York University | COSC6115 | April 30, 2001

Homework Assignment #4
Due date: May 18, 2001

1. [6 marks] Let FACTORING = $\{(N, K) : N, K \in \mathbb{N}$ and N has a factor smaller than $K\}$. (As usual, N and K are represented in binary.) Show that FACTORING is in $\mathbf{NP} \cap \mathbf{coNP}$. Hint: this isn't a hard question, if you use stuff we have done in class.

2. [8 marks] Problem 10.4.6 in the text.

3. [6 marks]

[3] **(a)** Show that **BPP** is closed under union.

[3] **(b)** Show that **RP** is closed under intersection.

4. [12 marks]

[2] **(a)** Show that **RP** is closed under reductions.

[8] **(b)** Show that if SAT is in **BPP**, then SAT is also in **RP**. Hint: read Example 10.3 on page 228 of the text. Also, remember that you can "amplify" a **BPP** algorithm so that the probability that it makes a mistake is really tiny.

[2] **(c)** Show that $\mathbf{NP} \subseteq \mathbf{BPP}$ implies $\mathbf{NP} = \mathbf{RP}$.

5. [9 marks] Let MAJORITY-CIRCUIT-SATISFIABILITY (MCS) be the problem of determining whether a given circuit has the value TRUE for more than half of its inputs (i.e. for at least $2^{m-1} + 1$ of the 2^m possible inputs to the circuit if there are m variable gates in the circuit). Show that MCS is **PP**-complete. Hint: think about the constructions we used to show that CVP is **P**-complete and CIRCUIT-SAT is **NP**-complete.

6. [9 marks]

[3] **(a)** Let A be an array of n elements. Each element is either 0 or 1. Explain how an EREW PRAM can find the leftmost 1 in the array using $O(\log n)$ time and $O(n)$ work.

[3] **(b)** Let S and T be two strings of length n. They are stored as arrays of characters. Show how an EREW PRAM can compare the two strings (to see which one comes first alphabetically) using $O(\log n)$ time and $O(n)$ work.

[3] **(c)** Show how a CRCW PRAM can check whether the two strings S and T are equal using $O(1)$ time and $O(n)$ work.