UNIVERSITY OF CAMBRIDGE

MAMA/124, NST3AS/124, MAAS/124

MAT3

MATHEMATICAL TRIPOS Part III

Friday, 9 June, 2023 9:00 am to 11:00 am

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 **FIVE** 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) The *majority function* $f_{n,r} : \{0,1\}^n \to \{0,1\}$ takes the value 1 if and only if at least r of its inputs take the value 1. Prove that if $0 < r < n$, then the decision-tree depth of $f_{n,r}$ is n.

(ii) State the switching lemma.

(iii) Let n be even. Prove that a layered circuit of depth d (with alternations of AND and OR gates) that computes the majority function $f_{n,n/2}$ must have size at least $\exp(cn^{1/d-1})$ for an absolute constant $c > 0$. [You may assume the switching lemma, and also the Chernoff estimate $\mathbb{P}[X < (1-\delta)\mu] \leqslant e^{-\delta^2\mu/2}$, where X is a sum of independent random variables taking values in $[0,1]$ and $\mu = \mathbb{E}X$. Any other lemmas you might need should be proved.]

2 Let $\mathcal{L}$ be the lattice of subsets of $\{0,1\}^n$ of the form $\lceil A \rceil$, where A is an r-closed subset of $[n]^{(\leqslant l)}$. Throughout this question, assume that $2(r-1)m \leqslant n$ and $l^2 \leqslant m$.

(i) Define the operations $\sqcap$ and $\sqcup$ that make $\mathcal{L}$ into a lattice, and state a lemma concerning the difference between a set A computed by a monotone circuit of size at most M and the set $\tilde{A} \in \mathcal{L}$ computed in the corresponding way using the operations $\sqcap$ and $\sqcup$ in the place of $\cap$ and $\cup$.

(ii) Prove that if A is r-closed, then either $\lceil A \rceil$ is the set of all graphs or it contains at most half the cliques of size m.

(iii) Prove that if A and B are closed sets, then $\delta_\sqcap(\lceil A \rceil, \lceil B \rceil)$ contains at most $4.2^{-l/2}\binom{n}{m}$ cliques of size m.

(iv) Prove that if A and B are closed sets, then $\delta_\sqcup(\lceil A \rceil, \lceil B \rceil)$ contains a proportion of at most $n^l 2^{-r}$ of the complete $(m-1)$-partite graphs.

(v) Explain very briefly why these facts show that the monotone complexity of the clique function is exponentially large in a power of the number of inputs.

(vi) Let g_m be the function defined on graphs G by setting $g_m(G)$ to equal 1 if and only if G does not contain an independent set of size m. Deduce that (for suitable m that depends on the number of vertices) the monotone complexity of g_m is also exponentially large.

3 (i) Let a, b, c and d be four indeterminate variables. Show that there are three polynomials of the form $L(a, b, c, d)M(a, b, c, d)$, where L and M are linear in a, b, c, d (in other words, three rank-1 quadratic forms), such that the three polynomials ac, bd, and $ad + bc$ all belong to their linear span.

(ii) Let $f(k)$ be the smallest number of times two digits need to be multiplied together when one is computing a product of two numbers with 2^k digits each. Use the answer to part (i) to show that $f(k + 1) \leqslant 3f(k)$. Deduce that there is an algorithm for computing the product of two n-digit numbers that requires $O(n^\alpha)$ multiplications, where $\alpha = \log 3/ \log 2$ (beating long multiplication, which needs more like n^2 multiplications). [You may choose whether to consider numbers represented in base 10 or in base 2.]

(iii) A *Horn clause* is a disjunction of literals, at most one of which is positive. (Examples of Horn clauses are $x \vee \neg y \vee \neg z$, $\neg x \vee \neg y$, and x.) Show that there is a polynomial-time algorithm for determining whether a CNF formula in which all the clauses are Horn clauses is satisfiable. [Hint: show first that if all clauses contain at least two literals, then the formula is satisfiable.]

4 (i) Give a high-level account of how to prove that $\#3\mathrm{SAT}^{\mathrm{bal}}$ (counting solutions to instances of 3SAT with the same number of occurrences of x_i and $\neg x_i$ for each i) can be polynomially reduced to computing the permanent of a matrix that takes values in $\{-1, 0, 1\}$. [You should describe the gadgets used and explain how they do what they do, but do not need to give all the details of the arguments. In particular, if a fact can be proved by a routine case analysis, you can simply state the conclusion. You may also assume definitions and basic facts associated with cycle covers.]

(ii) Let M be an $n \times n$ matrix, each of whose entries is an integer between 0 and $2^n - 1$. Give a method that constructs in polynomial time a 01-matrix N with the same permanent. [Hint: for each edge weight in the corresponding directed graph, consider its binary expansion.]

5 (i) State and prove the theorem of Razborov and Rudich concerning the natural-proofs barrier to obtaining lower bounds for circuit complexity.

(ii) A *formal complexity measure* on the set of functions $f : \{0, 1\}^n \to \{0, 1\}$ is a function μ with the following properties.

1. If $f(x) = x_i$ for every x, or $f(x) = 1 - x_i$ for every x, then $\mu(f) = 1$.
2. For every f, g, $\mu(f \wedge g) \leqslant \mu(f) + \mu(g)$.
3. For every f, g, $\mu(f \vee g) \leqslant \mu(f) + \mu(g)$.

Prove that if μ is a formal complexity measure, then $\mu(f)$ is a lower bound for the size of the smallest formula that computes f.

END OF PAPER