Quantum Computing 2020 - Homework notes

February 28, 2020

Introduction

This document aims at correcting common mistakes and explaining in what form we would like the students to write down their solutions. We will update both the general notes and specific notes usually every week. We strongly recommend that you read the new notes every other week.

General notes

Writing & Grading

- Please take your time and check what you write down; if your solution is unreadable or messy then we will deduct points. The same holds for low-resolution scans or low-contrast pictures.
- We do not require you to repeat the question in your answer. However, read the questions carefully, because there are usually students who answer a different question than asked, and thus lose points unnecessarily. Also, if you do repeat the question, be clear about where the question ends and your answer starts. You also do not have to repeat definitions from the lecture notes.
- Say what your symbols mean, don't let us guess. Explain where a specific formula you introduce comes from, especially if you try to prove something indirectly by deriving a contradiction from the assumption that what you want to prove is false. State the conclusion of your arguments explicitly.
- Be careful with the usage of the word "this"; it should be unambiguous what you're referring to. Similarly with "clearly", "it is evident", and "it is easy to see"; often these words get used to avoid writing down necessary explanation.
- The bra (conjugate transpose) of a vector reverses the order of matrix product, but not the order of states (tensor factors). For example, $(U|\phi\rangle)^* = \langle\phi|U^*$, but $(|\phi\rangle|\psi\rangle)^* = \langle\phi|\langle\psi|$.
- Try to use Dirac notation instead of matrix-vector notation when possible. Once you get used to it, it's very convenient. Stick to the notation of the notes, don't do funny things like using kets inside bras (which is meaningless).
- If you're applying a gate to some of the qubits of a state, you have to put identity matrices for the qubits that are left alone. For example, writing $H|01\rangle$ is wrong because it could be $H \otimes I|01\rangle$ or $I \otimes H|01\rangle$ depending on whether the H is applied to the first or second of the two qubits.
- If we ask for a circuit, you really have to draw a circuit. To show that the circuit works correctly on all possible quantum states, it suffices to show that it works correctly on all basis states (linearity implies that then it will also work correctly on all superpositions of basis states).

- When talking about measurement, be precise who measures which qubits and how (most commonly, "in the computational basis"). Say "Alice's measurement outcome is 0" instead of "Alice measures 0"; the latter is ambiguous between measuring a qubit that is in state $|0\rangle$, and receiving outcome 0 from the measurement.

- The convention when you use additional workspace-qubits to implement a unitary U, is that these workspace-qubits should start and end the computation in a fixed state (typically $|0\rangle$). You don't want the workspace-qubits to end in a state that depends on the initial state that U operates on, because this would mess up intended interference effects. Exercise 9 of Ch 2 illustrates what goes wrong if you do not set the workspace qubits(s) back to $|0\rangle$.

- Sometimes a hint is given (in Appendix C) that sketches the proof, requiring you to work out the details. In these cases, do not assume the hint as part of the question, write a full proof. In general, an answer should be clear without knowing the hint. If a hint gives you a fact (for instance the existence of an efficient algorithm for testing if a number is prime), then you can invoke that fact in your answer without first proving/deriving that fact. You can email Ronald if a question is unclear, but don't email asking for more hints.

- For grading: when we give the points for an exercise we write things like 1.5/2, meaning that you get 1.5 points out of 2 for this exercise.

Specific comments for Homework set 2 (Ch 2,3)

- 2.5:
  Be careful about the order of A, B, C here; operations are applied right-to-left in matrix multiplication but left-to-right in the circuit.

- 2.8, Example solution:
  (a) The following implements a regular query (i.e., one of the first type) using one controlled phase query and a few other gates. Assume for simplicity that the control-qubit is at the end, so the controlled phase query maps, for $i \in \{0, \dots, N-1\}$ and $c \in \{0,1\}$:

  $$|i, c\rangle \mapsto (-1)^{cx_i}|i, c\rangle.$$

  We want to implement a regular query on basis state $|i, b\rangle$. Start by a Hadamard gate on the last qubit, which turns the state into:

  $$|i\rangle\frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle).$$

  Applying a controlled phase query gives

  $$|i\rangle\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{b+x_i}|1\rangle).$$

  Applying another Hadamard on the last qubit gives $|i, b \oplus x_i\rangle$. This shows that we've implemented the regular query correctly on all basis states $|i, b\rangle$. By linearity we have then implemented it correctly on all possible states.

