Quantum Computing (5314QUCO6Y), Final exam

Ronald de Wolf

Monday June 4, 2018
14:00–17:00
UvA Roeterseiland, REC A1.02

The exam is "open book," meaning you can bring any kind of paper you want but no electronic devices. 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. **(1.5 points)**

   (a) What are the eigenvectors (as qubits in Dirac notation) and eigenvalues of the 1-qubit unitary $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$?

   (b) Suppose we can apply a query to bitstring $x \in \{0,1\}^N$ in the usual form:

   $$O_x : |i, b\rangle \mapsto |i, b \oplus x_i\rangle.$$

   Give a circuit, involving one application of O_x and some other gates, to implement the following controlled-phase-query:

   $$C_x : |c, i, 0\rangle \mapsto (-1)^{cx_i}|c, i, 0\rangle.$$

   The idea here is that we implement a phase-query to x, but only in case the control-qubit ($c \in \{0,1\}$) is set to 1.

2. **(2 points)** Alice and Bob share an EPR-pair, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Suppose they each measure their qubit with an X-observable (which corresponds to a particular projective measurement with possible outcomes $+1, -1$).

   (a) Show that Alice's measurement outcome is uniformly distributed, so 50% probability of outcome $+1$ and 50% probability of outcome -1.

   (b) Show that Alice's and Bob's measurement outcomes are always equal.
   Hint: it's helpful here to write the EPR-pair in the basis $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

(c) Suppose we view $X \otimes X$ as one 2-qubit observable (with possible outcomes $+1, -1$) instead of two 1-qubit observables. What is the probability distribution on the two possible outcomes?

3. **(2.5 points)**

(a) Suppose you have a state $\frac{1}{\sqrt{2}}(|0\rangle|\phi\rangle + |1\rangle|\psi\rangle)$, where $|\phi\rangle$ and $|\psi\rangle$ are quantum states with real amplitudes. Suppose you apply a Hadamard gate to its first qubit and then measure that first qubit. Show that the probability of measurement outcome 0 is $\frac{1}{2}(1 + \langle\phi|\psi\rangle)$.

(b) Suppose H is a subgroup of a finite additive group G, and $g \in G$ some element. Show (1) if $g \in H$ then the cosets $g + H$ and H are equal
and (2) if $g \notin H$ then the cosets $g + H$ and H are disjoint.

(c) Consider the following communication complexity problem. Alice and Bob both know a finite group G, Alice gets as input some subgroup $H \leq G$ (for instance in the form of a generating set for H) and Bob gets input $g \in G$. Give a one-way quantum protocol where Alice sends to Bob a message of $O(\log|G|)$ qubits, and then Bob decides with success probability $\geq 2/3$ whether $g \in H$.
Hint: Alice could send a uniform superposition over all $h \in H$.

4. **(3 points)** Let $v \in [-1, 1]^N$ be a vector with real entries, of dimension $N = 2^n$, indexed by $i \in \{0, 1\}^n$. Suppose we can query the entries of this vector by a unitary that maps

$$O_v : |i\rangle|0^p\rangle \mapsto |i\rangle|v_i\rangle,$$

so where the binary representation of the ith entry of v is written into the second register. We assume this second register has p qubits, and the numbers v_i can all be written exactly with p bits of precision (it doesn't matter how, but for concreteness say that the first bit indicates the sign of the number, followed by the $p-1$ most significant bits after the decimal dot). Our goal is to prepare the n-qubit quantum state

$$|\psi\rangle = \frac{1}{\|v\|} \sum_{i \in \{0,1\}^n} v_i|i\rangle.$$

(a) Show how you can implement the following 3-register map (where the third register is one qubit) using one application of O_v and one of O_v^{-1}, and some v-independent unitaries (you don't need to draw detailed circuits for these unitaries, nor worry about how to write those in terms of elementary gates).

$$|i\rangle|0^p\rangle|0\rangle \mapsto |i\rangle|0^p\rangle(v_i|0\rangle + \sqrt{1 - v_i^2}|1\rangle).$$

(b) Suppose you apply the map of (a) to a uniform superposition over all $i \in \{0, 1\}^n$. Write the resulting state, and calculate the probability that measuring the last qubit in the computational basis gives outcome 0.

(c) What is the resulting 3-register state if the previous measurement gave outcome 0?

(d) Assume you know $\|v\|$ exactly. Give an algorithm that prepares $|\psi\rangle$ exactly, using $O\left(\frac{\sqrt{N}}{\|v\|}\right)$ applications of O_v and O_v^{-1}, and some v-independent unitaries.

Solutions

1. **(1.5 points)**
   (a) $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ with eigenvalue 1, and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ with eigenvalue -1.
   (b) You don't need any auxiliary qubits to implement C_x. First you do a CNOT from the first to the last qubit, then H on the last qubit (which puts that qubit into $|+\rangle$ or $|-\rangle$ depending on c). Then apply O_x, which adds phase $(-1)^{x_i}$ if the target qubit is set to $|-\rangle$ (i.e., if $c = 1$), and does nothing if the target qubit is $|+\rangle$. Thus we induce the right phase $(-1)^{cx_i}$. Finally, do another H and CNOT to put the last qubit back to 0.

