UNIVERSITY OF EDINBURGH

FACULTY OF SCIENCE AND ENGINEERING

COMPUTER SCIENCE FOUR

COMPUTATIONAL COMPLEXITY

Thursday 19 April 2001

09:30 to 11:00

Examiners:

Prof. K. Turner (External)

Prof. G. Plotkin (Chairman)

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

1. (a) Define the language classes NP and PSpace. *[4 marks]*

   (b) Prove, by direct simulation, that NLog $\subseteq$ NP $\subseteq$ PSpace, where NLog $=$ NSpace$(\log n)$. *[13 marks]*

   (c) Recall that Sat is the language of (encodings of) all satisfiable Boolean formulas in CNF, and that TQBF is the language of all true quantified Boolean formulas (with no free variables). Consider the four assertions:

      i. Sat $\in$ NP,

      ii. Sat $\in$ NLog,

      iii. TQBF $\in$ NP, and

      iv. TQBF $\in$ NLog.

   Under the assumption NLog $\subset$ NP $\subset$ PSpace (note the *strict* inclusions here), which of (i)–(iv) are known to be true, which known to be false, and which are open? Briefly justify your answers. *[4 marks]*

   (d) Repeat part (c) but in the absence of the assumption of strict inclusions between the complexity classes. *[4 marks]*

2. (a) Suppose CON is the language of (encodings of) all directed graphs G on vertex set $\{0, 1, \ldots, n-1\}$ such that there is a path from 0 to $n-1$ in G. Demonstrate that CON $\in$ NLOG, where NLOG = NSPACE($\log n$). [*8 marks*]

(b) Prove that CON is hard for NLOG with respect to log-space reducibility. [*8 marks*]

(c) Suppose UNCON is the language of all directed graphs G on vertex set $\{0, 1, \ldots, n-1\}$ such that there is *no* path from 0 to $n-1$ in G. Suppose 2-SAT is the language of satisfiable CNF formulas with at most two literals per clause. Let f be the function that maps directed graphs G on vertex set $\{0, 1, \ldots, n-1\}$ to CNF formulas φ on variable set $\{x_0, x_1, \ldots, x_{n-1}\}$ defined as follows: if E is the edge set of G then the clauses forming the formula $\varphi = f(G)$ are $(\neg x_i \vee x_j)$, for all $(i, j) \in E$, together with the two clauses (x_0) and $(\neg x_{n-1})$. Prove that f is a log-space reduction from UNCON to 2-SAT. [*9 marks*]

3. This question concerns an extension to the familiar Boolean circuit model, which is intended to capture randomised computation. A *probabilistic* Boolean circuit C is a Boolean circuit whose input nodes are of two kinds: *ordinary* and *probabilistic*. Suppose C has n ordinary input nodes and p probabilistic ones, and let $C(x_0, \ldots, x_{n-1}, v_0, \ldots, v_{p-1})$ denote the output of C when presented with Boolean values $(x_0, \ldots, x_{n-1})$ at the ordinary input nodes and Boolean values $(v_0, \ldots, v_{p-1})$ at the probabilistic ones. We say that C *computes* the Boolean function $f : \{0,1\}^n \to \{0,1\}$ if and only if:

   (i) $f(x_0, \ldots, x_{n-1}) = 0$ entails $C(x_0, \ldots, x_{n-1}, v_0, \ldots, v_{p-1}) = 0$ for all of the 2^p possible truth assignments to $(v_0, \ldots, v_{p-1})$;

   (ii) $f(x_0, \ldots, x_{n-1}) = 1$ entails $C(x_0, \ldots, x_{n-1}, v_0, \ldots, v_{p-1}) = 1$ for at least half of the 2^p possible truth assignments to $(v_0, \ldots, v_{p-1})$.

   This completes the description of the model.

   (a) What would it mean to say that a language $L \subseteq \{0,1\}^*$ has "polynomial-size uniform probabilistic circuits"? [*4 marks*]

   (b) Define the complexity class RP (Randomised Polynomial time). [*3 marks*]

   (c) Prove that every language in RP has polynomial-size uniform probabilistic circuits. [*12 marks*]

   (d) Suppose that part (ii) of the definition above is tightened by changing "at least half" to "at least a fraction $1 - 2^{-n}$". Show that result proved in part (c) remains true under this more demanding notion of computation. [*6 marks*]