Advanced Complexity Theory
18.405/6.841
Due: Thursday, April 12th, 2001

Dan Spielman

# Problem Set 2

1 Let ZPP = $\{A$: there is a probabilistic Turing machine accepting $A$ that, on all inputs, outputs the correct answer and runs in expected polynomial time$\}$.
Show that ZPP = RP $\cap$ co-RP.

**"Fun" with Operators:** Recall the definitions of the following operators on complexity classes.

- $L \in \Sigma \cdot \mathcal{C}$ if there exists an $L' \in \mathcal{C}$ and a polynomial $p(n)$ such that for all $x \in \{0,1\}^n$, $x \in L$ if and only if there exists a string $y$ of length $p(n)$ such that $(x, y) \in L'$. One can define $\Pi\cdot$ analogously.
- $L \in \mathrm{BP} \cdot \mathcal{C}$ if there exists an $L' \in \mathcal{C}$ and a polynomial $p(n)$ such that for all $x \in \{0,1\}^n$,
  (a) if $x \in L$ then for at least two-thirds of strings $y$ of length $p(n)$, $(x, y) \in L'$, and
  (b) if $x \notin L$ then for at least two-thirds of strings $y$ of length $p(n)$, $(x, y) \notin L'$.
- $L \in \bigoplus \cdot \mathcal{C}$ if there exists an $L' \in \mathcal{C}$ and a polynomial $p(n)$ such that for all $x \in \{0,1\}^n$,

$$x \in L \Leftrightarrow |\{y : |y| = p(|x|) \text{ and } (x, y) \in A\}| \text{ is odd.}$$

2a. Show that $\Sigma \cdot \mathrm{BP} \cdot P \subseteq NP/poly$ and $\mathrm{BP} \cdot \Sigma \cdot P \subseteq NP/poly$.
(do as much of this as you can)

2b. Also show that $\Sigma \cdot \mathrm{BP} \cdot P \subseteq \mathrm{BP} \cdot \Sigma \cdot P$.

**Analyzing Quantum Fourier Transforms:** Let $q > 2p$ and let $\omega_p = e^{2\pi i/p}$. Let $x \in \{0, \ldots, p-1\}$ and let

$$z = \lceil qx/p \rceil.$$

3a Show that there exists a constant $c$ for which $q > cp$ implies

$$\left| \frac{1}{\sqrt{pq}} \sum_{y=0}^{p-1} \omega_p^{-xy} \omega_q^{yz} \right| \geq (9/10) \sqrt{\frac{p}{q}}$$

3b Prove that for all $0 \leq u \leq 1/2$,

$$2u/\pi \leq \left| \int_0^u e^{2\pi i t} dt \right| \leq u.$$

3c For $u = l + \delta < p/2$ where $l$ is an integer and $-1/2 < \delta < 1/2$, prove that

$$\left| \sum_{y=0}^{p-1} \omega_p^{uy} \right| \leq \frac{\pi\, |\delta p|}{2u}.$$

3d Let $z' = \lceil qx'/p \rceil$, where $x'$ is an integer not equivalent to $x$ modulo $p$. Prove that

$$\frac{1}{\sqrt{pq}} \sum_{y=0}^{p-1} \omega_p^{-xy} \omega_q^{yz'} \leq \sqrt{\frac{p}{q}} \frac{\pi p}{2q \min\left(\left|x - x'\right|, p - \left|x - x'\right|\right)}.$$

4 Prove that $BQP$ is contained in $P^{\#P}$. Partial credit will be given for a proof that $BQP$ is in $PSPACE$.

5 Prove that $\sum_2^P \subseteq \mathrm{BP} \cdot \bigoplus \cdot \mathrm{BP} \cdot \bigoplus \cdot P$.

## Homework policy:

If you work with anyone else on the homework, please give them due credit (i.e., list who you worked with on which problems). Cite any sources you use, but please don't look up the answer. If you don't know the answer to a problem, then just don't answer it. Do not write anything you don't believe. Avoid making yourself believe a false proof—it damages your brain.