TUTORIAL 8

1 Assignment 6

The objective of this problem is to show how to obtain unitaries that prepare a given vector given access to an appropriate oracle. It is an adaptation (de Wolf, Exercie 9.7)

Let $v \in [-1, 1]^N$ be a vector with real entries, of dimension $N = 2^n$, indexed by $i \in \{0, 1\}^n$. Suppose we can query the entries of this vector by a unitary that maps

$$O_v : |i\rangle|0^p\rangle \mapsto |i\rangle|v_i\rangle,$$

so where the binary representation of the i-th entry of v is written into the second register. We assume this second register has p qubits, and the numbers v_i can all be written exactly with p bits of precision (it doesn't matter how, but for concreteness say that the first bit indicates the sign of the number, followed by the $p - 1$ most significant bits after the decimal dot). Our goal is to prepare the n-qubit quantum state $|\psi\rangle = \dfrac{1}{\|v\|} \displaystyle\sum_{i \in \{0,1\}^n} v_i |i\rangle$.

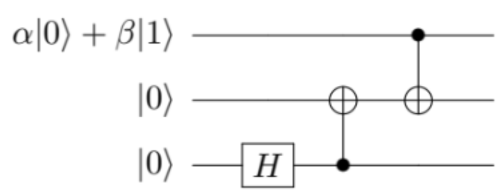
1. Show how you can implement the following 3-register map (where the third register is one qubit) using one application of O_v and one of O_v^{-1}, and some v-independent unitaries (you don't need to draw detailed circuits for these unitaries, nor worry about how to write those in terms of elementary gates).
$$|i\rangle|0^p\rangle|0\rangle \mapsto |i\rangle|0^p\rangle(v_i|0\rangle + \sqrt{1 - v_i^2}|1\rangle).$$

2. Suppose you apply the map of (a) to a uniform superposition over all $i \in \{0, 1\}^n$. Write the resulting state, and calculate the probability that measuring the last qubit in the computational basis gives outcome 0.

3. What is the resulting 3-register state if the previous measurement gave outcome 0?

2 Calculations

1. Consider the following circuit



   (a) Compute the state on the three qubits at the end of the circuit as a function of α and β. The H corresponds to the usual Hadamard gate and the represented two-qubit gate is the usual CNOT gate, where the black dot is the control qubit and the $\oplus$ is the target qubit.

(b) If we perform a measurement of the first qubit (from the top), what is the probability of outcomes 0 and 1? For each one of these outcomes, what the postmeasurement state?

2. Consider the state on three qubits $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

   (a) Show that this state is entangled, i.e., it is not of the form $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes |\phi_3\rangle$ for some qubit states $|\phi_i\rangle \in \mathbb{C}^2$ for $i \in \{1, 2, 3\}$.

   (b) Assume I measure the first qubit (in the basis $|0\rangle, |1\rangle$), show for all the possible outcomes of this measurement, the postmeasurement state is *not* entangled.

   (c) Consider the previous question for the state $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$, i.e., suppose I measure the first qubit. Show that there is an outcome such that the postmeasurement state is entangled.

3 The collision problem

Consider a query problem where given a block box access to $f : \{0, 1\}^n \to \{0, 1\}^n$ with the promise that either f is a bijection ("yes" instance) or f is 2-to-1, i.e., for every $y \in \{0, 1\}^n$, $|\{x \in \{0, 1\}^n : f(x) = y\}| \in \{0, 2\}$ ("no" instance). We would like to construct an algorithm (classical or quantum) to decide whether we have a "yes" or a "no" instance while minimizing the number of queries to the black box f. We will call this problem the collision problem.

1. Give a deterministic classical algorithm solving the collision problem using $2^{n-1} + 1$ queries.

2. We now consider a quantum algorithm which has access to a quantum black box given by the unitary transformation U_f on $2n$ qubits defined by $U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |f(x) \oplus y\rangle$ for all $x \in \{0, 1\}^n, y \in \{0, 1\}^n$ and $\oplus$ denotes the bitwise XOR. Our objective is to give a quantum algorithm for the collision problem making $O(2^{n/3})$ queries to U_f succeeding with probability at least $2/3$.

   (a) For a subset $C \subseteq \{0, 1\}^n$. Define U_f^C to be the unitary acting on $n + 1$ qubits defined by for all $x \in \{0, 1\}^n, b \in \{0, 1\}$:

   $$U_f^C|x\rangle \otimes |b\rangle = \begin{cases} |x\rangle \otimes |b \oplus 1\rangle & \text{if } f(x) \in C \\ |x\rangle \otimes |b\rangle & \text{if } f(x) \notin C \end{cases}.$$

   Show how to compute U_f^C using only two uses of U_f. Note that you can use any other fixed unitary as long as it does not depend on f (but it can of course depend on C). You may use ancilla qubits prepared in the state $|0\rangle$ but they should be restored to $|0\rangle$.

   (b) Assume $S \subseteq \{0, 1\}^n$ and $|S| \leq 2^{n-1}$ with $f(x) \neq f(x')$ for all $x, x' \in S$. Show that if f is a "yes" instance, then for all $x \notin S$, $f(x) \notin f(S)$ and if f is a "no" instance, then there exists $S' \subseteq \{0, 1\}^n - S$ such that for all $x \in S'$, $f(x) \in f(S)$ and $|S'| = |S|$. Here $f(S) = \{f(x) : x \in S\}$.

   (c) Using the previous questions with a well chosen S and C, design and analyze a quantum algorithm for the collision problem using $O(2^{n/3})$ queries.

   You may use, without proof, the following extension of Grover's algorithm. Let $T \subseteq \{0, 1\}^n$ and consider a unitary O_T on $n+1$ qubits (the black box) satisfying $O_T|x\rangle \otimes |b\rangle = |x\rangle \otimes |b \oplus 1\rangle$ if $x \in T$ (the marked elements) and $O_T|x\rangle \otimes |b\rangle = |x\rangle \otimes |b\rangle$ if $x \notin T$. Assume that either $T = \emptyset$ or $|T| = M$ for $M \geq 1$. Then there exists an algorithm that uses $O(\sqrt{2^n/M})$ queries to O_T and decides if $T = \emptyset$ or $|T| = M$ with success probability at least $2/3$.