Problem Set 4

There will be no class on November 13 and 15

This problem set is due on by Friday, November 16, 5pm by email

1. [60/100] The problem of deciding if a given function $f : \{0,1\}^n \to \{0,1\}$ has at least one "solution" x such that $f(x) = 1$ becomes easier if the number of solutions is larger. If the number of solutions is r, then the running time of Grover's algorithm becomes about $\sqrt{2^n/r}$. You will have to show that if, however, we are looking at the problem of counting the number of solutions, then the problem does not becomes easier. In the following we use the notation $\#f := |\{x : f(x) = 1\}|$ for the number of solutions of f.

   (a) [30/100] Show that there is a quantum algorithm that, given a classical circuit of size S computing a function $f : \{0,1\}^n \to \{0,1\}$, runs in time $poly(\#f, n) \cdot \sqrt{2^n}$ and computes, with high probability, $\#f$.

   (b) [30/100] Show that every algorithm for computing $\#f$ must have running time $\Omega(\sqrt{2}^n)$ even if $\#f$ is large. In particular, show that every quantum algorithm that accepts with probability $\geq 90\%$ all functions $f : \{0,1\}^n \to B$ such that $\#f \geq \frac{1}{2} \cdot 2^n$ and that rejects with probability $\geq 90\%$ all functions $f : \{0,1\}^n \to \{0,1\}$ such that $\#f \leq \frac{1}{2} \cdot 2^n - 1$ must have running time $\Omega(\sqrt{2^n})$ in the model analyzed in class. (That is, in the model in which the algorithm has access to f only via a unitary operation U_f such that $U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$.

2. [40/100] In class we mentioned that applying the same unitary operation to both bits of an EPR pair and then measuring the bits will always give, as an outcome, two identical bits. You will have to show that this is true for real-valued unitary matrices but not necessarily for all matrices.

   (a) [25/100] Prove that if U is a 1-qubit unitary matrix with real entries, and if we apply $U \otimes U$ to $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and then measure, then the outcome will always be an identical pair of bits.

   (b) [15/100] Give an example of a 1-qubit unitary matrix U with complex entries for which the above is not true.