UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday, 4 June, 2013 1:30 pm to 3:30 pm

PAPER 59

COMPUTATIONAL COMPLEXITY

Attempt no more than ***THREE*** *questions.*

There are ***FOUR*** *questions in total.*

The questions carry equal weight.

STATIONERY REQUIREMENTS
Cover sheet
Treasury Tag
Script paper

SPECIAL REQUIREMENTS
None

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1

(a) State and prove the Cook-Levin Theorem.

(b) Let 2UN-SAT be the language of satisfiable boolean formulae in conjunctive normal form in which at most 2 variables in each clause appear un-negated. An example of such a formula is

$$(x_1 \vee x_2) \wedge (\neg x_2 \vee x_4 \vee x_5) \wedge (\neg x_1 \vee \neg x_4)\,.$$

Show that 2UN-SAT is NP-complete.

2

(a) Define the complexity classes $\mathsf{SPACE}(s(n))$ and $\mathsf{NSPACE}(s(n))$ and prove Savitch's Theorem: for any function $s : \mathbb{N} \to \mathbb{N}$ such that $s(n) \geqslant \log_2 n$, $\mathsf{NSPACE}(s(n)) \subseteq \mathsf{SPACE}(s(n)^2)$.

(b) The k-layering $G^{(k)}$ of a directed graph $G = (V, E)$ is the graph whose nodes are indexed by pairs (v, i), where $v \in V$, $1 \leqslant i \leqslant k$, and there is an arc $(u, i) \to (v, j)$ if and only if $j = i + 1$ and either $u = v$ or $(u, v) \in E$.

Let $\textsc{Cycle}$ be the language of directed graphs G such that G contains a cycle, where a cycle is a directed path whose final node is the same as its initial node.

By considering layerings, or otherwise, show that $\textsc{Cycle}$ is NL-complete. You may assume that $\textsc{Path}$ is NL-complete, where $\textsc{Path}$ is the language of triples (G, s, t) such that there is a path in the directed graph G from node s to node t.

3

(a) Define the complexity classes $\mathsf{SIZE}(T(n))$ and $\mathsf{P/poly}$. Prove that $\mathsf{P/poly} \neq \mathsf{NP}$.

(b) Prove that, for any $\mathcal{L} \subseteq \{0,1\}^*$, $\mathcal{L} \in \mathsf{SIZE}(O(n2^n))$.

(c) Let Circuit Value be the language of pairs (C, x), where $x \in \{0,1\}^n$ (for some n) and C is the description of an n-input circuit, such that $C(x) = 1$. Let the language And-Not Circuit Value be defined similarly, but where C is restricted such that all its gates are either AND or NOT gates.

Prove that And-Not Circuit Value is P-complete. [You may assume that Circuit Value is P-complete.]

(d) Let Mod3 be the language $\{x \in \{0,1\}^* : x \equiv 0 \pmod 3\}$, where x is interpreted as a non-negative integer written in binary.

Define the complexity class NC^1 and show that Mod3 $\in \mathsf{NC}^1$. [*Hint:* $2^m \equiv (-1)^m (\mathrm{mod} 3)$.]

4

For $f : \{0,1\}^n \to \{0,1\}$, let $D(f)$ denote the minimal depth of a decision tree that computes f. f is said to be *evasive* if $D(f) = n$.

(a) Let $\mathrm{wt}(x) = |\{i : x_i = 1\}|$. Show that, if there is a decision tree of depth $d < n$ which computes $f : \{0,1\}^n \to \{0,1\}$, then $\sum_{x \in \{0,1\}^n} (-1)^{\mathrm{wt}(x)} f(x) = 0$.

(b) An undirected graph G is said to be a *star* if there is a distinguished vertex v_0 such that every edge in G has v_0 as an endpoint. For example, the graph on vertices $\{1,2,3,4\}$ with edges $\{(1,3),(1,4)\}$ is a star.

The function $\mathrm{STAR}_n : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ is defined as follows. The bits of each $G \in \{0,1\}^{\binom{n}{2}}$ are indexed by pairs of distinct integers (i,j), $1 \leqslant i, j \leqslant n$. G corresponds to an undirected graph on n vertices, with bit (i,j) of G being set to 1 if there is an edge (i,j) in the graph. Then $\mathrm{STAR}_n(G) = 1$ if and only if G is a star.

Show that, for $n \geqslant 3$, STAR_n is evasive. [*Hint: (a) may be useful.*]

(c) Define the notion of *certificate complexity* and prove that the certificate complexity of STAR_n is $\Omega(n^2)$.

END OF PAPER