CS121 Lecture 21 Nov 12, 2019

Modeling Randomized Computation

Midterm 2

- 105 minute midterm now (from 90 min)
- 1st q: T/F/Unknown
- Partial credit for understanding steps in reductions
- For algorithms/reductions: separate operations from analysis
- Partial credit for reductions: if you understand the steps (clear about what you did/didn't do)

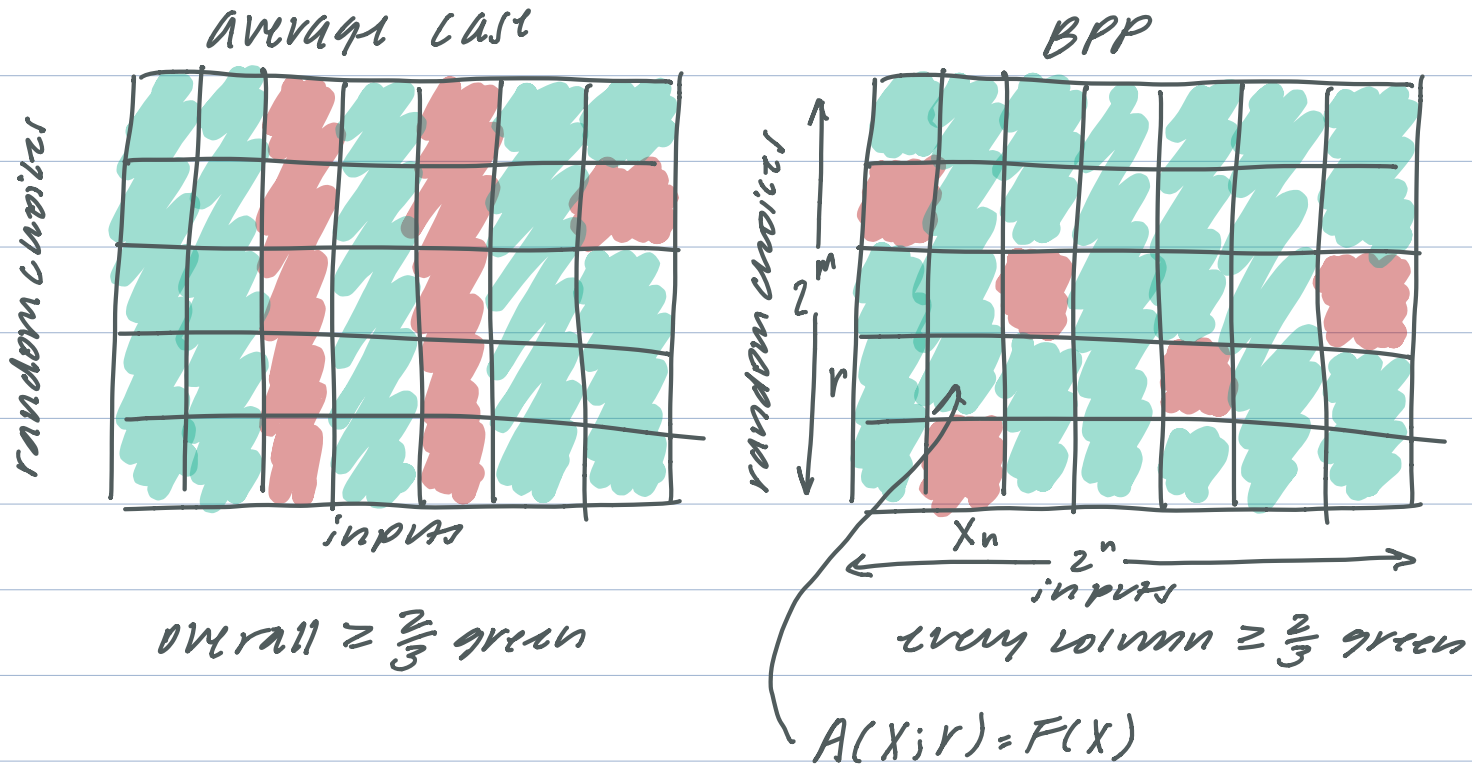
Today

- $P \subseteq BPP \subseteq EXP$
- Success amplification via Chernoff Bound
- $BPP \subseteq P/poly$
- If $P = NP$ then $BPP = P$
- Pseudorandom generators and why researchers think $BPP = P$

