TÉCNICO LISBOA

Pers. Diaconis - Lecture 1

How many times should a deck of cards be shuffled to mix it

We think of cards as S_n the symmetric grp on n letters $|S_n| = n!$. For me $n = 52$ but we'll keep n

Will study this way of shuffling  (cut the cards in half and go bzzrr)

Shuffle cut of j cards $\frac{\binom{n}{j}}{2^n}$ cut most in the middle $j \approx 26$ if $n = 52$

Left hand	right hand
A cards	B cards

Chance that next card is from left is $A/A+B$

This completely determines a probability distribution. It is called the Gilbert-Shannon-Reeds model (all mathematicians of Bell-Labs). It is a good model for how most people shuffle cards. We'll see this is the most random way of shuffling cards.
[I've done experiments to confirm this]
I would let each card come from each side successively and that's no good. After 8 iterations the deck is back in the same position.

Let $Q(\pi)$ be the chance of permutation π after one GSR shuffle

$Q(\pi) \geq 0 \quad \sum_{\pi \in S_n} Q(\pi) = 1$

$\pi(i)$ label of card at position i

$Q * Q(\pi) = \sum_{\xi \in S_n} Q(\xi)\, Q(\pi \xi^{-1})$ ← probability of obtaining π after 2 shuffles.

↑ convolution on the symm grp

↑ permutation that takes ξ to π

This is under the assumption that the successive shuffles are independent (one can also model the situation where this isn't so but that is more complicated).

$$Q^{*k}(\pi) = \sum_{\xi \in S_n} Q(\xi)\, Q^{*(k-1)}(\pi \xi^{-1})$$

↑ probability

We have defined cards and shuffle. What about mix?

An ideal shuffle would be the uniform distribution $U(\pi) = \frac{1}{n!}$

What k to large that $Q^{*k}(\pi) \approx \max U(\pi)$

Theorem (Poincaré) $Q^{*k}(\pi) \longrightarrow U(\pi)$ (This happens for many distributions on the symmetric grp)

Define a distance: $\| Q^{*k} - U \|_{TV} = \max_A | Q^{*k}(A) - U(A) |$ A subset of permutations.

↑ total variation

↑ chance the deck is in one of the permutations in $A \subset S_n$: $Q^{*k}(A) = \sum_{\xi \in A} Q^{*k}(\xi)$

If this is small then for any arrangement A there is not much difference.

Exercise: $\| Q^{*k} - U \| = \frac{1}{2} \sum_{\xi} | Q^{*k}(\xi) - U(\xi) |$ (two L^1-distance)

Math problem: Given $\varepsilon > 0$ how large must k be so that $\| Q^{*k} - U \| < \varepsilon$?

This is what we will study for a while. Before here is a question that should be asked more often

WHO CARES?

Every one knows that after 3 or 4 shuffles cards are well shuffled. This is like many things people think they know wrong.

A card trick:

cutting a deck of cards just cycles the cards. (cutting doesn't do much)

shuffle once ⇝ two rising sequences

shuffling twice ⇝ 4 rising sequences.

" ⇝ 8 rising sequences

Card in the middle ⇝ 9th rising sequence of length 1

Homework 2nd exercise

try this!

This explains why 3 shuffles isn't enough to mix 52 cards

Similarly 5 shuffles isn't enough

When we proved this theorem with D. Bayer we made the front page of the NY Times. One reason to also cares is that people really do shuffle cards.

2) Shuffling is a basic operation of algebra

AB with XYZ ABXYZ + AXBYZ + AXBYZ + XYZAB (This (with a sign) is how we multiply differential forms. First studied by Grassman in the 19th century)

Theorems in algebra can be found from card shuffle and conversely theorems in algebra lead to good card tricks!

3) Shuffling is a Markov chain (Lectures 4+5).

Every area of scientific enquiry uses simulations. A basic tool in simulations is Markov chains. If we want to know how many tellers to have in order not to have long lines - these are simulated via Markov chains. A basic question is how long we have to run the simulations.

Shuffling is a model problem. The group theory allows us to find closed formulas which serve as a guide for harder problems.

Theorem (with D. Bayer) $n = 52$

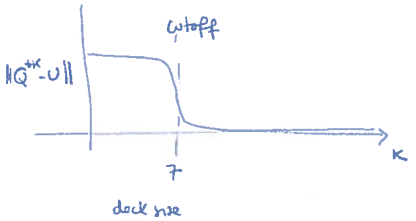
k	1	2	3	4	5	6	7	8	...
$\|\|Q^{*k} - U\|\|$	1	1	1	1	.924	.68	.32	.16	→

↑ .99...9... (12 nines)

keeps going down by a factor of 2 (approx)

I usually call this the 7 shuffles theorem. (The cutoff where exponential convergence to 0 starts is 7)

The graph looks like



deck size

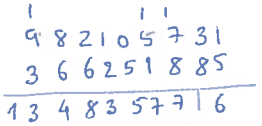
More precisely $k = \frac{3}{2}\log_2 n + c$. Then $\|Q^{*k} - U\| = 1 - 2\Phi\left(\frac{-2^{-c}}{4\sqrt{3}}\right) + O\left(\frac{1}{n}\right)$ $\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}\,dt$

The cutoff happens at $\frac{3}{2}\log_2 n$

Outline of the lectures that are coming:

2. Prove the theorem (combinatorics, algebra, analysis; other distances; a-shuffles. GSR is a=2)

3. "Adding numbers"



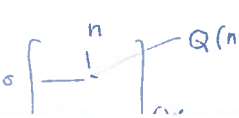
how do the carries work? need n when does one need carries this is important in computer architecture.

This is the same subject as before!!!

4. "Markov chains Monte Carlo revolution" (title of an article I wrote)

5. Going further • in shuffling • in magic

(Homework 3: n=3.



Find the matrix and compute eigenvalues