Quantum Computing (5334QUCO8Y), Resit exam

Ronald de Wolf

Monday July 4, 2022
10:00–13:00, SP C1.110

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 points)** Suppose you have a quantum algorithm for some computational problem that takes $\sqrt{N}$ operations on inputs of size N, each operation of constant cost C. And the best-possible classical algorithm for the same computational problem takes N operations, each of constant cost c. Suppose C is much larger than c (which is certainly the case in the current state of quantum technology: doing one elementary quantum gate is much more expensive than one doing classical logic gate). How large does the input-size N have to be before the quantum algorithm has lower cost than the best-possible classical algorithm?

2. **(2 points)** Recall that F_N denotes the N-dimensional Fourier transform.

   (a) Its square F_N^2 turns out to map computational basis states to computational basis states. Describe this map, i.e., determine to which basis state a basis state $|k\rangle$ gets mapped.

   (b) Show that $F_N^4 = I$.

   (c) Show that $F_N^{-1} = F_N^3$.

   (d) Suppose $|\psi\rangle_{AB}$ is an arbitrary unknown n-qubit state where Alice holds the first $n/2$ qubits and Bob holds the last $n/2$ qubits (assume n is even). Show that converting $|\psi\rangle_{AB}$ into the bipartite state $F_N|\psi\rangle_{AB}$ (where Alice still holds the first $n/2$ qubits and Bob the last $n/2$ qubits) requires $\Omega(n)$ qubits of communication between Alice and Bob.
   Hint: Remember Exercise 14.6, which we did in one of the exercise sessions.

3. **(2 points)** Let $g : \{0,1\}^n \to \{0,1\}^{n-1}$ be a 2-to-1 function, meaning that every $y \in \{0,1\}^{n-1}$ has exactly two distinct pre-images $x, x' \in \{0,1\}^n$, with $g(x) = g(x') = y$. Suppose there is an efficient quantum circuit (i.e., with a number of elementary gates that's polynomial in n) that computes g, in the sense of mapping $|x, 0^{n-1}\rangle \mapsto |x, g(x)\rangle$.

   Show how a quantum computer can efficiently generate a uniformly random string $y \in \{0,1\}^{n-1}$ and an associated n-qubit state $|\phi_y\rangle$ such that:
   (1) when asked, from $|\phi_y\rangle$ you can efficiently generate an x such that $g(x) = y$;
   and
   (2) when asked, you can efficiently sample uniformly from the set
   $\{a \in \{0,1\}^n : a \cdot (x \oplus x') = 0 \bmod 2\}$, where x and x' are the pre-images of the generated y.

   Comment (which you may ignore): You're not supposed to do both *tasks (1) and (2) one after another, only either one of the two (whichever you're asked to do). This problem may look arbitrary but was recently used (for a g where, given $x \in \{0,1\}^n$, even a quantum computer cannot efficiently find $x' \neq x$ such that $g(x) = g(x')$) to design a protocol through which a* classical *computer can efficiently verify that a quantum computer works as intended.*

4. **(2 points)** Consider the 3-bit majority function $f : \{0,1\}^3 \to \{0,1\}$:
   $f(x_0, x_1, x_2) = 1$ if at least 2 of the 3 input bits are 1, and $f(x_0, x_1, x_2) = 0$ otherwise.

   (a) How many queries to bits of x does a classical deterministic algorithm need to compute $f(x)$? (note that because the algorithm is deterministic, it always has to give the correct output) Your explanation should have a lower-bound and an upper-bound part.

   (b) Give a quantum algorithm that computes f with success probability 1 using 2 queries (a precise description suffices, you don't need to write out the full circuit).

   (c) Show that 2 quantum queries is optimal: there is no quantum algorithm that computes f with success probability 1 using only 1 query.
   Hint: You may invoke the result of Exercise 11.5 for $N = 2$.

5. **(2 points)** Suppose $|\phi\rangle$ and $|\psi\rangle$ are unknown n-qubit pure states.

