# Quantum Computing (5334QUCO8Y), Final exam

Ronald de Wolf

Monday June 14, 2021
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)** Suppose we have the state $\frac{1}{\sqrt{2}}(|0\rangle|\phi\rangle + |1\rangle|\psi\rangle)$, where $|\phi\rangle$ and $|\psi\rangle$ are unknown normalized quantum states with the same number of qubits. Suppose we apply a Hadamard gate to the first qubit and then measure that first qubit in the computational basis. Give the probability of measurement outcome 1, as a function of the states $|\phi\rangle$ and $|\psi\rangle$.

2. **(2 points)** Suppose we have a qubit in mixed state $\rho$ that we want to hide from Alice and Bob individually, but in such a way that if Alice and Bob cooperate, then they can recover $\rho$.

   Describe how we can change $\rho$ into some other 1-qubit state $\rho'$, what secret keys we give to Alice and Bob, why individually they can get no information about $\rho$ from the qubit $\rho'$, and why jointly they can fully recover the qubit in state $\rho$ from $\rho'$. The keys should be classical.
   Hint: Use the encoding of Ex 17.5, so that Alice and Bob need to cooperate to learn the key used to change $\rho$.

3. **(2 points)**

   (a) Let $x \in \{0,1\}^n$. Suppose we apply the $2n$-qubit Fourier transform $F_{2^{2n}}$ on the $2n$-bit basis state $|x\rangle|0^n\rangle$, followed by $F_{2^n}^{-1}$ on the last $n$ qubits (and identity on the first $n$ qubits). Show that we end up with the $2n$-qubit state $|+\rangle^{\otimes n}|x\rangle$.

   (b) Consider a circuit $C$ that implements $F_{2^{2n}}$ in some way using arbitrary 1-qubit and 2-qubit gates ($C$ can do anything, it need not be one of the specific QFT circuits from the lecture notes). Show that there must be $\Omega(n)$ two-qubit gates in $C$ where the control bit lies in the first $n$ qubits of the state and the target qubit lies in the second $n$ qubits (or vice versa).
   Hint: Think of the first $n$ qubits as Alice and the last $n$ qubits as Bob; use Holevo's theorem.

4. **(2 points)** A function $f : \{0,1\}^n \to \{0,1\}$ is called *affine linear* if there exist $a \in \{0,1\}^n$ and $b \in \{0,1\}$ such that for all $x \in \{0,1\}^n$ we have $f(x) = a \cdot x + b \bmod 2$. A *query* to $f$ is the unitary $O_f$ that maps $|x, d\rangle \mapsto |x, d \oplus f(x)\rangle$ for all $x \in \{0,1\}^n$ and $d \in \{0,1\}$.

   (a) Show how to recover $a$ and $b$ using 2 queries to an affine-linear function $f$.
   Hint: Use the Bernstein-Vazirani algorithm.

   (b) Suppose $\varepsilon > 0$ is a known small constant, and $f : \{0,1\}^n \to \{0,1\}$ is known to be either
   (1) affine linear, or
   (2) far from all affine linear functions: for every affine-linear $g$, we have that $f$ and $g$ differ on at least an $\varepsilon$-fraction of all $x \in \{0,1\}^n$.
   Give a quantum algorithm that can distinguish these two cases with success probability $\geq 2/3$, using $O(1/\sqrt{\varepsilon})$ queries to $f$.

5. **(2 points)** Suppose Alice has an $n$-bit agenda $x = x_1 \dots x_n$ and Bob has an $n$-bit agenda $y = y_1 \dots y_n$. In Section 15.4 we saw how they can find a time-slot for an appointment (i.e., an $i \in \{1, \dots, n\}$ where $x_i = y_i = 1$, if such an $i$ exists) with success probability $\geq 2/3$, using $O(\sqrt{n} \log n)$ qubits of communication.

   (a) Suppose Alice knows integers $a, b$ such that $1 \leq a \leq b \leq n$. Show how Alice and Bob can find a time-slot $i \in \{a, \dots, b\}$ for an appointment (if such an $i$ exists) with success probability $\geq 2/3$, using $O(\sqrt{b-a+1} \log n)$ qubits of communication.

