CS58400 - Theory of Computation and Computational Complexity Spring 2026

Assignment 3 *Due: Apr 2*

Note: Use LaTeX to typeset your solutions. You can use the source code of this file as a template or reference. Bonus questions are still capped by the total assignment grades, so only work on them if you want a challenge.

Problem 1 (Careless definition of RL). Define $\mathsf{RL}^{\times}$ as the class of languages L such that there exists a probabilistic Turing machine M that on every input $x \in \{0,1\}^*$, runs in space $O(\log |x|)$, and:

- If $x \in L$, then $\Pr[M(x) = 1] \geq 1/2$;
- If $x \notin L$, then $\Pr[M(x) = 1] = 0$.

(in other words, it is "RL" but without time constraint).

(5 pts). Prove that $\mathsf{RL}^{\times}$ is in fact NL.

Problem 2 (Zero-error probabilistic poly-time). Define ZPP as the class of languages L such that there exists a probabilistic Turing machine M that on every input $x \in \{0,1\}^*$, runs in time $\mathrm{poly}(|x|)$, and:

- $\Pr[M(x) \in \{0,1\}] \geq 1/2$;
- If $x \in L$, then $\Pr[M(x) = 0] = 0$;
- If $x \notin L$, then $\Pr[M(x) = 1] = 0$.

Note that $M(x)$ could potentially output anything in $\{0,1\}^*$, not just 0 or 1. However, the above requirements implies that, whenever $M(x)$ outputs 0 or 1, it must be correct.

(5 pts). Prove that $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$.

Problem 3 (Approximate counting). Although exact computation of $\#\mathsf{P}$ problems is extremely hard, one can relatively easily approximate them using randomness and an NP oracle. In this problem we will work out this celebrated result initially proved by Stockmeyer.

1. **(5 pts)**. Let $\mathcal{H}_{n,m}$ be a family of pairwise uniform hash functions $h : \{0,1\}^n \to \{0,1\}^m$. For every subset $S \subseteq \{0,1\}^n$, prove that

$$\mathop{\mathbf{E}}_{h \sim \mathcal{H}_{n,m}} \left[|S \cap h^{-1}(0^m)|^2 \right] = \frac{|S|}{2^m} + \frac{|S|^2 - |S|}{2^{2m}}.$$

And use it to show that

$$1 - \frac{2^m}{|S|} \le \Pr_{h \sim \mathcal{H}_{n,m}} \left[|S \cap h^{-1}(0^m)| \ge 1 \right] \le \frac{|S|}{2^m}.$$

Hint. Use Chebyshev's inequality and Markov's inequality.

2. **(5 pts)**. Consider the following algorithm for approximating #Sat: Given a Boolean formula $\phi(x_1, \ldots, x_n)$,

   - Use NP oracle to decide if $\phi \in$ Sat; if not then output 0.
   - For $m = 0, 1, \ldots, n$:
     - Randomly pick $h \sim \mathcal{H}_{n,m}$;
     - Use NP oracle to decide if $\phi \in L_h$ where

       $$L_h = \{\psi \mid \exists x \in \{0,1\}^n, \psi(x) = 1 \text{ and } h(x) = 0^m\}.$$

   - Output $2^{m'}$, where m' is the largest m such that $\phi \in L_m$.

   Prove that with probability at least 3/4, the above algorithm outputs a multiplicative 16-approximation of $\#\phi = \#\{x \in \{0,1\}^n \mid \phi(x) = 1\}$. That is, the outputted number N satisfies

   $$\frac{1}{16} \cdot \#\phi \le N \le 16 \cdot \#\phi.$$

3. **(5 pts)**. Let $\varepsilon = 1/\text{poly}(n)$. Give a randomized polynomial-time algorithm with NP oracle that on input Boolean formula ϕ, with probability at least 3/4 would output a multiplicative $(1+\varepsilon)$-approximation of $\#\phi$.

Problem 4 (Closure properties of #P).

1. **(5 pts)**. Prove that #P is closed under addition and multiplication. That is, if $f, g \in$ #P, then $f + g \in$ #P and $f \cdot g \in$ #P.

2. **(10 pts)**. Prove that #P $\subseteq \mathsf{FP}^{\mathsf{PP}}$, and conclude that $\mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\mathsf{PP}}$.

   Hint. Use the closure property of #P *under addition.*

3. **(Bonus, 5 pts)**. Prove that if #P is closed under subtraction (that is, if $f, g \in$ #P and $f(x) \ge g(x)$ for every $x \in \{0,1\}^*$, then $f - g \in$ #P), then PH collapses.

   Hint. Notice that for every $S \subseteq \{0,1\}^n$, $|S| \ge 2^{n-1}$ if and only if there exists $x \in S$ such that

   $$\#\{y \in \{0,1\}^n \mid y \le x, y \in S\} = 2^{n-1}.$$

   Use this fact and the assumption to put PP *in the lower levels of* PH.