Quantum Computing (5334QUCO8Y), Exam

Ronald de Wolf

Wednesday Jan 24, 2024, 14:00–17:00
IWO Geel 4.04B, Meibergdreef 29, Amsterdam

The exam is "open book": you can bring any kind of paper you want, but no electronic devices. 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 the earlier parts in order to answer later parts, even if you didn't provide answers to the earlier parts. The total number of points adds up to 9; your exam grade is your number of points +1. An exam grade ≥ 5 is a necessary condition for passing the course. Your final grade is 60% exam + 40% homework, rounded to the nearest integer.

1. **(1.5 points)** Consider the 9-qubit code from Section 20.4, where the logical 0 and 1 states are defined as:

$$|\overline{0}\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|\overline{1}\rangle = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

   Give a circuit that encodes an arbitrary qubit, i.e., that maps $(\alpha|0\rangle + \beta|1\rangle)|0^8\rangle$ to $\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle$ for all possible α, β. Your circuit can use CNOTs and arbitrary single-qubit gates, but no extra workspace qubits.
   Hint: Because of linearity it suffices if your circuit works if $\alpha = 1$ and $\beta = 0$, or $\alpha = 0$ and $\beta = 1$.

2. **(1.5 points)** Suppose U is an unknown unitary that you are allowed to apply once. You're also given one copy of an unknown eigenstate $|\psi\rangle$ of U that has eigenvalue 1 (so $U|\psi\rangle = |\psi\rangle$). Give a circuit for implementing a *controlled* version of U on an unknown state $|\phi\rangle$. Your circuit can use one application of U, as well as other gates that do not depend on U. It can act also on $|\psi\rangle$ but without changing it. Explain why the circuit works.
   Hint: Consider controlled-SWAP.

3. **(1.5 points)** Let V be a subspace of $\{0,1\}^n$ (with bitwise addition mod 2), and let

$$|V\rangle = \frac{1}{\sqrt{|V|}} \sum_{v \in V} |v\rangle$$

   be the n-qubit state that is the uniform superposition over the elements of V. Let

$$V^\perp = \{w \mid v \cdot w = 0 \bmod 2 \text{ for all } v \in V\}$$

   be the subspace orthogonal to V. Show that $H^{\otimes n}$ maps $|V\rangle$ to the n-qubit state $|V^\perp\rangle$.

4. **(2 points)** The *address function* $f : \{0,1\}^N \to \{0,1\}$ has $N = k + 2^k$. Here the N-bit input x is viewed as consisting of a k-bit string y followed by a 2^k-bit string z, and the function value $f(y,z)$ is defined as z_y where we view y as an integer in $\{0,\ldots,2^k-1\}$ (an "address" pointing to one of the bits in $z = z_0 \ldots z_{2^k-1}$).

   (a) Show there is a classical deterministic algorithm to compute f with $\leq k+1$ queries to x.

   (b) Let $g : \{0,1\}^k \to \{0,1\}$ be some arbitrary but known function (i.e., we know its values on all k-bit inputs). Show how a T-query algorithm for f can be used to obtain a T-query algorithm for g (it doesn't matter here whether the algorithm is quantum or classical).

   (c) Show that quantum algorithms that compute f with worst-case error probability $\leq 1/3$, need at least $k/2$ queries.
   Hint: Think of the k-bit parity function.

5. **(2.5 points)** Suppose we have a quantum communication protocol that starts with an unentangled state $|x\rangle_A|0\rangle_C|y\rangle_B$, where $x,y \in \{0,1\}^n$. Alice and Bob can also each have many $|0\rangle$-qubits at the start of the protocol for workspace. The channel-register C consists of one special qubit, initially $|0\rangle$. Alice starts the protocol. When it's Alice's turn to send a qubit, she applies a unitary that acts on the A- and C-registers; when it's Bob's turn to send a qubit, he applies a unitary that acts on the C- and B-registers. The protocol's one-bit output is obtained by a computational-basis measurement on the last qubit sent over the channel.

