Lecture 9 - Randomized Algorithms, BPP $\subset$ P$_{/poly}$ and BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Rafael Oliveira
rafael.oliveira.teaching@gmail.com
University of Waterloo

CS 860 - Graduate Complexity Theory
Fall 2022

Overview

- Error Reduction and BPP $\subset$ P$_{/poly}$

- BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Error Reduction

- Given a TM $M \in \mathrm{BPP}$ deciding a language L, we have that

$$\Pr_r[M(x,r) = L(x)] \geq 2/3$$

where $r \in \{0,1\}^{p(|x|)}$.

Error Reduction

- Given a TM $M \in \mathsf{BPP}$ deciding a language L, we have that

$$\Pr_r[M(x,r) = L(x)] \geq 2/3$$

  where $r \in \{0,1\}^{p(|x|)}$.

- To improve our confidence, just run the same algorithm multiple times, outputting the majority.

  Let A be the following algorithm (with $t = 2k - 1$):

  1. On input $x \in \{0,1\}^n$, sample $r_1, \ldots, r_t \in \{0,1\}^{p(n)}$
  2. Output $\mathsf{MAJ}(M(x,r_1), \ldots, M(x,r_t))$

Error Reduction

- Given a TM $M \in \text{BPP}$ deciding a language L, we have that

$$\Pr_r[M(x,r) = L(x)] \geq 2/3$$

  where $r \in \{0,1\}^{p(|x|)}$.

- To improve our confidence, just run the same algorithm multiple times, outputting the majority.

  Let A be the following algorithm (with $t = 2k - 1$):
  1. On input $x \in \{0,1\}^n$, sample $r_1, \ldots, r_t \in \{0,1\}^{p(n)}$
  2. Output MAJ$(M(x,r_1), \ldots, M(x,r_t))$

- If $X_i := 1_{M(x,r_i)=L(x)}$, we have $\Pr[X_i = 1] = p \geq 2/3$. By Chernoff:

$$\Pr_r[A(x,r) \neq L(x)] = \Pr\left[\sum_{i=1}^{t} X_i < k\right] \leq \exp\left(-\frac{t}{200p(1-p)}\right)$$

Error Reduction in BPP

Proposition 1 (Error Reduction in BPP)

If $L \in$ BPP and $c > 0$ is a constant, then there is a poly-time PTM M such that for all $x \in \{0,1\}^*$

$$\Pr_r[M(x,r) = L(x)] \geq 1 - 2^{-|x|^c}$$

- Apply the error reduction from previous slide with $t(|x|) = O(|x|^c)$.

Adleman's theorem: BPP $\subset$ P$_{/poly}$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is poly-time PTM M such that

$$\forall n \in \mathbb{N}, x \in \{0,1\}^n,\ \Pr_r[M(x,r) \neq L(x)] \leq \frac{1}{2^{n+1}}$$

Adleman's theorem: BPP $\subset$ P$_{/poly}$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is poly-time PTM M such that

$$\forall n \in \mathbb{N}, x \in \{0,1\}^n,\ \Pr_r[M(x,r) \neq L(x)] \leq \frac{1}{2^{n+1}}$$

- Suppose M uses m random bits, thus $r \in \{0,1\}^m$
- r is bad for x if $M(x,r) \neq L(x)$.

Adleman's theorem: BPP $\subset$ P$_{/poly}$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is poly-time PTM M such that

$$\forall n \in \mathbb{N}, x \in \{0,1\}^n,\ \Pr_r[M(x,r) \neq L(x)] \leq \frac{1}{2^{n+1}}$$

- Suppose M uses m random bits, thus $r \in \{0,1\}^m$
- r is bad for x if $M(x,r) \neq L(x)$.
- Count number of pairs (x,r) such that r is bad for x

Adleman's theorem: BPP $\subset$ P$_{/poly}$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is poly-time PTM M such that

$$\forall n \in \mathbb{N}, x \in \{0,1\}^n,\ \Pr_r[M(x,r) \neq L(x)] \leq \frac{1}{2^{n+1}}$$

- Suppose M uses m random bits, thus $r \in \{0,1\}^m$
- r is bad for x if $M(x,r) \neq L(x)$.
- Count number of pairs (x,r) such that r is bad for x
- For each x, there are $\leq 2^{m-n-1}$ such r's $\qquad L \in$ BPP

Adleman's theorem: BPP $\subset$ P$_{/poly}$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is poly-time PTM M such that

$$\forall n \in \mathbb{N}, x \in \{0,1\}^n,\ \Pr_r[M(x,r) \neq L(x)] \leq \frac{1}{2^{n+1}}$$

