UNIVERSITY OF CAMBRIDGE

MAMA/124, NST3AS/124, MAAS/124

MAT3

MATHEMATICAL TRIPOS Part III

Friday 31 May 2024 1:30 pm to 3:30 pm

PAPER 124

INTRODUCTION TO COMPUTATIONAL COMPLEXITY

Before you begin please read these instructions carefully

Candidates have TWO HOURS to complete the written examination.

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
Rough 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 (i) Prove that if $\mathbf{P} \neq \mathbf{NP}$, then there is a problem in **NP** that is neither in **P** nor **NP**-complete. [Any facts you might need about encodings of problems or Turing machines as bit sequences may be assumed.]

(ii) Show that the following problem is **NP**-complete. The input is a system of m quadratic equations over $\mathbb{F}_2$ in n variables $x_1, \ldots, x_n$ and the output is 1 if they have a solution. Here a *quadratic equation* is an equation of the form $\sum_{i,j} a_{ij}x_ix_j + \sum_i b_ix_i + c = 0$, where the coefficients a_{ij}, b_i, c belong to $\mathbb{F}_2$. [Hint: consider the quadratic equation $(1-u)(1-v) = (1-w)$.]

2 (i) What does it mean for a function to be **NL**-*complete*? Given an example of an **NL**-complete function and explain briefly why it is **NL**-complete. [You may assume the definition of **NL**.]

(ii) Prove that **NL** = co-**NL**.

(iii) A directed graph is said to be *strongly connected* if for every pair of vertices u, v there is a directed path from u to v and a directed path from v to u. Prove that the problem of determining whether a directed graph is strongly connected is **NL**-complete.

3 (i) Suppose that $\mathbf{NP} \subset \mathbf{P}/\text{poly}$. Show that for every function $f \in \mathbf{NP}$ there is a family of circuits (C_n) of polynomial size such that for every n and every input x of size n, if $f(x) = 1$ then the output of $C_n(x)$ is a certificate that $f(x) = 1$ that can be verified in polynomial time.

(ii) Prove that if $\mathbf{NP} \subset \mathbf{P}/\text{poly}$, then the polynomial hierarchy collapses to Σ_2^P.

(iii) Let A be an oracle such that $\mathbf{P}^A = \mathbf{NP}^A$. Must it be the case that $\mathbf{P}^A = \mathbf{PH}^A$?

4 (i) Define the complexity class **RP**, and prove that $\mathbf{RP} \subset \mathbf{P}/\text{poly}$.

(ii) The complexity class **ZPP** can be defined to be the intersection of **RP** and co-**RP**. An alternative definition is that f belongs to **ZPP** if there is a Turing machine T with an infinite supply of random bits such that for every x, the expected time for T to halt is at most polynomial in $|x|$ (so in particular, T halts with probability 1), and if T halts, then it outputs $f(x)$. Prove that these two definitions are equivalent.

(iii) Show that primality testing belongs to co-**RP**. [You may assume divisibility results concerning binomial coefficients, and also a lower bound for the number of monic irreducible polynomials of degree d over $\mathbb{F}_p$ when p is prime.]

END OF PAPER