Quantum Computing: Exercise Sheet 2

Maris Ozols

November 9, 2016

Lecture 5: Quantum information processing protocols

1. **Transpose trick.** Let $|\Psi\rangle = \sum_{i=1}^{n} |i\rangle \otimes |i\rangle$ and M be any $n \times n$ matrix and I be the $n \times n$ identity matrix. Show that $(M \otimes I)|\Psi\rangle = (I \otimes M^{\mathsf{T}})|\Psi\rangle$ (see Hint 1).

---

2. **Bell states.** Let $z, x \in \{0, 1\}$ and $|\beta_{zx}\rangle = \frac{1}{\sqrt{2}}(|0, x\rangle + (-1)^z|1, \bar{x}\rangle)$ be one of the four Bell states. Note that $H|z\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^z|1\rangle)$ and $\text{CNOT}|z, x\rangle = |z, x \oplus z\rangle$. Verify the following identities:

   (a) preparation: $|\beta_{zx}\rangle = \text{CNOT} \cdot (H \otimes I) \cdot |z, x\rangle$,

   (b) unpreparation: $|z, x\rangle = (H \otimes I) \cdot \text{CNOT} \cdot |\beta_{zx}\rangle$,

   (c) local conversion: $|\beta_{zx}\rangle = (I \otimes X^x Z^z) \cdot |\beta_{00}\rangle = (Z^z X^x \otimes I) \cdot |\beta_{00}\rangle$ (see Hint 2).

---

3. **Superdense coding.** Verify the superdense coding identity:

$$(H \otimes I) \cdot \text{CNOT} \cdot (Z^z X^x \otimes I) \cdot |\beta_{00}\rangle = |z, x\rangle$$

   Explain in your own words how it corresponds to the picture given in Lecture 5 slides.

---

4. **Teleportation.** Explain in your own words how the teleportation identity

$$|\psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{2} \sum_{z,x \in \{0,1\}} |\beta_{zx}\rangle \otimes (X^x Z^z |\psi\rangle)$$

   corresponds to the picture of the teleportation protocol given in the Lecture 5 slides (see Hint 3).

   (☠) It can be checked that $\frac{1}{2} \sum_{z,x \in \{0,1\}} (Z^z X^x) \otimes (X^x Z^z)$ is the SWAP gate (see Lecture 4) between the first and the second qubit. Given this, verify the teleportation identity.

Lecture 6: Quantum search

5. **Grover's algorithm.** Let $a \in \{1, \ldots, N\}$ denote the unique marked element and $|a\rangle \in \mathbb{C}^N$ be the corresponding standard basis vector. Let

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{s=1}^{N} |s\rangle \in \mathbb{C}^N, \qquad |u\rangle = \frac{1}{\sqrt{N-1}} \sum_{s \neq a} |s\rangle \in \mathbb{C}^N$$

be the uniform superpositions over all elements and all unmarked elements, respectively (note that $\{|a\rangle, |u\rangle\}$ is an orthonormal basis). Let θ be an angle such that $\cos\theta = \sqrt{\frac{N-1}{N}}$ and $\sin\theta = \sqrt{\frac{1}{N}}$.

(a) Show that $|\Psi\rangle = \sin\theta|a\rangle + \cos\theta|u\rangle$.

(b) Describe by 2×2 matrices how $V = I - 2|a\rangle\langle a|$ and $W = 2|\Psi\rangle\langle\Psi| - I$ act in the basis $\{|a\rangle, |u\rangle\}$.

(c) Compute the 2×2 matrix corresponding to the Grover iterate $G = WV$ in the basis $\{|a\rangle, |u\rangle\}$.

(d) Compute the 2×2 matrix corresponding to G^t for any integer t (see Hint 4).

(e) Substitute $t = \frac{\pi/2}{2\theta}$ in the above matrix and compute $|\langle a|G^t|\Psi\rangle|^2$, i.e., the probability of finding the marked element a, and express it as a function of N.

(f) (☠) We would like $t = \frac{\pi/2}{2\theta}$ to be an integer since t corresponds to the number of iterations in Grover's algorithm. While in general $t = \frac{\pi/2}{2\theta}$ is not an integer, we can simply round it down to the *closest integer*. Explain why this can only increase the success probability (see Hint 5).

Lecture 7: Quantum factoring

6. **Using order finding to factor.** We want to factor $N = 21$ using order finding. Assume the random number a we picked in the first step of the reduction is

   (a) $a = 7$

   (b) $a = 10$

   Go through the remaining steps of the reduction and determine the factors of N. (You can use a calculator or computer to compute gcd and to find orders.)

