Quantum Computing (5334QUCO8Y), Exam

Ronald de Wolf

Tuesday Jan 13, 2026, 10:00–13:00
rooms NTH A5.01+A5.02, 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. You are allowed to refer to things explained in the lecture notes, or things that were part of homework exercises that you did, without re-explaining their details in your answer (just state clearly what the invoked construction achieves and where you got it from).

The total number of points adds up to 9; your exam grade is 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 half-integer (except 5.5).

1. **(1 point)** $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$ is sometimes called "the square root of NOT." Explain why.

2. **(2 points)** This exercise is about reducing the error probability in Simon's algorithm to 0.

   (a) Suppose we have $k \leq n-2$ linearly independent strings $j_1, \ldots, j_k \in \{0,1\}^n$ that are orthogonal to the hidden string s (i.e., $j_\ell \cdot s = 0 \bmod 2$, for all $\ell \in \{1,\ldots,k\}$). Let V be the subspace of 2^k strings that they span (with bitwise addition mod 2). In the setting of Simon's problem, give a quantum algorithm that uses $O(1)$ queries and *with probability 1* outputs some $j \notin V$ such that $j \cdot s = 0 \bmod 2$. You don't need to write out the circuit fully, but be precise about what you're applying, what the different components are etc. *Hint: Amplitude amplification (Sec 7.3) can be made exact if we know p; you may use this without proof.*

   (b) Give a quantum algorithm that finds s with probability 1, using $O(n)$ queries.

3. **(1.5 points)** Suppose Alice, Bob, and Charlie share the 3-qubit "GHZ-state" $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, each of them holding one qubit.

   (a) What is the local density matrix of Charlie's qubit (viewing the 2 qubits of Alice and Bob as one party)?

   (b) What is the local density matrix of the 2-qubit state held by Alice and Bob?

   (c) Give a protocol where Charlie measures his qubit in some way, communicates the outcome (one classical bit) to Bob, who then applies a local operation so that Alice and Bob end up with an EPR-pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

4. **(2 points)** This exercise gives a version of Trotter methods with a better dependence of the circuit-size on the evolution-time t and the approximation error ε than the $O(t^2/\varepsilon)$ 2-qubit gates of basic Trotter (Section 9.2). Let A, B be Hermitian matrices of the same dimension and operator norm $\| A \|, \| B \| \leq 1$. You may assume the following fact without proof[1]: for every $\eta \in [0,1]$ there exists a matrix E of operator norm $\| E \| = O(\eta^3)$ such that

$$e^{i\eta(A+B)} = e^{i\eta A/2} e^{i\eta B} e^{i\eta A/2} + E. \tag{1}$$

Suppose $H = H_1 + H_2$ is an n-qubit Hamiltonian where H_1, H_2 are 2-local terms of operator norm ≤ 1. For every $t \geq 0$ and $\varepsilon \in (0, 1/2)$, give a circuit $\widetilde{U}$ of $O(t^{1.5}/\sqrt{\varepsilon})$ 2-qubit gates that approximates the unitary $U = e^{iHt}$ up to error ε (i.e., $\| U - \widetilde{U} \| \leq \varepsilon$). Every 2-qubit unitary counts as a 2-qubit gate here (don't worry about writing out in CNOTs and 1-qubit gates).
Hint: Very similar to the analysis of basic Trotter of Section 9.2.

5. **(2.5 points)** This exercise is about the Steane code, which (as you'll show) encodes 1 logical qubit into 7 physical qubits, and can correct an error on any one of the 7 physical qubits.

   (a) Consider the subspace $C \subseteq \{0,1\}^7$ spanned by the 3 elements $0001111, 0110011, 1010101$. Write out a list of the 8 elements of C.

