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 $\underbrace{\text{probability it exists is} > 0}$ $\underbrace{\text{so must be 1}}$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad$ can only be 0 or 1

I think therefore I AM

Descarte

$ $

I toss coins therefore I AM

Erdös

—or— "fancy counting" using language of probability

Example:

<u>Input</u> Given $S_1 \ldots S_m \leq S$
$\qquad\qquad\qquad$ each of size l

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

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

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

$$3 < 2^{3-1} \qquad\qquad vs \qquad\qquad 3 > 2^{2-1}$$
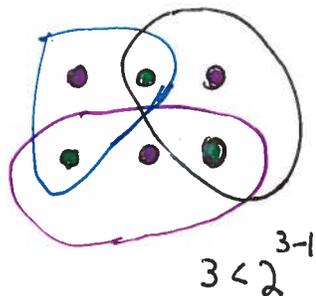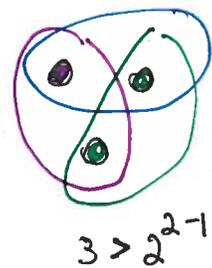
<u>Pf</u>   • randomly color elts of S red/blue (independently, prob ½)

• $\forall i$, $\Pr[S_i \text{ monochromatic}] = \dfrac{1}{2^\ell} + \dfrac{1}{2^\ell} = \dfrac{1}{2^{\ell-1}}$

$\underbrace{}_{\substack{\text{all} \\ \text{red}}}$ $\underbrace{}_{\substack{\text{all} \\ \text{blue}}}$

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

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

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

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

ie. 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. $|A| > \dfrac{n}{3}$

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

An example!

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

Can take $A = \{\lceil \tfrac{n}{2} \rceil, ..., n\}$

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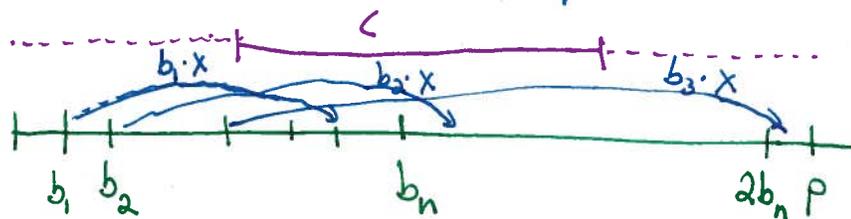
Let $C = \{k+1, ..., 2k+1\}$ "middle third"

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

too bad we don't know that $C \leq B$!

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

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

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

But there is a s.t. subset of B that is!

Constructing A:

pick $X \in_R \{1..p-1\}$ (x defines a random linear map)

$\overbrace{}^{\mathbb{Z}_p^*}$

let $A_x \leftarrow \{ b_i \quad \text{st.} \quad (x b_i \bmod p) \in C \}$

elements of B in preimage of **C** under x

<u>Claim 1</u> A_x is sum-free

<u>Pf</u> let $b_i, b_j, b_k \in A_x$ st. $b_i + b_j = b_k$

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

all in C by construction
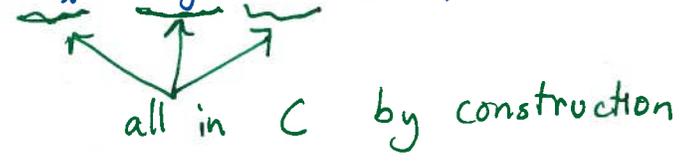
$\Rightarrow C$ not sumfree $\quad \to\leftarrow$

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

<u>Pf</u>

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

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

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

<u>Proof of fact</u>: essentially follows from b_i has an inverse

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

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

so $x \not\equiv 0$ & exists

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

$\qquad\qquad$ then $x_1 \equiv x_2 \pmod p$ ▤

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

$\qquad$ (one for each elt of C)

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

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

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

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