Probabilistic Techniques

Continuation of L1-L7 of Martin Tancer.

Martin Klazar (1)
Lecture 8

• Probability: $\underbrace{\text{formalised}}_{\text{a method of enumeration}}$ × $\underbrace{\text{in the world out there}}$
- incomplete information
- future is unknown
- quantum mechanics

Literature on probability

• P. Diaconis and B. Skyrms: Ten Great Ideas about Chance (Measurement, Judgment, Psychology, Frequency, Mathematics, Inverse Inference, Unification, Algorithmic Randomness, Physical Chance, Induction) – no enumer.!

• G. J. Székely: Paradoxes in Probability Theory and Mathematical Statistics

• J. Haigh: Probability: A Very Short Introduction [p. 109: „The subject of Probability is wholly free from real paradoxes."] ?!

• E. T. Jaynes: Probability Theory: The Logic of Science (available online) • Edwin T. Jaynes (1922-1998)

• G. Shafer and V. Vovk: Game-Theoretic Foundations for Probability and Finance (prelim. version available online) [Ch. 13.5 Getting Rich Quick with the Axiom of Choice]

- P. Billingsley: Probability and Measure (av. online)
- Patrick Billingsley (1925–2011) – am. mathem. & stage and screen actor

A result on independence I

Prob-space: (Ω, Σ, Pr) where $\Sigma \subset \mathcal{P}(\Omega)$ (powerset) is a σ-algebra on Ω and $Pr: \Sigma \to [0,1]$ is σ-additive and $Pr(\Omega) = 1$. ($\Rightarrow Pr(\emptyset) = 0$) (finitely add. ?!)

For example, $\Omega = \mathbb{N} = \{1, 2, 3, \dots\}$, $\Sigma = \mathcal{P}(\mathbb{N})$, $c_1, c_2, \dots \in [0,1]$ s.t. $\sum_{i=1}^{\infty} c_i = 1$, and $Pr(A) := \sum_{i \in A} c_i$.

– Countable discrete prob. space – $\boxed{\text{CDPS}}$

Events $A_1, A_2, \dots, A_n \in \Sigma$, $n \in \mathbb{N}$, are independent:

$$Pr\left(\bigcap_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} Pr(A_i).$$

(Infin. many) Independent coin tosses:

Events $A_i \in \Sigma$, $i \in \mathbb{N}$, such that $\forall$ finite $I \subset \mathbb{N}$: $Pr\left(\bigcap_{i \in I} A_i\right) = \left(\frac{1}{2}\right)^{|I|}$.

That is, $A_1, A_2, \dots$ are mutually independent tosses, flippings of a fair coin (head and tale have prob. $\frac{1}{2}$). Is there a CDPS with infinitely many independent coin tosses?

We will show that it is not.

$\boxed{\text{Lemma}}$ Suppose that $A_1, A_2, \dots, A_n \in \Sigma$ are s.t. $\forall I \subset [n] \,(:= \{1, 2, \dots, n\})$: $\Pr(\bigcap_{i\in I} A_i) = (\frac{1}{2})^{|I|}$.

Then $\forall I \subset [n]$: $\Pr(\bigcap_{i\in I} A_i') = (\frac{1}{2})^{|I|}$, where for $i \in [n]$, $A_i' = A_i$ or $A_i' = \overline{A_i} := \Omega \setminus A_i$.

Proof. By induction on the number $c \in \mathbb{N}_0$ ($\{0, 1, 2, \dots\}$) of complemented events $\overline{A_i}$. For $c = 0$ - assumed. For $c > 0$; for instance $c = 2$ and $|I| = 5$: $\Pr(A_2 \overline{A_4} A_6 \overline{A_7} A_9)$ ($\cap$ as a product) $=$

$= \Pr(A_2 A_6 \overline{A_7} A_9) - \Pr(A_2 A_4 A_6 \overline{A_7} A_9)$
$= (\frac{1}{2})^4 - (\frac{1}{2})^5 = (\frac{1}{2})^5$. $\boxtimes$

$\boxed{\text{Theorem}}$ In no countable discrete prob. space there are infinitely many independent coin tosses.

