Quantum Computing (5314QUCO6Y), Final exam

Ronald de Wolf

Monday June 8, 2020
9:45–13:15
online

The exam is "open book," meaning you can use any kind of paper you want but no electronic devices beyond what is needed to download and read the exam questions, and (at the end) to scan and upload your solutions. Please answer in English. Use a black or blue pen, not a pencil. Write clearly and explicitly, and explain your answers. For a multipart-question, you may assume answers for earlier parts of the question to answer later parts, even if you don't know the earlier answers. The total number of points adds up to 9; your exam grade will be your number of points +1. An exam grade of at least 5 is a necessary condition for passing the course. Your final grade will be 60% exam + 40% homework, rounded to the nearest integer.

1. **(1 point)** Pop quiz: answer the following two questions with "true" or "false" (no further explanation required for this question).

   (a) Quantum computers can solve NP-hard problems like satisfiability and Traveling Salesman efficiently by trying out all (exponentially many) solutions in superposition.

   (b) Using shared EPR-pairs, Alice and Bob can communicate with each other instantaneously (so faster than light).

2. **(2 points)**

   (a) Consider the following variant of the search problem: we are given query access to a string $x \in \{0,1\}^N$, $N = 2^n$, and we know a set $S \subseteq [N]$ of $k < N$ elements such that $x_i = 0$ for all $i \notin S$. Show that there is a quantum algorithm that can find a solution for this search problem (i.e., an i such that $x_i = 1$, if there is one) with success probability $\geq 2/3$, using $O(\sqrt{k})$ queries to x.

   (b) Consider the following variant of the intersection problem of communication complexity: Alice holds a string $x \in \{0,1\}^N$ of Hamming weight k, and Bob holds a string $y \in \{0,1\}^N$ of Hamming weight k. Give a quantum communication protocol that finds an i such that $x_i = y_i = 1$ (if such an i exists) with success probability $\geq 2/3$, using $O(\sqrt{k}\log N)$ qubits of communication.

3. **(2 points)** Suppose $n + 1 = 2^k$ for some integer k. For $\ell \in \{0, \ldots, n\}$ define n-qubit state

$$|\psi_\ell\rangle = \frac{1}{\sqrt{\binom{n}{\ell}}} \sum_{x \in \{0,1\}^n : |x| = \ell} |x\rangle,$$

where $|x|$ denotes the Hamming weight (number of 1s) in x.

(a) Show that $\langle\psi_\ell|\psi_{\ell'}\rangle$ equals 1 if $\ell = \ell'$, and equals 0 otherwise.

(b) Consider a qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. Show that the n-qubit state $|\phi\rangle^{\otimes n}$ can be written as a linear combination of the states $|\psi_\ell\rangle$. Say explicitly what the coefficients of this linear combination are.

(c) Give a unitary V, independent of α, β, that encodes $|\phi\rangle^{\otimes n}$ into a k-qubit state $|\psi\rangle$ in the sense that

$$V : |\phi\rangle^{\otimes n} \mapsto |\psi\rangle \otimes |0^{n-k}\rangle.$$

Say explicitly what your state $|\psi\rangle$ is and how it depends on α and β (you're not required to write out circuits).

4. **(2 points)** Alice and Bob share n EPR-pairs. Call their shared $2n$-qubit state $|\psi\rangle_{AB}$.

(a) Let U be an arbitrary n-qubit unitary and $\bar{U}$ be U after conjugating its entries (without transposing). Prove that $(U \otimes \bar{U})|\psi\rangle_{AB} = |\psi\rangle_{AB}$.

(b) Suppose Alice receives some input x, and she does an n-qubit unitary U_x on her part of the state and then measures in the computational basis, obtaining a classical outcome $a \in \{0,1\}^n$. What is the probability distribution over Alice's measurement outcomes, and why?

(c) Suppose Bob receives the same input x as Alice already received. How can he learn Alice's measurement outcome a without communication?