   (a) Prove that the (normalized) final state of the protocol after c qubits have been sent, but before the output qubit is measured, can be written as

   $$\sum_{i \in \{0,1\}^c} |a_i(x)\rangle_A |i_c\rangle_C |b_i(y)\rangle_B$$

   for some (unnormalized) states $|a_i(x)\rangle$ on Alice's side that depend only on x, and some (unnormalized) states $|b_i(y)\rangle$ on Bob's side that depend only on y.[1] Here i_c is the last (i.e., rightmost) bit of the c-bit string i.
   Hint: Use induction on c (with $c = 0$ as the easy base case; define $i_0 = 0$ if i is a string of length 0). This part (a) is the most technical part of this question, and you could consider working on it only after you answered the other parts. There is no reason to set workspace qubits back to $|0\rangle$ in this exercise.

   (b) Let $P(x,y) \in [0,1]$ denote the probability that the output is 1, on inputs x and y. Give a formula for $P(x,y)$, as a function of x and y, in terms of (sums of products of) the inner products $\langle a_i(x)|a_j(x)\rangle$ and $\langle b_i(y)|b_j(y)\rangle$.
   Hint: Calculate the squared norm of the expression in (a) projected on the part where $i_c = 1$.

   (c) Show that the $2^n \times 2^n$ matrix with entries $P(x,y)$ has rank $\leq 2^{2c-2}$.
   Hint: For fixed i,j, the $2^n \times 2^n$ matrix that has entries $\langle a_i(x)|a_j(x)\rangle \cdot \langle b_i(y)|b_j(y)\rangle$ has rank 1.

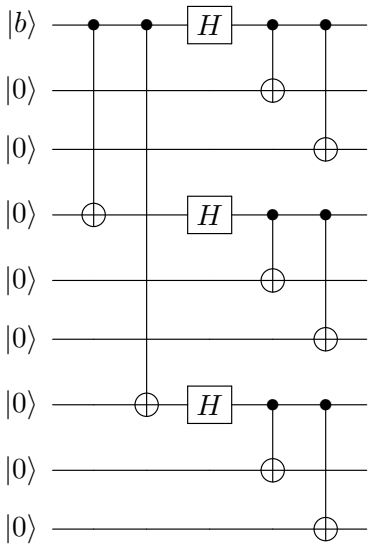
   (d) Suppose we have a protocol that computes the equality function (i.e., $f(x,y) = 1$ iff $x = y$) with error probability 0. What is the matrix P in this case?

   (e) Suppose you have a protocol that computes the equality function with error probability 0, using c qubits of communication. Prove that $c \geq n/2 + 1$.
   Hint: What is now the rank of the matrix P of part (d)? Don't think of Ex 16.1–3 here, since those only apply to one-way protocols for the equality function, while here we allow back-and-forth communication.

[1] The point of this way of writing the final state, is to separate the x-dependence from the y-dependence.

Solutions

1. **(1.5 points)** For $b \in \{0,1\}$, it's straightforward to convert $|b\rangle|00\rangle$ into $\frac{1}{\sqrt{2}}(|000\rangle + (-1)^b|111\rangle)$ using a Hadamard on the first qubit followed by two CNOTs. We just prepare this 3-qubit block three times (first making two copies of the classical bit b using CNOTs that have the 4th and 7th qubit as target, respectively). Here's the circuit:



2. **(1.5 points)** Suppose the first qubit is the one we want to control on. We start with the 3-register state $|b\rangle|\phi\rangle|\psi\rangle$, where $b \in \{0,1\}$ is the control bit (if the circuit works for the cases where the control qubit is a basis state, then by linearity it will also work if the state is in superposition). We want to apply U to $|\phi\rangle$ if $b = 1$, and do nothing if $b = 0$.

   The circuit swaps the 2nd and 3rd registers controlled by the first qubit, applies U to the 3rd register, and again swaps the 2nd and 3rd registers controlled by the first qubit.

