UNIVERSITY OF CAMBRIDGE

MAMA/324, NST3AS/324, MAAS/324

MAT3

MATHEMATICAL TRIPOS Part III

Monday 9 June 2025 1:30 pm to 3:30 pm

PAPER 324

QUANTUM COMPUTATION

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

(a) Consider any finite group G with identity element e, and any set X. An action of G on X is a map $F : G \times X \to X$ that associates a function $F(g, \cdot) : X \to X$ to each group element g. In particular, F associates the identity function $x \mapsto x$ with e, and for any pair of group elements $g, h \in G$ it holds that $F(gh, x) = F(g, F(h, x))$. Consider the set $\mathsf{Stab}_F(x) = \{g \in G \mid F(g, x) = x\}$ of *stabilisers* of x under the action F.

(i) Show that $\mathsf{Stab}_F(x)$ is a subgroup of G for any fixed $x \in X$.

(ii) Fix $x \in X$ and suppose you are given a function $f_x : G \to X$ such that $f_x(g) = F(g, x)$ for each $g \in G$. Explain how the problem of determining $\mathsf{Stab}_F(x)$ from an oracle for f_x can be formulated as a Hidden Subgroup Problem for G.

(b) Now fix a positive integer N and consider the group action of $\mathbb{Z}_N$ on the set $X = \{0 < x < N \mid \gcd(x, N) = 1\}$, defined by $F(z, x) \equiv x^z \mod N$ for each $z \in \mathbb{Z}_N$ and $x \in X$. Let $\mathcal{H}_N$ be an N-dimensional state space with standard orthonormal basis $\mathcal{B} = \{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. For each $x \in X$, let U_x denote the operator on $\mathcal{H}_N$ defined by $|y\rangle \mapsto |xy \mod N\rangle$ for all $y \in \mathbb{Z}_N$.

(i) Prove that U_x is unitary.

(ii) Fix an element $a \in X$ and let $1 \leqslant r < N$ be the smallest value such that $a^r \equiv 1 \mod N$. Show that the states

$$|\psi_s\rangle := \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} \, |F(k, a)\rangle$$

are eigenvectors of U_a for each $0 \leqslant s < r$, and compute the corresponding eigenvalues.

(iii) Prove that $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle = |1\rangle$.

(iv) Given a copy of the state $|1\rangle$, outline a procedure using the quantum phase estimation algorithm to output (with constant probability) an m-bit approximation to s/r for a value of $0 \leqslant s < r$ drawn uniformly at random. You may quote and use results about quantum phase estimation without proof.

2

(i) Consider a linear system of equations $Ax = b$ with $x, b \in \mathbb{C}^N$ and A Hermitian. State the conditions required on A and b for the Harrow-Hassidim-Lloyd (HHL) quantum algorithm to run in time $O(\text{poly}\log N)$ and output a normalised state $|\xi\rangle$ that is proportional to the solution vector x, with high probability (ignoring issues of precision).

(ii) Suppose U is an implementation of the HHL algorithm in the following sense: on the N-dimensional Hilbert space $\mathcal{H}$, the unitary U performs the map

$$U|b\rangle = p|\xi\rangle + q|\phi\rangle \ ,$$

where $p, q \in (0, 1)$, $|b\rangle$ is the normalised quantum state corresponding to the vector b in the definition of the linear system, $|\xi\rangle$ is as defined above in (i), and $|\phi\rangle$ is a normalised state in $\mathcal{H}$ that is orthogonal to $|\xi\rangle$. Defining the necessary operators, state the Amplitude Amplification Theorem as it applies to the target state $|\xi\rangle$.

(iii) Suppose the value of p is known. Explain how the state $|\xi\rangle$ can be prepared exactly using Amplitude Amplification. You may use ancillary qubits if necessary, and assume that arbitrary single-qubit states may be prepared efficiently.

(iv) For any $z \in (0, 2\pi)$, suppose we can implement a unitary $R(\xi, z)$ with the action

$$\begin{aligned} R(\xi, z)|\xi\rangle &= e^{iz}|\xi\rangle \ , \\ R(\xi, z)|\psi\rangle &= |\psi\rangle \qquad\qquad \text{if } \langle\xi|\psi\rangle = 0 \ . \end{aligned}$$

Consider the transformation

$$G = U[(1 - e^{iz})|b\rangle\langle b| - I]U^\dagger R(\xi, z) \ ,$$

where I is the identity operation on $\mathcal{H}$. Under what condition on p and q is it possible to choose z such that G can be used to prepare $|\xi\rangle$ exactly with certainty?

