Quantum Computation **CMU 15-859BB, Fall 2015**

Homework 5

Due: Tuesday November 24, 11:59pm; email the pdf to pgarriso@andrew.cmu.edu

---

Solve 4 out of 5

1. **[Query complexity of Parity.]** Suppose we have quantum query access to a string $w \in \{0,1\}^N$ and we wish to know the *parity* (sum mod 2) of its bits. Assume N is even.

   (a) Show that this problem can be solved with zero error using $N/2$ quantum queries. (Hint: first solve the problem for $N = 2$.)

   (b) Show that $N/2$ quantum queries are necessary, even to solve the problem with the standard $1/3$ error. (Hint: polynomial method.)

2. **[Query lower bound for Connectivity.]** Suppose we have quantum query access to the $n \times n$ adjacency matrix of an undirected graph G. We wish to decide whether or not G is connected. On Homework 3 we saw this could be done with $O(n^{3/2})$ quantum queries. Show that $\Omega(n^{3/2})$ quantum queries are necessary. (Hint: Did you know that all cycles-graphs are connected, and that all graphs that consist of two disjoint cycles each of length at least $n/3$ are not connected? Anyway, we suggest you use the Basic Adversary Method.)

3. **[Query upper bound for Bipartiteness.]** Suppose we have quantum query access to the $n \times n$ adjacency matrix A of an undirected graph $G = (V, E)$. We wish to decide whether or not G is bipartite (i.e., has no odd-length cycles). In this problem you will use Reichardt's span program method to show that this can be done with $O(n^{3/2})$ quantum queries. We will actually give a span program for *non*-bipartiteness.

   The "A$\bar{\text{A}}$ Span Program": Works in the the space $\mathbb{R}^{2n^2+1}$ spanned by orthonormal vectors named $|\bot\rangle$, and $|s, v, b\rangle$ (for $s, v \in V$ and $b \in \{0,1\}$). The target vector will be $|\bot\rangle$. If entry $A[u, v] = 1$ then we make available the vectors $|s, u, 0\rangle + |s, v, 1\rangle$ and $|s, u, 1\rangle + |s, v, 0\rangle$, for all $s \in V$. Also, for each $s \in V$ we *always* make available the vector $|\bot\rangle + |s, s, 0\rangle + |s, s, 1\rangle$. (We can achieve this by making it available for both $A[s, s] = 0$ and $A[s, s] = 1$.) Note that there are $O(n^3)$ total input vectors.

   (a) Show that if G is not bipartite then the target vector is in the span of the available input vectors.

   (b) Show that if G is bipartite then the target vector is not in the span of the available input vectors.

   (c) Show that whenever G is not bipartite there is a positive witness of size $O(1)$. (Hint: if G has an odd cycle of length ℓ, then this odd cycle can be considered to have ℓ different starting points. Average your witnesses.)

   (d) Show that whenever G is bipartite there is a negative witness that has dot-product either 0, 1, or -1 with all the input vectors.

   (e) Deduce that there is an $O(n^{3/2})$ quantum query algorithm for Bipartiteness.

4. **[Finishing Reichardt.]** Recall that we showed (on Piazza) the following:

   Phase Detection: Let U be a unitary operation on $\mathbb{R}^M$, given to a quantum circuit as a "black box". Assume the circuit is given as input $|\psi\rangle \otimes |0\rangle$, where in the first register we have an (unknown) eigenvector of U, and where the second register has dimension $M = \Theta(1/\delta)$. Then with $O(1/\delta)$ applications of U, the circuit can achieve the following: (i) if the eigenvalue of $|\psi\rangle$ is 1 then the final state of the circuit will always be $|\psi\rangle \otimes |0\rangle$; (ii) if the eigenvalue of $|\psi\rangle$ is $e^{i\theta}$ where $\theta \in (-\pi/2, \pi/2]$ satisfies $|\theta| \geq \delta$, then the final state will be of the form $|\psi\rangle \otimes |\phi\rangle$, where $|\langle\psi|0\rangle|^2 \leq 1/4$.

   Recall also that in class we showed that given a span program computing a function $F : \{0,1\}^N \to \{0,1\}$ with cost T, and given oracle access $O_w^{\pm}$ to a string $w \in \{0,1\}^N$, we could construct a unitary matrix U acting on some $\mathbb{R}^M$ and making $O(1)$ calls to $O_w^{\pm}$ and satisfying the following two properties: (i) if $F(w) = 1$ then $\|P_0|0\rangle\| \geq .99$; (ii) if $F(w) = 0$ then $\|P_\delta|0\rangle\| \leq .01$. Here $\delta = 1/O(T)$, the vector $|0\rangle$ is a certain fixed unit vector in $\mathbb{R}^M$, and operator P_η denotes projection into the eigenspaces of U with eigenvalues $e^{i\theta}$ where $|\theta| \leq \eta$.

   Combine all of this to show there is a quantum query algorithm deciding F with $O(T)$ queries.

5. **[Simulating POVMs.]** In this exercise you will show that general quantum measurements can be simulated by good old projective measurements, when adding ancillas is allowed. For simplicity we will assume that we only want to simulate the "POVM"; i.e., we only want to get the outcomes with correct probabilities, and don't care about how the state collapses afterward. So suppose $E_1, \dots, E_m$ are PSD operators on $\mathbb{C}^d$ satisfying $\sum_j E_j = I$.

   (a) Why may we assume, without loss of generality, that each E_j is of rank (at most) one? Why may we assume, without loss of generality, that $m = kd$ for some positive integer k?

   (b) In light of the previous problem, let us assume that $E_j = |\widetilde{\psi}_j\rangle\langle\widetilde{\psi}_j|$ (where $|\widetilde{\psi}_j\rangle \in \mathbb{C}^d$ is not necessarily of unit length). Let $G \in \mathbb{C}^{d\times m}$ be the matrix formed by putting the column vectors $|\widetilde{\psi}_j\rangle$ next to one another, and let $\langle\phi_1|, \dots, \langle\phi_d|$ be the rows of G. Show that the $\langle\phi_i|$'s are orthonormal.

   (c) Explain why we can add news rows to G to make it into a unitary matrix $U \in \mathbb{C}^{m\times m}$. We henceforth write $|\widetilde{\psi}'_j\rangle$ for the jth column of U.

   (d) Suppose $|v\rangle \in \mathbb{C}^d$, and write $|v'\rangle \in \mathbb{C}^m$ for the longer vector gotten by padding with zeroes. Show that the squared-length of the projection of $|v\rangle$ onto $|\psi_j\rangle$ is the same as that of $|v'\rangle$ onto $|\widetilde{\psi}'{}_j\rangle$.

   (e) Show that measuring a density matrix $\rho \in \mathbb{C}^d$ according to the POVM $\{E_1, \dots, E_m\}$ is equivalent to doing a certain "projective measurement" on $\rho \otimes |1\rangle\langle 1|$, where here we think of the second register as being $(k-1)$-dimensional (spanned by $|1\rangle, \dots, |k-1\rangle$).