   Let's see why this works. If the control-bit $b = 0$ then the two controlled-SWAPs don't do anything, so we have $|\psi\rangle$ in the 3rd register when we apply U, and nothing changes because $U|\psi\rangle = |\psi\rangle$. If, on the other hand, the control-bit $b = 1$, then the first controlled-SWAP puts $|\phi\rangle$ in the 3rd register (and $|\psi\rangle$ in the 2nd), we apply U to it to get $U|\phi\rangle$, and the second controlled-SWAP puts $U|\phi\rangle$ in the 2nd register (and $|\psi\rangle$ back in the 3rd). So the controlled-U operation is applied to the first two registers, and $|\psi\rangle$ remains unchanged in the 3rd register.

3. **(1.5 points)**

$$\begin{aligned} H^{\otimes n}|V\rangle &= \frac{1}{\sqrt{|V|}} \sum_{v \in V} H^{\otimes n}|v\rangle \\ &= \frac{1}{\sqrt{|V|}} \sum_{v \in V} \frac{1}{\sqrt{2^n}} \sum_{w \in \{0,1\}^n} (-1)^{v \cdot w}|w\rangle \\ &= \sum_{w \in \{0,1\}^n} \left(\frac{1}{\sqrt{|V|2^n}} \sum_{v \in V} (-1)^{v \cdot w} \right) |w\rangle \end{aligned}$$

Let's analyze the amplitude inside the big parentheses (this is similar to Ex 3.4). Suppose $w \in V^\perp$. Then w has inner product 0 with all of the $v \in V$. Hence $(-1)^{v \cdot w} = 1$ for every $v \in V$, so the amplitude of $|w\rangle$ is $|V|/\sqrt{|V|2^n} = \sqrt{|V|/2^n}$. The number of elements of $V^\perp$ is $2^n/|V|$ because the dimensions of V and $V^\perp$ add up to n. Therefore the squared amplitudes of the $w \in V^\perp$ sum up to 1, meaning the $w \notin V^\perp$ all have amplitude 0. Accordingly, $H^{\otimes n}|V\rangle$ is exactly a uniform superposition over the $w \in V^\perp$, which is $\left|V^\perp\right\rangle$.

4. **(2 points)**

   (a) A deterministic classical algorithm can just query the k address bits (i.e., the k bits of y) and then query the bit z_y that the address points to. That's $k+1$ queries.

   (b) Set z to the 2^k "truth-table" (i.e., sequence of values) of the function g. Now to compute g on an unknown k-bit string y, we can run the algorithm for the address function on the input yz (with z fixed as above). The number of queries made by this algorithm to its k-bit input y, is at most the number of queries made by the T-query algorithm to its N-bit input yz, so at most T. The function g is computed correctly, because the bit z_y that the address y points to, has been set to $g(y)$.

   (c) Suppose we have a T-query quantum algorithm for the address function. Using (b) with g set to the k-bit parity function, we obtain a T-query algorithm for computing parity with error probability $\leq 1/3$. But we know from Chapter 11 that computing parity, needs $\geq k/2$ quantum queries. Hence $T \geq k/2$.

5. **(2.5 points)**

   (a) As the hint says, we use induction on c.
   Base case. For $c = 0$, the final state is just $|x\rangle|0\rangle|y\rangle$, so we let i range only over the empty string, and define $|a_i(x)\rangle = |x\rangle$ and $|b_i(y)\rangle = |y\rangle$.
   Inductive step ($c \to c+1$). The induction hypothesis is that after c qubits of communication, the state can be written as

$$|\psi\rangle = \sum_{i \in \{0,1\}^c} |a_i(x)\rangle_A |i_c\rangle_C |b_i(y)\rangle_B$$