   (b) Let $C' = \{c \oplus 1^7 \mid c \in C\}$ be the set of binary complements of C. It is easy to verify that the minimal Hamming distance between any two elements of $C \cup C'$ is at least 3 (you may assume this without proof in your answer). Show that there exists a procedure that, for every $c \in C \cup C'$, maps $X_j|c\rangle|0\rangle \mapsto X_j|c\rangle|j\rangle$, where $j \in \{1, \ldots, 7\}$ (so the bitflip-error acts on the jth qubit, and the procedure finds out the location j) and the second register consists of a number of initially-$|0\rangle$ qubits. You don't have to write out the details, just argue clearly why such a procedure exist.

   (c) The Steane code is defined by the two logical basis states

$$|\overline{0}\rangle = \frac{1}{\sqrt{8}} \sum_{c \in C} |c\rangle \quad \text{and} \quad |\overline{1}\rangle = \frac{1}{\sqrt{8}} \sum_{c' \in C'} |c'\rangle$$

   What is the 7-qubit unitary $\overline{X}$ on the physical qubits that corresponds to the logical X-gate? In other words, what simple 7-qubit unitary maps $|\overline{b}\rangle \mapsto |\overline{1-b}\rangle$?

   (d) Show that there exists a quantum procedure (which may involve measurements in the computational basis) that identifies and corrects a bitflip-error on any one of the 7 qubits, i.e., that maps $X_j(\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle)|0\rangle \mapsto (\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle)|j\rangle$.

   (e) Show that there exists a quantum procedure (which may involve measurements in the computational basis) that identifies and corrects a phaseflip-error on any one of the 7 qubits, i.e., that maps $Z_j(\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle)|0\rangle \mapsto (\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle)|j\rangle$.
   Hint: Consider the "dual code" $C^\perp = \{z \mid z \cdot c = 0 \pmod 2 \ \forall c \in C\}$. The set $C^\perp \cup (C^\perp \oplus 1^7)$ also has minimal distance 3 (you may assume this without proof). Use that $H^{\otimes 7}$ maps a uniform superposition over C to a uniform superposition over $C^\perp$ (this was part of homework Exercise 3.4, you may also assume this without proof). Also note that $HZ = XH$, so in some sense the Hadamard gate converts phaseflip-errors into bitflip-errors.

[1] This fact can be proved by taking 2nd-order Taylor expansions of the four exponentials involved in Eq. (1), and showing that the left- and right-hand sides match up to $O(\eta^3)$ terms. But you don't need to provide that proof. In the formula used for basic Trotter, the right-hand side was $e^{i\eta A} e^{i\eta B}$ with a bigger error term, of norm $O(\eta^2)$.

Model solutions

1. Because if you square this matrix then you get

$$\tfrac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \cdot \tfrac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$
$$= \tfrac{1}{4}\begin{pmatrix} (1+i)^2+(1-i)^2 & 2(1+i)(1-i) \\ 2(1+i)(1-i) & (1-i)^2+(1+i)^2 \end{pmatrix} = \tfrac{1}{4}\begin{pmatrix} 0 & 4 \\ 4 & 0 \end{pmatrix} = X$$

   which is the NOT-gate.

2. (a) The basic subroutine of Simon's algorithm (without the measurements) can be thought of as a unitary algorithm A that makes one query and that maps $|0^{2n}\rangle$ to a superposition $|\psi\rangle$ whose first register is uniform (up to ± 1 phases) over all 2^{n-1} strings $j \in \{0,1\}^n$ that are orthogonal to 0. But 2^k of those j's are in V, and we would like to remove those from the superposition using amplitude amplification. Define a j as "good" if $j \notin V$ and "bad" if $j \in V$, then we can write $|\psi\rangle = \sqrt{p}|G\rangle + \sqrt{1-p}|B\rangle$, where $p = (2^{n-1}-2^k)/2^{n-1}$ and the "good state" $|G\rangle$ has only good j's in its first register. Note that $p \geq 1/2$ because $k \leq n-2$. There exists a circuit (based on the strings $j_1, \ldots, j_k$) that puts a minus in front of good $|j\rangle$ and that leaves all other states alone, which (in the 2-dimensional space spanned by $|G\rangle$ and $|B\rangle$) corresponds to a reflection through $|G\rangle$. Because we know p exactly, we can now apply exact amplitude amplification to rotate $|\psi\rangle$ to exactly $|G\rangle$, and measuring the first register then gives a $j \notin V$ such that $j \cdot s = 0 \pmod 2$.
   Amplitude amplification uses $O(1/\sqrt{p}) = O(1)$ iterations, each of them using 1 application each of A and A^{-1}, hence we use $O(1)$ queries in total.

