CS 593/MA 595 - Intro to Quantum Computation
Theoretical Homework 4

Due Wednesday, October 1 at 11:59PM (upload to Brightspace)

Recommended exercises from Mike and Ike (not to be turned in): 4.6, 4.11, 4.12, 4.17, 4.34, 4.35, 4.38, 4.39.

1. Prove that the gate set $\{CNOT, H, S\}$ does not satisfy the following "strong" version of universality: for every positive integer k, the circuits built using H, S and $CNOT$ as gates generate a dense subgroup of $PU(2^k)$ (the projective unitaries on k qubits). (Hint: take $k = 1$.)

   Note: to show that the gate set $\{CNOT, H, S\}$ does not satisfy the more general notion of universality I gave in class (that allows ancillas) would be more-or-less equivalent to proving the Gottesman-Knill theorem. (This is too hard for our homework, but really isn't all that hard.)

2. Prove that $\{CZ, K, T\}$ is universal. Here CZ is controlled-Z and

$$K = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

3. In this problem, we will see an easy example of a "BQP-universal problem".

   Suppose you have the following power: given a description of a quantum circuit C on n qubits, decide if the probability that C outputs 1 in its first qubit is greater than 2/3, when the input to C is the basis state $|0 \cdots 0\rangle$.

   Show that—given that you have this power—it only takes *classical polynomial time* to solve every problem in BQP.