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
Lovász Local Lemma
graph expansion, extractors
Szemerédi Regularity lemma
The probabilistic method

+ excuse for probability review

Show object exists by proving probability of existence is > 0

I toss coins.

I think therefore I AM

Descartes

Erdős

---

or- "fancy counting" using language of probability

Example: \( X \) is a set of elements.

Input

Given \( S_1, \ldots, S_m \subseteq X \)

each of size \( l \)

Output

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

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

Thm: if \( m > 2^{l-1} \) then no proper 2-coloring.

\[
\begin{align*}
m &= 3 \\
l &= 3
\end{align*}
\]

\[ 3 < 2^{l-1} \]

\[
\begin{align*}
m &= 3 \\
l &= 2
\end{align*}
\]

\[ 3 > 2^{l-1} \]
\[ \text{Pr} \cdot \text{randomly color elts. of } X \text{ red/blue (independently, prob } \frac{1}{2}) \]

\begin{align*}
\forall i, \quad & \text{Pr} \left[ S_i \text{ monochromatic} \right] = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2} \quad \forall \text{ red, blue} \\
\text{\Pr} \left[ \exists i \text{ st. } S_i \text{ monochromatic} \right] & \leq \sum_i \text{Pr} \left[ S_i \text{ monochromatic} \right] \\
& \leq m \cdot \frac{1}{2^{2^{k-1}}} \\
& \leq \frac{2^{k-1}}{2^{k-1}} < 1 \quad \text{by assumption on } m
\end{align*}

\[ \therefore \text{Pr} \left[ \text{all } S_i \text{ 2-colored} \right] > 0 \implies \exists \text{ setting of colors which give 2-coloring} \]

\[ \text{i.e. there are many colorings, but if rule out monochromatic ones, still have some leftover. We don't know how many.} \]

\[ \text{Can we explicitly output a good 2-coloring?} \]

\[ \text{Brute force algorithm: try all possible colorings (exponential time)} \]
Another example:

A is subset of positive integers ($\geq 0$)

**Def** A is sum-free if $\not\exists a_1, a_2, a_3 \in A$ s.t. $a_1a_2 = a_3$

**Thm** (Erdős '65)

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

Note: not true if $|A|$ greater than $\frac{10n}{9}$

An example:

$B = \{1, \ldots, n^3\}$

Can take $A = \{\lceil \frac{n^3}{2} \rceil, \ldots, n^3\}$

**Proof**

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 $C = \{k+1, \ldots, 2k+3\}$ "middle third"
\[ Z_p = \{ 0, \ldots, p-1 \} \]
\[ Z_p^* = \{ 1, \ldots, p-1 \} \]

Note: (1) \( C \subseteq Z_p \)

(2) \( C \) is sum-free, even in \( Z_p \)

(3) \( \frac{|C|}{p-1} = \frac{k+1}{3k+1} = \frac{k+1}{3k+2} > \frac{1}{3} \)

Constructing \( A \):

- Pick \( x \in \{ 1, \ldots, p-1 \} \); then define a random linear map \( f_x(a) = xa \mod p \)
- Let \( A_x \subseteq \{ b_i \} \) s.t. \( (xb_i \mod p) \in C \)

Claim 1: \( A_x \) is sum-free

Proof: Suppose not, then let \( b_i, b_j, b_k \in A_x \) s.t. \( b_i + b_j = b_k \)

Then \( x \cdot b_i + x \cdot b_j \equiv x \cdot b_k \mod p \)

all in \( C \) by construction

\( \Rightarrow \) \( C \) not sum-free (in \( Z_p \))
Claim 2. \( \exists x \text{ s.t. } |A_x| > \frac{n}{3} \)

Proof:

Fact: \( \forall y \in \mathbb{Z}_p^* \land \forall i, \text{ exactly one } x \in \mathbb{Z}_p^* \text{ satisfies } y \equiv x \cdot b_i \pmod{p} \)

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

Proof of fact: essentially follows from \( b_i \) has an inverse

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

since \( b_i \in \{1, \ldots, p-1\}, \) \( b_i \not\equiv 0 \pmod{p} \)

so \( x \neq 0 \) exists

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

then \( x_1 \equiv x_2 \pmod{p} \)

\( \Rightarrow x \text{ is unique} \)

\( \forall i, \text{ the Fact } \Rightarrow |C| \text{ choices of } x \text{ s.t. } x \cdot b_i \equiv c \pmod{p} \)

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

define \( \delta_i(x) \leftarrow \begin{cases} 1 & \text{if } x \cdot b_i \equiv c \pmod{p} \\ 0 & \text{otherwise} \end{cases} \)

\( E_x[\delta_i(x)] = P_x[y \equiv b_i \pmod{p}] = \frac{|C|}{p-1} > \frac{1}{3} \)

Average value of \( |A_x| \)

\( \Rightarrow E_x[|A_x|] = E_x[\sum \delta_i(x)] = \sum E_x[\delta_i(x)] \geq \frac{n}{3} \)

\( \Rightarrow \text{ at least one } x \text{ s.t. } |A_x| > \frac{n}{3} \)