Quantum Computing (5314QUCO6Y), Final exam

Ronald de Wolf

Monday June 24, 2019
10:00–13:00
UvA Roeterseiland, REC C1.04

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)** Suppose we have a 2-bit input $x = x_0x_1$ and a phase query that maps

$$O_{x,\pm} : |b\rangle \mapsto (-1)^{x_b}|b\rangle \quad \text{for } b \in \{0,1\}.$$

   (a) Suppose we run the 1-qubit circuit $HO_{x,\pm}H$ on initial state $|0\rangle$ and then measure (in the computational basis). What is the probability distribution on the output bit?

   (b) Now suppose the query leaves some workspace in a second qubit, which is initially $|0\rangle$:

$$O'_{x,\pm} : |b,0\rangle \mapsto (-1)^{x_b}|b,b\rangle \quad \text{for } b \in \{0,1\}.$$

   Suppose we just ignore the workspace and run the algorithm of (a) on the first qubit with $O'_{x,\pm}$ instead of $O_{x,\pm}$ (and $H \otimes I$ instead of H). What is now the probability distribution on the output bit (i.e., if we measure the first of the two bits)?

2. **(2.5 points)** Here we will *approximately count* the number of 1s in a string $x \in \{0,1\}^N$. Let $t = |x|$ denote that (unknown) number.

   (a) Given an integer $m \in \{1,\ldots,N\}$, describe a quantum algorithm that makes $O(\sqrt{N/m})$ queries to x and decides between the cases $t \leq m/2$ and $t \in [m,2m]$ with probability at least $2/3$. That is, the algorithm has to output 0 with probability $\geq 2/3$ whenever $t \leq m/2$, has to output 1 with probability $\geq 2/3$ whenever $t \in [m,2m]$, and can output whatever it wants for other values of t.

   (b) Give a quantum algorithm that uses $O(\sqrt{N}\log\log N)$ queries to x and that outputs an integer m such that, with probability $\geq 2/3$, the unknown t lies between $m/2$ and $2m$.

3. **(2.5 points)** Alice and Bob share an EPR-pair, $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

   (a) Let C be a 2×2 matrix. Show that $\mathrm{Tr}((C \otimes I)|\psi\rangle\langle\psi|) = \frac{1}{2}\mathrm{Tr}(C)$.

   (b) Alice could apply one of the 4 Pauli matrices (I, X, Y, Z) to her qubit. Use part (a) to show that the 4 resulting 2-qubit states form an orthonormal set.
   Hint: Use the facts that $\mathrm{Tr}(D|\psi\rangle\langle\psi|) = \langle\psi|D|\psi\rangle$ and that products of 2 distinct Paulis have trace 0.

   (c) Suppose Alice applies one of the 4 Pauli matrices to her qubit and then sends that qubit to Bob. Give the 4 projectors of a 4-outcome projective measurement that Bob could do on his 2 qubits to find out which Pauli matrix Alice actually applied.

4. **(2.5 points)** Consider a quantum-error correcting code that encodes k qubits (and $n-k$ $|0\rangle$s) into an n-qubit codeword state, via the unitary encoding map

$$U : \left|x, 0^{n-k}\right\rangle \mapsto |C(x)\rangle, \text{ where } x \in \{0,1\}^k, \text{ and } |C(x)\rangle \text{ need not be a basis state.}$$

   A "weight-w Pauli error" is the tensor product of n Pauli matrices, of which at most w are not identity (e.g., something like $X \otimes I \otimes Z \otimes I \otimes I$ if $w = 2$ and $n = 5$). Suppose that there is a unitary map S on $3n$ qubits that can identify every weight-w Pauli error E on a codeword, by writing the name of E (the "error syndrome", which we can think of as a $2n$-bit string "E", for example writing 00 for I, 10 for X, 01 for Z, 11 for Y) in a second register that's initially 0^{2n}. In other words, for every $x \in \{0,1\}^k$ and weight-w Pauli error E, this S maps

$$S : (E|C(x)\rangle)\left|0^{2n}\right\rangle \mapsto (E|C(x)\rangle)|\text{"}E\text{"}\rangle.$$

   (a) Show that if x and y are k-bit strings, and E and F are weight-w Pauli errors, then the n-qubit states $E|C(x)\rangle$ and $F|C(y)\rangle$ are orthogonal unless both $x = y$ and $E = F$.

