Introduction to Quantum Computing 2022

Bonus Homework

Exercise 2. *Suppose we run Simon's algorithm on the following input x (with $n = 3$ and so $N = 2^3 = 8$): $f(000) = f(111) = 000$, $f(001) = f(110) = 001$, $f(010) = f(101) = 010$ and $f(011) = f(100) = 011$.*

Note that f is indeed a 2-to-1 function and the "period" is $s = 111$.

1. *Give the starting state of Simon's algorithm.*
2. *Give the state after the first Hadamard transforms on the first 3 qbits.*
3. *Give the state after applying the quantum oracle query for f.*
4. *give the state after the final Hadamard transform.*

5. *Why does a measurement of the first 3 qbits of the final state give information about s?*

6. *Suppose the first run of the algorithm gives $j = 011$ and a second run gives $j = 101$. Show that, assuming $s \neq 000$, those two runs of the algorithm are enough to already determine s.*

Exercise 3. *A parity function is a boolean function of the form $f_s(x) = x \cdot s \mod 2$. Here, x, s are binary strings of length n and $x \cdot s$ is their inner (dot) product: $x \cdot s = \sum_{i=1}^{n} x_i s_i$.*

1. *Show that for every possible choice of s except the all-zero vector, that f_s is* balanced.

2. *Imagine we apply the circuit from the Deutsch-Jozsa algorithm with the oracle f_s. Show that the measured output is precisely the string s.*

3. *Consider the following problem: given oracle access to a parity function f_s for some $s \in \{0,1\}^n$, determine s using the minimal number of queries to f_s.*

   Conclude from that there is a quantum algorithm that solves this problem with one query to f_s.

   Also, give an exact bound on the number of queries to f_s required for a classical algorithm to solve the problem with absolute certainty.

Exercise 4. *Suppose we are given access to a black box $\mathbf{U}$ which we are told that it implements one of the four Pauli operators $\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}$ (I is the identity matrix - if you do not remember them, refer to the slides).*

We have no idea which of these four Pauli operators the black box implements.

1. *Show that*

$$(P \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

   where P is one of the four single Qbit Pauli matrices, are orthogonal *for the four different Ps.*

2. *Suppose that we are only allowed to use a single Qbit state input $|\psi\rangle$ into the black box, but that we can choose this single Qbit state arbitrarily.* After *whatever is in the black box has acted on $|\psi\rangle$, we are allowed to apply any other single Qbit unitary operator $\mathbf{V}$ we wish and then measure in the standard $\{|0\rangle, |1\rangle\}$ basis.*

   Prove that it is not always possible to distinguish what the black box hides. In other words, prove that it is impossible to choose an operator $\mathbf{V}$ and an input $|\psi\rangle = a|0\rangle + b|1\rangle$ such that it is always possible to distinguish with perfect certainty which Pauli the black box implements.

3. *Now suppose that instead of the restricted circuit used in the previous question, we are now allowed to input two-Qbit states $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ into*

the black box (which still acts on the first Qbit), then perform a two-Qbit unitary transform after the evolution of the black box, and then perform a measurement (in the standard) basis.

Show that it is now possible to distinguish each of the four possible Pauli operators from each other with certainty by choosing the appropriate two Qbit input state $|\psi\rangle$ and a certain two-Qbit unitary $\mathbf{V}$.

You can use appropriately entangled Qbits as input.

What this exercise demonstrates is that it is possible to use entangled quantum states to help distinguish between different unknown unitary gates. This idea, generalized, is one way to think about how quantum algorithms work.

Exercise 5. *Alice and Bob share the entangled state*

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

Now Alice wants to send two classical bits to Bob by sending him a single qbit.

Suppose that Alice wants to send $m_1, m_2 \in \{0,1\}^2$. If $m_1 = 1$, she applies the Pauli X (i.e., NOT) gate to her qbit in the entangled pair, else she does nothing. If $m_2 = 1$, she applies the Pauli Z gate to her qbit, else she does nothing.

Then she sends her half of $|\psi\rangle$ to Bob (who then possesses all of $|\psi\rangle$).

1. *Find an appropriate basis so that Bob can measure and determine exactly Alice's message consisting of m_1, m_2.*
2. *Find a circuit that uses only CNOT gates, arbitrary 1-qubit gates, and only measurements in the standard basis that always outputs Alice's message as the outcome.*

Exercise 6. *Let Alice and Bob each have one Qbit of a Bell pair for example $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Let Bob and Charlie also each have one half of another Bell pair.*

If Bob uses the Bell pair he shares with Charlie, to teleport his Qbit from the Bell pair he (Bob) shares with Alice, show that the result is that Alice and Charlie now share a Bell pair.