Today

- Amplification of error
- BPP in $P/poly$.
- BPP in PH.

Clarification on Games

Few lectures back ... we said some wrong things.

- Game is in PSPACE only if there is an a priori polynomial upper bound on its running time.
- Go: # of pieces on board increase all the time.
- Geography: Path length bounded by size of Atlas.
- Chess: No “a priori” upper bound - hence not known to be in PSPACE.

Last lecture

- Introduced randomness.
- Defined many classes (BPP, RP, RL etc.)
- Showed Poly. Ident. Testing in RP.
- Claimed USTCON in RL.
- Next on agenda: completeness and soundness.

RP Amplification

Suppose M accepts language $L$ with completeness $c(n) = 1/n^2$ (and $s(n) = 0$). How to amplify completeness?

Amplification: Run machine $n^4$ times on independent random strings $y_1, \ldots, y_{n^4}$, and accept if one of the $y_i$’s accepts.

$$\Pr_y [\exists i \text{ s.t. } M(x, y_i) \text{accepts}] \geq 1 - (1 - 1/n^2)^{n^4} \geq 1 - \exp(n)$$

Thus completeness $1/poly(n)$ vs. $1 - \exp(n)$ are equivalent.
BPP amplification

- How to use the above idea for BPP?
- Natural idea:
  - Repeat $N$ times.
  - Accept if $\#$ acceptances more than $(c + s)N/2$.
- Analysis?
  - Use “tail inequalities”.
  - “Chernoff bound”.

Consequence

Let $X_i = 1$ if $M(x, y_i)$ accepts and $0$ o.w.

Applying Chernoff bounds, we see that if $N \sim m/(c - s)^2$ then amplification increases completeness to $1 - \exp(-m)$ and decreases soundness to $\exp(-m)$.

Next: Use this to show $\text{BPP in } \mathsf{P/poly}$.

Consequence: $\text{BPP in } \mathsf{P/poly}$

Say $L \in \text{BPP}$. Assume w.l.o.g. that $M$ is a two input machine recognizing $L$ with $c(n) \geq 1 - 4^{-n}$ and $s(n) \leq 1 - 4^{-n}$. (Notice we get this by amplification.)

Say $M$ uses $m$-bit random strings.

Claim: Exists $r \in \{0, 1\}^m$ such that for every $x$, $M(x, r) = L(x)$.

Proof: Say $y \in \{0, 1\}^m$ is BAD for $x$ if $M(x, y) \neq L(x)$.

For any $x \in \{0, 1\}^n$ there are at most $2^{m-2n}$ $y$’s that are BAD for $x$.

Taking the union of all BAD sets, there are at most $2^{m-n}$ strings that are BAD for some $x$. 

Since $2^m > 2^{m-n}$ there exists at least one $y$ which is not BAD for any $x$. Setting $r \leftarrow y$ gives the Claim.

Thm: $\text{BPP} \subseteq \text{P/poly}$.

Proof: $\text{P/poly}$ machine is $M$ from the argument above. For every $n$, advice string is the $r \in \{0,1\}^m$ from the claim.

Next: BPP in PH

Note note quite trivial. How to have a bounded round interaction to convince $x \in L$?

Consider following game: Deniss & I are all powerful players. I want to convince you (the audience) that $x \in L$ and Deniss claims otherwise. How can we prove our claims?

Draw picture here.

Most strings are good ($M(x,y) = \text{accept}$); or very few are good. How to convince you?

Idea 1: I’ll divide space into two equal parts with all bad strings in one part and a bijection $pi$ between the two parts. I claim every string or its map under bijection is good! If Deniss wants, he can challenge me!

If Deniss finds a string $y$ where neither $M(x,y)$ nor $M(x,pi(y))$ accept - he wins.

Else I win.

Seems convincing. I can win if bad set is smaller than 1/2. I can’t win if bad set more than 1/2.

Problem: How do I give the bijection?

Bijections have to simple: So we’ll stick $\pi_r : y \mapsto y \oplus r$.

In this space of bijections the proof doesn’t go through. But the idea is starting to emanate.

Debate for membership in BPP

Theorem: If $x \in L$ there exist $r_1, \ldots, r_{2m} \in \{0,1\}^m$ such that the $y$’s are covered; i.e., for every $y$ there exists an $i \in [2m]$ such that $M(x, \pi_{r_i}(y))$ accept.

If $x$ not in $L$, then for any $r_1, \ldots, r_{2m} \in \{0,1\}^m$ there is an uncovered $y$.

Assuming theorem: Debate: I announce $r_1, \ldots, r_{2m}$. Deniss challenges with a $y$. You compute $M(x,y \oplus r_1) \lor \cdots \lor M(x,y \oplus r_{2m})$. If true, I win ($x \in L$) else Deniss wins ($x \notin L$) - you decide!
Proof of theorem

If $x$ in $L$

$$\Pr_r[M(x, y \oplus r)] \geq 1 - 2^{-n} \geq 1/2.$$  
$$\Pr_{r_1, \ldots, r_{2m}}[\exists i \in [2m] \text{ s.t. } M(x, y \oplus r_i)] \geq 1 - 2^{-2m}.$$  
$$\Pr_{r_1, \ldots, r_{2m}}[\forall y \in \{0, 1\}^m, \exists i \in [2m] \text{ s.t. } M(x, y \oplus r_i)]$$

Yields first part.

Proof of theorem (second part)

If $x$ not in $L$. Say I pick best possible $r_1, \ldots, r_{2m}$ below.

$$\Pr_y[M(x, y \oplus r)] \leq 1/100m.$$  
$$\Pr_y[\exists i \in [2m] \text{ s.t. } M(x, y \oplus r_i)] \leq 1/50.$$  

QED!

Power of the prover

If I am right - I just need to pick $r_1, \ldots, r_{2m}$ at random!

If Deniss is right, he just needs to pick $y$ at random.

So we just need randomness to simulate randomness!

Hmm.... that didn’t sound so impressive - I should have said ...

So we just need one-sided randomness to simulate two-sided randomness! You’ll figure out what I mean in problem set!

Current issues in randomness

- Reducing randomness
  - Algorithm specific: Limited independence, Epsilon-bias.
  - Generically, during amplification: “Recycling”.

- Using imperfect randomness: Extractors.

- Derandomization: Pseudorandomness, hardness versus randomness.