   (b) Prove the inequality $2^k \sum_{i=0}^{w} \binom{n}{i} 3^i \leq 2^n$.
   Comment: This inequality implies a useful lower bound on n, but you don't need to derive that.

Solutions

1. **(1.5 points)**

   (a) We have $O_{x,\pm}H|0\rangle = \frac{1}{\sqrt{2}}((-1)^{x_0}|0\rangle + (-1)^{x_1}|1\rangle) = \frac{(-1)^{x_0}}{\sqrt{2}}(|0\rangle + (-1)^{x_0 \oplus x_1}|1\rangle)$.
   The second application of H turns this into $(-1)^{x_0}|x_0 \oplus x_1\rangle$. Hence a measurement in the computational basis will give outcome $x_0 \oplus x_1$ with probability 1.

   (b) Now we have $O'_{x,\pm}(H \otimes I)|00\rangle = \frac{1}{\sqrt{2}}((-1)^{x_0}|00\rangle + (-1)^{x_1}|11\rangle))$.
   Applying the second $H \otimes I$ turns this into

   $$\frac{1}{2}((-1)^{x_0}|00\rangle + (-1)^{x_0}|10\rangle + (-1)^{x_1}|01\rangle - (-1)^{x_1}|11\rangle)).$$

   Measuring the first qubit now gives outcomes 0 and 1 with probability 1/2 each.

2. **(2.5 points)**

   (a) Suppose we run Grover's algorithm assuming that there are $2m$ solutions, and then query the location it outputs to verify whether this actually is a solution. This takes $T \leq \frac{\pi}{4}\sqrt{\frac{N}{2m}}$ queries to x (plus 1 for the verification). Let $p = \sin((2T+1)\arcsin(\sqrt{t/N}))^2$ denote the probability that this run of Grover finds a solution. If $t = 2m$ then $p \approx 1$, and if $t \in [m, 2m]$ then $p \in [c, 1]$ for some constant c. On the other hand, if $t \leq m/2$ then the algorithm is significantly less likely to find a solution: $p \leq c'$ for some constant $c' < c$ (you can calculate that if $t \ll N$ then $c \approx 0.8$ and $c' \approx 0.5$). Now it suffices to repeat such runs of Grover $O(1)$ times to distinguish the cases $p \leq c'$ and $p \geq c$ with success probability $\geq 2/3$. This takes $O(\sqrt{N/m})$ queries.

   (b) The intuition here is as follows. If we run Grover with a too-high guess for t, then we are unlikely to find a solution. Hence we can approximate t by trying different guesses 2^i for t, and using the largest one where we find a solution as our estimate for t.

   To make this precise, we reduce the error probability of the algorithm of part (a) from 1/3 to $1/(10 \log N)$ using $O(\log \log N)$ repetitions in the standard way (as in Appendix B of the lecture notes). Now consider the following algorithm:

   (1) For $i = 0, \ldots, \lfloor \log_2 N \rfloor$:
   Run the error-reduced (a)-algorithm for $m = 2^i$ and record its output.
   (2) If all runs in (1) gave output 0, then output $m = 0$.
   (3) Else, let i^* be the largest i for which the corresponding run in (1) gave output 1. Output $m = 2^{i^*}$.

   The total number of queries is $\sum_{i=0}^{\lfloor \log_2 N \rfloor} O(\sqrt{N/2^i} \log \log N) = O(\sqrt{N} \log \log N)$.
   It remains to show that this algorithm outputs (with high probability) a good approximation of t. First, if $t = 0$ then the algorithm will not find any solutions (because there aren't any) and will correctly output $m = 0$. Second, if $t > 0$ then define i' to be the unique integer for which $t \in [2^{i'}, 2^{i'+1})$. Then the run of the error-reduced (a)-algorithm with $m = 2^{i'}$ outputs 1 with probability $\geq 1 - 1/(10 \log N)$. On the other hand, for all $i \geq i' + 2$ we have $t \leq 2^i/2$, hence the error-reduced (a)-algorithm with $m = 2^i$ outputs 0

with probability $\geq 1 - 1/(10 \log N)$. So with probability at least 0.9, the i^* in line (3) of the algorithm will be i' or $i'+1$. In the first case our algorithm's output is $m = 2^{i'}$ and $t \in [m, 2m]$; in the second case our output is $m = 2^{i'+1}$ and $t \in [m/2, m]$.

3. **(2.5 points)** Comment: This exercise is just superdense coding in disguise.

