6.842 Randomness & Computation

Ronitt Rubinfeld

Scribed by Edward Z. Yang <ezyang@mit.edu>

esp distributed systems

Randomness is a resource: lets us do NEW things, and old things FASTER & SIMPLER

prove existence of combinatorial objects (non-constructively),

expander graphs

inherent in the model

in proofs it's a language for counting, also interactive proofs

learning and testing algorithms

↳ (to predict)

Do We Require Randomness?

more, less? when?

Learning vs Randomness — complexity theory

Hardness v. Randomness

Average case hardness of probs

$\boxed{\text{Algorithms} \\ \text{Learning} \\ \text{Complexity}}$ ⇒ a lot of materials!

Tools: Fourier representation

Algebraic Techniques

Lovas Local Lemma

TODAY'S LECTURE:

- The Probabilistic Method
- The Lovász Local Lemma

The Probabilistic Method

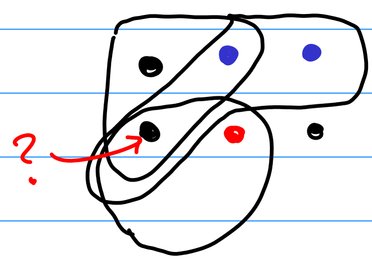
Descartes: "I think, therefore I am."
Erdös: "I toss coins, therefore I am." (paraphrased)

Show $\exists$, by showing it probably exists: if the probability it exists is positive (non-zero), it must exist (existence is a binary proposition) "Fancy counting"

Example 1

<u>Input</u>: given $\underbrace{S_1, \ldots, S_m}_{\text{each of size } \ell} \subseteq S$ (ground set)

<u>Output</u>: can we 2-color objects in S s.t. each S_i not monochromatic (not all the same color)



Coloring is nontrivial

<u>Def</u>: Hypergraph is (V, E), where each $e \in E$ is subset of V (an ordinary graph is when all subsets have two elements.)
(So this is hypergraph coloring.)

early proofs were very short! (But then they got longer)

<u>Goal</u>: Show there exists a coloring, when $m < 2^{\ell - 1}$

Proof: Randomly color each element of S red or blue with probability $1/2$ (independently).

$$\Pr[S_i \text{ monochromatic}] = \frac{1}{2^{\ell-1}}$$

abuse of notation, we haven't defined the event S_i monochromatic

$$\Pr[\exists i \text{ such that } S_i \text{ monochromatic}]$$
$$= \Pr\left[\bigcup_i S_i \text{ monochromatic}\right]$$
$$\leq \sum_i \Pr[S_i \text{ monochromatic}] \quad \text{(union bound)}$$
$$= m \cdot \frac{1}{2^{\ell-1}} \underbrace{< 1}_{\text{by assumption}}$$

$$\therefore \Pr[\text{good coloring}] > 0 \quad \blacksquare$$

Intuitively: There exist many colorings, but even when we rule out monochromatic ones, there are left-over colorings.

Note: We don't know what coloring works, or even how many colorings exist. Algorithm to find this takes exponential time.

Example 2

A is a subset of positive integers (>0)

Def A is "sum-free" if $\neg \exists\, a_1, a_2, a_3 \in A$ s.t. $a_1 + a_2 = a_3$

Thm [Erdös 65] $\forall B = \{b_1, \dots, b_n\}$, $\exists$ sum-free $A \subseteq B$ s.t. $|A| \geq \frac{n}{3}$ (but this is not true for $|A| \geq \frac{12}{29} n$)

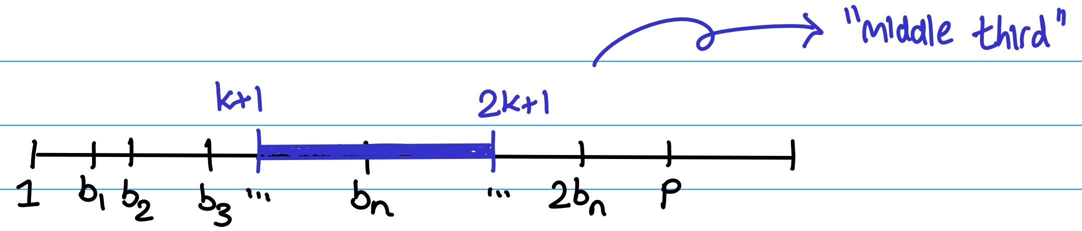
e.g. $B = \{1, \dots, n\}$

$A = \{\frac{n}{2}+1, \dots, n\}$ (as all pairs sum to value greater than n)

Proof wlog. b_n is max elt of B

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

i.e. $p = 3k+2$ for some $k \in \mathbb{Z}$



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

Note: $C \subseteq \mathbb{Z}_p^*$ (numbers mod p, relatively prime to p)