   (b) For $k = 0$ to $n-2$, apply the algorithm of (a) to generate (with probability 1) a sequence $j_1, \ldots, j_{n-1} \in \{0,1\}^n$ of linearly independent strings that are all orthogonal to $s \pmod 2$. Once we have these $n-1$ strings, we can classically solve (for instance using Gaussian elimination) the linear system $\{j_\ell \cdot z = 0\}_{\ell \in \{1,\ldots,n-1\}}$. This linear system has two solutions, namely $z = 0^n$ and $z = s$, so we find s with probability 1. Since we called the algorithm of (a) $n-1$ times, and each call uses $O(1)$ queries, the total number of queries is $O(n)$.

3. (a) The density matrix of the 3-qubit state can be written as

$$\frac{1}{2}(|00\rangle\langle 00|_{AB}|0\rangle\langle 0|_C + |00\rangle\langle 11|_{AB}|0\rangle\langle 1|_C + |11\rangle\langle 00|_{AB}|1\rangle\langle 0|_C + |11\rangle\langle 11|_{AB}|1\rangle\langle 1|_C)$$

   Tracing out the AB-system gives Charlie's local state as

$$\begin{aligned}\rho_C &= \tfrac{1}{2}(\mathrm{Tr}(|00\rangle\langle 00|)|0\rangle\langle 0| + \mathrm{Tr}(|00\rangle\langle 11|)|0\rangle\langle 1| + \mathrm{Tr}(|11\rangle\langle 00|)|1\rangle\langle 0| + \mathrm{Tr}(|11\rangle\langle 11|)|1\rangle\langle 1|) \\ &= \tfrac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|),\end{aligned}$$

   where we used $\mathrm{Tr}(|00\rangle\langle 00|) = \mathrm{Tr}(|11\rangle\langle 11|) = 1$ and $\mathrm{Tr}(|00\rangle\langle 11|) = \mathrm{Tr}(|11\rangle\langle 00|) = 0$.

   (b) Tracing out the C-system gives

$$\begin{aligned}\rho_{AB} &= \tfrac{1}{2}(|00\rangle\langle 00|\mathrm{Tr}(|0\rangle\langle 0|) + |00\rangle\langle 11|\mathrm{Tr}(|0\rangle\langle 1|) + |11\rangle\langle 00|\mathrm{Tr}(|1\rangle\langle 0|) + |11\rangle\langle 11|\mathrm{Tr}(|1\rangle\langle 1|)) \\ &= \tfrac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|),\end{aligned}$$

   where we used $\mathrm{Tr}(|0\rangle\langle 0|) = \mathrm{Tr}(|1\rangle\langle 1|) = 1$ and $\mathrm{Tr}(|0\rangle\langle 1|) = \mathrm{Tr}(|1\rangle\langle 0|) = 0$

(c) Charlie applies a Hadamard gate to his qubit, which turns the 3-qubit state into

$$\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle) = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle + \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)|1\rangle\right).$$

Charlie then measures his qubit and sends the result (0 or 1) to Bob. If Bob received 0 then the AB-state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and if Bob received 1 then the AB-state is $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. So Bob can apply a Z-gate to his qubit conditioned on the bit he received from Charlie, then Alice and Bob end up with an EPR-pair.

