COMS 4236 – Test 2 Practice Problems

For these practice problems you may use the following Chernoff bounds.

Chernoff bounds available for this question. Let $X_1, \ldots, X_t$ be independent 0–1 random variables, $X = \sum_{j=1}^{t} X_j$, and $\mu = \mathbb{E}[X]$.

Multiplicative form. For $0 < \delta \leq 1$,

$$\Pr[X \geq (1+\delta)\mu] \leq \exp\left(-\frac{\delta^2 \mu}{3}\right),$$

$$\Pr[X < (1-\delta)\mu] \leq \exp\left(-\frac{\delta^2 \mu}{2}\right).$$

Additive form (Chernoff–Hoeffding). For $a > 0$,

$$\Pr[|X - \mu| \geq a] \leq 2\exp\left(-\frac{2a^2}{t}\right).$$

1. What would $\mathsf{L} = \mathsf{NL}$ buy at larger space bounds?

Assume $\mathsf{L} = \mathsf{NL}$. Prove that, for every space-constructible $s(n) \geq \log n$, $\mathsf{NSPACE}(s(n)) = \mathsf{DSPACE}(s(n))$. Use the configuration graph of an $s(n)$-space machine, but do not construct that graph explicitly. Account for the space used to simulate an input-head position in the graph's exponentially long encoding and to answer a request for one symbol of that encoding.

2. The strength of the reduction matters

(a) Suppose a language K is PSPACE-complete under *polynomial-time* many-one reductions and $K \in \mathsf{NL}$. Prove that $\mathsf{P} = \mathsf{PSPACE}$. Explain why the same simulation argument does not put every language in PSPACE in NL.

(b) Show unconditionally that no language in NL can be PSPACE-hard under *logspace* many-one reductions. You may use Savitch's theorem and the deterministic space hierarchy theorem.

3. Error amplification: RP versus BPP

Let A be a language and let $0 < \delta < 1/2$ be a desired error bound.

(a) Suppose a polynomial-time randomized algorithm A never accepts an input $x \notin L$ and for every $x \in L$, $Pr_r[A(x, r) = 1] \geq 1/q(n)$ where $q(n) \geq 2$ is a fixed polynomial. Give a polynomial-time algorithm that never accepts a NO instance and has error at most 2^{-n} on every YES instance. Prove that your new randomized algorithm achieves this acceptance criterion, and explain why it still runs in polynomial-time.

(b) Suppose instead that a polynomial-time randomized algorithm gives the correct membership answer with probability at least $2/3$ on every input. Give an amplification procedure with error at most δ. Identify the independent indicator variables to which you apply a concentration bound, and give an explicit sufficient number of repetitions.

For both parts, specialize your bound to $\delta = 2^{-n}$ and state whether the amplified algorithm is still polynomial-time.

4. BPP closure properties

Let $L, L' \in \mathsf{BPP}$. Is $L \cap L' \in BPP$? Justify your answer.

5. A short-seed PRG would imply P = BPP

Suppose there is a fixed constant c and a family of deterministic generators

$$G_s : \{0,1\}^{\ell(s)} \longrightarrow \{0,1\}^s, \qquad \ell(s) \le c \log s.$$

The seed length $\ell(s)$ is computable in time polynomial in s, and a single algorithm computes $G_s(z)$ from $(1^s, z)$ in time polynomial in s. For every Boolean circuit C with s input bits and at most s gates, assume

$$\left| \Pr_{z \in \{0,1\}^{\ell(s)}}[C(G_s(z)) = 1] - \Pr_{r \in \{0,1\}^s}[C(r) = 1] \right| \le \frac{1}{10}.$$

All distributions in this display are uniform. The circuit bound is measured in the *output length* s, not in the much shorter seed length.

Prove that $\mathsf{P} = \mathsf{BPP}$. Describe a deterministic simulation of an arbitrary BPP algorithm, justify its correctness on both YES and NO inputs, and bound its running time. You may use the fact that, after fixing an input x, a polynomial-time computation $A(x, r)$ has a circuit of size polynomial in $|x|$ as a function of its random bits.

6. Multiplicative Chernoff

You are given a Boolean formula φ on $n \ge 2$ variables. Let

$$p = \Pr_{a \in \{0,1\}^n}[\varphi(a) = 1],$$

where a is uniformly random. You are promised that $p \ge 1/n$, but you do not know p.

Give a sampling algorithm that outputs an estimate $\widehat{p}$ satisfying

$$\frac{p}{2} \le \widehat{p} \le \frac{3p}{2}$$

with probability at least $1 - 1/n^2$, using only $O(n \log n)$ evaluations of φ. Prove your guarantee using the multiplicative Chernoff bound.