  (b) If you only have *un*controlled phase queries, then you cannot implement a regular query (i.e., one of the first type). This can be seen as follows. If the input string x is all-0, then the unitary $O_{x,\pm}$ is the identity matrix I, while if x is all-1, then $O_{x,\pm} = -I$. This means that a circuit that uses $O_{x,\pm}$ any number of times, cannot see the different between all-0 and all-1 input x: the two circuits for those two inputs will differ only by a global phase ± 1, and there's no measurement that can detect this global phase. In contrast, a regular query can see the difference between all-0 and all-1 inputs, for instance by querying the first bit. Therefore it is impossible to implement a regular query using a circuit consisting only of uncontrolled phase queries and elementary gates.

- 3.3.d:
  After applying a measurement to the state the measured state will "collapse" to a normalized state. Hence you must normalize the resulting state.

- 3.1, Example solution:
  For $z \in \{0,1\}^n$, define $P_z = I \otimes |z\rangle\langle z|$, where the first identity has dimension 2^n. The projective measurement is described by the set $\{P_z : z \in \{0,1\}^n\}$ of 2^n projectors, one for each possibly measurement outcome z.

- 3.4, Example solution:
  The measurement of the second register in Simon's algorithm yields some value x_i, and the first register then collapses to a uniform superposition of all $k \in \{0,1\}^n$ for which $x_k = x_i$:

  $$\frac{1}{\sqrt{|V|}} \sum_{v \in V} |i \oplus v\rangle.$$

  Now the algorithm does Hadamard gates on these n qubits, which turns the state of the first register into

  $$\frac{1}{\sqrt{|V|}} \sum_{v \in V} \frac{1}{\sqrt{2^n}} \sum_{j \in \{0,1\}^n} (-1)^{(i \oplus v)\cdot j} |j\rangle = \frac{1}{\sqrt{|V| 2^n}} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} \left(\sum_{v \in V} (-1)^{v \cdot j} \right) |j\rangle.$$

  We want to analyze the sum within the parentheses. First, suppose j is such that $v \cdot j = 0 \pmod 2$ for all $v \in V$. Then all the terms in the sum are $(-1)^0 = 1$, so the sum is $|V|$, and the overall amplitude of such a basis state $|j\rangle$ is $(-1)^{i \cdot j} \sqrt{|V|/2^n}$.

  Second, suppose j is such that $w \cdot j = 1 \pmod 2$ for some particular $w \in V$. Then $v \cdot j = 1 \pmod 2$ for *exactly half* of the elements $v \in V$. This can be seen for instance by pairing up the elements $v \in V$ with $v \oplus w$ (which is also in V because V is a subspace): $v \cdot j \neq (v \oplus w) \cdot j$ because $w \cdot j = 1$. Hence one of the vectors of the pair $v, v \oplus w$ has inner product 1 with j, and the other vector of the pair has inner product 0. Therefore the sum within the parentheses contains equally many $+1$s as -1s, and adds up to 0. So js of the second kind have amplitude 0. (Another way to see this fact is to observe that there are $2^n/|V|$ js of the first kind, and since each of them has squared amplitude $|V|/2^n$, there's no amplitude "left" for the js of the second kind.)

  Accordingly, if we now measure the first register, we will sample uniformly from the js of the first kind (i.e., where $v \cdot j = 0 \pmod 2$ for all $v \in V$).

Specific comments for Homework set 1 (Ch 1)

- 1.7, Example solution:
  Assume, towards a contradiction, that there exists a 2-qubit unitary U such that $U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$ for every 1-qubit state $|\phi\rangle$. Then in particular, if $|\phi\rangle$ is one of the two basis states, we get:

  $$U|0\rangle|0\rangle = |0\rangle|0\rangle \text{ and } U|1\rangle|0\rangle = |1\rangle|1\rangle.$$

  Now we try U on $|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Using linearity of U and its above behaviour on $|0\rangle|0\rangle$ and $|1\rangle|1\rangle$, we get

  $$U|\phi\rangle|0\rangle = U\left(\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle\right) = \frac{1}{\sqrt{2}}U|0\rangle|0\rangle + \frac{1}{\sqrt{2}}U|1\rangle|0\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle.$$

  But the latter state is an EPR-pair, hence entangled, hence cannot be equal to the intended product state $|\phi\rangle|\phi\rangle$.

- 1.11.c: Bob doesn't measure, so don't give probabilities for measurement outcomes on Bob's side, but describe the states that his qubits ends up in when Alice's measurement gives outcome 0 or 1, respectively.
- 1.11.d: say explicitly that & what Alice communicates. Just like in regular teleportation, the communication of classical information (i.e., sending over Alice's measurement outcome) is crucial. Note that Bob does not learn the value θ.