Proof. Suppose the space is given by $c_i \in [0, 1]$, $i \in \mathbb{N}$, and $A_n \subset \mathbb{N}$, $n \in \mathbb{N}$, are indep coin tosses. Let $j \in \mathbb{N}$ be arbitrary, so then $\Pr(\{j\}) = c_j$. We define events $B_n \subset \mathbb{N}$, $n \in \mathbb{N}$, s.t.

$$B_n := \begin{cases} A_n \dots & j \in A_n \\ \overline{A_n} = \mathbb{N} \setminus A_n \dots & j \notin A_n \end{cases}$$

Then

$\forall n \in \mathbb{N}: \{j\} \subset B_1 \cap B_2 \cap \ldots \cap B_n$ and therefore

$$c_j = Pr(\{j\}) \leq Pr\left(\bigcap_{i=1}^{n} B_i\right) \underset{\text{Lemma}}{=} \left(\tfrac{1}{2}\right)^n \to 0,\ n \to \infty.$$

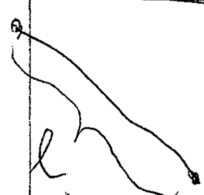
Hence $\forall j \in \mathbb{N}: c_j = 0$. This contradicts that $\sum_{j=1}^{\infty} c_j = 1$. $\lightning$ $\boxtimes$

Independence is a <u>tricky notion</u> (in applications, not in the formulization), see pp. 24–25 (2.1–2.2) in R. O'Donell's LN (link on M. Tancer's page).

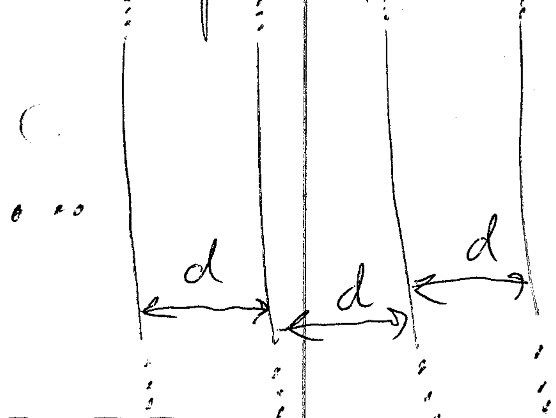
Thus, to model indep. coin tosses we have to turn to the <u>uncountable prob. space</u> $[0,1]$ where $\Omega = [0,1]$ (the unit real interval), $\Sigma \subset \mathcal{P}([0,1])$ are <u>Lebesgue measurable sets</u>, and $Pr: \Sigma \to [0,1]$ is the normalized Lebesgue measure (so that $Pr([0,1]) = 1$). Or a similar space. $\boxed{\text{UCPS}}$ I mention three results/problems/paradoxes on UCPS. (This is outside the syllabus.)

---

(1) <u>Buffon's needle problem</u>, or <u>Buffon's noodle problem</u>. Dropping randomly(?) a <u>needle</u> of length $\ell > 0$



In the plane $\mathbb{R}^2$ ~~with~~ split in stripes by parallel lines of width $d>0$. We assume that $\ell \le d$. // $\mathbb{E}X$, where $X :=$ the (5

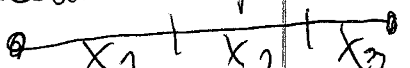


$p := \Pr(\text{needle crosses a line}) = ?$

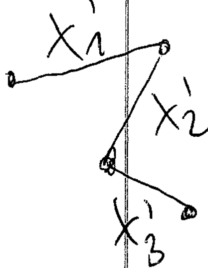
(the needle intersects a line)

# of intersections (of the needle with a line) $\in \{0,1\}$.

needle in 3 parts:



$\rightsquigarrow X = X_1 + X_2 + X_3$, by linearity of expectation: $\mathbb{E}X = \mathbb{E}X_1 + \mathbb{E}X_2 + \mathbb{E}X_3$



$\rightsquigarrow \mathbb{E}X_1' = \mathbb{E}X_1,\ \mathbb{E}X_2' = \mathbb{E}X_2,\ \mathbb{E}X_3' = \mathbb{E}X_3$