Hint: you may assume Bob knows the map $x \mapsto U_x$.

5. **(2 points)** Consider a standard quantum query algorithm (similar to Chapter 11): it makes T queries to a string $x \in \{0,1\}^N$, with arbitrary unitaries $U_0, U_1, \ldots, U_T$ (that are independent of x) around the queries, and then measures a POVM $\{M, I - M\}$ on the final m-qubit state $|\psi_x\rangle$.

(a) Show that the probability $P(x)$ of getting the first measurement outcome (on input x) is $\langle\psi_x|M|\psi_x\rangle$, and that this can be written as an N-variate multilinear polynomial in the bits of x of degree $\leq 2T$.

(b) A *k-wise independent distribution* D is a probability distribution over $\{0,1\}^N$, such that for each set $S \subseteq [N]$ of at most k coordinates, the distribution on the k-bit substring $x_S = (x_i)_{i \in S}$ is uniformly random (i.e, for each $z \in \{0,1\}^k$, the probability under distribution D of the event that $x_S = z$, is $1/2^k$).

Show that a T-query quantum algorithm cannot distinguish the uniform distribution U on its input x from a $2T$-wise independent distribution D on x, in the sense that no matter what binary measurement the algorithm does at the end, the probability of output 1 is the same under U and under D.

Hint: compare the expected value of a monomial of degree $\leq 2T$ under distributions U and D.

Solutions

1. **(1 point)**

   (a) False (see the $\sqrt{N}$ lower bound for search).

   (b) False (see Exercise 16.6).

2. **(2 points)**

   (a) Let $\mathcal{A}$ be a quantum algorithm that generates a uniform superposition $\frac{1}{\sqrt{k}}\sum_{i\in S}|i\rangle$ (this uses no queries). This algorithm has probability $p \geq 1/k$ of finding a solution, if there is one in S. Now apply amplitude amplification (Section 7.4) to $\mathcal{A}$ to obtain an algorithm that finds a solution with probability $\geq 2/3$, using $O(1/\sqrt{p}) = O(\sqrt{k})$ iterations (and hence queries to x).

   (b) Alice can run the algorithm of part (a) to find such an i in the string $z = x \wedge y$, using two messages of $O(\log N)$ qubits to and from Bob (exactly as in Section 14.4) to implement each query to the string z. So the total communication would be $O(\sqrt{k}\log N)$.

3. **(2 points)**

   (a) If $\ell = \ell'$: $\langle\psi_\ell|\psi_\ell\rangle = \parallel|\psi_\ell\rangle\parallel^2 = \frac{1}{\binom{n}{\ell}}|\{x : |x| = \ell\}| = 1$.

   If $\ell \neq \ell'$: note that $|\psi_\ell\rangle$ and $|\psi_{\ell'}\rangle$ have support on disjoint sets of basis states, so their inner product is 0.

   (b) The amplitude of each basis state $|x\rangle$ of weight ℓ in $|\phi\rangle^{\otimes n}$ is $\gamma_\ell := \alpha^{n-\ell}\beta^\ell$. Therefore

   $$|\phi\rangle^{\otimes n} = \sum_{\ell=0}^{n}\sum_{x:|x|=\ell}\gamma_\ell|x\rangle = \sum_{\ell=0}^{n}\gamma_\ell\sqrt{\binom{n}{\ell}}|\psi_\ell\rangle.$$

   (c) Note that because $n+1 = 2^k$, the integers $\ell \in \{0,\ldots,n\}$ can all be written in k bits. Let V be a unitary that maps $|\psi_\ell\rangle \mapsto |\ell\rangle|0^{n-k}\rangle$. Such a unitary (in fact, many such unitaries) exist because of part (a). By linearity and part (b), V maps $|\phi\rangle^{\otimes n}$ to

   $$\sum_{\ell=0}^{n}\gamma_\ell\sqrt{\binom{n}{\ell}}V|\psi_\ell\rangle = \underbrace{\sum_{\ell=0}^{n}\gamma_\ell\sqrt{\binom{n}{\ell}}|\ell\rangle}_{|\psi\rangle}|0^{n-k}\rangle.$$