   (a) Show how a quantum computer can estimate the overlap $|\langle\phi|\psi\rangle|$ (in absolute value) up to additive error $1/100$ using $O(1)$ given copies of $|\phi\rangle$ and $|\psi\rangle$, and $O(n)$ elementary gates.
   Hint: Use the SWAP-test from Section 15.6. "$O(1)$ given copies" means you are allowed to use any number of copies of $|\phi\rangle$ and $|\psi\rangle$, as long as that number is independent of n. The 3-qubit gate which is the controlled SWAP of a pair of qubits counts as an elementary gate here.

   (b) Assume the inner product $\langle\phi|\psi\rangle$ is a real number. Show that $\| \, |\phi\rangle - |\psi\rangle \, \|^2 = 2 - 2\langle\phi|\psi\rangle$.

   (c) Assume $\langle\phi|\psi\rangle$ is real and positive. Show how a quantum computer can estimate the distance $\| \, |\phi\rangle - |\psi\rangle \, \|$ up to additive error $1/100$ using $O(1)$ copies of $|\phi\rangle$ and $|\psi\rangle$, and $O(n)$ gates.

   (d) Can a quantum computer detect the difference between the two cases $|\psi\rangle = |\phi\rangle$ and $|\psi\rangle = -|\phi\rangle$, given arbitrarily many copies of these two states? Explain your answer.

Intended solutions

1. $C\sqrt{N} < cN$ iff $N > (C/c)^2$.
   Comment: If $C \gg c$ then a quadratic quantum speedup will only be relevant for rather large instance size N.

2. (a) Just write it out:

$$\begin{aligned} F_N(F_N|k\rangle) &= F_N \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{jk} |j\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{jk} F_N |j\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{jk} \frac{1}{\sqrt{N}} \sum_{j'=0}^{N-1} \omega_N^{jj'} |j'\rangle \\ &= \sum_{j'=0}^{N-1} \left(\frac{1}{N} \sum_{j=0}^{N-1} \omega_N^{j(k+j')} \right) |j'\rangle. \end{aligned}$$

   The geometric sum inside the parentheses equals 1 if $k+j' = 0 \bmod N$ (i.e., if $k = j' = 0$ or $j' = N-k$), and equals 0 otherwise. Hence F_N^2 maps $|k\rangle \mapsto |N-k\rangle$ (and $|0\rangle \mapsto |0\rangle$).

   (b) $N-(N-k) = k$, so from (a) we see that F_N^2 is its own inverse. Hence $F_N^4 = F_N^2 \cdot F_N^2 = F_N^2 \cdot (F_N^2)^{-1} = I$.

   (c) This follows immediately from (b) by multiplying left and right by F_N^{-1}.

   (d) From the result of Exercise 14.6.a (with n replaced by $n/2$) we know that for every string $x \in \{0,1\}^{n/2}$, we have

$$(I_{2^{n/2}} \otimes F_{2^{n/2}}^{-1}) F_{2^n} |x\rangle_A |0^{n/2}\rangle_B = |+\rangle_A^{\otimes n/2} |x\rangle_B.$$

   This means that if Alice and Bob can jointly apply F_{2^n} to an arbitrary n-qubit state of which Alice holds the first $n/2$ qubits and Bob the last $n/2$ qubits, then they can transfer $n/2$ bits of information, namely an arbitrary string x, from Alice to Bob (Bob has to do a local $F_{2^{n/2}}^{-1}$ on his $n/2$ qubits at the end, but that doesn't cost any communication between them). But by Holevo's theorem, this requires $\Omega(n)$ qubits of communication between Alice and Bob.

3. This is basically a twist on Simon's algorithm (though x has a different meaning here; it's not a string whose entries we query but rather the input to a function).

   Start with $|0^n\rangle|0^{n-1}\rangle$, apply a Hadamard gate to each of the first n qubits and then compute g on the superposition. This gives you the state

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |g(x)\rangle.$$

   Measure the second register (in the computational basis) and call the $(n-1)$-bit measurement outcome y. This y is uniformly random because each $y \in \{0,1\}^{n-1}$ has the same number

of pre-images. Let x, x' be the two pre-images of y. The first register has now become the n-qubit state

$$|\phi_y\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |x'\rangle).$$

If we're asked to do task (1), then we just measure $|\phi_y\rangle$ in the computational basis and we obtain one of the two pre-images of y (either x or x', each with probability 1/2).

