Exercise 5: Non-Local Games, Circuits and Quantum Money

1. Alice, Bob and Charlie are given bits a, b and c respectively. Their bits $a, b, c \in \{0, 1\}$ are promised to be such that $a \oplus b \oplus c = 0$. Their goal is to output bits A, B, C, without communicating, such that $A \oplus B \oplus C = a \vee b \vee c$. They are allowed to decide on a strategy in advance.

   (a) Show that no classical strategy can win on every input.

   (b) Suppose that each player holds a qubit, such that their combined shared state is

   $$\frac{1}{2}\left(|000\rangle - |011\rangle - |101\rangle - |110\rangle\right).$$

   Suggest a strategy that always wins on every input.

   (c) Suggest a strategy that always wins on every input, assuming the shared state is $\frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$.

2. (a) For n-qubit states $|\psi_1\rangle, |\psi_2\rangle$ consider the circuit in Figure 5.1, which uses the controlled swap gate, which is a controlled version of the SWAP circuit (Figure 3.1 in Exercise 3):

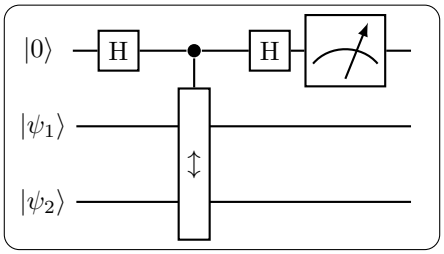

Figure 5.1: The swap test.

   What is the probability we will measure $|0\rangle$ as a function of $\langle\psi_1|\psi_2\rangle$? What is this circuit useful for?

   (b) Suppose we have circuits U_1, U_2 such that $U_i |0^n\rangle = |\psi_i\rangle$.

i. Show how to generate the $(n+1)$-qubit state $|\varphi\rangle = (|0\rangle|\psi_1\rangle + |1\rangle|\psi_2\rangle)/\sqrt{2}$.

ii. Suppose we apply H on the first qubit of $|\varphi\rangle$ and measure it. What is the probability we will measure $|0\rangle$ as a function of $\langle\psi_1|\psi_2\rangle$?

3. Let $f : \{0,1\}^n \to \{0,1\}^m$, $g : \{0,1\}^m \to \{0,1\}^n$ be such that $g(f(x)) = x$ for all $x \in \{0,1\}^n$. Assume that f, g can be computed by polynomial-size (classical) circuits. Show that there exists a polynomial-size quantum circuit that maps $|x,0\rangle$ to $|f(x),0\rangle$. Would you expect this to be possible without the assumption that g has a polynomial size circuit?

4. Finish the analysis for Wiesner's quantum money we started in class:

   (a) Show that for any $q_1 \in \{-,0,1\}$, after all the c iterations of the protocol, if the bank did not reject the bill, then our control qubit is in the state $|0\rangle$. (You may require an additional property of the integer c).

   (b) Upper bound the probability that the bank rejects the bill.

   (c) Describe and analyse the 3 missing protocols: how to check if $q_1 = -$ VS $q_1 \in \{+,0,1\}$, if it's 0 VS in $\{+,-,1\}$ and if it's 1 VS in $\{+,-,0\}$.