Assignment 4

You can either submit it electronically to Canvas or bring a physical copy to the lecture. This assignment is 12% in your total points. For the simplicity of the grading, the total points for the assignment is 60.

1 Problems that you’re required to submit solutions

Please only submit the solutions to problems in this section.

Problem 1.1 [10 points; 5 pts each]. Searching when the fraction of marked items is $1/4$ and $1/2$.

(1) Suppose that $f : \{0, 1\}^n \to \{0, 1\}$ has the property that, for exactly $\frac{1}{4}2^n$ of the values of $x \in \{0, 1\}^n$, $f(x) = 1$ and the goal is to find such an $x$. Show how to do this with a single query to $f$. (Hint: consider a single iteration of Grover’s algorithm.)

(2) Same question as part (1), except assume that $f$ has the property that for exactly $\frac{1}{2}2^n$ of the values of $x \in \{0, 1\}^n$, $f(x) = 1$. Can the $x$ still be found with one query?

Problem 1.2 [20 points; 4 pts each]. Classical and quantum algorithms of the AND problem.

Recall that, for Deutsch’s problem, there is a function $f : \{0, 1\} \to \{0, 1\}$ and the goal is to determine $f(0) \oplus f(1)$ with a single query to $f$. There is no classical algorithm that succeeds with probability more than $1/2$, whereas there is a quantum algorithm that succeeds with probability 1. This question pertains to a variation of Deutsch’s problem, which we’ll call the AND problem, where the goal is to determine $f(0) \land f(1)$ with a single query to $f$. ($\land$ denotes the logical AND operation.)

(1) Give a classical probabilistic algorithm that makes a single query to $f$ and predicts $f(0) \land f(1)$ with probability at least 2/3. (Note: the probability should be respect to the random choices of the algorithm; the input instance of $f$ is assumed to be worst-case.) It turns out that no classical algorithm can succeed with probability greater than 2/3 (but you are not asked to show this here).

(2) Give a quantum circuit that, with a single query to $f$, constructs the two-qubit state

$$\frac{1}{\sqrt{3}} \left((-1)^{f(0)} |00\rangle + (-1)^{f(1)} |01\rangle + |11\rangle \right).$$

(3) The quantum states of the form in part (a) are three-dimensional and have real-valued amplitudes. This makes it easy for us to visualize the geometry of these states (as vectors or lines in $\mathbb{R}^3$). Consider the four possible states that can arise from part (1), depending on which of the four possible functions $f$ is. What is the absolute value of the inner product between each pair of those four states?

(4) Based on parts (2) and (3), give a quantum algorithm for the AND problem that makes a single query to $f$ and: succeeds with probability 1 whenever $f(0) \land f(1) = 1$; succeeds with probability $8/9$ whenever $f(0) \land f(1) = 0$. 

1
(5) Note that the error probability of the algorithm from part (4) is one-sided in the sense that it is always correct in the case where \( f(0) \land f(1) = 1 \). Give a quantum algorithm for the AND problem that makes a single query to \( f \) and succeeds with probability 9/10. (Hint: take the output of the one-sided error algorithm from part (4) and do some classical post-processing on it, in order to turn it into a two-sided error algorithm with higher success probability.)

Problem 1.3 [15 points]. Another construction of the quantum Fourier transform. Here we consider another, recursive, construction of \( F_{2^n} \), the quantum Fourier transform on \( n \) qubits. This construction works if \( n \) is a power of 2. Suppose that we have an implementation of \( F_{2^n} \) and want to implement \( F_{2^{2n}} \).

Divide the \( 2^n \) qubits into two registers: the first \( n \) qubits, and the last \( n \) qubits. Define the unitary \( P \) on two registers such that \( P |x⟩|y⟩ = (e^{2πi/2^n})^m(x,y) |x⟩|y⟩ \), for all \( x,y ∈ \{0,1\}^n \), and where \( m(x,y) \) denotes the product of \( x \) and \( y \) as \( n \)-bit integers (e.g., 1101 denotes 13, and 0100 denotes 4, so \( m(1101,0100) = 13 \times 4 = 52 \)).

(1) Show that the above circuit followed by a swap of the two \( n \)-bit registers computes \( F_{2^n} \). (This swap is the unitary such that \( |x⟩|y⟩ \rightarrow |y⟩|x⟩ \) for \( x,y ∈ \{0,1\}^n \).)

(2) You may assume without proof that the operation \( P \) can be implemented at the asymptotic cost of multiplying two \( n \)-bit integers, which is \( O(n \log n \log \log n) \). Based on this, what is the resulting cost of computing \( F_{2^n} \)? (Hint: express the cost as a recurrence and then solve it.)

Problem 1.4 [15 points]. Generalized form of period-finding by quantum algorithms. Let \( σ : \{0,1\}^n \rightarrow \{0,1\}^n \) be a bijection (hence a permutation on the set \( \{0,1\}^n \)). Let \( z ∈ \{0,1\}^n \). Then the sequence

\[
z, σ(z), σ(σ(z)), σ(σ(σ(z))), \cdots = σ^{(0)}(z), σ^{(1)}(z), σ^{(2)}(z), σ^{(3)}(z), \cdots
\]

eventually comes back to \( z \). Consider the size of this cycle: that is, the minimum \( r > 0 \) such that \( σ^{(r)}(z) = z \). Suppose that we are given a black box for the mapping.

\[
|x⟩|y⟩ \rightarrow |x⟩|σ^{(r)}(y⟩),
\]

where \( x,y ∈ \{0,1\}^n \equiv \{0,1,2,\cdots,2^n - 1\} \). Suppose that we are also promised that \( r ≤ 2^n/2 \), but that otherwise \( r \) is unknown to us, and our goal is to determine \( r \). Let \( ω = e^{2πi/r} \), and \( |φ⟩ = 1/\sqrt{r} \sum_{s=0}^{r-1} ω^{-s} |σ^{(s)}(z)⟩ \).

Show that there is a quantum circuit that, given the additional help of one copy of \( |φ⟩ \), determines \( r \) with a single query to the black box, plus an additional number of 1- and 2-qubits gates that is polynomial in \( n \).

(Note: \( r \) can also be determined with a constant number of queries to the black box without being provided with any special quantum state; however, you are not asked to show this here.)