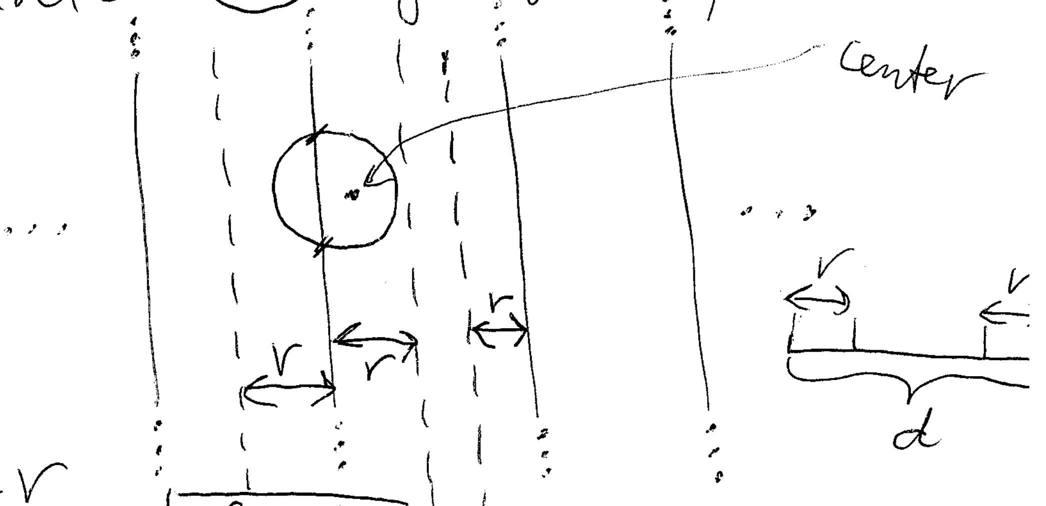
$\rightsquigarrow$ For $X' := X_1' + X_2' + X_3'$ one has that

$$\mathbb{E}X' = \mathbb{E}X$$

a needle $\rightsquigarrow$ a noodle (of the same length!) Best

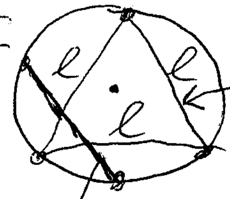
$\mathbb{E}X = \mathbb{E}X'$.

noodle is the circle X' of length ℓ, thus with radius $r = \frac{\ell}{2\pi}$.



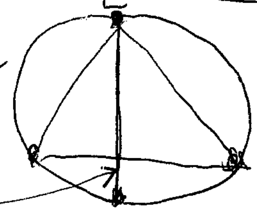
$$\rightsquigarrow \mathbb{E}X' = 2 \cdot \frac{2r}{d} = \boxed{\frac{\ell}{d} \cdot \frac{2}{\pi}} = \mathbb{E}X = p \qquad \boxtimes$$

(2) Bertrand paradox (1889)



A random (?) chord S is selected in the circle C. $P := P_r(|S|>\ell) = ?$ $|S| :=$ the length

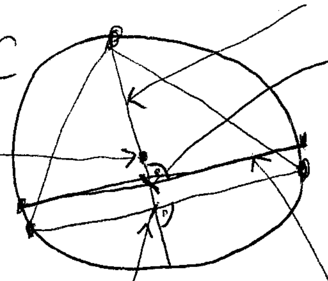
A)



The equil. △ is rotated so that one of its vertices coincides with the endpoint E of S $\Rightarrow$ $\boxed{P=\frac{1}{3}}$.

random endpoints method

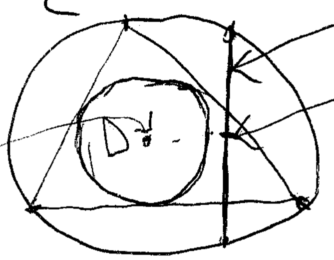
B)



The equil. △ has side $\perp$ to the diameter, the side bisects the radius $\Rightarrow$ $\boxed{P=\frac{1}{2}}$.

random diameter method

C)



the midpoint M of S

$|S|>\ell \iff M\in D$

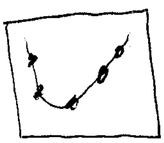
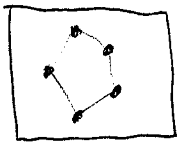
random midpoint method $\quad$ $\mathrm{area}(D)=\frac{1}{4}\,\mathrm{area}(C)$

$\Rightarrow$ $\boxed{P=\frac{1}{4}}$. $\quad \frac{1}{3}, \frac{1}{2}, \frac{1}{4}$?. ?, ?

