Practice exam Computational Complexity

Friday 27 February 2017

You're allowed to use the book and any paper notes you have brought. Using electronic devices is not allowed.

When using a result from the book, please mention the theorem number or page number.

Definition 1. Define **ZPP** to be the class of languages L for which there is a constant c and a polytime TM M which outputs either 0, 1 or ?, such that for all $x \in \{0,1\}^*$,

$$\Pr_r[M(x,r) = ?] \leq 1/2,$$
$$\text{if } M(x,r) = 1, \text{ then } x \in L,$$
$$\text{if } M(x,r) = 0, \text{ then } x \notin L,$$

where r is drawn from the uniform distribution over $\{0,1\}^{|x|^c}$. To get $\mathbf{ZPP}^O$ one replaces the above M by the oracle TM M^O.

Question 1. (2 pts) Prove: $\mathbf{ZPP}^{\mathbf{ZPP}} = \mathbf{ZPP}$.
Use the above definition of **ZPP** or the definition in the book.

Definition 2. Let L be a language. We say L is *length-decreasing self-reducible* if there is a polytime oracle TM M, such that

$$x \in L \iff M^L(x) = 1,$$

and the computation of $M^L(x)$ only queries L on strings of length strictly less than $|x|$.

Question 2. (2 pts) Let L be a language such that $L \subseteq \{0\}^*$.
Prove: L is in **P** if and only if L is length-decreasing self-reducible.

Please see next page.

Question 3. (2.5 pts) Show that there is an oracle A such that $\mathbf{P}^A \neq \mathbf{ZPP}^A$.

Hint. This statement is a strengthening of Theorem 3.7 of Baker, Gill and Solovay. Use the language $L_A = \{0^n \mid \exists y \text{ such that } 1y \in A \cap \{0,1\}^n\}$. Define a function f by $f(1) = 2$ and $f(i+1) = 2^{f(i)}$. Define A in stages, where you diagonalise against polytime Turing machine i at length $f(i)$. Make sure L_A is in $\mathbf{ZPP}^A$: for every stage i either put many strings of the form $0y$ in A or put many strings of the form $1y$ in A.

Definition 3. We define the circuit class A as the class of languages L that can be decided by a family of circuits $\{C_n\}_{n\in\mathbb{N}}$, in the sense that C_n decides $L \cap \{0,1\}^n$, where C_n has constant depth and consists only of

- fan-in 2 AND gates, $\wedge_2$
- fan-in 2 OR gates, $\vee_2$
- NOT gates, $\neg$
- unbounded fan-in XOR gates, $\oplus$.

Question 4. (2.5 pts) Let $L = \{1\}^*$, the language of strings consisting of ones.

(a) Prove: L is not in A.

(b) Define a new class B by changing *constant dept* to *log depth* in the definition of A. Prove: L is in B.

Hint. Use the degree of polynomials over the finite field of size 2.

End of exam.