2. **(2 points)** NB: Don't treat X as a unitary gate here!
   (a) The local density matrix of Alice is $\rho_A = I/2$, hence the expectation value of the observable X is $\mathrm{Tr}(X\rho_A) = 0$, which means the outcomes $+1$ and -1 are equally likely.
   (b) $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle)$. You can think of measuring observable X as measuring in the $\{|+\rangle, |-\rangle\}$ basis. If Alice and Bob both do this, they will either both get outcome $+1$ or both get -1.
   (c) Write the observable $X \otimes X = P_+ - P_-$, where P_+ projects on the span of $|+\rangle|+\rangle$ and $|-\rangle|-\rangle$. Since the EPR-pair lies in that space, the outcome will be $+1$ with probability 1.

3. **(2.5 points)**
   (a) After doing H on the first qubit, the state is

$$|\chi\rangle = \frac{1}{2}((|0\rangle + |1\rangle)|\phi\rangle + (|0\rangle - |1\rangle)|\psi\rangle) = |0\rangle \left(\frac{|\phi\rangle + |\psi\rangle}{2}\right) + |1\rangle \left(\frac{|\phi\rangle - |\psi\rangle}{2}\right).$$

   The probability to get outcome 0 when measuring the first qubit, is

$$\| (|0\rangle\langle 0| \otimes I)|\chi\rangle \|^2 = \| |0\rangle \otimes \frac{|\phi\rangle + |\psi\rangle}{2} \|^2 = \frac{1}{4}(\| |\phi\rangle \|^2 + \| |\psi\rangle \|^2 + 2\langle\phi|\psi\rangle) = \frac{1}{2}(1 + \langle\phi|\psi\rangle).$$

   (b) Recall from Chapter 6.1 that any two cosets of H are either equal or disjoint. (1) Since (sub)groups are closed under the group operation, if $g \in H$ then $g + H = H$. (2) If $g \notin H$ then the cosets $g + H$ and H cannot be equal, hence they must be disjoint.
   (c) Alice and Bob agree to use the first $|G|$ basis states in a $\lceil \log_2 |G| \rceil$-qubit space to label the elements $g \in G$. On input H, Alice prepares the state $|\phi\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |h\rangle$ and sends this to Bob. Define $|\psi\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |g + h\rangle$. Note that because of (b), we have $\langle\phi|\psi\rangle = 1$ if $g \in H$, and $\langle\phi|\psi\rangle = 0$ if $g \notin H$.
   Bob adds an auxiliary $|+\rangle$-qubit on the left of the state he received, and applies (controlled on the auxiliary qubit) the unitary $|h\rangle \mapsto |g + h\rangle$, where g is Bob's input. Our state is now exactly the state of (a), which allows Bob to detect with probability 1/2 whether $g \notin H$. If Alice sends a few copies of $|\phi\rangle$, then Bob can decide whether $g \in H$ with probability close to 1.

4. **(3 points)**

(a) For $a \in [-1,1]$, let V_a be the single-qubit gate $\begin{pmatrix} a & -\sqrt{1-a^2} \\ \sqrt{1-a^2} & a \end{pmatrix}$. Let U be the $(p+1)$-qubit unitary that applies V_a to the last qubit conditioned on the value a in the first p qubits, where we're using the same p-bit encoding of numbers $a \in [-1,1]$ as explained at the start of the question. In other words, $U = \sum_{a\in\{0,1\}^p} |a\rangle\langle a| \otimes V_a$. This U is independent of the vector v. We implement the required map as follows:
- apply O_v to the first $n+p$ qubits
- apply U to the last $p+1$ qubits
- apply O_v^{-1} to the first $n+p$ qubits.
If you track what this does to basis state $|i\rangle|0^p\rangle|0\rangle$, it implements exactly the right map.

(b) The resulting state is

$$\frac{1}{\sqrt{N}} \sum_{i\in\{0,1\}^n} |i\rangle|0^p\rangle(v_i|0\rangle + \sqrt{1-v_i^2}|1\rangle)$$

$$= \frac{1}{\sqrt{N}} \left(\sum_{i\in\{0,1\}^n} v_i|i\rangle \right) |0^p\rangle|0\rangle + \frac{1}{\sqrt{N}} \left(\sum_{i\in\{0,1\}^n} \sqrt{1-v_i^2}|i\rangle \right) |0^p\rangle|1\rangle).$$

The probably that measuring the last qubit gives 0, is $p = \frac{1}{N}\sum_{i\in\{0,1\}^n} v_i^2 = \| v \|^2 /N$.

(c) $\sum_{i\in\{0,1\}^n} v_i|i\rangle|0^p\rangle|0\rangle$, normalized by $\| v \|$, i.e., $|\psi\rangle$ followed by $p+1$ $|0\rangle$-qubits.

(d) We can apply amplitude amplification as in Section 7.3. The algorithm $\mathcal{A}$ is the algorithm of (b), χ marks the basis states that end with $|0\rangle$, and $p = \| v \|^2 /N$ was computed in (b). Amplitude amplification will amplify the part of the state ending in $|0\rangle$ using $O(1/\sqrt{p}) = O(\sqrt{N}/ \| v \|)$ applications of $\mathcal{A}$ and $\mathcal{A}^{-1}$. This gives us $|\psi\rangle$.