6.842 Randomness & Computation : Lecture 1

Lecturer: Prof. Ronitt Rubinfeld

What is course about?

- How can randomness help?
  - algorithm design
    simpler, faster, new problems
  - show existence of combinatorial objects
    expander graphs, codes, good solutions
  - easy to verify proofs
    interactive proofs, PCPs
  - distributed algorithms
  - learning, testing algorithms

Do we require randomness?

- can we do without it?
- can we use less?
- in what settings do we need it?

Settings where randomness is inherent:

- uniform generation - approximate counting
- learning theory
- testing

Relation to complexity theory

- hardness vs. randomness
- hardcore sets

...

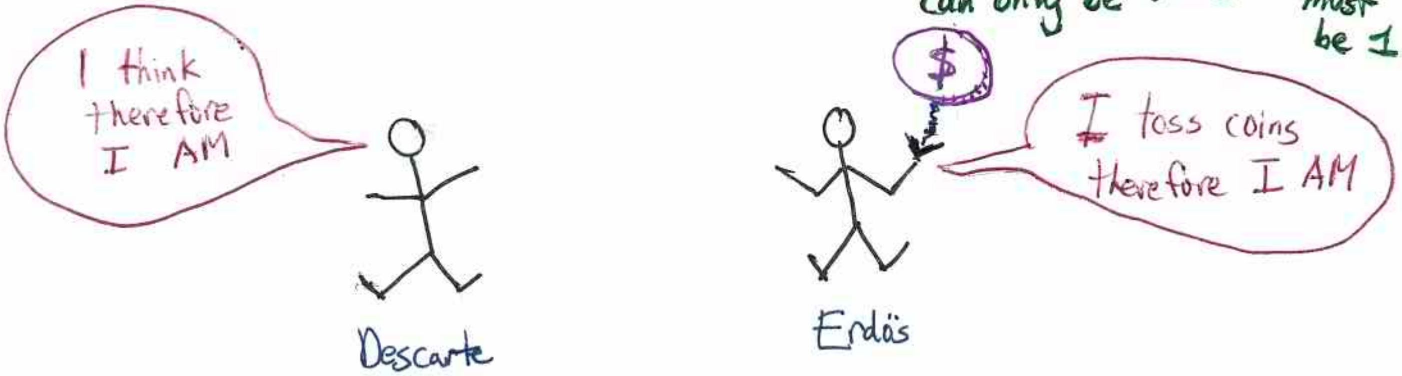
Tools:

Fourier representation
random walks / Markov chains
algebraic techniques
probabilistic proofs
Lovasz Local Lemma
graph expansion, extractors
Szemeredi Regularity Lemma

The probabilistic method

+ excuse for probability review

Show object exists by proving $\underbrace{\text{probability it exists}}_{\text{can only be 0 or 1}}$ is $\underbrace{>0}_{\text{so must be 1}}$



-or- "fancy counting" using language of probability

Example:

<u>Input</u> Given $\underbrace{S_1 \dots S_m}_{\text{each of size } \ell} \subseteq S$

<u>Output</u> Can we 2-color objects in S s.t. each S_i not monochromatic?

Important special case: $m < 2^{\ell-1}$ (not too many sets)

<u>Thm</u> if $m < 2^{\ell-1}$, $\exists$ proper 2-coloring

$3 < 2^{3-1}$ $\qquad$ $3 > 2^{2-1}$

Pf · randomly color elts of S red/blue (independently, prob $\frac{1}{2}$)

· $\forall i$, $\Pr[S_i \text{ monochromatic}] = \underbrace{\frac{1}{2^\ell}}_{\text{all red}} + \underbrace{\frac{1}{2^\ell}}_{\text{all blue}} = \frac{1}{2^{\ell-1}}$

· $\Pr[\exists i \text{ s.t. } S_i \text{ monochromatic}] \le \sum_i \Pr[S_i \text{ monochromatic}]$ union bnd

$\le m \cdot \frac{1}{2^{\ell-1}}$

$< \frac{2^{\ell-1}}{2^{\ell-1}} < 1$ by assumption on m

$\therefore \Pr[\text{all } S_i \text{ 2-colored}] > 0 \Rightarrow \exists$ setting of colors which gives 2-coloring ∎

i.e. there are many colorings, but if rule out monochromatic ones, still have some left over. We don't know how many.