---

7. **Roots of unity.** Let $\omega = \exp(2\pi i/M)$ be the M-th root of unity. Verify the following properties:

   (a) $\sum_{k=0}^{M-1} \omega^k = 0$ (see Hint 6),

   (b) $\sum_{k=0}^{M-1} \omega^{ak} = M\delta_{a,0}$ for any integer a, where $\delta_{a,0} = 1$ if $a \equiv 0 \pmod{M}$ and $\delta_{a,0} = 0$ otherwise.

---

8. **Discrete Fourier transform.** Let D denote the $M \times M$ discrete Fourier transform. Write down an expression for the matrix entry $(D^\dagger)_{kl}$. Verify that D is unitary.

---

9. (☠) **Product representation of the QFT output.** Let D be the $2^n \times 2^n$ discrete Fourier transform. Prove that

$$D|b_1 b_2 \ldots b_n\rangle = \frac{1}{\sqrt{2^n}}\big(|0\rangle + \beta_n|1\rangle\big) \otimes \big(|0\rangle + \beta_{n-1}|1\rangle\big) \otimes \cdots \otimes \big(|0\rangle + \beta_1|1\rangle\big)$$

   where $\beta_j = \exp(2\pi i 0.b_j b_{j+1} \ldots b_n)$ and $0.b_j b_{j+1} \ldots b_n \in [0, 1]$ (see Hint 7).

---

10. **QFT on 1 qubit.** Write down the matrix corresponding to the 1-qubit quantum Fourier transform.

---

11. **QFT on 2 qubits.** Write down the matrix corresponding to the 2-qubit quantum Fourier transform and draw the quantum circuit for implementing it. Write down also the matrix product that corresponds to this circuit and the matrix representation of each gate in the product. (You don't need to actually multiply the matrices together to verify that this is correct.)

---

12. **Shor's algorithm.** The quantum part of Shor's algorithm determines the period of some function f by evaluating it in superposition on all inputs x and then measuring the value of $f(x)$ (this is the first measurement in Shor's algorithm).

    (a) How is the outcome f_0 of this measurement used later in Shor's algorithm?

    (b) How does this measurement help us to reveal the period of f?

    (c) Why does it make no difference whether we measure the second register before or after we apply the QFT?

Lecture 8: Quantum automata and complexity

13. **Language accepted by a quantum automaton.** Consider a quantum automaton with a single-letter input alphabet $\Sigma = \{a\}$ and states $Q = \{q_0, q_1\}$, where q_0 is the initial as well as the unique accepting state. The transition matrix corresponding to the input letter a is given by

$$M_a = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

where $\theta = \pi/3$. What is the language accepted by this automaton? (Recall that a word belongs to the language if it is accepted with probability $\geq 2/3$, while it does not belong if it is rejected with probability $\geq 2/3$.) How many states would a deterministic automaton need to accept the same language?

---

14. **Probability amplification.** Let M be a randomized (or quantum) algorithm. Suppose a string w is such that M either accepts or rejects it with probability $\geq 2/3$. We construct a new algorithm M' that executes $2n+1$ independent runs of M on the same input w and decides acceptance/rejection based on majority vote. What is the acceptance/rejection probability threshold for M' if

    (a) $2n+1 = 3$,

    (b) (☠) $2n+1 = 101$?

---

15. **Complexity classes.** Explain in your own words why we have the following inclusions:

    (a) $\mathsf{P} \subseteq \mathsf{QMA}$,

    (b) (☠) $\mathsf{BQP} \subseteq \mathsf{EXP}$ (try to give a direct argument!).

    Which complexity classes would become equal if

    (c) deterministic classical computers could simulate quantum computers;

(d) a polynomial-time deterministic classical algorithm for factoring would be found?

Hint 1. Check that both sides agree entry-wise.

Hint 2. The second equality follows from the transpose trick.

Hint 3. Bell measurement corresponds to measuring in the orthonormal basis given by the Bell states $|\beta^{zx}\rangle$. If Alice's Bell measurement gives outcomes $z, x \in \{0, 1\}$, what is Bob's post-measurement state?

Hint 4. The action of G in the 2-dimensional subspace spanned by $\{|a\rangle, |u\rangle\}$ is described by

$$\begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}.$$

This is a rotation by angle 2θ, so G^t is a rotation by angle $2\theta t$.

Hint 5. If $t = \frac{\pi/2}{2\theta}$ then G^t rotates by what angle? Draw a picture and find where the final state ends up.

Hint 6. You can prove this by contradiction (assume the sum is not 0 and multiply both sides by ω) or using the formula for the sum of the first M terms in a geometric progression.

Hint 7. Left-multiply both sides by $\langle a_1 a_2 \cdots a_n|$ to verify that they agree entry-wise.