---

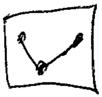
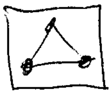
(3) The theorem of Pavel Valtr, and my problem related to it.

Let $C_n=\frac{1}{n}\binom{2n-2}{n-1}$ be the n-th Catalan number, $(C_n)_{n\geq 1}=(1,1,2,5,14,42,\dots)$

P. Valtr, 1995: $\underset{p_n}{\underset{\parallel}{\Pr}}$ ( | ) $= \frac{1}{C_n}$.

$(= 1/C_5 = \frac{1}{14})$

(Prob. that n random points in a square form a convex chain, if they already form a convex n-gon)

Clearly, $P_3 = \Pr$( | ) $= \frac{1}{2} = \frac{1}{C_3}$, due to the symmetry $\updownarrow$.

$\boxed{\text{PROBLEM}}$

(OPEN)

Prove in the same way the general case

<u>The lower bound on the Ramsey number $R(k)$, $k \in \mathbb{N}$, revisited.</u> Recall that $R(k) := \min N$ s.t. $\forall G = (V, E)$ with $|V| \geq N$: $G \supset$  or $G \supset$ .

k-clique $\qquad$ k-independent set

$\boxed{\text{Theorem (Erdős)}}$

$(k \geq 3) \Rightarrow R(k) \geq \frac{k}{2e} 2^{k/2}$.

<u>Proof.</u> $G = (V, E)$ with $|V| = N$, $k \in \mathbb{N}$. Then the #(of G s.t. $G \supset$ a k-clique) $\leq \binom{N}{k} 2^{\binom{N}{2} - \binom{k}{2}}$; same bound holds for k-indep. set. Thus if N is s.t. $2\binom{N}{k} 2^{\binom{N}{2} - \binom{k}{2}} < 2^{\binom{N}{2}} =$ the #(all $G = (V, E)$ with $V = \{1, 2, \ldots, N\}$), then $R(k) > N$.

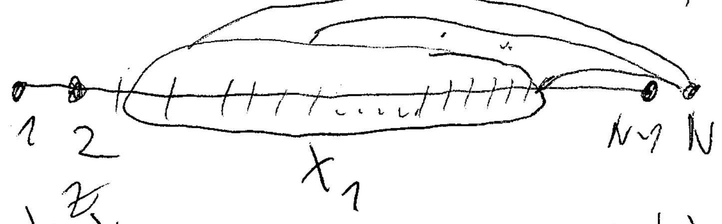
We need to solve the inequality. We use the estimate: $\binom{N}{k} \leq \left(\frac{eN}{k}\right)^k$. Then N is as we want if

$\left(\frac{eN}{k}\right)^k < \frac{1}{2} 2^{\binom{k}{2}} \iff N < \frac{k}{e} 2^{\frac{k-1}{2} - \frac{1}{k}} \geq \frac{k}{2e} 2^{k/2}$ for $k \geq 2$. $\square$

– purely enumerative proof; probability is only a way of counting things. Similarly, for $p \in [0,1]$ the random graph $G(p) = G(n,p)$ on n vertices is just a set of pairs

$\boxed{G(n,p) = \{(E, w(E)) \mid E \subset \mathcal{P}(\binom{[n]}{2})\}}$, where $\binom{[n]}{2} = \{A \mid A \subset \{1,2,\dots,n\}, |A| = 2\}$ and $w(E) = p^{|E|}(1-p)^{\binom{n}{2} - |E|}$. Then we can do some weighted counting on $G(n,p)$ ... $R(k)$ is defined (why not consider just $G \supset$?) $\boxed{\text{Theorem}}$ $R(k) \leq 4^k$, $k \in \mathbb{N}$.