4. **(2 points)**

   (a)

   $$(U\otimes\bar{U})|\psi\rangle_{AB} = \frac{1}{\sqrt{2^n}}\sum_{j\in\{0,1\}^n}U|j\rangle\overline{U}|j\rangle = \frac{1}{\sqrt{2^n}}\sum_{j\in\{0,1\}^n}\sum_{i\in\{0,1\}^n}U_{ij}|i\rangle\sum_{i'\in\{0,1\}^n}U^*_{i'j}|i'\rangle$$
   $$= \frac{1}{\sqrt{2^n}}\sum_{i,i'}\left(\sum_{j\in\{0,1\}^n}U_{ij}U^*_{i'j}\right)|i\rangle|i'\rangle = \frac{1}{\sqrt{2^n}}\sum_{i\in\{0,1\}^n}|i\rangle|i\rangle = |\psi\rangle_{AB}.$$

   the penultimate equality is because the sum in parentheses is $\delta_{ii'}$ since the rows of U are an orthonormal set.

(b) Alice's local density matrix is the maximally mixed state ($I/2^n$) before applying U_x, and hence also after applying U_x since $U_x(I/2^n)U_x^* = I/2^n$. Therefore each measurement outcome has probability $1/2^n$.

(c) Given x, Bob applies $\overline{U_x}$. By part (a), $U_x \otimes \overline{U_x}$ leaves $|\psi\rangle_{AB} = \frac{1}{\sqrt{2^n}}\sum_{a\in\{0,1\}^n}|a\rangle_A|a\rangle_B$ invariant. Hence if Alice and Bob each measure in the computational basis, then they will get the same outcome a (it doesn't matter whether Alice's measurement precedes Bob's actions or not, because operations on different spaces commute).

5. **(2 points)**

(a) Let the final state be

$$|\psi_x\rangle = \sum_{z\in\{0,1\}^m} \alpha_z(x)|z\rangle.$$

As shown in the polynomial method in Chapter 11, the amplitudes α_z are N-variate multilinear polynomials (in x) of degree $\leq T$. Working out the vector-matrix-vector product, we have

$$P(x) = \mathrm{Tr}(M|\psi_x\rangle\langle\psi_x|) = \langle\psi_x|M|\psi_x\rangle = \sum_{z,z'\in\{0,1\}^m} \alpha_z^*(x)\alpha_{z'}(x)\langle z|M|z'\rangle = \sum_{z,z'\in\{0,1\}^m} \alpha_z^*(x)\alpha_{z'}(x)M_{zz'}.$$

Since the α_z are polynomials (in x) of degree $\leq T$, and the entries $M_{zz'}$ are independent of x, the latter expression is a polynomial of degree $\leq 2T$.

(b) Fix a T-query algorithm, and let $P(x)$ be the probability that it outputs 1 on input x. By part (a), P is a linear combination of monomials $M_S(x) = \prod_{i\in S} x_i$ of degree $|S| \leq 2T$. Note that M_S has the same expectation under U and under D:

$$\mathbb{E}_{x\sim U}[M_S(x)] = \frac{1}{2^{|S|}} = \mathbb{E}_{x\sim D}[M_S(x)].$$

Since $P = \sum_{S:|S|\leq 2T} a_S M_S$ is a linear combination of such monomials, by linearity of expectation, $\mathbb{E}_{x\sim U}[P(x)] = \sum_S a_S \mathbb{E}_{x\sim U}[M_S(x)]$ and $\mathbb{E}_{x\sim D}[P(x)] = \sum_S a_S \mathbb{E}_{x\sim D}[M_S(x)]$ are equal. Hence our algorithm cannot detect the difference between $x \sim U$ and $x \sim D$.