Undergraduate Complexity Theory
Lecture 21: Randomized Complexity: RP, coRP, and ZPP

Marcythm

July 23, 2022

1 Lecture Notes

Computational resources: randomness

Can you save time/space if you allow randomness?

Why randomness? Even for decision problems, with nothing to do with randomness. Sometimes the fastest algo we know is randomized.

Why not randomness? error: can generally reduce error to $< 2^{-n}$ prob at expense of factor $O(n)$ in time. where to get random bits? in practice PRNG.

Randomize algo = A-OK, randomized poly-time = "feasible algo". some faster randomized algos:

1. Primality Testing
2. Median Finding
3. Verifying Matrix Multiplication
4. Minimum Spanning Tree
5. $\mathsf{3SAT}$
6. Undirected $\mathsf{ST\text{-}PATH}$
7. Bipartitle Perfect Matching
8. Polynomial Identity Testing

Definition 1.1. A *probabilistic (randomized) TM* is a normal TM with two transition functions δ_0, δ_1. In its computation, at each step either δ_0 or δ_1 is used with probability half each, independently. For each input x, we care about $\mathbf{Pr}[M(x) \text{ accepts}]$.

Remark 1.2. We assume $M(x)$ always halts for all x.

Definition 1.3. M decides language L with one-sided error ϵ if

$$\forall x \in L : \mathbf{Pr}[M(x) \text{ acc}] \geq 1 - \epsilon$$
$$\forall x \notin L : \mathbf{Pr}[M(x) \text{ acc}] = 0$$

i.e. no false positive.

Randomness from algo itself (not input)

Definition 1.4.

$$\mathsf{RTIME}(f(n)) = \{L : \exists \text{ prob } M \text{ with running time } O(f(n)) \text{ which accepts } L \text{ with one-sided error } 1/3\}$$

Definition 1.5. *Running time* of a RTM M is the maximum number of steps $M(x)$ may take over all possible random choices, similar to the definition on NTM.

Lemma 1.6 (Success amplification / error reduction)**.** *Suppose M decides L with one-sided error ϵ. Let $k \in \mathbb{N}$, define TM $M^{(k)}$: on input x, run $M(x)$ k times. If ever accepts, overall accept. If all runs reject, at end rejects. Then $M^{(k)}$ decides L with one-sided error $1 - \epsilon^k$.*

Definition 1.7. $\mathsf{RP} = \bigcup_{k \in \mathbb{N}} \mathsf{RTIME}(n^k)$.

Proposition 1.8. $\mathsf{P} \subseteq \mathsf{RP} \subseteq \mathsf{NP}$.

Recall: $\mathsf{COMPOSITES} \in \mathsf{NP}$.

Theorem 1.9 ('74)**.** $\mathsf{COMPOSITES} \in \mathsf{RP}$.

Proof. Let $x \in \mathbb{N}$, write $x = 2^s d$ where d is odd. $b \in \mathbb{N}$ is called a "compositeness witness" for x if:

$$b^d \not\equiv 1 \pmod{x}, b^d, b^{2d}, b^{4d}, \dots, b^{2^{s-1}d} \not\equiv -1 \pmod{x}$$

If x is prime, then no b is a witness for x. If x is composite, $\geq 3/4$ of all $b's$ in $[0, x)$ are witnesses for x. Check whether $0 \leq b < x$ is a witness is in time $\mathrm{poly}(|x|)$.
Miller-Rabin'25: Pick a random $0 \leq b < x$, check if it's a witness. $x \in \mathsf{COMPS} \implies \mathbf{Pr}[\mathrm{acc}] = 3/4 > 2/3$ □

Corollary 1.10. $\mathsf{PRIMES} \in \mathsf{coRP}$.

Theorem 1.11. $\mathsf{P} \in \mathsf{coRP} \subseteq \mathsf{coNP}$.

Theorem 1.12 (Adlemm-Huang '87)**.** $\mathsf{PRIMES} \in \mathsf{RP}$. *witnesses for primality easily checkable & findable with randomness.*

Definition 1.13. $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$. (Zero-sided error)

2 Reading

2.1 sipser 10.2 (Probabilistic Algorithms)

definition of BPP, Probabilistic TM, amplification lemma