(y) \text{sep}(\ell) = \text{sep}(\ell),$$

so **separation is an upper bound for total variation** (often off by a factor of 2 in practice).

Lemma 252

Let T be a strong stationary time for (K, π). Then $\text{sep}(k) \leq \mathbb{P}(T > k)$. Conversely, for every K, π, there is some strong stationary time T such that $\text{sep}(k) = \mathbb{P}(T > k)$ for all k, meaning there is indeed some "optimal" one.

Like in last lecture, this converse is an argument which is unfortunately "useless" in practice, since we would need to know everything about the chain to find what that T is. But we can do the proof of the easier direction:

Proof of the forward direction. We have for any n that

$$\begin{aligned} 1 - \frac{\mathbb{P}(X_n = y)}{\pi(y)} = \frac{1 - \mathbb{P}(X_n = y, T \leq n)}{\pi(y)} & \\ = 1 - \frac{\mathbb{P}(X_n = y | T \leq n)\mathbb{P}(T \leq n)}{\pi(y)} & \\ = 1 - \mathbb{P}(T \leq n) = \mathbb{P}(T > n), & \end{aligned}$$

which is the desired result. □

Constructing good strong stationary times, just like finding a good coupling, is an art that takes time to refine. We'll see a few examples to build our intuition now.

Example 253

Consider random walk on C_2^d, and consider the walk on the group with $Q(0) = \frac{1}{2}$ and $Q(e_i) = \frac{1}{2d}$ for all i. We'll make a strong stationary time out of this.

Our cube has d coordinates, and we can imagine the walk steps as "pick a coordinate at random and flip a coin; if it's tails flip that coordinate and if it's heads do nothing. Additionally, we check off a coordinate every time we pick it for the first time, and we let T be the first time all coordinates have been picked. This is then a strong stationary time (after all coordinate have been visited we are uniform), and the coupon collector's problem tells us $T = d(\log d + c)$ when $||P^{*k} - U||_{\text{TV}} \leq e^{-c}$.

Remark 254. *Notice that this is off by a factor of 2 from the correct answer – it actually takes $\frac{1}{2} d \log d$ with holding probability $\frac{1}{2}$. (And it's because we just need to get to the middle of the cube to get small TV, but we need to be able to get all the way to the other side for uniformity.)*

Example 255

Next, consider the random transpositions chain where $G = S_n$ where with probability $\frac{1}{n}$ we do nothing and probability $\frac{2}{n^2}$ for each transposition. Put a checkmark on some **uniformly random** card, and do the following process when we swap cards: if our left-hand card has a checkmark and the right-hand has no checkmark, then switch them check the other card too. Then the first time all cards are checked is a strong stationary time (we can read the book for more details).

There are many different variations of this which also sound similarly plausible, but it turns out they'll be wrong for one reason or another – with strong stationary times, it's important to be very careful with the proof to see if we do have a uniform distribution if we condition on T. And this gets us $n \log n$ for random transpositions – interestingly, there's provably no **Markovian** coupling that does better than n^2 for this chain. (There's some subtlety here with the maximal coupling theorem in Theorem 244 – in that setting, the marginal chains can be Markovian but the bivariate chain is allowed to look at the past.)

Example 256

Next, let's think about a continuous-time example: consider Brownian motion B_t mod 1 on S^1. Then we can understand rates of convergence via a strong stationary time argument: let T_1 be the first time the Brownian motion hits $-\frac{1}{2}$ or $\frac{1}{2}$, let T_2 be the first time it's $\frac{1}{4}$ or $-\frac{1}{4}$ from the location at time T_1, and so on. Then even given the times T_i, we'll be uniformly distributed on one of the 2^i possible stopped points.

This turns out to be a sharp argument, and we can do it for diffusions on compact spaces too. But not much else has been done in the continuous case since then.

Example 257

We'll now see how to use this argument for riffle shuffling (specifically looking at total variation for inverse 2-shuffles).

The construction is as follows: build an $n \times k$ $\{0, 1\}$-valued matrix with entries all iid. We can use the ith column as instructions for our ith inverse shuffle – after the first shuffle, all cards with a 0 in the first column are on top, and

all cards with a 1 are on the bottom. Then after the second shuffle, the cards with 00 are on top, then the cards 10 are directly below that, then 01, then 11. So we are sorting the cards in right-to-left lexicographic order, meaning that we've taken enough columns that all rows of our matrix are distinct, our deck will be fully shuffled.

This means we can let T be the first time those k-tuples are all distinct – this is a strong stationary time, and now calculating the distribution of T is now just the birthday problem! Specifically, we find that

$$\begin{aligned}\mathbb{P}(T > t) &= \mathbb{P}(\text{at least one repeat with } n \text{ uniform balls in } 2^k \text{ boxes }) \\ &= 1 - \prod_{j=1}^{t-1} \left(1 - \frac{j}{2^k}\right) \\ &= 1 - \exp\left(\sum_{j=1}^{t-1} \log\left(1 - \frac{j}{2^k}\right)\right) \\ &= 1 - \exp\left(-2^{-k}\binom{t}{2}\right) + \text{error},\end{aligned}$$

and in particular if $t = 2\log_2 n + c$ this expression is $1 - \exp(2^{-c} + O(1/n))$. So separation shows that we need $2\log_2 n$, while total variation needs $\frac{3}{2}\log_2 n$.

This argument works in some more generality as well – we can handle the biased-θ-shuffle with the same argument, just with a trickier birthday problem. We find that

$$k = \frac{2\log n + c}{-\log(\theta^2 + (1-\theta)^2)} \implies \text{sep}(k) \leq e^{-c},$$

and indeed this shows that the optimal mixing occurs at $\theta = \frac{1}{2}$. (And Sellke managed to get total variation in the θ-biased case too, using various ideas that we've covered in this class and some others as well!)

We won't develop duality in too much detail here, but the big picture is that we've taken a Markov chain, constructed a stopping time T, and analyzed its distribution. So we have a way to turn Markov chains into other probability problems (like the coupon collector or birthday problems), and it turns out there's a full theory of this – there are dual processes to Markov processes, involving dropping balls into boxes where the dual process is an absorbing Markov chain. Possibly the most interesting part of this is that there's a **stochastic interpretation for eigenvalues**. In the top-to-random shuffle, we found that the eigenvalues are multiples of $\frac{1}{n}$, and the stopping-time geometric random variables also have those parameters – it turns out there are generalizations of that, where parameters in geometric random variables come from eigenvalues of the original chain!