CS 6846: Quantum Algorithms and Cryptography Aug 14, 2022

Homework 1

Instructor: Shweta Agrawal *Due: Aug 24, 5 pm.*

Instructions:

1. Please type up your solutions using latex.
2. You may collaborate with other students. Please mention the names of your collaborators or any other source that you use for the solution.
3. Please type up your solutions *individually* without any help.

Problem 1: Building Gates

1. Construct a CNOT from two Hadamard gates and one controlled-Z (the controlled-Z gate maps $|11\rangle$ to $-|11\rangle$ and acts like the identity on the other basis states).
2. A SWAP-gate interchanges two qubits: it maps basis state $|a, b\rangle$ to $|b, a\rangle$. Implement a SWAP gate using a few CNOTs (when using a CNOT, you're allowed to use either of the 2 bits as the control, but be explicit about this).

Problem 2: Understanding Unitary

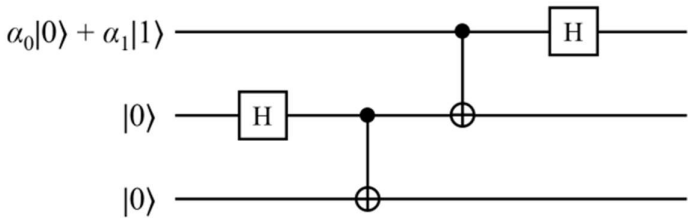
A matrix A is inner product-preserving if the inner product $\langle Av|Aw\rangle$ between Av and Aw equals the inner product $\langle v|w\rangle$, for all vectors v, w. A is norm-preserving if $\|Av\| = \|v\|$ for all vectors v, i.e., A preserves the Euclidean length of the vector. A is unitary if $A^\dagger A = AA^\dagger = I$. In the following, you may assume for simplicity that the entries of the vectors and matrices are real, not complex.

1. Prove that A is norm-preserving if, and only if, A is inner product-preserving.
2. Prove that A is inner product-preserving iff $A^\dagger A = AA^\dagger = I$.
3. Conclude that A is norm-preserving iff A is unitary.

Bonus: prove the same for complex instead of real vector spaces.

Problem 3: Quantum Circuits

Consider the following quantum circuit:



- Determine with proof the state of the three qubits at the end of the circuit's operation.
- If we then measure the three qubits, give the outcomes and their probabilities that arise.

Problem 4: Leveraging Parity

Let $N = 2^n$. A parity query to input $x \in \{0,1\}^N$ corresponds to the $(N+1)$-qubit unitary map $Q_x : |y, b\rangle \rightarrow |y, b \oplus xy\rangle$, where $xy = \sum_{i=0}^{N-1} x_i y_i \mod 2$. For a fixed function $f : \{0,1\}^N \rightarrow \{0,1\}$, give a quantum algorithm that computes $f(x)$ using only one such query (i.e., one application of Q_x), and as many elementary gates as you want.

Problem 5: Classical Comparison

Give a randomized classical algorithm that makes only two queries to x, and decides the Deutsch-Jozsa problem with success probability at least 2/3 on every possible input.

Problem 6: Fun with Deutsch-Jozsa

Let $N = 2^n$. Suppose that the truth table of our function $f : \{0,1\}^n \rightarrow \{0,1\}$ satisfies the following promise: either (1) the first $N/2$ bits of the truth table are all 0 and the second $N/2$ bits are all 1; or (2) the number of 1s in the first half of the truth table plus the number of 0s in the second half, equals $N/2$. Modify the Deutsch-Jozsa algorithm to efficiently distinguish these two cases (1) and (2).

Problem 7: Simon's Algorithm

Suppose we run Simon's algorithm for the function $f : \{0,1\}^3 \to \{0,1\}^3$ described as:

$f(000) = f(111) = 000$
$f(001) = f(110) = 001$
$f(010) = f(101) = 010$
$f(011) = f(100) = 011.$

Note that f is 2-to-1 and $f(x) = f(x \oplus 111)$ for all $x \in \{0,1\}^3$, so $s = 111$.

1. Give the starting state of Simon's algorithm.
2. Give the state after the first Hadamard transforms on the first 3 qubits.
3. Give the state after applying the oracle.
4. Give the state after measuring the second register (suppose the measurement gave $|001\rangle$).
5. Using $H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{\langle x,z \rangle} |z\rangle$, give the state after the final Hadamards.
6. Why does a measurement of the first 3 qubits of the final state give information about s?
7. Suppose the first run of the algorithm gives $z = 011$ and a second run gives $z = 101$. Show that, assuming $s \neq 000$, those two runs of the algorithm already determine s.

Problem 8: Superdense Coding

Alice and Bob prepare an EPR pair (that is, two qubits in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. They each take one qubit home. Suddenly, Alice decides she wishes to convey one of 4 messages to Bob; in other words, she wants to convey a classical string $uv \in \{0,1\}^2$ to Bob. Alice does the following in the privacy of her own home: First, if $u = 1$, she applies a NOT gate to her qubit (else if $u = 0$ she does nothing here). Next, if $v = 1$, she applies a Z gate, to her qubit (else if $v = 0$, she does nothing here). Finally, she walks to Bob's house and silently hands him her qubit. Show that by measuring in an appropriate basis, Bob can exactly determine Alice's message $uv \in \{0,1\}^2$.

Problem 9: Deferred Measurements

For $0 \leq p \leq 1$, let COIN_p denote a gate that has no input and one output, the output being a random bit which is 1 with probability p and 0 with probability $1-p$. The standard way to augment the basic circuit model with randomness is to allow the use of $\mathsf{COIN}_{1/2}$ gates.

In our definition of quantum circuits, we allowed quantum gates, plus measurement at the very end. We saw in class that CCNOT can simulate the AND, OR, and NOT gates. To simulate $\mathsf{COIN}_{1/2}$ gates we suggested to pass a $|0\rangle$ qubit through a Hadamard gate and then measure it. However, if we want to use this random bit within our circuit, we need to augment the quantum circuit model by allowing "intermediate measurements" (i.e., measuring some qubits prior to the end of the computation). While this is okay both theoretically and physically, it makes the model somewhat more complicated.

Luckily, we can show that any computation done by a quantum circuit using intermediate measurements can be equivalently and nearly as efficiently done by a quantum circuit that only has a single measurement at the end. In this problem you won't quite prove this in full, but you'll get the essential idea.

Precisely, suppose C is a randomized circuit with n input bits, a ancilla bits, r $\mathsf{COIN}_{1/2}$ gates, s CCNOT gates, and m output bits (possibly including garbage). Describe a straightforward transformation to a quantum circuit C' with n input bits, $a+2r$ ancilla bits, $s+2r$ CCNOT/CNOT/Hadamard gates, and $m+r$ output bits, such that when the output bits are measured at the end of $C'(x)$, the probability distribution on the first m of them is exactly the same as the probability distribution on the output bits of $C(x)$.

Problem 10: Amplifying Success

Let $f : \{0,1\}^n \to \{0,1\}$ be a function and C be a randomized (or quantum) circuit that computes the function f in the sense that for every input x, it holds that

$$\Pr\big(C(x) = f(x)\big) \geq \frac{2}{3}$$

In class we discussed how by repeating this computation several times, we can make the probability of successful computation arbitrarily large. Formalize this. In more detail, design a circuit C' such that

$$\Pr\big(C'(x) = f(x)\big) \geq 1 - 2^{-n}$$