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

...

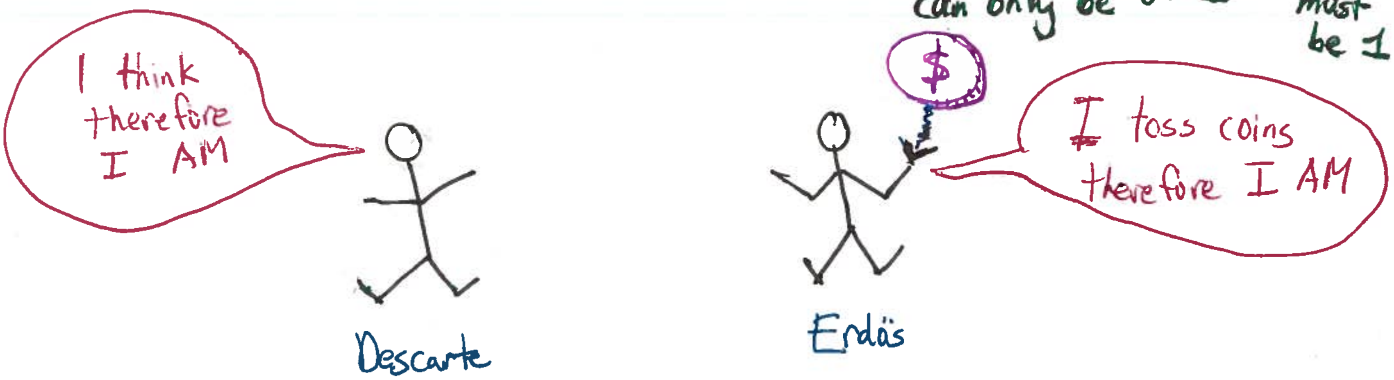
Tools:

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: X is a set of elements.

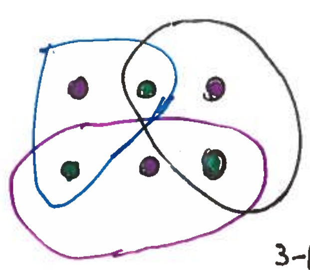
Input Given $\underbrace{S_1 \dots S_m}_{\text{each of size } \ell} \subseteq X$

Output Can we 2-color objects in X s.t. each S_i not monochromatic?

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

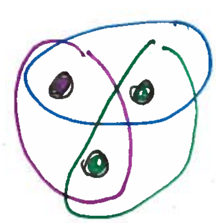
Thm if $m < 2^{\ell-1}$, $\exists$ proper 2-coloring

$m=3$
$\ell=3$



$3 < 2^{3-1}$

vs



$m=3$
$\ell=2$

$3 > 2^{2-1}$

<u>Pf</u> • randomly color elts of X red/blue (independently, prob $\frac{1}{2}$)

want to "delete" all colorings that make any set monochromatic & show that there is still a leftover

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

• $\Pr[\exists i \text{ s.t. } S_i \text{ monochromatic}] \le \sum_i \Pr[S_i \text{ monochromatic}]$ 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 $\nexists\ a_1, a_2, a_3 \in A$ st. $a_1 + a_2 = a_3$

<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 $|A|$ greater than $\frac{12n}{29}$

An example!

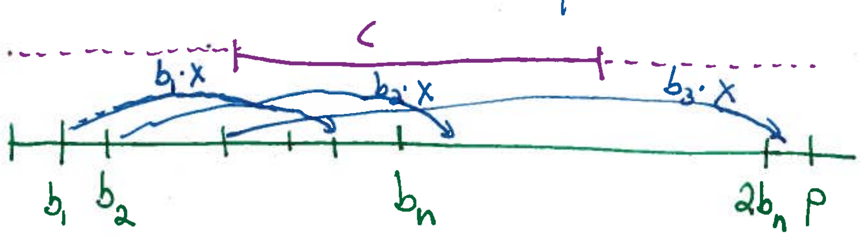
$B = \{1..n\}$

Can take $A = \{\lceil \frac{n}{2} \rceil, \ldots, n\}$

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

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

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



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

$\mathbb{Z}_p = \{0, \dots p-1\}$

$\mathbb{Z}_p^* = \{1 \dots p-1\}$ group, has multiplicative inverses (mod p) $\Leftarrow$ need p to be a prime

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

(2) C sum-free, even in $\mathbb{Z}_p$ $\leftarrow$ why? any 2 elts sum to at least $2k+2$ & at most $(4k+2)$, which is $\equiv k \mod (3k+2)$ & thus $\notin C$

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

Constructing A:

pick $x \in_R \underbrace{\{1 \dots p-1\}}^{\mathbb{Z}_p^*}$: then x defines a random linear map $f_x(a) = x \cdot a \mod p$

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

i.e. x maps these guys to "middle $\frac{1}{3}$"

Claim 1 A_x is sum-free

Pf suppose not, then let $b_i, b_j, b_k \in A_x$ st. $b_i + b_j = b_k$

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

all in C by construction

$\Rightarrow C$ not sum free (in $\mathbb{Z}_p$) $\rightarrow\leftarrow$ ∎

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 $y \equiv x \cdot b_i \pmod p$

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

this is why p is chosen to be prime

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 $x_1 \equiv x_2 \pmod p$ $\Rightarrow$ x is unique ∎

$\forall i$, 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 $\sigma_i^{(x)} \leftarrow \begin{cases} 1 & \text{if } x b_i \overset{\bmod p}{\in} C \\ 0 & \text{o.w.} \end{cases}$ ← b_i maps to C

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

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

$\underbrace{\sum_i \sigma_i^{(x)}}_{\#\text{ of } b_i\text{'s that map to } C}$

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