4. Use Eq. (1) with $A = H_1$ and $B = H_2$. Let $r = t/\eta$ (for some η to be chosen later) be an integer. Define $\widetilde{U} = (e^{i\eta H_1/2}e^{i\eta H_2}e^{i\eta H_1/2})^r$. Because each of $e^{i\eta H_1/2}, e^{i\eta H_2}, e^{i\eta H_1/2}$ is a 2-qubit gate (with identities on the other $n-2$ qubits), $\widetilde{U}$ is a circuit of $3r$ 2-qubit gates. We can upper bound the approximation error by

$$\begin{aligned}\|\,U - \widetilde{U}\,\| &= \|\,(e^{i\eta(H_1+H_2)})^r - (e^{i\eta H_1/2}e^{i\eta H_2}e^{i\eta H_1/2})^r\,\| \\ &\le r\cdot \|\underbrace{e^{i\eta(H_1+H_2)} - e^{i\eta H_1/2}e^{i\eta H_2}e^{i\eta H_1/2}}_{E}\| = r\cdot O(\eta^3) = O(t\eta^2),\end{aligned}$$

where the first inequality follows like in Ex 4.4 of the homework. Choose $\eta = O(\sqrt{\varepsilon/t})$ with a sufficiently small constant in the $O(\cdot)$ so that the approximation error is $\le \varepsilon$. The number of 2-qubit gates in $\widetilde{U}$ is $3r = 3t/\eta = O(t^{1.5}/\sqrt{\varepsilon})$.

5. (a) $0000000, 0001111, 0110011, 1010101, 0111100, 1011010, 1100110, 1101001$.

(b) Because any two distinct strings $c, c' \in C \cup C'$ are at Hamming distance at least 3, the string $\tilde{c}$ that is c with the jth bit flipped, is closer to c than to any other $c' \in C \cup C'$. There is a classical procedure to find out what the closest c is to such a given $\tilde{c}$, and then the location j is the one location where c and $\tilde{c}$ differ. There is a classical circuit (say, made up of Toffoli gates, possibly with extra auxiliary qubits that start and end in $|0\rangle$) that does the procedure, writes j in the second register, sets any additional workspace qubits back to $|0\rangle$ by reversing, and thus implements the required map.[2]

(c) Note that $|\overline{1}\rangle = X^{\otimes 7}|\overline{0}\rangle$ because there is a 1-to-1 correspondence between the elements of C and C' by flipping all 7 bits, so we can set $\overline{X} = X^{\otimes 7}$.

Comment: This is an example of a transversal operation: the logical X-gate on the logical qubit corresponds to applying an X-gate to each of the physical qubits.

(d) First assume the logical qubit before the bitflip-error is just $|\overline{0}\rangle$ (i.e., $\alpha = 1, \beta = 0$) or $|\overline{1}\rangle$ (i.e., $\alpha = 0, \beta = 1$). We can run the procedure of part (b) as a unitary quantum circuit. Then conditioned on the value in the second register, apply an X-gate to the jth location to correct the bitflip-error (it doesn't matter here that the second register is left in state $|j\rangle$ rather than $|0\rangle$, because these are now classical bits, in tensor product with the logical qubit).

Note that by linearity, this bitflip-correction procedure will also work on superpositions $X_j(\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle)$.

[2]The Steane code is designed to make this circuit very simple, measuring a few Pauli-terms to write down syndrome bits in the second register from which j can easily be inferred, but you don't have to write it out.

(e) Suppose the state where we need to correct a phaseflip-error is $Z_j|\overline{0}\rangle$. Applying $H^{\otimes 7}$ and using that $HZ = XH$, we get $X_j H^{\otimes 7}|\overline{0}\rangle$. The state $H^{\otimes 7}|\overline{0}\rangle$ is a superposition over the elements of $C^{\perp}$, which have pairwise distance at least 3. The X_j is a *bitflip*-error on this superposition. Hence by a procedure like in (b) we can find the location j of that bitflip and write it in the second register. Doing another $H^{\otimes 7}$, we map $Z_j|\overline{0}\rangle|0\rangle \mapsto Z_j|\overline{0}\rangle|j\rangle$.

Exactly the same procedure will map $Z_j|\overline{1}\rangle|0\rangle \mapsto Z_j|\overline{1}\rangle|j\rangle$.

Now conditioned on the value in the second register, apply a Z-gate to the jth qubit to correct the phaseflip-error.

By linearity, this phaseflip-correction also works on superpositions $Z_j(\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle)$.