   (a) By the cyclicity of the trace we have $\mathrm{Tr}((C \otimes I)|\psi\rangle\langle\psi|) = \langle\psi|(C \otimes I)|\psi\rangle$. Let $C_{i,j}$ (with $i, j \in \{0,1\}$) denote the entries of C. We have

   $$\begin{aligned}(C \otimes I)|\psi\rangle &= \frac{1}{\sqrt{2}}\left((C|0\rangle)|0\rangle + (C|1\rangle)|1\rangle\right) = \frac{1}{\sqrt{2}}\left((C_{00}|0\rangle + C_{10}|1\rangle)|0\rangle + (C_{01}|0\rangle + C_{11}|1\rangle)|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(C_{00}|00\rangle + C_{10}|10\rangle + C_{01}|01\rangle + C_{11}|11\rangle\right)\end{aligned}$$

   Taking inner product with $|\psi\rangle$ gives $\langle\psi|(C \otimes I)|\psi\rangle = \frac{1}{2}(C_{00} + C_{11}) = \frac{1}{2}\mathrm{Tr}(C)$.

   (b) Let A and B be distinct elements of $\{I, X, Y, Z\}$, and $C = AB$. The inner product between the states $(A \otimes I)|\psi\rangle$ and $(B \otimes I)|\psi\rangle$ is

   $$\langle\psi|(A^* \otimes I)(B \otimes I)|\psi\rangle = \langle\psi|(AB \otimes I)|\psi\rangle = \langle\psi|(C \otimes I)|\psi\rangle = \frac{1}{2}\mathrm{Tr}(C) = 0,$$

   where the latter equality is because the product of any two distinct Paulis has trace 0.

   (c) For $D \in \{I, X, Y, Z\}$, define 2-qubit pure state $|\phi_D\rangle = (D \otimes I)|\psi\rangle$. By part (b) these 4 states are pairwise orthogonal. Hence $\{|\phi_D\rangle\langle\phi_D| : D \in \{I, X, Y, Z\}\}$ is a well-defined 4-outcome projective measurement (i.e., its elements sum up to the 4-dimensional identity). Given one of the states $|\phi_A\rangle$, this measurement will output D with probability $\mathrm{Tr}(|\phi_D\rangle\langle\phi_D||\phi_A\rangle\langle\phi_A|) = |\langle\phi_D|\phi_A\rangle|^2$, which is 1 if $D = A$ and 0 otherwise.

4. **(2.5 points)**

   (a) The inner product between $E|C(x)\rangle$ and $F|C(y)\rangle$ equals the inner product between $E|C(x)\rangle|0^{2n}\rangle$ and $F|C(y)\rangle|0^{2n}\rangle$; this (by unitarity of S) in turn equals the inner product between $E|C(x)\rangle|"E"\rangle$ and $F|C(y)\rangle|"F"\rangle$, which is

   $$w = \langle C(x)|E^*F|C(y)\rangle \cdot \langle "E"|"F"\rangle.$$

   First, if $E \neq F$ then $\langle "E"|"F"\rangle = 0$ (because "E" and "F" are distinct bitstrings), and hence $w = 0$. Second, if $E = F$ then $E^*F = I$ (because Pauli matrices are their own inverse) and $\langle "E"|"F"\rangle = 1$, and hence $w = \langle C(x)|C(y)\rangle$ which (by unitary of U) equals $\langle x0^{n-k}|y0^{n-k}\rangle = \langle x|y\rangle$. The latter is 0 unless $x = y$. Hence $w = 0$ unless both $x = y$ and $E = F$.

   (b) For each $x \in \{0,1\}^k$, define the set $F_x = \{E|C(x)\rangle : E \text{ is a weight-}w \text{ Pauli error}\}$. This is a set of n-qubit states, which has $|F_x| = \sum_{i=0}^{w}\binom{n}{i}3^i$ elements, because that's the number of different weight-w Pauli errors (you can choose i locations in $\binom{n}{i}$ ways, and then put X, Y, Z in those chosen locations in 3^i ways). Let $F = \cup_{x\in\{0,1\}^k} F_x$ be the union of the 2^k sets F_x. Note that every pair of elements of F is orthogonal by part (a). Hence F is a set of $2^k \sum_{i=0}^{w}\binom{n}{i}3^i$ pairwise orthogonal n-qubit states. But these are 2^n-dimensional vectors, and one can have at most 2^n pairwise-orthogonal vectors in a 2^n-dimensional space. Hence $|F| \leq 2^n$.