Problem Set 1

1. Hadamard For $x, y \in \{0,1\}^n$ show that the (x,y) entry of $H^{\otimes n}$ is $\frac{(-1)^{x\cdot y}}{\sqrt{2^n}}$ in two different ways.

2. CNOT Construct a CNOT gate from two Hadamards and one controlled Z gate.

3. Reading circuits

1. What is the output of the two circuits in Fig. 1 and Fig. 2? In what way does the circuit in Fig. 2 simulate the one with intermediate measurements in Fig. 1?
2. Trace the evolution of the states in the circuit in Fig. 3. What could this circuit be used for?

4. Projectors

1. Let $A, B \succeq \mathbf{0}_n$ be n-by-n positive semidefinite matrices. Show that
   - $\mathrm{Tr}(AB^*) \geq 0$
   - If $\mathrm{Tr}(AB^*) = 0$ then $AB^* = \mathbf{0}_n$.
2. Let $P_1, \ldots, P_m \in \mathbb{C}^{n\times n}$ be such that
   - $P_i^* = P_i$ and $P_i^2 = P_i$ for all $i = 1, \ldots, m$. That is, each P_i is an orthogonal projector.
   - $\sum_{i=1}^m P_i = \mathbf{I}_n$.

   Show that this implies $P_i P_j = \mathbf{0}_n$ for all $i \neq j$.

Figure 1: A circuit with intermediate measurements.

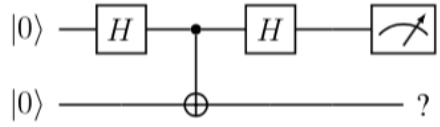

Figure 2: A circuit with measurement at the end.

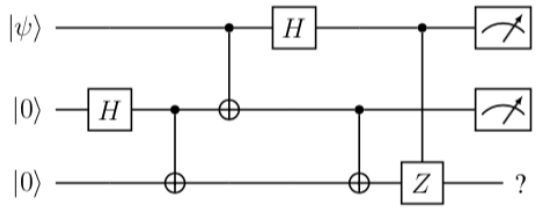

Figure 3: $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ is an arbitrary one-qubit state. What does this circuit do?

5. Simulating randomized circuits In lecture we discussed how a randomized circuit can be simulated by a quantum circuit with Hadamard and Toffoli gates that allows measurements during the computation. A cleaner model for quantum circuits, however, is to defer all measurements to the end. This exercise is to show that quantum circuits with measurements deferred to the end can also simulate classical randomized circuits.

More precisely, consider a randomized circuit C using Toffoli gates with n input wires, c ancilla wires, r coin toss wires, and m output wires. Give a quantum circuit C' using Toffoli and Hadamard gates with n input wires, $c + r$ ancilla wires, and $m + r$ output wires, such that the probability distribution over the outcomes on the first m wires of C can be simulated by a measurement on C'.

6. Only real numbers

1. Develop a mapping $f : \mathbb{C} \to \mathbb{R}^{2\times 2}$ with the properties that for all $z_1, z_2 \in \mathbb{C}$
   - $f(z_1) + f(z_2) = f(z_1 + z_2)$.
   - $f(z_1) \cdot f(z_2) = f(z_1 \cdot z_2)$.
   - $f(z_1) \cdot f(z_1)^T = |z_1|^2 \mathbf{I}_2$.
2. Given a unitary $U \in \mathbb{C}^{n\times n}$ come up with an *orthogonal* matrix $X \in \mathbb{R}^{2n\times 2n}$ such that for any $|z\rangle \in \mathbb{C}^n$ it holds that
   $$X(|0\rangle|\Re(|z\rangle)\rangle + |1\rangle|\Im(|z\rangle)\rangle) = |0\rangle|\Re(U|z\rangle)\rangle + |1\rangle|\Im(U|z\rangle)\rangle \ .$$
   Here $\Re(|z\rangle) \in \mathbb{R}^n$ is the real part of the vector $|z\rangle$ and $\Im(|z\rangle) \in \mathbb{R}^n$ is the imaginary part.
3. Let C be a quantum circuit on n qubits with 1 and 2 qubit gates. Design a circuit C' on $n+1$ qubits with gates on at most 3 qubits such that a measurement in the computational basis on C can be simulated by a measurement on C'.

7. Corrupted Bernstein-Vazirani In the Bernstein-Vazirani problem we were given oracle access to the function $f(x) = x \cdot s \bmod 2$. Now suppose that the oracle function is corrupted, that is, it does not always give the correct answer. Formally, let $e : \{0,1\}^n \to \{0,1\}$ where $\frac{|e^{-1}(1)|}{2^n} \leq \frac{1}{4}$ and say we have oracle access to the function f' where $f'(x) = x \cdot s + e(x) \bmod 2$. Show that there is a quantum query algorithm making 1 query to f' that recovers s with probability at least $\frac{1}{4}$.