If we're asked to do task (2), then we apply $H^{\otimes n}$ to $|\phi_y\rangle$. By the same calculation as for Simon's algorithm (page 24 of the lecture notes), the resulting state will be uniform (with amplitudes $\pm 1/\sqrt{2^{n-1}}$) over the 2^{n-1} strings $a \in \{0,1\}^n$ mentioned in the question. Hence a measurement in the computational basis gives us a uniformly random such a.

4. (a) 3 queries obviously suffice, since that's the number of input bits (if you query them all, then you know x and hence its majority). To show that a deterministic algorithm also *needs* 3 queries, suppose its first two queries yield a 0-bit and a 1-bit as answers. Then the algorithm has to query the 3rd bit of x as well in order to know the majority value.

   (b) Use Deutsch's algorithm (= the Deutsch-Jozsa algorithm for $N = 2$) to compute the parity $x_0 \oplus x_1$ using one quantum query. If $x_0 \oplus x_1 = 0$, then $x_0 = x_1$ so x_0 is the majority value, and we use our second query to find x_0. If $x_0 \oplus x_1 = 1$, then x_2 determines the majority value, so we use our second query to find x_2.

   (c) Suppose we have T-query quantum algorithm that computes f with success probability 1. Note that if we restrict to inputs where $x_2 = 0$, then this algorithm computes the AND of x_0 and x_1. But we know from Exercise 11.5 that this requires 2 queries. Hence $T \geq 2$ (which is optimal because of the algorithm of (b)).

5. (a) Suppose we do the SWAP-test on a copy of the two states $|\phi\rangle$ and $|\psi\rangle$. By Section 15.4, the probability to get measurement outcome 0 is $p = \frac{1}{2} + \frac{1}{2}|\langle\phi|\psi\rangle|^2$. Think of this as a coin flip with 0-probability p. By flipping this coin $r = O(\log(1/\delta)/\varepsilon^2)$ many times (each time consuming a fresh copy of $|\phi\rangle$ and of $|\psi\rangle$ to do a new SWAP-test), with probability $\geq 1 - \delta$ the average of your coin flips will be within $[p - \varepsilon, p + \varepsilon]$ (you can analyze the tail probability using a Chernoff bound, see Appendix B.2). This allows us to estimate $|\langle\phi|\psi\rangle|^2$ (and hence also $|\langle\phi|\psi\rangle|$) up to any small constant additive error that we want, using only a constant number of copies of $|\phi\rangle$ and $|\psi\rangle$. Since each SWAP-test uses $O(n)$ elementary gates and we do $O(1)$ SWAP-tests, the total number of elementary gates used is $O(n)$.

   (b) $\| |\phi\rangle - |\psi\rangle \|^2 = (|\phi\rangle - |\psi\rangle)^*(|\phi\rangle - |\psi\rangle) = \langle\phi|\phi\rangle + \langle\psi|\psi\rangle - (\langle\phi|\psi\rangle + \langle\psi|\phi\rangle)$.
   Note that $\langle\phi|\psi\rangle + \langle\psi|\phi\rangle = \langle\phi|\psi\rangle + \overline{\langle\phi|\psi\rangle}$ is twice the real part of $\langle\phi|\psi\rangle$ (the imaginary part cancels), which by assumption equals $\langle\phi|\psi\rangle$ itself.

   (c) Use part (a) to estimate $|\langle\phi|\psi\rangle|$ (which by assumption is the same as $\langle\phi|\psi\rangle$) up to additive error 1/20000 using a constant number of copies of the two states. Then use the equation of (b) to derive an approximation of $\| |\phi\rangle - |\psi\rangle \|$ with additive error 1/100.

   (d) These two states differ only by a global phase, hence no matter how many copies k we have of the two states, $|\phi\rangle^{\otimes k}$ and $|\psi\rangle^{\otimes k}$ also only differ by a global phase (which can be $+1$ or -1). No quantum algorithm or measurement can distinguish these two cases.