Today

Reductions & NP-completeness
- 3 colorability

Randomized Complexity
- RP, coRP, ZPP
  RP ∩ coRP = ZPP

How to Prove NP-completeness

To prove X is NP-complete, must show two things

1) X is in NP
   - give a poly-time algorithm to check membership

2) X is NP-hard
   - start with known NP-hard problem, e.g. 3SAT
   - give a poly-time computable function f s.t.
     \[ \text{if } \text{y} \in \text{3SAT} \Rightarrow f(y) \in X \]
     \[ \text{if } \text{y} \notin \text{3SAT} \Rightarrow f(y) \notin X \]

Example: 3-colorability (3-COL)

Given a graph \( G = (V, E) \), can you assign a color from \( \{R, G, B\} \) to each vertex, s.t. \( \forall (u, v) \in E, \text{color}(u) \neq \text{color}(v) \)?

Claim: 3-COL is NP-complete

Proof:

1) 3-COL is in NP
   - given \( G \) and a coloring, just iterate through each edge \( (u, v) \in E \)
     and check that \( \text{color}(u) \neq \text{color}(v) \)

2) 3-COL is NP-hard
   - we give a reduction from 3-SAT
     Need poly-time way to transform a 3-CNF formula to a graph, s.t. formula is satisfiable iff graph is colorable
     Idea: assignment corresponds to coloring
     Need analogues of variables & clauses (called "gadgets")

Example formula: \( (x_1 \lor \overline{x}_2 \lor x_3) \land (x_1 \lor x_4 \lor \overline{x}_5) \)
Think of colors as assignments. But since 3-colors, let them be $E, F, \text{grey}$.

To get started, for each variable $x_i$, create

To force nodes to get $T/F$ colors, add extra nodes.

To get the "or" of two variables, use

Note this implies $X$ and $Y$ cannot both be $F$

For each clause, use (two OR gadgets)

Example: $(x_1 \lor \overline{x}_2 \lor x_3)$

Repeat for every clause

Easy to verify that a 3-coloring of $G \implies$ satisfying assignment of $f$, and satisfying assignment $\implies$ 3-coloring of $G$
Randomized Complexity

Review: RP = Prob poly-time w/1-sided error

A problem \( \Pi \) is in RP if there is a poly-time alg \( A \) using random bits \( r \) s.t.

\[ \forall x \in \Pi \implies P_r[A(x, r) \text{ accepts}] > \frac{1}{2} \]

\[ \forall x \not\in \Pi \implies P_r[A(x, r) \text{ accepts}] = 0 \quad (\text{"too critical"}) \]

\( \text{CoRP} = \text{complement of RP} \)

\[ \forall x \in \Pi \implies P_r[A(x, r) \text{ accepts}] = 1 \]

\[ \forall x \not\in \Pi \implies P_r[A(x, r) \text{ accepts}] < \frac{1}{3} \quad (\text{"too lenient"}) \]

Containment Picture

RP and \( \text{CoRP} \) called "monte-carlo" algorithms: always poly-time, sometimes make mistakes

ZPP = class of "las-vegas" algorithms: \( E[\text{running-time}] = \text{poly}(n) \), never makes mistakes

Thm: \( ZPP = \text{RP} \cap \text{coRP} \)

Proof: First we show \( \text{RP} \cap \text{coRP} \subseteq \text{ZPP} \)

- Let \( \Pi \) be a problem in \( \text{RP} \cap \text{coRP} \)
- Let \( A_1 \) be the RP algorithm for \( \Pi \)
- \( A_2 \) is \( \text{coRP} \) for \( \Pi \)

Then ZPP algorithm is:

1) Run \( A_1 \) and then \( A_2 \)

2) If they both accept, "then accept"

"reject", "reject"

If they disagree, repeat step 1
- Analysis

How many times will step 1 repeat, in expectation?

It only repeats if one of $A_1$ or $A_2$ makes an error.

$$\Pr[A_1 \text{ or } A_2 \text{ makes an error}] = \frac{1}{3} + \frac{1}{3} = \frac{2}{3}$$

$$E[\text{# of repeats}] = \frac{1}{\Pr[\text{success}]} = \frac{1}{1 - \Pr[\text{error}]} = \frac{1}{\frac{1}{3}} = 3$$

$$E[\text{running time}] = 3 \cdot (\text{running-time}(A_1) + \text{running-time}(A_2)) = \text{poly}(n)$$

Next we show $\text{ZPP} \subseteq \text{RP} \cap \text{coRP}$

- We show $\text{ZPP} \subseteq \text{RP}$ (argument for $\text{coRP}$ the same)

Let $T$ be a problem in $\text{ZPP}$

Let $A$ be a $\text{ZPP}$ algorithm for $T$

Then $\text{RP}$ algorithm is:

1) Run $A$ for $3 \cdot E[\text{running-time}(A)]$ steps

2) If $A$ hasn’t terminated already, reject

Analysis: Clearly alg rejects inputs not in $T$

What’s the probability it accidentally rejects inputs in $T$?

$$\Pr[\text{mistake}] \leq \Pr[A \text{ terminates too early}]$$

Let $X$ be a random variable to denote running time of $A$

$$\Pr[A \text{ terminates too early}] = \Pr[X > 3E[X]]$$

$$\leq \frac{1}{3} \text{ by Markov’s inequality}$$

(Markov says $\Pr[X > t] \leq \frac{E[X]}{t}$ for non-negative random variable.)