Class BPP

$F: \{0,1\}^* \to \{0,1\}$ in BPP if $\exists$ poly-time ~~deterministic~~ algo A, poly $q(n)$ s.t. $\forall n \; \forall x \in \{0,1\}^n$

$$\Pr_{r \sim \{0,1\}^{q(n)}}[A(x;r) = F(x)] \geq \frac{2}{3}$$



Q1. Prove that $P \subseteq BPP$

$B(X) = F(X)$

do-time $A(X;r) = B(X)$ ← deterministically calc, throw out randomness

Q2. Prove that $BPP \subseteq EXP$

Polynomial-time randomized algorithm ↓

↔ $\bigcup_c TIME(2^{n^c})$, there is some algo w/ time complexity 2^{n^c} that computes it

Compute w/ 100% accuracy by iterating over all outputs of the coin tosses and check if correct (run A) ↓ $2^m \cdot poly(n)$

$$\Pr_{r \sim \{0,1\}^m}[A(X;r)=1] = \frac{|\{r \mid A(X;r)=1\}|}{2^m}$$, check if $\geq \frac{2}{3}$, then 1

randomness can speed things up but cannot make some uncomputable function computable.

Amplification for 2-sided error

If $F \in BPP$ then $\exists$ poly-time B, poly $q(n)$ s.t. $\forall n, \forall x \in \{0,1\}^n$, $\Pr_{r \sim \{0,1\}^{q(n)}}[B(x;r) = F(x)] \geq 1 - 2^{-2n^2}$

- B will run A $1000n^2$ times and return majority vote

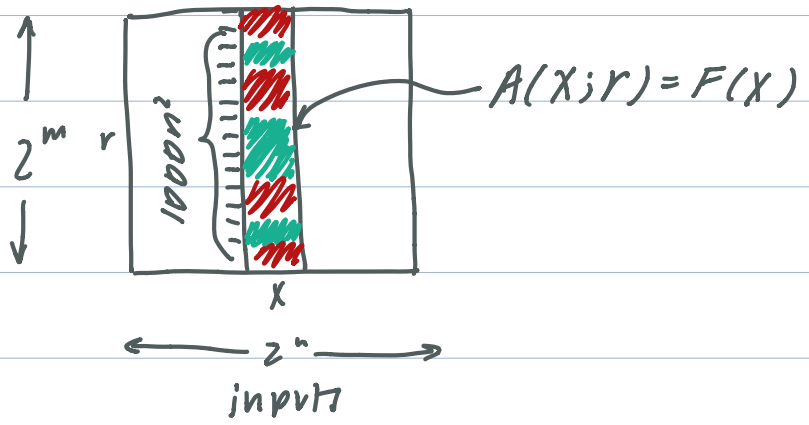
Input: x

for $i = 1, \ldots 1000n^2$:

$r_i \sim \{0,1\}^m$

$y_i \leftarrow A(x; r_i)$

return $Maj(y_1, y_2 \ldots y_{1000n^2})$



Define $X_i = \begin{cases} 1, & A(x, r_i) = F(x) \\ 0, & A(x, r_i) \neq F(x) \end{cases}$

$X_1 \ldots X_{1000n^2}$ iid w/ $\mathbb{E}[X_i] \geq 2/3$

By Chernoff,

$\Pr\left[\frac{1}{1000n^2} \sum X_i < 0.51\right] < 2^{-n^2}$

∎

Ultra-amplification and Offline BPP

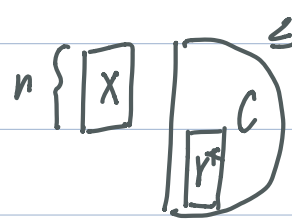
Can bring $\Pr_{r \sim \{0,1\}^m}[A(x;r) \neq F(x)] < 0.01 \cdot 2^{-n}$

$\Pr[\text{Failure}] < \frac{1}{100N}$ → every column has $\leq \frac{M}{100N}$ "reds"

∴ some rows have no "reds" → favorable choice of random string w/ no errors

By $P \subseteq P/poly$, there is a circuit C of $\leq n^{42}$ computing

$x, r \mapsto A(x;r)$



$X \mapsto A(X; r)$ is the map F on $\{0,1\}^n$

Q3. Unknown if BPP=P, BPP=EXP.

Can it be that P=BPP=EXP?

By time hierarchy thm, $P \neq EXP$, so this cannot be true.

