Persi Diaconis - lecture 2

TÉCNICO LISBOA

4 ways of shuffling:

1) cut off & then drop (G-S-R model)

2) Inverse ~~shuffling~~ description

1 ——
2 ——
⋮
n ——

(i) ~~for each card~~ flip a fair coin and label the card with the flip 0/1
(ii) Take all 0s and put them on top (in same order)

We'll see this is the "inverse" of 1)

3) Maximal entropy: make all 2^n shuffles equally likely

4) Geometric description: $0 \; x_1 \; \ldots \; x_n \; 1$ Put down n points at random, label them left to right

Apply Baker's transformation: $[0,1] \longrightarrow [0,1]$, $x \longmapsto 2x \bmod 1$. This ~~transfer~~ shuffles the points and hence gives a probability measure on the symmetric group.

Baker's map is a mainstay of statistical physics. (Baker because the map describes what a baker does to dough)

Theorem: The 4 descriptions are the "same".

Proof: From 1) suppose we cut off 1-card.

n-1 ≡ —— 1

probability card 1 goes to n is $\frac{1}{n}$

1 " to n-1 is $\frac{n-1}{n}\cdot\frac{1}{n-1} = \frac{1}{n}$

similarly for any other place in the deck

n-2 ≡ = 1, 2

probability 2 cards drop first: $\frac{2}{n}\cdot\frac{1}{n-1} = \frac{1}{\binom{n}{2}}$

check that this is the probability that 1,2 go anywhere in the deck.

Similarly for a cut of j cards all $\binom{n}{j}$ arrangements are equally likely.

Inverse description: "cut" = number of 0's $\overset{d}{=}$ j with probability $\frac{\binom{n}{j}}{2^n}$ so this is the same as above.

3) is free

4) dropping in n points results in j on the left of ½ with probability $\binom{n}{j}/2^n$ (this follows from the properties of Lebesgue's measure)

Moreover Baker's transformation preserves Lebesgue measure. □

Let $a \in \{1,2,3,\ldots\}$. Want to define "a-shuffles".

Cut a piles of size $j_1, \ldots, j_a$ with $\sum_{i=1}^{a} j_i = n$ $\qquad P(j_1,\ldots,j_a) = \frac{\binom{n}{j_1 \cdots j_a}}{a^n}$ a-nomial distribution.

Shuffle by dropping cards sequentially from the piles with probability proportional to packet size.

Inverse description:

1 ——
2 ——
⋮
n ——

choose labels $\{0,1,\ldots,a-1\}$ randomly for each of the cards.

put 0s on top in order, then 1s, etc...

Maximal entropy: OK

Geometric: apply the transformation $x \longmapsto ax \pmod 1$

Again all 4 descriptions give the same outcome.

Main Theorem$^{\vee}$: Let $Q_a(\pi)$ be the probability of $\pi \in S_n$ after an a-shuffle.

1) $Q_a(\pi) = \dfrac{\binom{a+n-r}{n}}{a^n}$ where $r = r(\pi)$ is the number of rising sequences in π

2) $Q_a * Q_b(\pi) \overset{\text{def}}{=} \sum_{\eta} Q_b(\eta) Q_a(\pi \eta^{-1}) = Q_{ab}(\pi)$ "An a-shuffle after a b shuffle is an ab-shuffle"

Aside on rising sequences and descents.

$\pi \in S_n$ decomposes into a disjoint union of rising sequences: ← this is best explained in an example

Example: $\pi =$ 10 8 5 3 1 2 6 7 4 9 $\rightsquigarrow$ 12, 34, 567, 89, 10

Hence $r(\pi) = 5$ for this particular permutation.

Descents were introduced by Euler in 1780 and its an enormous subject

$\pi \in S_n$ has a descent at i if $\pi(i+1) < \pi(i)$. In the above permutation there are 5 descents.

Check: $r(\pi) = \underset{\uparrow \text{ number of descents.}}{d}(\pi^{-1}) + 1$

For instance $r(id) = 1$ $d(id) = 0$

$r(n \cdots 1) = n$ $(n \cdots 1)$ is an involution and $d(n \cdots 1) = n-1$

Example$^{\vee}$ of statement of theorem: $a = 2$ $Q_a(\pi) = \begin{cases} \frac{n+1}{2^n} & \text{if } \pi = 1 \\ \frac{1}{2^n} & \text{if } r(\pi) = 2 \end{cases}$

Part 2 says in particular $Q_2^{*k}(\pi) = Q_{2^k}(\pi)$ and we have a formula for these!

