CS667/CO681/PH767 Quantum Information Processing (Fall 07)

Assignment 2 *Extra Challenge Questions*

Note: these questions are entirely optional, but credit will be added for any solutions given.

1. **Leading coefficients of general polynomials.** This is a generalization of question 5 in Assignment 2 to polynomials of degree d. Let p be a prime such that $p > d$, and consider the problem where one is given black-box access to a function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ (where $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$) such that $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ (arithmetic here is modulo p). The coefficients $a_0, a_1, \ldots, a_d \in \mathbb{Z}_p$ are unknown—suppose that they are independently uniformly sampled from $\mathbb{Z}_p$. The goal is to determine just the *leading* coefficient, a_d.

   (a) Show that any classical algorithm for this problem must make $d+1$ queries. That is, if only d queries are made then no information about a_d is acquired. (This is fairly straightforward.)

   (b) What is the *quantum* query complexity of this problem? Can it be solved with asymptotically fewer than $O(d)$ queries? (*I do not know the answer to this!*)

   The problem might become easier to solve if a condition such as $p \gg d$ is introduced. One can also consider a version of this problem relative to another finite field, such as $GF(2^n)$, where $2^n > d$.