Problem Set 2

This problem set is due on Thursday, October 18, by 2:15pm. You can either hand it in class or email a pdf to Joongyeub.

1. [30/100] We proved that every unitary operation can be realized by a quantum circuit that uses only U_{CNOT} gates and 1-qubit gates. Show that it is not true that every bijective boolean function can be computed by a classical circuit that uses only CNOT gates and NOT gates.

   [Hint: use linear algebra over the field $\mathbb{F}_2$]

2. [40/100] Let us say that an *efficient experiment* on a quantum state is a polynomial time quantum computation, followed by a measurement, followed by a polynomial time classical computation on the outcome of the measurement.

   For a binary string $x = (x_1, \ldots, x_n)$ let $mod3(x)$ be 0 if $\sum_i x_i \equiv 0 \pmod 3$ and let $mod3(x)$ be 1 otherwise. Show that there is an efficient experiment that distinguishes with high probability the quantum state $q_{uniform} := \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$ from the quantum state $q_{mod3} := \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{mod3(x)} |x\rangle$. That is, there is an efficient experiment that outputs YES with higher probability (by an additive constant term) than when executed on $q_{uniform}$.

3. Consider a quantum circuit that, on an n-qubit input, first applies an Hadamard gate to each input bit, and applies the quantum Fourier transform over $\mathbb{Z}_{2^n}$. If we give the state $|0 \cdots 00\rangle$ as an input to the circuit, what is the output state?