PhD Comprehensive examination in Quantum Computation

Department of C&O
University of Waterloo

Examiners: David Gosset and Ashwin Nayak
Fall term, November 10, 2020, 1–4pm

Instructions

Answer any **five** out of the following six questions. Each question carries 10 marks. Partial answers get appropriate credit.

You may be able to answer parts of a question independently of the previous parts, or by assuming them.

The questions vary in how long they may take to answer, in novelty as well as difficulty. They are ordered according to topic. You may find it useful to pick out your favorite three or four questions as a first pass. If you provide multiple answers, and at least one answer contains a critical mistake, an appropriate penalty will be given.

Question 1. Errors and approximation in quantum circuits

Recall that for any single-qubit unitary W there exists a sequence of Hadamard and T gates that approximates it to within error δ. That is,

$$\|W - V_m V_{m-1} \dots V_1\| \leq \delta \qquad \text{where} \quad V_j \in \{H, T\}$$

Recall that the Solovay-Kitaev theorem states that such a sequence exists with $m = O(\log^c(\delta^{-1}))$ for some constant c.

(a)[4 marks] Suppose we are given an n-qubit quantum circuit

$$U = U_M U_{M-1} \dots U_1$$

which is a product of M gates $\{U_j\}_{j=1}^M$ each of which is either a two-qubit CNOT gate, or a single-qubit gate. Suppose we wish to approximate U by a sequence $\tilde{U} = \tilde{U}_L \tilde{U}_{L-1} \dots \tilde{U}_1$ of Hadamard, T , and CNOT gates such that

$$\|U - \tilde{U}\| \leq \epsilon \tag{1}$$

Using the Solovay-Kitaev theorem, establish an upper bound on L as a function of ϵ and M.

(b)[6 marks] Next consider the quantum computation in which the n-qubit quantum circuit U is applied to the all-zeros initial state and then the first w qubits are measured. The output is a bit-string $x \in \{0,1\}^w$ sampled according to the distribution

$$p(x) = \langle 0^n | U^\dagger \left(|x\rangle\langle x| \otimes I_{n-w} \right) U | 0^n \rangle.$$

Now suppose we approximate U as described in part (a), so that Eq. (1) holds. Let $\tilde{p}$ be the corresponding output probability distribution

$$\tilde{p}(x) = \langle 0^n | \tilde{U}^\dagger \left(|x\rangle\langle x| \otimes I_{n-w} \right) \tilde{U} | 0^n \rangle.$$

Establish the following upper bound on the total variation distance between p and $\tilde{p}$:

$$\frac{1}{2} \sum_{x \in \{0,1\}^w} |p(x) - \tilde{p}(x)| \leq 2\epsilon.$$

Question 2. Trace norm.

Let $\mathrm{L}(\mathcal{H})$ denote the space of linear operators on the finite dimensional Hilbert space $\mathcal{H}$. The trace norm of an operator $M \in \mathrm{L}(\mathcal{H})$ is defined as $\|M\|_{\mathrm{tr}} \coloneqq \mathrm{Tr}(\sqrt{M^\dagger M}\,)$.

(a) [3 marks] Prove that $|\mathrm{Tr}(M)| \leq \|M\|_{\mathrm{tr}}$.

(b) [7 marks] Prove that $\mathrm{Tr}(M) = \|M\|_{\mathrm{tr}}$ if and only if M is positive semi-definite.

Question 3. The polynomial method.

For $z \in \{0,1\}^n$, let $|z|$ denote the Hamming weight of z. Define the function $f : \{0,1\}^{2n} \to \{0,1\}$ as $f(x,y) \coloneqq 1(|x| = |y|)$, i.e., the function evaluates to 1 iff the strings x, y have the same Hamming weight.

(a) [5 marks] Construct a real multi-linear polynomial p in $2n$ variables that represents f, i.e., satisfies $p(x,y) = f(x,y)$ for all $x, y \in \{0,1\}^{2n}$.

(b) [5 marks] Suppose there is a real multi-linear polynomial q with degree d approximates f, i.e., $|q(x,y) - f(x,y)| \leq 1/3$ for all Boolean inputs x, y. Show that there is a real *bivariate* polynomial r with degree d such that for any integers $u, v \in [0,n]$, we have $|r(u,v) - f(x,y)| \leq 1/3$ for any x, y with Hamming weights u, v, respectively.