Proof of thm Part 1: $Q_a(\pi) = \#\text{ways to cut into } a \text{ piles can yield } \pi \,/\, a^n$

π decomposes into r rising sequences.

There must be a cut between each pair of rising sequences. 4 15623 ⇒ must have cut between 3 and 4

This forces $(r-1)$ of the cuts.

The other $a-(r-1)$ cuts can be any place. (for instance in the example above could have 2 cuts 12 3 and 3 happen to have fallen below 12)

The # ways of choosing $k = a-(r-1)$ integers $d_1, \ldots, d_k$ $0 \le d_i \le n$, $\sum_{i=1}^{a} d_i = n$

This is a classical problem: stars and bars problem $\underbrace{* \ * \ | \ \ldots \ | \ *}_{n+k-1}$

The answer is $\binom{n+k-1}{k-1} = \binom{n+k-1}{n}$ drop $k-1$ bars

$d_1 = \#$ stars before first bar, etc.

For us $k = a-(r-1)$ so we get $\binom{n+a-(r-1)-1}{n} = \binom{n+a-r}{n}$.

Note: The first proof of this theorem was geometric, involving computing volumes. This is simpler.

Part 2: from geometric version $x \longmapsto ax \bmod 1 \longmapsto b(ax) \bmod 1$ is the same as $x \longmapsto (ab)x \bmod 1$.

This theorem is not true if $a = \frac{3}{2}$ (if they are not integers - think about it!), or in general if they are not integers. $\square$

Main corollary

$$\|Q^{*k} - U\|_{TV} = \frac{1}{2}\sum_{\pi\in S_n}\left|Q^{*k}(\pi) - \frac{1}{n!}\right|$$

We now have formulas for this. It equals $\frac{1}{2}\sum_{\pi\in S_n}\left|\frac{\binom{n+2^k-r(\pi)}{n}}{2^{nk}} - \frac{1}{n!}\right| =$

$$= \frac{1}{2}\sum_{r=1}^{n} b(n,r)\left|\frac{\binom{n+2^k-r}{n}}{2^{nk}} - \frac{1}{n!}\right|$$

with $b(n,r) = \#\{\pi : r(\pi) = r\} = A(n,r-1)$

Eulerian number.

where

$$A(n,k) = \#\{\pi \mid d(\pi) = k\}$$

We know "everything" about these numbers. In particular we have the simple recurrence

$$A(n,k) = (n-k)\,A(n-1,k-1) + (k+1)\,A(n-1,k).$$

For $n=52$ the first sum is hopeless: $52!$ is bigger than the number of atoms in the universe. The sum to 52 can easily be done on a computer.

For asymptotics

$$\frac{A(n,k)}{n!} = P(a < U_1 + \dots + U_n < a+1) \qquad 0 \le a \le n-1$$

chance a permutation at random has k descents

$U_1, \dots, U_n$ are independent uniform random variables on $[0,1]$

⇝ this is very well understood

To see the kind of analysis that is involved. Recall (from Eviatar's lectures) the separation distance

$$sep(k) = \max_{\pi\in S_n} 1 - \frac{Q^{*k}(\pi)}{U(\pi)} \quad \text{and} \quad \|Q^{*k} - \pi\|_{TV} \le sep(k)$$

For us $sep\,k = 1 - n!\,\frac{\binom{2^k}{n}}{2^{nk}}$ (because the maximum is achieved for $\pi = n \dots 1$)

Now

$$n!\,\frac{\binom{2^k}{n}}{2^{nk}} = \frac{n!\,2^k(2^k-1)\cdots(2^k-n+1)}{n!\,2^{nk}} = \frac{2^k}{2^k}\left(1-\frac{1}{2^k}\right)\cdots\left(1-\frac{n-1}{2^k}\right)$$

$$= e^{\sum_{i=1}^{n-1}\log\left(1-\frac{i}{2^k}\right)} \qquad \log(1-x) = -x + O(x^2)$$

$$= e^{-\sum_{i=1}^{n-1}\frac{i}{2^k} + O\left(\frac{i}{2^k}\right)^2}$$

$$= e^{-\frac{\binom{n}{2}}{2^k} + O\left(\frac{k^3}{2^{2k}}\right)} \qquad k = 2\log_2 x + c$$

see beginning of Chap. 3 of notes.

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