UNIVERSITY OF EDINBURGH

FACULTY OF SCIENCE AND ENGINEERING

MASTER OF SCIENCE IN COMPUTER SCIENCE

COMPUTATIONAL COMPLEXITY

Monday 1 May 2000

9:30 to 11:00

Examiners:

I. Watson (External)

R.N. Ibbett (Chairman)

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

1. Savitch's Theorem states the following:

   The inclusion $\text{NS}\textsc{pace}(S(n)) \subseteq \text{DS}\textsc{pace}(S(n)^2)$ *holds for every space-constructible function* $S(n) \geq \log n$.

   (a) Prove Savitch's Theorem. Concentrate on covering the key ideas behind the proof. At what point in the proof is the assumption $S(n) \geq \log n$ used? [*13 marks*]

   (b) For every deterministic complexity class (e.g., P) there is a corresponding nondeterministic class (e.g., NP). However, the complexity class "NPSPACE" of languages accepted by some polynomial-space-bounded nondeterministic Turing machine is rarely mentioned. Why is this? [*6 marks*]

   (c) We know that $\text{NS}\textsc{pace}(\log n) \subseteq \text{P}$. Does it follow from this fact and your answer to part (a) that every language in $\text{NS}\textsc{pace}(\log n)$ is accepted by a deterministic Turing machine that uses $O((\log n)^2)$ space and runs in polynomial time? Explain your answer. [*6 marks*]

2. (a) Recall that a language $L \subseteq \Sigma^*$ belongs to the class RP if there exists a polynomial-time Turing machine M such that, for all $x \in \Sigma^*$,

$$\Pr(M \text{ accepts } x) \begin{cases} \geq \frac{1}{2}, & \text{if } x \in L; \\ = 0, & \text{otherwise.} \end{cases}$$

Prove a "powering lemma" for RP: namely, show that the language class RP remains unaltered if the acceptance probability in the above definition is increased to $1 - 2^{-|x|}$. [*7 marks*]

(b) A *polynomial non-identity* is a true assertion of the form $Q \not\equiv R$, where Q and R are built from integer constants and variables using $+$, $\times$ and bracketing. Prove that the language of polynomial non-identities is in RP. You may use without proof the following lemma:

> *Let $P \not\equiv 0$ be a polynomial of degree d in variables $x_0, \ldots, x_{n-1}$. Then the number of zeros of P that lie in the set $\{0, 1, \ldots, 2d-1\}^n$ is at most $\frac{1}{2}(2d)^n$.* [*10 marks*]

(c) Suppose it could be shown that the language of polynomial identities (i.e., true assertions of the form $Q \equiv R$) is also in RP. Demonstrate that there would exist a probabilistic Turing machine M with the following specification:

- M correctly identifies polynomial identities and non-identities;
- the expected run-time of M is polynomial in the input length. [*8 marks*]

3. Two possible complexity classes capturing the notion of "exponential-time computability" are:

$$\textsc{Exp} = \bigcup_{k=1}^{\infty} \mathrm{D}\textsc{Time}(2^{n^k})$$

and

$$\mathrm{E} = \bigcup_{k=1}^{\infty} \mathrm{D}\textsc{Time}(2^{kn}).$$

(a) Prove that the class $\textsc{Exp}$ is closed under polynomial-time reducibility; i.e., if $L \in \textsc{Exp}$ and $L' \leq_{\mathrm{P}} L$ then $L' \in \textsc{Exp}$. *[6 marks]*

(b) If L is any language in $\mathrm{D}\textsc{Time}(2^{n^2})$, then the "padded" language

$$L_{\text{pad}} = \{x \underbrace{\#\# \ldots \#}_{|x|^2 \text{ times}} : x \in L\}$$

is in $\mathrm{D}\textsc{Time}(2^n)$. Using this fact (which you need not prove), show that the class E is *not* closed under polynomial-time reducibility. *[7 marks]*

(c) In the light of your answers to parts (a) and (b), which of the classes $\textsc{Exp}$ or E seems to provide the better definition of exponential-time computability? *[2 marks]*

(d) Consider the following two facts:

- the "Succinct Circuit Value Problem" (SCVP) is complete for $\textsc{Exp}$ with respect to polynomial-time reducibility;
- there is a language in $\textsc{Exp}$ that is not in $\mathrm{D}\textsc{Time}(2^n)$.

Deduce the existence of a constant $\alpha > 0$ such that SCVP $\notin \mathrm{D}\textsc{Time}(2^{n^\alpha})$. *[10 marks]*