   (b) Show how Alice and Bob can find the *first* time-slot for an appointment (i.e., the smallest $i$ where $x_i = y_i = 1$, assuming such an $i$ exists) with success probability $\geq 2/3$, using $O(\sqrt{n} \log n)$ qubits of communication. Assume for simplicity that $n$ is a power of 2.
   Hint: Use binary search, with the protocol of (a) as a subroutine with properly reduced error probabilities (lower error for cheaper binary-search steps), in such a way that the sum of the error probabilities of those subroutines is still $\leq 1/3$. You have to describe this in sufficient detail; just repeating this hint won't score any points.

## Solutions

1. **(1 point)** After the Hadamard gate the state is

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

Using a 2-outcome projective measurement with operators $P_0 = |0\rangle\langle 0| \otimes I$ and $P_1 = |1\rangle\langle 1| \otimes I$, the probability of measurement outcome 1 is

$$\| P_1|\chi\rangle \|^2 = \| \frac{1}{2}(|\phi\rangle - |\psi\rangle) \|^2 = \frac{1}{4}(\langle\phi|\phi\rangle + \langle\psi|\psi\rangle - \langle\phi|\psi\rangle - \langle\psi|\phi\rangle) = \frac{1}{2} - \frac{1}{2}\mathbb{R}(\langle\phi|\psi\rangle),$$

where $\mathbb{R}(c)$ denotes the real part of a complex number $c$.

2. **(2 points)** We give Alice a uniformly random secret key $a \in \{0,1\}^2$ and Bob a uniformly random secret key $b \in \{0,1\}^2$. Define 2-bit string $c = a \oplus b$ (bitwise addition mod 2). Note that neither Alice nor Bob by themselves have any information about $c$. We use $c$ to select a uniformly random Pauli matrix $W \in \{I, X, Y, Z\}$ and let $\rho' = W\rho W$. By the calculation we did for Ex 17.5 (see "selected exercises" file), $\mathbb{E}_c[\rho'] = I/2$, the maximally mixed state. So since Alice has no knowledge of Bob's secret key $b$, the qubit $\rho'$ reveals no information about $\rho$ to her; and without knowledge of $a$, $\rho'$ reveals no information about $\rho$ to Bob. On the other hand, if Alice and Bob cooperate then they can compute $c$ from Alice's $a$ and Bob's $b$, then they know which $W$ was applied and can recover the qubit $\rho$ from $\rho'$ by undoing that $W$.

3. **(2 points)**

   (a) As usual, we identify integers with their binary representation. We also write $j = j_1 j_2$ for $j_1, j_2 \in \{0,1\}^n$. Let $k$ be the integer whose $2n$-bit binary representation is $x0^n$. Note that, as an integer, $k$ is $2^n$ times the integer $x$, and hence

$$\omega_{2^{2n}}^{jk} = \omega_{2^n}^{jx} = \omega_{2^n}^{j_2 x},$$

   where the exponents "$jk$", "$jx$", "$j_2x$"are the products of 2 integers. We now have:

$$\begin{aligned} F_{2^{2n}}|x\rangle|0^n\rangle &= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1} \omega_{2^{2n}}^{jk}|j\rangle = \frac{1}{2^n}\sum_{j_1=0}^{2^n-1}\sum_{j_2=0}^{2^n-1} \omega_{2^n}^{j_2 x}|j_1 j_2\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{j_1=0}^{2^n-1}|j_1\rangle \otimes \frac{1}{\sqrt{2^n}}\sum_{j_2=0}^{2^n-1}\omega_{2^n}^{j_2 x}|j_2\rangle = |+\rangle^{\otimes n} \otimes F_{2^n}|x\rangle. \end{aligned}$$

   Then applying $F_{2^n}^{-1}$ to the last $n$ qubits gives final state $|+\rangle^{\otimes n}|x\rangle$.

   (b) Suppose there exists such a circuit $C$ which uses $T$ two-qubit gates where the control bit lies in the first $n$ qubits of the state and the target qubit lies in the second $n$ qubits (or vice versa), and an arbitrary number of other gates. We will use this to let Alice transfer an arbitary $n$-bit string $x$ to Bob using $2T$ qubits of communication, and then invoke Holevo's theorem to conclude $T = \Omega(n)$.

   To allow Alice to transfer her $x$ to Bob, Alice and Bob prepare the $2n$-qubit state $|x\rangle_A|0^n\rangle_B$, which they can do without any communication. Now they jointly run the

circuit $C$ gate-by-gate. Gates acting on qubits that are all in the first $n$ qubits can be done by Alice without Bob's help; gates acting on qubits that are all in the second $n$ qubits can be done by Bob without Alice's help. Whenever a two-qubit gate needs to be applied where the control bit lies in the first $n$ qubits of the state and the target qubit lies in the second $n$ qubits (or vice versa), Bob sends his qubit of that pair to Alice, who locally applies the two-qubit gate, and sends back Bob's qubit. So each such two-qubit gate "costs" 2 qubits of communication. This way they implement $C$ using $2T$ qubits of communication. Now Bob locally applies $F_{2^n}^{-1}$, for which no communication is needed. By part (a) the final state will be $|+\rangle_A^{\otimes n}|x\rangle_B$, so Bob has learned $x$.