3 (a) Consider the additive group of integers modulo Q for some fixed integer $Q > 1$. Let $2^{m-1} < Q < 2^m$, and view $\mathcal{H}_Q$ as a subspace of the m-qubit state space, spanned by $|a\rangle$ with $0 \leqslant a \leqslant Q-1$. Assume that for any value of $\phi \in [0, 2\pi)$, we can implement phase gates of the form

$$P(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix},$$

as well as all corresponding 2-qubit controlled phase gates $CP(\phi)$.

(i) Write down the action of the Quantum Fourier Transform QFT_Q over $\mathcal{H}_Q$ on a basis state $|a\rangle$.

(ii) Suppose the Boolean function on m-bits that outputs 1 if and only if the integer represented by the bit string x is smaller than Q, can be computed efficiently by a classical computer. Explain how the state $|\xi\rangle = \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} |b\rangle$ may be prepared efficiently with success probability at least $1-\delta$ for any $\delta > 0$ on a quantum computer, starting from the m-qubit all-zeros state $|0^m\rangle$.

(iii) Write down a circuit consisting of $O(m)$ many 1- and 2-qubit gates for the unitary U that maps any $|b\rangle$ to $\omega^b|b\rangle$ for each $0 \leqslant b \leqslant Q-1$. Hence or otherwise write down a circuit of $O(m^2)$ many 1- and 2-qubit gates for the unitary $V : |a\rangle|b\rangle \mapsto \omega^{ab}|a\rangle|b\rangle$.

(iv) Using your answers to parts (i)-(iii), describe how the mapping $|a\rangle|0^m\rangle \mapsto |a\rangle\mathrm{QFT}_Q|a\rangle$ may be implemented for any $0 \leqslant a \leqslant Q-1$.

(b) Consider the shift operator S that acts as $S|x\rangle = |(x-1) \bmod Q\rangle$ on $\mathcal{H}_Q$. Using the unitary part U_{PE} of the quantum phase estimation algorithm, describe a procedure to implement the map $|0^m\rangle\mathrm{QFT}_Q|a\rangle \mapsto |a\rangle\mathrm{QFT}_Q|a\rangle$. You may ignore issues of precision and assume that U_{PE} can be implemented exactly.

(c) Using your answers to parts (a)-(b), describe a procedure to prepare the state $\mathrm{QFT}_Q\left(\frac{|a\rangle+|b\rangle}{\sqrt{2}}\right)$ for any $0 \leqslant a < b \leqslant Q-1$. You may assume that the initial state $\frac{|a\rangle+|b\rangle}{\sqrt{2}}$ can be prepared efficiently, and use ancillary registers where necessary.

4

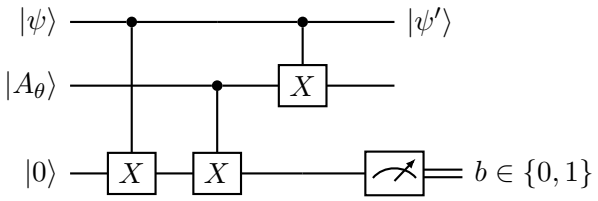
Let I, X, Z denote the identity and standard single-qubit Pauli operators. Let $\mathcal{P}_1$ be the set of operators $\{I, X, Z, XZ\}$ and their multiples by ± 1 and $\pm i$, and let $\mathcal{P}_n = \mathcal{P}_1^{\otimes n}$. Any unitary on n qubits that preserves the group $\mathcal{P}_n$ under conjugation is called a Clifford operation. You may assume that any n-qubit Clifford operation may be represented by a circuit of $\{H, CZ, S\}$ gates, where CZ is the two-qubit controlled-Z gate and $S^2 = Z$.

(a) Consider the quantum computational process that starts with an initial n-qubit state $|\psi\rangle$ and applies a poly(n) sized circuit of 1- and 2-qubit gates, followed by a measurement of a single specified output qubit in the computational basis.

(i) Define what it means for the output of a quantum computational process as described above to be *classically strongly efficiently simulatable.*

(ii) Suppose the input is a product of n single qubit states, $|\psi\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \ldots \otimes |\alpha_n\rangle$. Given a classical description of this input state and an n-qubit Clifford operation C as a circuit $U_N U_{N-1} \ldots U_1$ of length $N = \text{poly}(n)$, show that the outcome of measuring a single output qubit of $C|\psi\rangle$ in the computational basis can be classically strongly efficiently simulated.

(b) Consider the circuit shown in Eq. (1) below, where $|\psi\rangle$ is an arbitrary single-qubit state and $|A_\theta\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)$. Show that the state of the first qubit at the end of the circuit is either $P(\theta)|\psi\rangle$ or $P(-\theta)|\psi\rangle$ with equal probability, where $P(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$ is the phase gate.



(1)

END OF PAPER