$\boxed{\text{Proof.}}$ $\chi : \binom{[N]}{2} \to \{\text{red}, \text{blue}\}$, $N \geq 4^k = 2^{2k}$



$X_1 \subset [N-1]$, pairs $\{x, N\}$, $x \in X_1$, χ-monochromatic, and $|X_1| \geq 2^{2k-1}$. Same argument with $X_1 \setminus \{\max(X_1)\}$ and $\max(X_1)$ in place of $[N-1]$ and N, we get $X_2 \subset \underbrace{X_1 \setminus \{\max(X_1)\}}$ s.t. all $\{x, \max(X_1)\}$ are χ-monochr. and $|X_2| \geq 2^{2k-2}$, ... $\rightsquigarrow$ Sets $[N] \supset X_1 \supset X_2 \supset \dots \supset X_{2k}$. Let $Y := \{N > \max(X_1) > \max(X_2) > \dots > \max(X_{2k})\}$ – is χ-max-monochr.; for $A \in \binom{Y}{2}$, $\chi(A)$ depends only on $\max(A)$

$\rightsquigarrow \exists Z \subset Y : |Z| \geq k+1$ and $\chi | \binom{Z}{2} = \text{const}$. $\boxtimes$

We actually proved that $R(k) \leq 4^{k-1}$.

Big and hard open problem: Improve the bases of the exponential bounds ($\sqrt{2}$ and 4)

$$\boxed{a(k)(\sqrt{2})^k < R(k) < b(k)\, 4^k}, \quad k \in \mathbb{N},$$

where $a, b : \mathbb{N} \to [1/2, +\infty)$ are subexponential functions ($\forall c > 1 : a(t), b(t) < c^t$ for $t > t_0 = t_0(c)$).

Current records in bounds on $R(k)$:

$R(k) > (1+o(1)) \frac{\sqrt{2}}{e} k 2^{k/2}$ (J. Spencer, 1975, by LLL)

$R(k) < e^{-c \log^2 k} \underbrace{\binom{2k}{k}}_{\sim \frac{c'}{\sqrt{k}} 4^k}$ (A. Sah, 2020) — $c, c' > 0$

Probab. method too! using quasirandomness.

LLL: Lovász Local Lemma

(LLL also means Lenstra-Lenstra-Lovász algorithm) $A, A_1, \dots, A_n \in \Sigma$; A is mutually independent of $A_1, \dots, A_n$: $\forall I \subset [n] : \Pr(A \cap \bigcap_{i \in I} A_i) =$

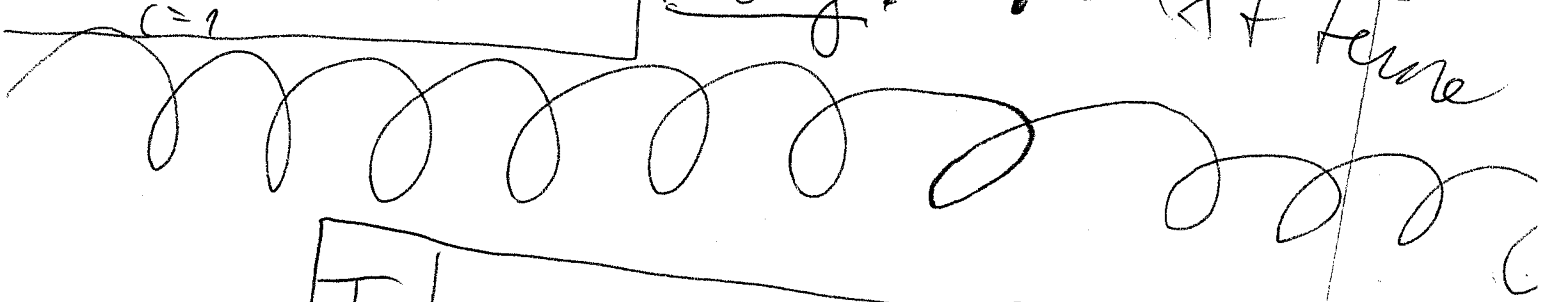
$\Pr(A)\Pr\left(\bigcap_{i\in I}\bar{A}_i\right)$. Depende[redacted]cy digraph of

$A_1,\dots,A_n$ is $D=([n],E)$ = [redacted]m.

General LLL $A_1,\dots,A_n\in$ [redacted], $D=([n],E)$ digraph of $A_1,\dots,A_n$, $x_i\in[0,$ [redacted] for $i\in[n]$ and $\Pr[A_i]\leq x_i\prod_{(i,j)\in E}(1-x_j)$. Then

$$\Pr\left(\bigcap_{i=1}^{n}\bar{A}_i\right)\geq\prod_{i=1}^{n}(1-x_i)>0.$$

Proof. Next time



Thank you!