Error Reduction for BPP

Lecture 16

BPP: $L \in BPP$ if $\exists$ PTM M

in strict polytime s.t.

$$\Pr[M(x) = L(x)] \geq 2/3$$

$\forall x$

"convenient"

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

$\forall x$ DTM

$BPP_{\frac{1}{2}+\varepsilon}$: $L \in BPP_{1/2+\varepsilon}$ if $\exists$

$\delta \geq 1/2$ PTM M in strict polytime

s.t. $\forall x$

$$\Pr[M(x) = L(x)] \geq \underbrace{\tfrac{1}{2} + \varepsilon(|x|)}_{\delta \geq \frac{1}{2}}$$

$\geq 1 - \sigma$

$BPP_{\frac{1}{2}+n^{-c}}$ $c > 0$ some constant

$n = |x|$

<u>Lemma</u>: $\forall c > 0$ constant.

$$BPP = BPP_{\frac{1}{2}+n^{-c}}$$

<u>Proof</u>:

① $BPP \subseteq BPP_{\frac{1}{2}+n^{-c}}$

$$2/3 \geq \frac{1}{2} + n^{-c} \quad \forall c > 0$$

for large enough $n \geq 2$

② $BPP_{\frac{1}{2}+n^{-c}} \subseteq BPP$

↳ <u>Claim</u>. Suppose L is decided by PTM (in polytime) M

s.t. $\Pr[M(x)=L(x)] \geq \frac{1}{2} + |x|^{-c}$

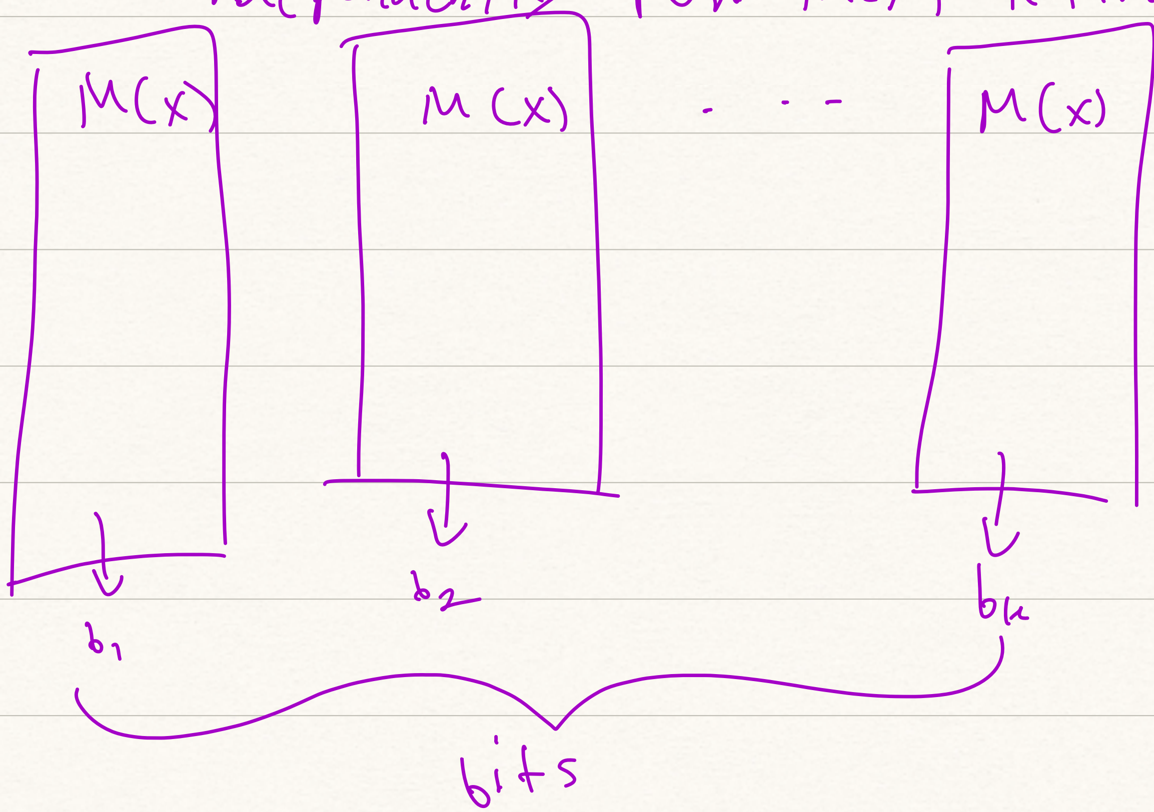
Then there exists PTM M' in polytime s.t.

$$\Pr[M'(x)=L(x)] \geq 1-2^{-|x|^d}$$

for some constant d.

Proof Idea

- $M'(x)$: $k = q(|x|) = 8\cdot|x|^{2c+d}+1$
  - Independently run $M(x)$ k times



$M'(x)$ outputs

$b = \text{majority}(\underbrace{b_1, \ldots, b_k}_{\text{bit that appears at least } \lceil \frac{k}{2} \rceil \text{ times}})$

Finishing Proof: $\boxed{\text{Chernoff Bound}}$

BPP vs. Other Classes

- P vs. BPP?

