Advanced Algorithm

Jialin Zhang
zhangjialin@ict.ac.cn

Institute of Computing Technology, Chinese Academy of Sciences

April 18, 2019

BPP vs Probabilistic Method

- A language $L \in BPP$, the randomized algorithm A
- Raise the probability of success by repeating algorithm A t times
  - The error probability: exponential small when t increases, e^{-ct}
- If we apply probabilistic method here...
  - Consider a BPP algorithm $\tilde{A}$ with error probability e^{-n^2}, suppose the number of different random strings is m

Theorem

$BPP \subseteq P/poly$

Lecture 6.1: Probabilistic Amplification

Probabilistic Amplification

- Ref: Randomized Algorithm - Chapter 3.4, Page 51
- Randomness is a resource.
- For a language $L \in RP$, consider the randomized algorithm A (uses k bits random variable, error probability $1/2$).
  - If we repeat the algorithm A t times
    - The error probability: 2^{-t}
    - number of one-bit random variable: kt
  - If we have only $2k$ bits random variable
    - error probability: $1/4$
    - Can we do better? $1/t$!
  - If we have more random bits?
    - Ref: Randomized Algorithm - Chapter 5.3, 6.8, using expander and random walk

Lecture 6.2: Algebraic Technique

Algebraic Technique

- Ref: Randomized Algorithm - Chapter 7.1, 7.2 , page 161
- Matrix multiplication - Freivald's Technique
- Communication complexity for EQ function

- Given polynomials f, g, h, decide wheter $f \cdot g = h$ or not?

Theorem (Schwartz-Zippel Theorem)

Let $Q(x_1, x_2, \cdots, x_n) \in \mathbb{F}[x_1, x_2, \cdots, x_n]$ be a multivariate polynomial of total degree d. Fix any finite set $S \subseteq \mathbb{F}$, and let $r_1, \cdots, r_n$ be chosen independently and uniformly at random from S. Then, $Pr[Q(r_1, r_2, \cdots, r_n) = 0 \mid Q(x_1, x_2, \cdots, x_n) \not\equiv 0] \leq \frac{d}{|S|}$.

perfect matching

- Ref: Randomized Algorithm - Chapter 7.3
- Given a bipartite graph $G(U, V, E)$, decide whether it contains a perfect matching.
  - Polynomial time algorithm: maximal flow algorithm, Hungarian algorithm, etc.
- Relation between perfect matching and algebra
  - randomized algorithm: running time = running time of matrix multiplication
- parallel computing ($O(\log^2 n)$ in expectation), ref. Randomized Algorithm - Chapter 12.4

Interactive Proof system (IP)

- Ref: Randomized Algorithm - Chapter 7.7, Page 172
- NP: exists short proof
- IP: exists short active proof (informal)
- Graph Isomorphism problem $\in NP$
- Graph non-Isomorphism problem: no known short proof now.
- GNI $\in IP$

Interactive Proof system (IP)

- Verifier: Arthur, polynomial-time
- Prover: Merlin, unlimited computational power, know Arthur's strategy
- Limitation of Merlin: cannot access to the random bits used by Arthur
- IP: all languages L that have an interactive proof system (P,V) with a randomized polynomial-time verifier V and an honest prover P such that for any input x,

$$
\begin{aligned}
x \in L &\Rightarrow \text{for the honest prover } P, Pr[V(x,P) \text{ accepts }] = 1 \\
x \notin L &\Rightarrow \text{for any prover } P', Pr[V(x,P') \text{ accepts }] \leq 1/2
\end{aligned}
$$

- IP $=$ PSPACE (we will not prove it in the class)

Interactive Proof system (IP)

Theorem

$\overline{3SAT} \in IP$.

Homework

- Randomized Algorithm, Problem 7.2, Page 188 (Algebraic Techniques)