   Now the protocol sends its $(c+1)$st qubit. Assume it's Alice who sends that qubit (if instead it's Bob's turn to send a qubit, the proof is completely analogous). Alice applies some unitary U to the first two registers (the A- and C-registers). Each term $|a_i(x)\rangle_A |i_c\rangle_C$ then becomes $U(|a_i(x)\rangle_A |i_c\rangle_C)$, which can be written as $|a_{i0}(x)\rangle_A |0\rangle_C + |a_{i1}(x)\rangle_A |1\rangle_C$ for some unnormalized states $|a_{i0}(x)\rangle_A$ and $|a_{i1}(x)\rangle_A$. Define $|b_{i0}(y)\rangle_B = |b_i(y)\rangle_B$ and $|b_{i1}(y)\rangle_B = |b_i(y)\rangle_B$. Then we can write the state after the $(c+1)$st qubit of communication as

$$\begin{aligned}
(U \otimes I_B)|\psi\rangle &= \sum_{i \in \{0,1\}^c} \left(|a_{i0}(x)\rangle_A |0\rangle_C + |a_{i1}(x)\rangle_A |1\rangle_C\right) |b_i(y)\rangle_B \\
&= \sum_{i \in \{0,1\}^c} |a_{i0}(x)\rangle_A |0\rangle_C |b_{i0}(y)\rangle_B + |a_{i1}(x)\rangle_A |1\rangle_C) |b_{i1}(y)\rangle_B \\
&= \sum_{j \in \{0,1\}^{c+1}} |a_j(x)\rangle_A |j_{c+1}\rangle_C |b_j(y)\rangle_B,
\end{aligned}$$

which concludes the inductive step.

(b) Let $I = \{i \in \{0,1\}^c : i_c = 1\}$ be the strings ending in a 1. Following the hint, we have

$$\begin{aligned} P(x,y) =& \| \sum_{i \in I} |a_i(x)\rangle_A |i_c\rangle_C |b_i(y)\rangle_B \|^2 \\ &= \sum_{i,j \in I} (\langle a_i(x)|_A \langle i_c|_C \langle b_i(y)|_B) \cdot (|a_j(x)\rangle_A |j_c\rangle_C |b_j(y)\rangle_B) \\ &= \sum_{i,j \in I} \langle a_i(x)|a_j(x)\rangle \cdot \langle i_c|j_c\rangle \cdot \langle b_i(y)|b_j(y)\rangle \\ &= \sum_{i,j \in I} \langle a_i(x)|a_j(x)\rangle \cdot \langle b_i(y)|b_j(y)\rangle, \end{aligned}$$

where the last equality is because $i_c = j_c = 1$, so $\langle i_c|j_c\rangle = 1$.

(c) For $i, j \in \{0,1\}^c$, define $2^n \times 2^n$ matrix M_{ij} whose (x,y)-entry is $\langle a_i(x)|a_j(x)\rangle \cdot \langle b_i(y)|b_j(y)\rangle$. Such a matrix M_{ij} has rank 1 (as the hint says), because it is the outer product of a 2^n-dimensional vector (with entries $\langle a_i(x)|a_j(x)\rangle$) with another 2^n-dimensional vector (with entries $\langle b_i(y)|b_j(y)\rangle$). From (b) we can see that P is the sum of the matrices M_{ij} where $i \in I$ and $j \in I$. There are $|I|^2 = 2^{2c-2}$ such M_{ij}. The rank of a sum of matrices is at most the sum of the ranks (Appendix A.8), hence the rank of $P = \sum_{i,j \in I} M_{ij}$ is at most 2^{2c-2} times 1.

(d) The protocol has to output the correct answer 1 with certainty whenever $x = y$, so the diagonal entries of P are 1. On the other hand, the protocol outputs the wrong answer 1 with probability 0 whenever $x \neq y$, so the off-diagonal entries of P are 0. In other words, P is the $2^n \times 2^n$ identity matrix in this case.

(e) The matrix P from part (d) has rank 2^n, so from part (c) we have $2^n \leq 2^{2c-2}$, which implies (by taking logarithms and rearranging) that $c \geq n/2 + 1$.