Problem Set 3

1. Parity $\mathrm{PARITY}_n : \{0,1\}^n \to \{0,1\}$ is the function where $\mathrm{PARITY}_n(x) = 1$ iff the number of ones in x is odd.

1. Show that PARITY_2 can be solved exactly with one quantum query. Hint: This is just Deutsch-Josza.
2. Show that PARITY_n can be solved exactly with $\lceil n/2 \rceil$ many quantum queries. No need to write out circuits here, keep your description of the algorithm high level.
3. Use the polynomial method to prove that $Q_{1/3}(\mathrm{PARITY}_n) \geq \lceil n/2 \rceil$.

2. Dual polynomials In lecture we only saw techniques to lower bound the approximate degree of *symmetric* functions. Proving lower bounds on the approximate degree of functions which aren't symmetric is challenging. One way to do this is by *dual polynomials*, which introduce here.

Let $f : \{-1,1\} \to \{0,1\}$. Show that if there exists a function $g : \{-1,1\}^n \to \mathbb{R}$ with the properties

1. $\sum_{x\in\{-1,1\}^n} g(x)f(x) > \frac{1}{3}\sum_{x\in\{-1,+1\}^n} |g(x)|$
2. $\sum_{x\in\{-1,1\}^n} g(x)\chi_S(x) = 0$ for all $S \subseteq \{1,\ldots,n\}$ with $|S| \leq d$

then $\deg_{1/3}(f) > d$.

In the dual polynomial method, one explicitly constructs a function g satisfying these properties for as large a d as possible.

3. Simple version of the adversary method The Hamming distance $d_H(x,y)$ between two strings $x, y \in \{0,1\}^n$ is the number of positions on which they differ, that is $d_H(x,y) = |x \oplus y|$.

Let $f : \{0,1\}^n \to \{0,1\}$. Suppose that for every $x \in f^{-1}(0)$ there are at least d_0 many $y \in f^{-1}(1)$ with $d_H(x,y) = 1$ and that for every $y \in f^{-1}(1)$ there are at least d_1 many $x \in f^{-1}(0)$ with $d_H(x,y) = 1$. Show that the quantum adversary bound for f is at least $\sqrt{d_0 d_1}$. In other words, construct a $|f^{-1}(0)|$-by-$|f^{-1}(1)|$ matrix Γ with

$$\frac{\|\Gamma\|}{\max_{i\in\{1,\ldots,n\}} \|\Gamma \circ D_i\|} \geq \sqrt{d_0 d_1}\ .$$

Hint: You can take all entries of Γ to be in $\{0,1\}$. Useful characterizations of the spectral norm of a matrix $A \in \mathbb{R}^{m\times n}$ include

1. $\|A\| = \max_{\substack{v\in\mathbb{R}^n \\ \|v\|=1}} \|Av\|$

2. $\|A\| = \max_{\substack{u\in\mathbb{R}^m, v\in\mathbb{R}^n \\ \|u\|=\|v\|=1}} |u^T Av|$

3. $\|A\| = \sqrt{\lambda_1(AA^T)}$ where $\lambda_1(B)$ is the largest eigenvalue of B.

4. Applying the simple adversary bound

1. Use the simple version of the adversary method to show that $Q_{1/3}(\mathrm{PARITY}_n) = \Omega(n)$.

2. For n a positive integer and $1 \leq k \leq n$ let $\mathrm{THRESHOLD}_{k,n}$ be a *partial* Boolean function with domain $\{x \in \{0,1\}^n : |x| \in \{k-1, k\}\}$ and where $\mathrm{THRESHOLD}_{k,n}(x) = 1$ iff $|x| = k$. Use the simple version of the adversary method to show that $Q_{1/3}(f_{n,k}) = \Omega(\sqrt{k(n-k)})$. Give a quantum query algorithm to show that this lower bound is tight up to logarithmic factors (hint: use one of the algorithms from the last problem set).

5. Not All Equal Let $f : \{-1,1\}^3 \to \{-1,+1\}$ be the Not-All-Equal function, which evaluates to -1 on input $x \in \{-1,1\}^3$ if not all the entries of x are equal and evaluates to 1 otherwise. In other words, it evaluates to 1 on the two inputs $111, -1-1-1$, and evaluates to -1 otherwise.

1. Write f as a polynomial. What is its degree?

2. Show that any $1/3$-error approximating polynomial for f has degree at least 2.

3. Give a 2 query quantum algorithm that computes f with success probability 1.

4. Challenge: Show that there is no quantum algorithm that computes f with success probability 1 using just 1 query.

6. Element Distinctness Let n be a positive integer and $M \geq n$. Element distinctness $\mathrm{ED}_n : \{0,\ldots,M-1\}^n \to \{0,1\}$ is the function where $\mathrm{ED}(x) = 1$ if $x_i \neq x_j$ for all $i,j \in \{1,\ldots,n\}$ with $i \neq j$ and $\mathrm{ED}(x) = 0$ otherwise. In other words, $\mathrm{ED}(x) = 1$ if all the elements of x are distinct.

1. What is the success probability of the following algorithm: Form a set S by choosing k elements from $\{1,\ldots,n\}$ uniformly at random (with replacement) and then use Grover to search for $j \notin S$ such that $x_j = x_i$ for some $i \in S$?

2. Use part 1 and amplitude amplification to show $Q_{1/3}(\mathrm{ED}_n) = O(n^{3/4})$. See Section 1.1 of the lecture notes on Grover's algorithm for a description of amplitude amplification.