- Suppose M uses m random bits, thus $r \in \{0,1\}^m$
- r is bad for x if $M(x,r) \neq L(x)$.
- Count number of pairs (x,r) such that r is bad for x
- For each x, there are $\leq 2^{m-n-1}$ such r's $\quad L \in$ BPP
- Total number of bad pairs is $\leq 2^n \cdot 2^{m-n-1} = 2^{m-1}$

Adleman's theorem: BPP $\subset$ P$_{/poly}$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is poly-time PTM M such that

$$\forall n \in \mathbb{N}, x \in \{0,1\}^n,\ \Pr_r[M(x,r) \neq L(x)] \leq \frac{1}{2^{n+1}}$$

- Suppose M uses m random bits, thus $r \in \{0,1\}^m$
- r is bad for x if $M(x,r) \neq L(x)$.
- Count number of pairs (x,r) such that r is bad for x
- For each x, there are $\leq 2^{m-n-1}$ such r's $\qquad L \in$ BPP
- Total number of bad pairs is $\leq 2^n \cdot 2^{m-n-1} = 2^{m-1}$
- Pigeonhole: there is one r which is good for all $x \in \{0,1\}^n$

Adleman's theorem: BPP $\subset$ P$_{/poly}$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is poly-time PTM M such that

$$\forall n \in \mathbb{N}, x \in \{0,1\}^n,\ \Pr_r[M(x,r) \neq L(x)] \leq \frac{1}{2^{n+1}}$$

- Suppose M uses m random bits, thus $r \in \{0,1\}^m$
- r is bad for x if $M(x,r) \neq L(x)$.
- Count number of pairs (x,r) such that r is bad for x
- For each x, there are $\leq 2^{m-n-1}$ such r's $\qquad L \in$ BPP
- Total number of bad pairs is $\leq 2^n \cdot 2^{m-n-1} = 2^{m-1}$
- Pigeonhole: there is one r which is good for all $x \in \{0,1\}^n$
- Hardwire this r into M

- Error Reduction and BPP $\subset$ P$_{/poly}$

- BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Sipser-Gács theorem: BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Theorem 2 (Sipser-Gács)

$$BPP \subseteq \Sigma_2^p \cap \Pi_2^p$$

Sipser-Gács theorem: BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Theorem 2 (Sipser-Gács)

$$BPP \subseteq \Sigma_2^p \cap \Pi_2^p$$

- Since BPP $=$ coBPP, enough to prove that BPP $\subseteq \Sigma_2^p$

Sipser-Gács theorem: BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Theorem 2 (Sipser-Gács)

$$\mathit{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is PTM M using $m := m(n) \geq n$ (poly(n)) random bits for $x \in \{0,1\}^n$ s.t.

$$\Pr_r[M(x,r) \neq L(x)] \leq 2^{-n}$$

Sipser-Gács theorem: BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Theorem 2 (Sipser-Gács)

$$\mathit{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is PTM M using $m := m(n) \geq n$ (poly(n)) random bits for $x \in \{0,1\}^n$ s.t.

$$\Pr_r[M(x,r) \neq L(x)] \leq 2^{-n}$$

- For $x \in \{0,1\}^n$ let $S_x \subset \{0,1\}^m$ be set of random strings r such that $M(x,r) = 1$

$$x \in L \Rightarrow |S_x| \geq (1 - 2^{-n})2^m$$

$$x \notin L \Rightarrow |S_x| \leq 2^{m-n}$$

Sipser-Gács theorem: BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Theorem 2 (Sipser-Gács)

$$\mathit{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$$

- $L \in$ BPP and Proposition 1 $\Rightarrow$ there is PTM M using $m := m(n) \geq n$ (poly(n)) random bits for $x \in \{0,1\}^n$ s.t.

$$\Pr_r[M(x,r) \neq L(x)] \leq 2^{-n}$$

- For $x \in \{0,1\}^n$ let $S_x \subset \{0,1\}^m$ be set of random strings r such that $M(x,r) = 1$

$$x \in L \Rightarrow |S_x| \geq (1 - 2^{-n})2^m$$

$$x \notin L \Rightarrow |S_x| \leq 2^{m-n}$$

- Enough to show which is the case using 2 quantifiers

Sipser-Gács theorem: BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Let $k = \lceil m/n \rceil + 1$