4. **(2 points)**

   (a) We first query $f(0^n)$, which is $b$. Then we apply the Bernstein-Vazirani algorithm: with one phase query we create state

   $$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle = (-1)^b\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x}|x\rangle.$$

   $H^{\otimes n}$ changes this state to $(-1)^b|a\rangle$, and a measurement in the computational basis gives us $a$. Thus we spent one query to learn $b$ and one query to learn $a$.

   (b) First run the algorithm from part (a), at the expense of 2 queries to $f$. This returns some $a\in\{0,1\}^n$ and $b\in\{0,1\}$. Define affine-linear function $g(x)=a\cdot x+b \bmod 2$. If we are in case (1), then $f=g$. If, on the other hand, we are in case (2), then $f(x)\neq g(x)$ for at least $t=\varepsilon 2^n$ of all $2^n$ $x\in\{0,1\}^n$. Use Grover with $O(\sqrt{2^n/t})=O(1/\sqrt{\varepsilon})$ queries to $f$ and the same number of applications of a circuit for $g$ (which costs no queries since we know $a,b$) to find an $x$ where $f(x)\neq g(x)$ with probability $\geq 2/3$, if such an $x$ exists. If Grover found such an $x$ then we know for certain that we are in case (2). If Grover did not find such an $x$ then we conclude that we are in case (1). This distinguishes the two cases with success probability $\geq 2/3$, using $2+O(1/\sqrt{\varepsilon})=O(1/\sqrt{\varepsilon})$ queries.

5. **(2 points)**

   (a) First Alice sends the numbers $a$ and $b$ to Bob, which costs $O(\log n)$ classical bits of communication. Now they both know the interval $[a,b]$, which contains $b-a+1$ indices. Then they can run the protocol of Section 15.4 to find an $i\in[a,b]$ such that $x_i=y_i=1$ (if such an $i$ exists), using $O(\sqrt{b-a+1}\,\log n)$ qubits of communication.

   (b) We will use binary search with a shrinking interval $[a,b]$, to "zoom in" on the smallest $i$ where $x_i=y_i=1$.

   There will be $\log(n)+1$ binary search steps, indexed by $j=1,\ldots,\log(n)+1$. For $j=1$, start with $a=1$ and $b=n$ and run the protocol from (a), with error probability reduced to $p_1=\frac{1}{3}2^{-1}$. This tells us whether there exists an $i\in[a,b]$ such that $x_i=y_i=1$.

   If we found a solution in the $j$th binary search step, then for the $(j+1)$st step we replace $b$ by $b-(b-a+1)/2$; and if we did not find a solution in the $j$th step then we replace $a$ by $a+(b-a+1)/2$. This way the search space is going down by a factor 2 in each binary search step: in the $j$th step we run the protocol of (a) on an interval $[a,b]$ with $b-a+1=n/2^{j-1}$. After $\log(n)+1$ steps (assuming none made an error)

we have $a = b$, and then it just remains to check whether $x_a = y_a = 1$. We reduce the error probability of the $j$th step to $p_j = \frac{1}{3}2^{-j}$ in the usual way, at the expense of $O(\log(1/p_j)) = O(j)$ repetitions of the (a)-protocol in the $j$th step. Thus the cost of the $j$th step is $O(j\sqrt{n/2^j}\,\log n)$ qubits of communication.

The overall error probability is at most the sum of error probabilities of the $\log n$ different runs, which is at most

$$\sum_{j=1}^{\log(n)+1} p_j = \sum_{j=1}^{\log(n)+1} \frac{1}{3}2^{-j} \leq \frac{1}{3}.$$

The overall communication is the sum over all $\log(n)+1$ binary search steps:

$$\sum_{j=1}^{\log(n)+1} O\left(j\sqrt{\frac{n}{2^j}}\,\log n\right) = O(\sqrt{n}\log n) \sum_{j=1}^{\log(n)+1} \frac{j}{\sqrt{2^j}} = O(\sqrt{n}\log n).$$