Final Exam

CAS705

December 20, 2004

Examiner: Michael Soltys

Duration: 3hrs

1. Show how to restrict the transition function of a Turing machine so that it recognizes precisely the set of (i) Regular languages, and (ii) Context-free languages.

2. Show that there exists an oracle A with respect to which $\mathbf{NP}^A \neq \mathbf{co\text{-}NP}^A$.

3. Prove that $\mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC}^2$.

4. Prove that

$$\text{CIRCUIT-SAT} = \{\langle C \rangle \mid C \text{ is a satisfiable Boolean circuit } \}$$

is **NP**-complete. Give your proof in the style of Cook's theorem (in the sense that you show that for all $A \in \mathbf{NP}$, $A \leq_p$ CIRCUIT-SAT).

5. Show that 2SAT is in **NL**.

6. Show that if $\mathbf{PH} = \mathbf{PSPACE}$, then the polynomial time hierarchy, **PH**, has only finitely many distinct levels.

7. Prove that all symmetric Boolean functions can be computed with circuits of linear size, i.e., of size $O(n)$, where n is the number of inputs.

8. Let $\mathbf{LINTIME} = \mathrm{TIME}(n)$ and $\mathbf{NLINTIME} = \mathrm{NTIME}(n)$. That is, **LINTIME** and **NLINTIME** denote time $O(n)$ on a deterministic and nondeterministic TM.

   (a) Show that **LINTIME** is not as robust as polynomial time; that is, show that there exists a language decidable in linear time on two tapes, but not decidable in linear time on a single tape (Hint: PALINDROMES.) (Aside: It is plausible, but not known, that for every k, there is a language decidable in linear time on $k+1$ tapes, but not on k tapes.)

   (b) Show that **NLINTIME** is more robust, in the sense that every set in this class can be accepted by a two tape nondeterministic linear time TM.

   Define $\Sigma_0^{\text{lin}} = \mathbf{LINTIME}$ and $\Sigma_{i+1}^{\text{lin}} = \mathbf{NLINTIME}^{\Sigma_i^{\text{lin}}}$. That is, $\mathbf{NLINTIME}^{\Sigma_i^{\text{lin}}}$ denotes the class of languages decidable in nondeterministic linear time with a Σ_i^{lin} oracle.

(c) Show that an equivalent definition of Σ_i^{lin} is the class of languages decidable in linear time on an alternating TM, with i alternations, beginning with an existential state.

(d) Show that yet another equivalent definition is in terms of quantifiers and linear time predicates. Give this definition first, and then show that it is equivalent to the other two.

Let $\mathbf{LTH} = \bigcup_{i=0}^{\infty} \Sigma_i^{\text{lin}}$, i.e., the linear time hierarchy. Let $\text{NTIMESPACE}(f(n), g(n))$ be the class of languages decided simultaneously in time $O(f(n))$ and space $O(g(n))$ on a nondeterministic (multitape) TM.

(e) **Nepomnjascij's Theorem:** Let $0 < \varepsilon < 1$ be a rational number, and let a be a positive integer. Then,

$$\text{NTIMESPACE}(n^a, n^\varepsilon) \subseteq \mathbf{LTH}$$

(Fat Hint: Suppose M is a nondeterministic TM running in time n^a and space n^ε. Then, M accepts an input x iff

$$\exists \mathbf{y}[\ \mathbf{y} \text{ represents an accepting computation for } x\ ] \tag{1}$$

So $\mathbf{y} = y_1 y_2 \ldots y_{n^a}$ where each $|y_i| = n^\varepsilon$, and so $|\mathbf{y}| = n^{a+\varepsilon}$. So $\mathbf{y}$ is too long to verify in linear time (in $n = |x|$). So we use a trick: let $\mathbf{z} = z_1 z_2 \ldots z_{n^{1-\varepsilon}}$ where the z_i represent every $(n^{a-1+\varepsilon})$-th string in $\mathbf{y}$. So now, (1) can be restated as follows:

$$(\exists \mathbf{z})(\forall i)(\exists \mathbf{u})[\ \mathbf{u} \text{ shows } z_{i+1} \text{ follows from } z_i \text{ in } n^{a-1+\varepsilon} \text{ steps } \&\ z_n \text{ is accepting }]$$

Did we improve things? What next?)

9. Show that $\mathbf{BPP} \subseteq \mathbf{P/poly}$. That is, show that every language in $\mathbf{BPP}$ has polynomial size circuits. Your circuits—most likely—will not be uniform (i.e., the map $n \mapsto C_n$ will not be polynomial time); why?

(Hint: Recall that it was mentioned in class that probabilistic TMs can be defined as deterministic TM with an oracle tape where once at the beginning a random string of a certain length appears. Define **BPP** in such a manner. Given such a TM M, explain briefly how to transform it to a polysize circuit $C(x; y)$ where x is the input string and y is the *random* string. Explain the relationship between x and y. Argue that for all x's of a certain length n, there must exist a random string y_n that "works" for all such x. Chernoff bound.)

10. A polynomial time onto function $f : \{0,1\}^* \longrightarrow$ TAUTOLOGIES is what we call a proof system. If $f(x) = \phi \in$ TAUTOLOGIES, then we say that x is a proof of ϕ. We say that a proof system is poly-bounded if there exists a polynomial $p(n)$ such that for every $\phi \in$ TAUTOLOGIES, there exists an $x \in \{0,1\}^*$ such that $|x| \leq p(|\phi|)$ and $f(x) = \phi$. Prove that a poly-bounded proof system exists iff $\mathbf{NP} = \mathbf{coNP}$.

End of Exam