Can we explicitly output a good 2-coloring?

bruteforce algorithm: try all possible colorings (exponential time)

Another example:

A is subset of positive integers (>0)

<u>Def</u> A is sum-free if $\nexists\ a_1, a_2, a_3 \in A$ s.t. $a_1 + a_2 = a_3$

<u>Thm</u> (Erdős '65)

$\forall\ B = \{b_1 .. b_n\}\ \exists$ sum-free $A \subseteq B$ s.t. $|A| > \frac{n}{3}$

note: <u>not true</u> if $|A|$ only greater than $\frac{12n}{29}$

An example:

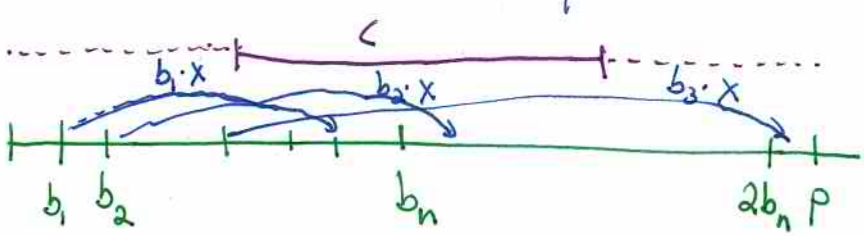
$B = \{1..n\}$

can take $A = \{\lceil \frac{n}{2} \rceil, \dots, n\}$

<u>Proof</u> wlog b_n is max

pick prime $p > 2b_n$ s.t. $p \equiv 2 \pmod 3$

i.e. $p = 3k+2$ for some int k



Let $C = \{k+1, \dots, 2k+1\}$ "middle third"

Note: (1) $C \subseteq \mathbb{Z}_p$

(2) C sum-free, even in $\mathbb{Z}_p$

$\underbrace{(4k+2) \bmod (3k+2) \equiv k}_{\notin C}$

(3) $\dfrac{|C|}{p-1} = \dfrac{k+1}{p-1} = \dfrac{k+1}{3k+1} > \dfrac{1}{3}$

Constructing A:

pick $x \in_R \overbrace{\{1..p-1\}}^{\mathbb{Z}_p^*}$ (x defines a random linear map)

let $A_x \leftarrow \{ b_i \text{ st. } (x \cdot b_i \bmod p) \in C \}$ elements of B in preimage of C under x

Claim 1 A_x is sum-free

Pf let $b_i, b_j, b_k \in A_x$ st. $b_i + b_j = b_k$

then $\underbrace{x \cdot b_i} + \underbrace{x b_j} \equiv \underbrace{x b_k} \pmod p$

all in C by construction

$\Rightarrow C$ not sumfree $\rightarrow\leftarrow$ ■

Claim 2 $\exists\ x$ s.t. $|A_x| > \frac{n}{3}$

Pf

Fact $\forall y \in \mathbb{Z}_p^*$ & $\forall i$, exactly one $x \in \mathbb{Z}_p^*$

satisfies $y \equiv x \cdot b_i \pmod{p}$

$\Rightarrow \forall y \in \mathbb{Z}_p^*,\ \forall i \quad \Pr_x[y \text{ mapped to } b_i] = \frac{1}{p-1}$

Proof of fact: essentially follows from b_i has an inverse

$x \equiv y \cdot b_i^{-1} \pmod{p}$

since $b_i \in \{1..p-1\}$, $b_i \not\equiv 0 \bmod p$ & has (non zero) inverse

so $x \not\equiv 0$ & exists

if x_1, x_2 satisfy $x_1 b_i \equiv x_2 b_i \pmod{p}$

then $x_1 \equiv x_2 \pmod{p}$ ∎

$\forall i$, the Fact $\Rightarrow$ $|C|$ choices of x s.t. $x \cdot b_i \overset{\bmod p}{\in} C$

(one for each elt of C)

define $\sigma_i^{(x)} \leftarrow \begin{cases} 1 & \text{if } x b_i \overset{\bmod p}{\in} C \\ 0 & \text{o.w.} \end{cases}$

$$E_x[\sigma_i^{(x)}] = \Pr_x[\sigma_i^{(x)} = 1] = \frac{|C|}{p-1} > \frac{1}{3}$$

Average value of $|A_x|$ $\rightarrow E_x[|A_x|] = E_x[\sum_i \sigma_i^{(x)}] = \sum_i E_x[\sigma_i^{(x)}] > \frac{n}{3}$

$\therefore$ at least one x s.t. $|A_x| > n/3$ ∎

The Lovász Local Lemma

Another way to argue that "nothing bad happens"

If $A_1 \cdots A_n$ are bad events

how do we know if there is positive probability that none occur?

usual way: Union bnd

$$\Pr[\cup A_i] \le \sum \Pr[A_i]$$

no assumptions on A_i's w.r.t. independence

if each A_i occurs with prob p, then need $p < \frac{1}{n}$ to get anything interesting (i.e. sum < 1)

if A_i's independent & "nontrivial":

$$\Pr[\cup A_i] \le 1 - \Pr[\cap \overline{A_i}]$$
$$= 1 - \prod \underbrace{\Pr(\overline{A_i})}_{>0}$$
$$< 1$$

What if A_i's have "some" independence?

def A "independent" of $B_1 \cdots B_k$ if $\forall J \subseteq [k]$, $J \ne \phi$

$$\Pr[A \cap \bigcap_{j \in J} B_j] = \Pr[A] \cdot \Pr[\bigcap_{j \in J} B_j]$$