Question 4. Quantum sampling

Suppose you are given a quantum black box specifying a probability distribution as follows: on input $j \in \{1,\ldots,n\}$, the black box computes $p_j \in [0,1]$, where $\sum_{j=1}^n p_j = 1$ (here we assume that each probability p_j can be represented using finitely many bits). You would like to prepare the quantum state $|p\rangle := \sum_{j=1}^n \sqrt{p_j}|j\rangle$.

(a) [6 marks] Show that $|p\rangle$ can be prepared using $O(\sqrt{n})$ quantum queries. (Hint: You could begin by explaining how to prepare the state $\frac{1}{\sqrt{n}}\sum_{j=1}^n(\sqrt{p_j}|j\rangle \otimes |0\rangle + \sqrt{1-p_j}|j\rangle \otimes |1\rangle)$ using only two queries.)

(b) [4 marks] Explain why $\Omega(\sqrt{n})$ queries are necessary to prepare $|p\rangle$ in general. (You may refer to any well-known quantum lower bound in your explanation.)

Question 5. Random stabilizer states

An n-qubit Pauli operator is an operator of the form $\pm P_1 \otimes P_2 \otimes \ldots \otimes P_n$ where each $P_i \in \{\mathbb{I}, \mathrm{X}, \mathrm{Y}, \mathrm{Z}\}$. An n-qubit stabilizer group S is a group not containing $-\mathbb{I}$ that is generated by a set of commuting n-qubit Pauli operators. For any n-qubit stabilizer group S with exactly n independent generators we associate a *stabilizer state* denoted $|S\rangle$ which is defined (up to a global phase) by

$$|S\rangle = P|S\rangle \qquad \text{for all } P \in S.$$

(a) [3 marks] Show that

$$|S\rangle\langle S| = \frac{1}{2^n}\sum_{P \in S} P.$$

(b) [1 mark] Suppose that Q is an n-qubit Pauli operator and $Q \notin \{\mathbb{I}, -\mathbb{I}\}$. Show that there exists an n-qubit Pauli operator R such that

$$RQR = -Q.$$

(c) [3 marks] Suppose S is selected uniformly at random from the set of all n-qubit stabilizer groups with exactly n independent generators. Show that for any n-qubit Pauli operators R, P we have

$$\Pr[P \in S] = \Pr[RPR \in S].$$

(d) [3 marks] Using the results of (a,b,c), show that

$$\mathbb{E}[|S\rangle\langle S|] = \frac{\mathbb{I}}{2^n}.$$

Question 6. Key generation.

Suppose Alice (A) and Bob (B) hold n qubits each of a quantum state entangled with Eve (E), and their joint state is ρ^{ABE}. Let $|\phi\rangle \coloneqq (|00\rangle + |11\rangle)/\sqrt{2}$.

(a) [5 marks] Let $R \in \{0,1\}^n$ be a uniformly random string. Suppose Alice and Bob measure their n qubits in the Hadamard basis, and obtain outcomes $X, Y \in \{0,1\}^n$, respectively. Let M be the number of indices i with $R_i = 1$ such that the outcomes of the measurement of the ith qubit differ (i.e., $X_i \neq Y_i$). Let K be the number of indices i such that $R_i = 0$ and the outcomes of their measurement of the i-th qubit differ. Let $\epsilon \in (0,1]$ be a constant. Prove that, with probability exponentially close to 1 (in terms of n), K is at most $M + \epsilon n$:

$$\Pr(K \leq M + \epsilon n) \quad \geq \quad 1 - \exp(-\Theta(n)) \quad .$$

(b) [5 marks] If the fidelity $\mathrm{F}(\rho^{AB}, \phi^{\otimes n}) \geq 1 - \epsilon$ for some $\epsilon \in [0,1]$, prove that

$$\left\| \rho^{ABE} - \phi^{\otimes n} \otimes \omega^E \right\|_{\mathrm{tr}} \quad \leq \quad f(\epsilon) \ ,$$

for some quantum state ω and function f such that $f \to 0$ as $\epsilon \to 0$.