Qualifying Examination

Theoretical Computer Science

Thursday, March 14, 2013

Part II: Automata and Complexity

Instructions:

1. This is a closed book exam.
2. The exam has four problems worth 25 points each. Read all the problems carefully to see the order in which you want to tackle them. You have all day (9am–5pm) to solve the problems.
3. Write clearly and concisely. You may appeal to some standard algorithms/facts from text books unless the problem explicitly asks for a proof of that fact or the details of that algorithm.
4. If you cannot solve a problem, to get partial credit write down your main idea/approach in a clear and concise way. For example you can obtain a solution assuming a clearly stated lemma that you believe should be true but cannot prove during the exam. However, please do not write down a laundry list of half baked ideas just to get partial credit.

May the force be with you.

Problem 1: Let $\mathcal{C}$ be a class of languages closed under concatenation, intersection, homomorphic images, inverse homomorphic images, and intersection with regular languages. Prove that $\mathcal{C}$ is also closed under union.

Problem 2: Let N be an NFA over the unary alphabet $\{0\}$. Prove that the problem of checking $L(N) = \{0\}^*$ is in co-NP.

Problem 3:

The complexity class **ZPP** is defined to be the class of languages which have "Las Vegas" algorithms: a randomized algorithm A is said to be a Las Vegas algorithm for a language L if:

- *(zero-error)*: on input $x \notin L$, A outputs 0 with probability 1, and on input $x \in L$ it outputs 1 with probability 1,
- *(expected polynomial time)*: there is a polynomial p such that, on any input x, the *expected* running time of A is at most $p(|x|)$.

(A) (Simple) Show that $\mathbf{ZPP} = \mathbf{coZPP}$, where **coZPP** is the class of languages L such that its complement $\overline{L} \in \mathbf{ZPP}$.

(B) (Simple) Use the above to how that if $\mathbf{ZPP} \subseteq \mathbf{X}$, then $\mathbf{ZPP} \subseteq \mathbf{X} \cap \mathbf{coX}$, where **X** is an arbitrary set of languages and **coX** is the set of languages whose complements are in **X**.

(C) The complexity class **RP** is defined as the class of languages for which there is a bounded error probabilistic polynomial time algorithm which never produces false-positives. That is, $L \in \mathbf{RP}$ iff there is an algorithm A such that:

- *(one-sided error)*: on input $x \notin L$, A outputs 0 with probability 1, and on input $x \in L$ it outputs 1 with probability at least $\frac{1}{2}$.
- *(strict polynomial time)*: there is a polynomial p such that, on any input x, the running time of A (for any choice of random tape) is at most $p(|x|)$.

Show that $\mathbf{ZPP} \subseteq \mathbf{RP}$.

(D) Show that $\mathbf{RP} \cap \mathbf{coRP} \subseteq \mathbf{ZPP}$. Conclude, from the above that $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$.

Problem 4:

In this problem, we are interested in two objects related to a function $f : \{0,1\}^n \to \{0,1\}$.

- A boolean circuit (using AND, OR and NOT gates) for computing f. All gates have fan-in 2. We are interested in the *depth* of such a circuit which is defined as the most number of AND/OR gates encountered in a path from the output wire to an input wire.
- A communication problem related to f, defined as follows. Alice gets an input x such that $f(x) = 0$ and Bob gets an input y such that $f(y) = 1$, and after exchanging some

messages, they must both output i such that $x_i \neq y_i$. (Clearly $x \neq y$ and therefore there must be at least one position i such that $x_i \neq y_i$.) We are interested in the maximum number of bits exchanged in this protocol (maximum over all pairs (x, y)).

Answer the following problems.

(A) (Simple) Show that any function $f : \{0,1\}^n \to \{0,1\}$ has a protocol for the above task, in which most $n + \lceil \log_2 n \rceil$ bits are exchanged. Can you suggest a slight improvement to reduce this number by 1?

(B) (Simple) Show that any function $f : \{0,1\}^n \to \{0,1\}$ has a circuit (with fan-in 2) of depth at most $n+\lceil \log_2 n \rceil$. Can you suggest a slight improvement to reduce this number by 1?

(C) Given a circuit of depth d for f, give a protocol for the above task in which at most d bits are exchanged. Argue the correctness of the protocol.

(D) Argue the converse, that any protocol for the above communication problem can be turned into a circuit of depth equal to the maximum number of bits exchanged in the protocol.