C is sum-free (the sum is outside the range)

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

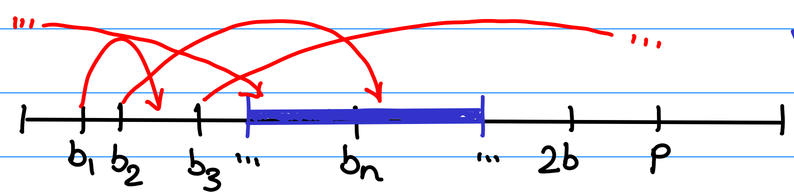
Constructing A:

$\overbrace{\{1 \dots p-1\}}^{\mathbb{Z}_p^*}$ (a nice set w/ lots of properties)

Pick $x \in_R \{1 \dots p-1\}$

→ pick x from set uniformly at random

Let $A_x = \{b_i \text{ s.t. } (xb_i \bmod p) \in C\}$



"land in random areas"

Claim: A_x is sum-free.

Pf: Let $b_i, b_j, b_k \in A_x$ s.t. $b_i + b_j = b_k$

But then $\underbrace{xb_i}_{} + \underbrace{xb_j}_{} = \underbrace{xb_k}_{} \pmod p$

by construction these $\in C$

Contradiction with C being sum-free. ∎

Warning: Why don't we just take the b_i which are in C?
Look closely at what the direction is.

Also note: C is sum-free mod p (since it's a third of the space)

Next goal: show A_x is big. (Will show exists one x w/ property)

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

<u>Fact</u> $\forall y \in \mathbb{Z}_p^*$ and $\forall i$, there is exactly one $x \in \mathbb{Z}_p^*$ that satisfies $y \equiv x \cdot b_i \pmod p$

(by existence of inverses, linear equation has unique solution)

Proof of fact in last year's notes.

Idea: show how many choices of x make a given b_i land in center area.

$\forall i$, Fact $\Rightarrow |C|$ choices of x such that $x \cdot b_i \in C$

(i.e. one for each element of C)

Define $\sigma_i(x) = \begin{cases} 1 & \text{if } x \cdot b_i \in C \\ 0 & \text{otherwise} \end{cases}$ (Indicator value)

$$\mathbb{E}_x[|A_x|] = \mathbb{E}_x\left[\sum_i \sigma_i(x)\right]$$

$$= \sum_i \underbrace{\mathbb{E}_x[\sigma_i(x)]}_{\text{What is this?}}$$ (linearity of expectation)

Intuitively, this is the average. So there must be some value that hits the average

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

(property of indicator variable)

$> \frac{n}{3}$ So since at least one x gives at least expectation; theorem follows. ∎

Lovász Local Lemma

how to argue nothing "bad" happens. Useful for union bound, since we need the probabilities to be low over many summed terms. (Situation is not as bad when events are independent.)

$A_1, \ldots, A_n$ bad events

Naive way: (best we can do in general)

$$\Pr\left[\bigcup_i A_i\right] \leq \sum_i \Pr[A_i] \quad \text{(union bound)}$$

In general, need that $\Pr[A_i] < \frac{1}{n}$ for each i

to show $\Pr[\bigcup A_i] < 1$ i.e. $\Pr[\bigcap \bar{A}_i] > 0$

(that is, it is possible no bad events happen)

very strong condition

If A_i's are independent and "non-trivial" $\rightarrow$ $\Pr[\bar{A}_i] > 0$ (the bad event doesn't always happen)

$$\Pr[\cap \bar{A}_i] = \prod \Pr[\bar{A}_i] > 0$$

In the naive case, we have stringent requirement on $\Pr[A_i]$, but no independence condition. In the second case, we have stringent indep. req. but relaxed $\Pr[A_i]$. We want something in the middle.

$[n] = \{1 \ldots n\}$

Def A "independent" of $B_1 \ldots B_K$ if $\forall J \subseteq [K]$ s.t. $J \neq \phi$

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

(Note: this is not pair-wise independence.)

Def Given events $A_1 \ldots A_n$, $D = (V, E)$ with $V = [n]$ is a "dependency digraph of $A_1 \ldots A_n$" if each A_i is independent of the set of all A_j that don't neighbor it in D.

Lovász Local Lemma (symmetric version)

Given $A_1 \dots A_n$ s.t. $\Pr[A_i] \leq p \quad \forall i$
and dependency digraph D of degree $\leq d$,
If $e \cdot p \cdot (d+1) \leq 1$

$$\text{then } \Pr\left[\bigcap_{i=1}^{n} \overline{A_i}\right] > 0$$

note the requirement doesn't rely on n; only the degree d.

Next Time: New version of hypergraph 2-coloring w/ bounding on intersection, rather than bound on number of subsets.