1. If $S \subset \{0,1\}^m$ with $|S| \leq 2^{m-n}$ and $u_1, \ldots, u_k \in \{0,1\}^m$

$$\bigcup_{i=1}^{k} (S + u_i) \neq \{0,1\}^m$$

Sipser-Gács theorem: BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Let $k = \lceil m/n \rceil + 1$

1. If $S \subset \{0,1\}^m$ with $|S| \leq 2^{m-n}$ and $u_1, \ldots, u_k \in \{0,1\}^m$

$$\bigcup_{i=1}^{k} (S + u_i) \neq \{0,1\}^m$$

2. If $S \subseteq \{0,1\}^m$ with $|S| \geq (1 - 2^{-n})2^m$, there are $u_1, \ldots, u_k \in \{0,1\}^m$ such that

$$\bigcup_{i=1}^{k} (S + u_i) = \{0,1\}^m$$

Sipser-Gács theorem: BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$

Let $k = \lceil m/n \rceil + 1$

1. If $S \subset \{0,1\}^m$ with $|S| \leq 2^{m-n}$ and $u_1, \ldots, u_k \in \{0,1\}^m$

$$\bigcup_{i=1}^{k} (S + u_i) \neq \{0,1\}^m$$

2. If $S \subseteq \{0,1\}^m$ with $|S| \geq (1 - 2^{-n})2^m$, there are $u_1, \ldots, u_k \in \{0,1\}^m$ such that

$$\bigcup_{i=1}^{k} (S + u_i) = \{0,1\}^m$$

3. Above show that

$$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \, \forall r \in \{0,1\}^m \bigvee_{i=1}^{k} M(x, r+u_i) = 1$$

Proof of item 2

Let $k = \lceil m/n \rceil + 1$

- If $S \subseteq \{0,1\}^m$ with $|S| \geq (1-2^{-n})2^m$, there are $u_1, \ldots, u_k \in \{0,1\}^m$ such that

$$\bigcup_{i=1}^{k} (S + u_i) = \{0,1\}^m$$

Proof of item 2

Let $k = \lceil m/n \rceil + 1$

- If $S \subseteq \{0,1\}^m$ with $|S| \geq (1-2^{-n})2^m$, there are $u_1, \ldots, u_k \in \{0,1\}^m$ such that

$$\bigcup_{i=1}^{k} (S + u_i) = \{0,1\}^m$$

1. For $r \in \{0,1\}^m$, let B_r event that $r \notin S_u := \bigcup_{i=1}^{k}(S + u_i)$.

   Equivalently, $u_i \notin S + r$ for $i \in [k]$.

Proof of item 2

Let $k = \lceil m/n \rceil + 1$

- If $S \subseteq \{0,1\}^m$ with $|S| \geq (1 - 2^{-n})2^m$, there are $u_1, \ldots, u_k \in \{0,1\}^m$ such that

$$\bigcup_{i=1}^{k} (S + u_i) = \{0,1\}^m$$

1. For $r \in \{0,1\}^m$, let B_r event that $r \notin S_u := \bigcup_{i=1}^{k}(S + u_i)$.
   Equivalently, $u_i \notin S + r$ for $i \in [k]$.
2. $|S| \geq (1 - 2^{-n})2^m \Rightarrow \Pr[B_r] \leq 2^{-nk} < 2^m$

Proof of item 2

Let $k = \lceil m/n \rceil + 1$

- If $S \subseteq \{0,1\}^m$ with $|S| \geq (1 - 2^{-n})2^m$, there are $u_1, \ldots, u_k \in \{0,1\}^m$ such that

$$\bigcup_{i=1}^{k} (S + u_i) = \{0,1\}^m$$

1. For $r \in \{0,1\}^m$, let B_r event that $r \notin S_u := \bigcup_{i=1}^{k} (S + u_i)$.

   Equivalently, $u_i \notin S + r$ for $i \in [k]$.
2. $|S| \geq (1 - 2^{-n})2^m \Rightarrow \Pr[B_r] \leq 2^{-nk} < 2^m$
3. By union bound:

$$\Pr\left[\exists r \in \{0,1\}^m \;\mid\; B_r\right] < 1.$$

References I

Arora, Sanjeev and Barak, Boaz (2009)
Computational Complexity, A Modern Approach — Chapter 7
Cambridge University Press

Trevisan, Luca (2002)
Lecture notes — Chapter 5
See webpage

Goldreich, Oded (2006)
Computational complexity: a conceptual perspective. — Chapter 6
https://www.wisdom.weizmann.ac.il/~oded/cc-drafts.html