☆ Believe P = BPP

$P \subseteq BPP$

Theorem $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$

$$BPP = coBPP$$

Proof: $BPP \subseteq \Sigma_2^P$

Let $L \in BPP_{1-2^n}$

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

$|x| = n.$

$r \in \{0,1\}^{P(|x|)}$ polynomial

$r \in \{0,1\}^m \quad m = p(n)$

- Let $S_x \subseteq \{0,1\}^m$ be good for x.

$$S_x = \{ r \mid M(x,r) = 1 \}$$

$\cancel{L(x)}$

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

② If $x \notin L$, $|S_x| \leq 2^m \cdot 2^{-n} = 2^{m-n}$

$$\Pr_r[M(x,r)=1 \mid x \notin L] =$$

$$1 - \Pr_r[M(x,r)=0 \mid \underbrace{x \notin L}_{L(x)=0}]$$

$$\leq 1-(1-2^{-n}) = 2^{-n}$$

Goal: Encode this set S_x idea in a Σ_2^P machine

Tool: For any $S \subseteq \{0,1\}^m$ an vector u

$$S+u := \{ s+u \mid s \in S \}$$

$$\boxed{* \text{ Let } K = \left\lceil \frac{m}{n} \right\rceil + 1 \; *}$$

Claim 1: If $|S| \leq 2^{m-n}$, then $\forall u_1, \ldots, u_k \in \{0,1\}^m$, we have

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

Proof: $|S + u_i| = |S| = 2^{m-n}$

$$\left|\bigcup_{i=1}^{k} (S+u_i)\right| \underset{\text{Union Bound}}{\leq} \sum_{i=1}^{k} |S + u_i| = k \cdot 2^{m-n} < 2^m$$

$k = \lceil \frac{m}{n} \rceil + 1$

Claim 2: If $|S| \geq (1 - 2^{-n}) \cdot 2^m$ then $\exists u_1, \ldots, u_k$ such that

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

Proof idea: Probabilistic Method

(1) Sample $u_1, \ldots, u_k \xleftarrow{\$} \{0,1\}^m$

· independent, uniform

(2) If $\Pr_{u_i}\left[\bigcup_{i=1}^{k} (S+a_i) = \{0,1\}^m \right] > 0$

then $\exists\, u_1^*, \ldots, u_k^*$ s.t.

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

can put in lecture notes

Encoding as Σ_2^P statement

$$\exists\, u_1, \ldots, u_k \ \forall r \in \{0,1\}^m :$$

$$r \in \bigcup_{i=1}^{k} (S_x + u_i)$$

$k = \mathrm{poly}(n)$

$m = \mathrm{poly}(n)$

$\square$

Randomized Reductions

Def.

- For B, C languages, we say B is randomized polynomial-time reducible to C, $B \leq_r C$, if

  $\exists$ poly-time PTM M s.t.

  $\forall x$

  $$\Pr[C(M(x)) = B(x)] \geq 2/3$$

poly-time reductions $B \leq_p C$

$$x \in B \iff f(x) \in C$$

* Not transitive! $A \leq_r B,\ B \leq_r C$

$\not\Rightarrow A \leq_r C$

* Still useful

$$\boxed{B \le_r C,\ C \in BPP \implies B \in BPP}$$

- NP under rand. reductions?

$$BP\cdot NP = \{ L \mid L \le_r 3SAT \} \supseteq \{ L \le_p 3SAT \} = NP$$

$\not\subseteq$ NP

Don't think this is true

- Don't think $\overline{3SAT} \in BP\cdot NP$

Lemma: If $\overline{3SAT} \in BP\cdot NP$, then $PH = \Sigma_3^p$

Randomized Space-bounded Computations

Def: $L \in BPL$ if $\exists$ PTM M
using $O(\log(n))$ space for inputs of length n s.t.

$$\Pr[M(x) = L(x)] \geq 2/3$$

- Similar for RP/coRP/ZPP.

Theorem:

1. $RL \subseteq NL \subseteq P$
2. $BPL \subseteq P$

Boolean Circuits

- non-uniform model
  - Turing Machines
    One Machine takes
    infinitely many inputs
    $M(x)$ for $x \in \{0,1\}^*$