Q4. Is there a poly-time deterministic algorithm that, given randomized alg A for $F \in BPP$ and $n \in \mathbb{N}$ outputs a circuit C_n that computes F on $\{0,1\}^n$?

- no because we know r^* exists but not what it is.

$P \subseteq P/poly : n, A \longmapsto C_n$

$BPP \subseteq P/poly : n, A \xrightarrow[r^*(n)]{?} C_n$

cannot be found in deterministic polynomial time. If it existed then P=BPP.

Q5. Suppose $F \leq_p G$ and $G \in BPP$. Prove $F \in BPP$.

have:

- F reduces in poly-time to G $\rightarrow \exists R$ (poly) s.t. $\forall X$ $F(X) = G(R(X))$
- $Pr[A(y) = G(y)] \geq 2/3$ $\forall y$

want:

poly B s.t. $\forall X$ $Pr[B(X) = F(X)] \geq \frac{2}{3}$

Define $B(x)$:

return $A(R(x))$

$\forall x$, let y be $R(x)$. $\Pr[A(y) = b(y)] \geq \frac{2}{3}$

$\Pr[B(x) = F(x)] \geq \frac{2}{3}$ — R

Corollary:

If $3SAT \in BPP$, then $NP \subseteq BPP$

Unknown: Is $BPP \subseteq NP$, is $NP \subseteq BPP$?

Sipser-Gács Theorem

Sipser-Gács Thm: If $P = NP$ then $BPP = P$

Proof idea:

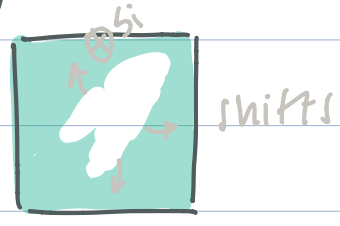
1. amplify: $\Pr_{r \sim \{0,1\}^m}[A(x;r) = F(x)] \geq 1 - 2^{-n} > 1 - \frac{1}{1000m}$

2^{-n}: greater than any polynomial

$\equiv \Pr[\text{fail}] \leq \frac{1}{1000m}$

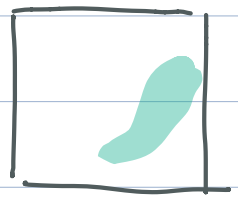
$A(x;r) = 0$

$A(x;r) = 1$



$F(x) = 0$

$|S_x| < \frac{1}{1000m} 2^m$



$F(x) = 1$

$|S_x| > (1 - \frac{1}{1000m}) 2^m$

$S_x : \{r \mid A(x;r) = 1\}$

Main Lemma: $F(x) = 1$ iff $\exists m$ shifts $s_1, \dots s_m$ s.t. $\{0,1\}^m = \bigcup (S_x \oplus s_i)$

if $F(x)=0$, no matter how you shift, you cannot cover everything

Claim 1.

* $S \oplus s := \{r \oplus s \mid r \in S\}$

$S \subseteq \{0,1\}^m$

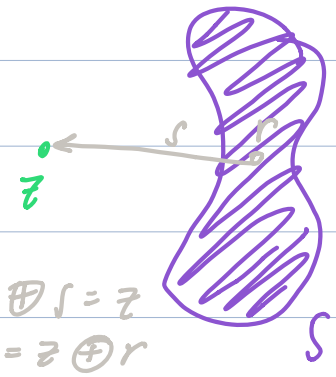
$|S| \le \frac{2^m}{1000m}$ $\forall s_1 \dots s_m$ $\bigcup (S \oplus s_i) \subsetneq \{0,1\}^m$

$|S| \ge \frac{2}{3} \cdot 2^m$ $\exists s_1 \dots s_m$ $\bigcup (S \oplus s_i) = \{0,1\}^m$

Claim 2.

If $|S| > \frac{2}{3} \cdot 2^m$ then $\exists s_1, \dots s_m \in \{0,1\}^m$ s.t. $\bigcup_i (S \oplus s_i) = \{0,1\}^m$

$$\Pr[z \notin S \oplus s] = \Pr[s \notin S + z]$$



Recap

- All theory of NP completeness stays the same if we use BPP as our model of "efficient computation"
- If P=NP, then P=BPP

Why do we think P=BPP?

Pseudorandom: takes short seed $x \in \{0,1\}^\ell$ → long output $y = G(x) \in \{0,1\}^m$

Conjecture: There is PRG s.t. $m \ge 2^{0.001\ell}$

· can reduce