Quantum Complexity Theory: Mock exam

Time allowed: 60 minutes. Closed book.

Answer **two** of the three questions. Each carries 50 marks; your two answers are marked out of 100. Give concise justifications for your answers. Definitions, theorem statements and named examples need not be proved unless explicitly requested. Supplied facts may be used without proof.

1 Mixed states and quantum channels

(a) One or two lines per postulate suffice; a side-by-side table is acceptable.

- (i) Formulate randomised computation using the four postulates of stochastic computation. *[4 marks]*
- (ii) State the four postulates of quantum computation. *[4 marks]*
- (iii) What are the key differences between the two formulations? *[4 marks]*

(b)

- (i) Define a density matrix. *[3 marks]*
- (ii) Write the density matrix of an ensemble $\{(p_j, |\psi_j\rangle)\}_j$. *[2 marks]*
- (iii) When does a density matrix represent a pure state? *[2 marks]*

(c) Write $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

- (i) Show that an equal mixture of $|0\rangle, |1\rangle$ is indistinguishable from an equal mixture of $|+\rangle, |-\rangle$. *[4 marks]*
- (ii) Give a projective measurement and guessing rule that distinguish $|+\rangle\langle+|$ from $I/2$ with success probability $3/4$, when the two states are equally likely. *[4 marks]*
- (iii) Using trace distance, show that the distinguishing probability achieved in (ii) is optimal. *[3 marks]*

(d)

- (i) Define a purification of a density matrix ρ_A. *[3 marks]*
- (ii) Given $\rho_A = \sum_j \lambda_j |b_j\rangle\langle b_j|$ in spectral form, construct a purification and verify it by taking a partial trace. *[7 marks]*

(e)

- (i) Define a quantum channel, including complete positivity and trace preservation. *[6 marks]*
- (ii) Why is positivity alone insufficient when a map acts on part of a larger quantum system? *[4 marks]*

2 Non-local games and MIP*

(*a*) (*i*) Define a two-player one-round non-local game, specifying the questions, answers, winning rule and communication restrictions. *[4 marks]*

(*ii*) What resources are allowed in a classical strategy? *[2 marks]*

(*iii*) Why can a deterministic strategy attain the optimal classical winning probability? *[3 marks]*

(*b*) (*i*) Define a Bell inequality for a non-local game. *[2 marks]*

(*ii*) State the CHSH game. *[3 marks]*

(*iii*) What phenomenon does the CHSH game capture? *[3 marks]*

(*iv*) State and briefly justify the optimal classical winning probability in the CHSH game. *[3 marks]*

(*v*) What winning probability does its best quantum strategy achieve? *[2 marks]*

(*vi*) Can a non-local game have a perfect quantum strategy but no perfect classical strategy? Give an example if so. *[3 marks]*

(*c*) (*i*) Define MIP*, including the verifier's computational power, the provers' resources, and the completeness and soundness quantifiers. *[7 marks]*

(*ii*) For a fixed input, how does a two-prover one-round MIP* verifier define a non-local game? *[3 marks]*

(*iii*) "Entangled provers may ignore their entanglement, so every classical MIP protocol remains sound against entangled provers." Is this argument correct? Discuss completeness and soundness separately. *[3 marks]*

(*d*) (*i*) State the characterisations of MIP and MIP* from the lecture. *[3 marks]*

(*ii*) Define RE and give a complete problem for this class. *[3 marks]*

(*iii*) Why is the complexity class characterisation of MIP* compatible with the halting problem being undecidable? *[6 marks]*

3 Quantum algorithms and verification

(*a*) State the definition of BQP in full detail, including uniformity, circuit size, and the acceptance probabilities on YES and NO instances. *[8 marks]*

(*b*) A quantum decision algorithm is correct with probability at least $2/3$ on every input.

(*i*) Describe how independent repetitions reduce its error. *[4 marks]*

(*ii*) Bound the number of repetitions needed for error at most ε, where $0 < \varepsilon < 1/2$. You may use, for independent $X_i \in \{0,1\}$ and $\overline{X} = t^{-1}\sum_{i=1}^{t} X_i$,

$$\Pr\left[|\overline{X} - \mathbb{E}\overline{X}| \geq \delta\right] \leq 2e^{-2t\delta^2}.$$

[6 marks]

(*c*) Let $f : \{0,1\} \to \{0,1\}$ be accessed through the phase oracle $U_f|x\rangle = (-1)^{f(x)}|x\rangle$.

(*i*) Starting in $|0\rangle$, write the state after applying H and then after applying U_f. *[4 marks]*

(*ii*) Show that one further H, followed by computational-basis measurement, returns $f(0) \oplus f(1)$ with certainty. *[6 marks]*

(*d*) In a QCMA query protocol, a quantum verifier receives a classical proof and access to $x \in \{0,1\}^n$ through the oracle $O_x|i,b\rangle = |i, b \oplus x_i\rangle$, where $i \in \{1,\ldots,n\}$ and $b \in \{0,1\}$. Its task is to decide whether x has even parity. Divide x into p equal blocks, ignoring rounding, and use a p-bit proof. Only queries to x count towards the query cost.

You may use that Grover search finds a marked item among p items, if one exists, with probability at least $2/3$ using $O(\sqrt{p})$ calls to a reversible checking procedure.

(*i*) What should the proof bits claim about the blocks? What condition should the verifier check on the proof before querying x? *[4 marks]*

(*ii*) If x has odd parity and the proof passes this check, show that at least one block claim is false. *[4 marks]*

(*iii*) How many queries to x suffice to check a block claim reversibly? *[3 marks]*

(*iv*) Use quantum search to give a verifier and bound its query cost q. *[4 marks]*

(*v*) Establish completeness and soundness for this verifier. *[4 marks]*

(*vi*) Using your query bound, choose p to minimise $\max\{p, q\}$ for this construction. State separately the resulting classical proof length and input-query complexity. *[3 marks]*

END OF PAPER