Homework 18

Austin Frownfelter Matthew Bialecki

February 23, 2018

1 Problem 29

Show BP·NP ⊆ NP/Poly

Let L ∈ BP·NP

∃ PTM M that runs nondeterministically in poly time.
$\forall x$ Probability(M(x) is wrong) ≤ 0.4

Construct an M', which is a randomized reduction of L to 3SAT, for n^2 times and takes the majority.
$\forall x$ P(M'(x) is wrong) $\leq \frac{1}{4^n}$
The probability on all inputs x that M' is wrong =
$\Sigma_{i=1}^{2^n} p(M'(x_i) wrong) \leq \frac{2^n}{4^n} < 1$
Therefore, ∃ random string such that M' is right on all inputs with that string as advice.
M' decides L. L is randomly reducible to 3SAT.
3SAT can be trivially solved by a family of NP/Poly circuits as it is verified in polynomial time.
Since L is reducible to 3SAT, L can be solved by a family of NP/Poly circuits.
Thus, L ⊆ NP/Poly. Therefore, BP·NP ⊆ NP/Poly.

2 Problem 30

Show BPL ∈ P

Let L be an arbitrary language in BPL
∃ PTM M ∃ k such that

1. M runs in space $\leq \log(|x|)$
2. $x \in L$ ЯA $M(x, A)$ accepts
3. $x \notin L$ ЯA $M(x, A)$ rejects

m = the number of bits in A.

Randomly marry pairs of inputs. P(wrong in entire marriage) = P(wrong)^2

$x \in L$ $\exists w$ $\forall A$ M(x,A) $\vee$ M(x,A$\oplus$w) accepts
$x \notin L$ $\forall w$ $\exists A$ M(x,A) $\wedge$ M(x,A$\oplus$w) rejects

$x \in L$ wrong $(\frac{1}{4^n})^2$
$x \notin L$ wrong $\frac{2}{4^n}$

$x \in L$: E[# bad advice at k weddings] $= 2^m * (\frac{1}{4^n})^{k+1} < 1$ (i.e. there is some chance)
$2^m < 4^{n(k+1)}$
$m < n(k+1) \rightarrow k > \frac{m}{2n} - 1$
$m < \log(n) \rightarrow k > \frac{\log(n)}{2n} < 1$

$x \notin L$: E[# bad advice at k weddings] $\leq \frac{k+1}{4^n}$
$\frac{\log(n)}{2n} * \frac{1}{4^n} < 1$

$\exists$ TM N in P:

Runs the BPL machine

Returns the result

The probability N returns an incorrect result is P(wrong)$^{\log(n)}$
It is possible to drive P(wrong) from $\frac{1}{3}$ to $\frac{1}{3^n}$ with the error reduction strategy in polynomial time. Thus, the probability N is correct is effectively 100%. Therefore, N is in P.
N only uses log space, therefore it can be used to solve L in BPL, satisfying BPL.
Therefore, L $\in$ P
Therefore, BPL $\in$ P