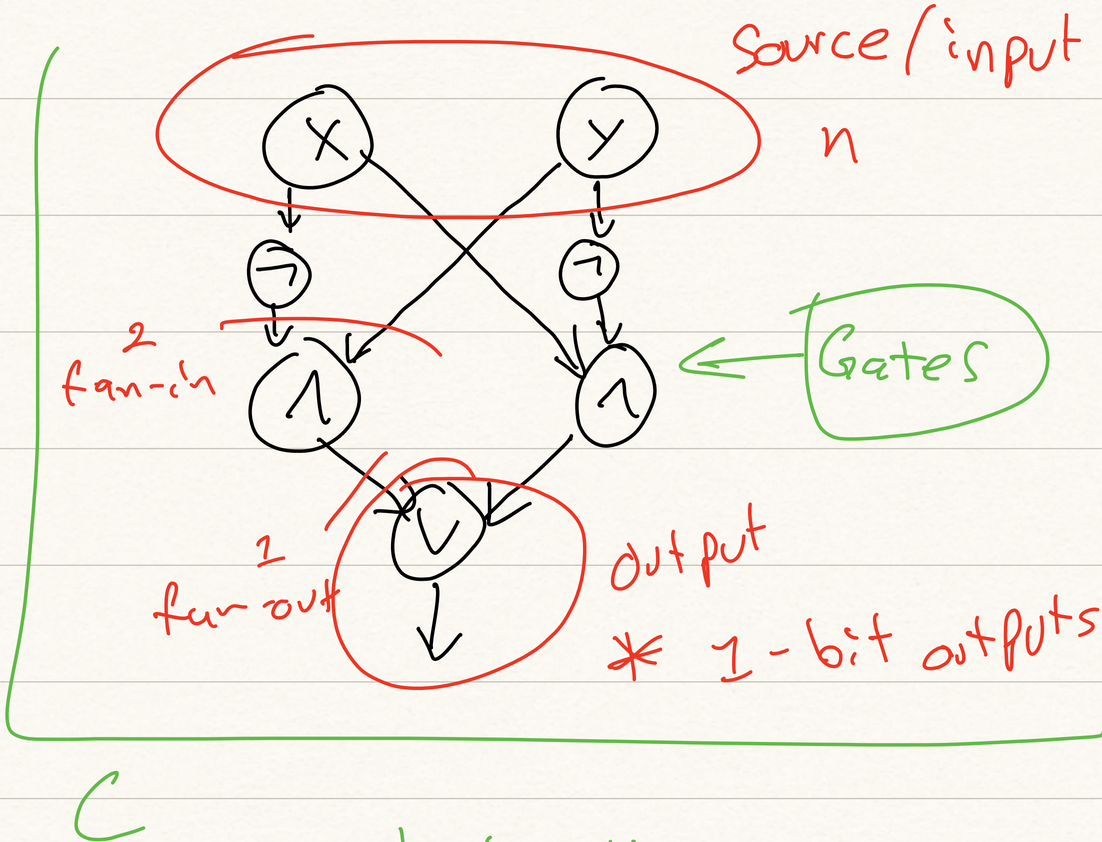
    Uniform

  - Circuits: for every input
    length n, single
    circuit C_n

Boolean Circuits

- AND, OR, NOT
- Fan-in 2, Fan-out 1

• Ex: $x, y \in \{0,1\}$ $x \oplus y$



$|C| = \#$ of nodes

$\geq n$ (# of inputs)

Circuit Families

Let $T: \mathbb{N} \to \mathbb{N}$ be a function.

A T-sized circuit family

is a sequence of circuits $\{C_n\}_{n\in\mathbb{N}}$ such that $|C_n| \le T(n)$ and C_n has n input gates $\forall n \in \mathbb{N}$

- language
  $L \in SIZE(T)$ if $\exists$ $O(T)$-sized circuit family which decides L

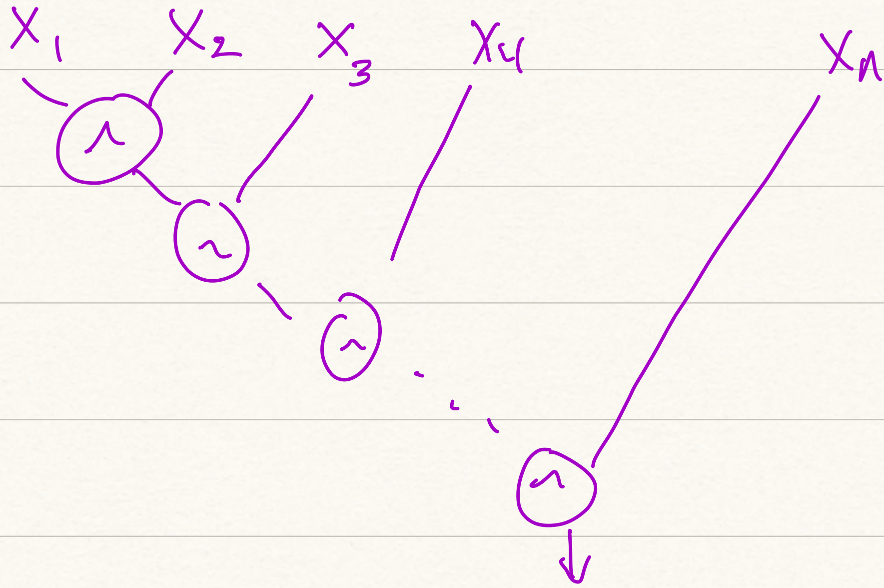
  $\forall n \in \mathbb{N}$, $\forall x \in \{0,1\}^n$

  $x \in L \iff C_n(x) = 1$

Examples

① $L = \{1^n : n \in \mathbb{N}\} \in SIZE(n)$

$x \in \{0,1\}^n$ $\quad x \in L$?



② $L = \{(x, y, z) : x, y, z \in \mathbb{N},\ z = x + y\}$

$\in SIZE(n^2)$

Lecture 1b