CS 599 P1: Introduction to Quantum Computation — Boston University
Instructor: Alexander Poremba — Fall 2025

PRACTICE WORKSHEET #3

This is the third practice worksheet—it will not be graded and is meant to help you practice the quantum circuit model, as well as simple quantum algorithms. I encourage you to work through these problems by **Tuesday, October 7th**—before the next homework assignment is out.

Problem 1 (Quantum SWAP Test). In this exercise, we will study the so-called *SWAP test*, a simple but powerful quantum circuit that can be used to estimate the *fidelity* (or closeness) between two unknown quantum states. This is a notion you previously encountered in the first homework assignment.

- **Fidelity.** Let us consider two single-qubit states

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad |\psi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle\,,$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ are amplitudes such that $|\alpha|^2 + |\beta|^2 = 1$ and $|\gamma|^2 + |\delta|^2 = 1$.
We define the *fidelity* between two pure states $|\phi\rangle$ and $|\psi\rangle$ as

$$F(\phi, \psi) = |\,\langle\phi|\psi\rangle\,|^2.$$

- **The SWAP gate.** The two-qubit `SWAP` gate exchanges the states of its two input qubits:

$$\texttt{SWAP}\,|x\rangle\,|y\rangle = |y\rangle\,|x\rangle\,, \quad \text{for } x, y \in \{0,1\}.$$

where we used that the two-qubit Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$ has four logical basis states

$$\{|0\rangle\,|0\rangle\,, |0\rangle\,|1\rangle\,, |1\rangle\,|0\rangle\,, |1\rangle\,|1\rangle\}.$$

- **The controlled-SWAP (Fredkin) gate.** The three-qubit `controlled-SWAP` gate (also called the *Fredkin gate*) applies the SWAP operation on the last two qubits (targets) if and only if the first qubit (control) is in the state $|1\rangle$. Formally, if we write a general three-qubit computational basis state as

$$|c\rangle\,|x\rangle\,|y\rangle\,, \quad c, x, y \in \{0,1\},$$

then the controlled-SWAP acts as

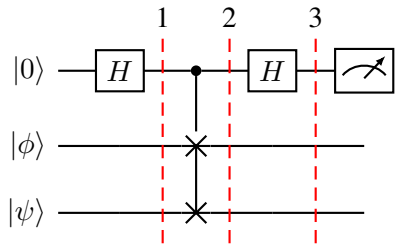
$$\texttt{cSWAP}\,|c\rangle\,|x\rangle\,|y\rangle = \begin{cases} |0\rangle\,|x\rangle\,|y\rangle\,, & \text{if } c = 0, \\ |1\rangle\,|y\rangle\,|x\rangle\,, & \text{if } c = 1. \end{cases}$$

where the three-qubit Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ has 8 logical basis states

$$\{|000\rangle\,, |001\rangle\,, |010\rangle\,, |011\rangle\,, |100\rangle\,, |101\rangle\,, |110\rangle\,, |111\rangle\}.$$

In the SWAP test, we apply a *controlled-SWAP* (also called a Fredkin gate): a three-qubit gate that applies a SWAP on two target qubits only if the control qubit is in the state $|1\rangle$.

The SWAP test uses one ancilla qubit and two input states $|\phi\rangle$ and $|\psi\rangle$ and consists of the following circuit:



where the three-qubit gate between steps 1 and 2 is the controlled-SWAP gate.

Exercises:

1. Write down the three-qubit state $|\psi_0\rangle$ before any gates are applied.
2. Apply the Hadamard gate to the ancilla qubit. Write the joint three-qubit state $|\psi_1\rangle$ explicitly.
3. Show that the state in the second step can be written as

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle \otimes |\phi\rangle \otimes |\psi\rangle \ + \ |1\rangle \otimes |\psi\rangle \otimes |\phi\rangle \Big).$$

4. Apply the Hadamard gate to the ancilla qubit, and write out $|\psi_3\rangle$ explicitly.
5. Compute the probability that the measurement outcome of the ancilla qubit is 0. Show that it is

$$\Pr\left[\boxed{\nearrow} = |0\rangle \right] = \frac{1}{2}\Big(1 + |\,\langle\phi|\psi\rangle\,|^2\Big).$$

6. Suppose you had many identical copies of $|\psi\rangle$ and $|\phi\rangle$. Explain how you can repeatedly use the SWAP test in order to estimate the fidelity to within arbitrary precision.

   Hint: Explain how you can get a good estimate for the probability that the SWAP Test returns $|0\rangle$*. Then, using that, explain how you can obtain an estimate for the fidelity.*

7. Recall that in Homework #1 you encountered the family of states

$$|\psi(\theta)\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{i\theta}\,|1\rangle\Big)$$

   for $\theta \in [0, 2\pi)$. Suppose we want to estimate the fidelity between $|\psi(\theta)\rangle$ and the Hadamard-basis state $|+\rangle$. Use the SWAP test to derive the measurement probability $\Pr\left[\boxed{\nearrow} = |0\rangle \right]$ in this case, and compare it with the fidelity $F(\theta)$ that you computed directly in Homework #1.

Problem 2 (Bernstein–Vazirani Algorithm). In this exercise, we will study the Bernstein–Vazirani algorithm, one of the first examples of a quantum algorithm that outperforms any classical deterministic algorithm. This particular algorithm allows us to identify a hidden bit string encoded in a linear Boolean function using only a single quantum query.

- **The problem.** Let $s = s_1 s_2 \dots s_n \in \{0,1\}^n$ be an unknown n-bit string. Define a Boolean function $f_s : \{0,1\}^n \to \{0,1\}$ as

$$f_s(x) = \langle s, x \rangle \mod 2 = s_1 x_1 \oplus s_2 x_2 \oplus \cdots \oplus s_n x_n,$$

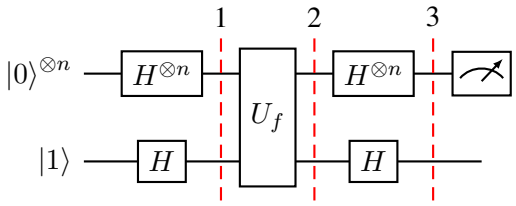
  where $x = x_1 x_2 \dots x_n$ and $\oplus$ denotes addition modulo 2. The goal is to determine s.

- **Classical approach.** Classically, determining s would require n queries to f_s, each querying $f_s(e_i)$ for the i-th basis vector e_i. Quantumly, we can find s in *one query*.

- **Quantum oracle.** The function f_s is implemented as a quantum oracle U_{f_s} acting on $n+1$ qubits:

$$U_{f_s} |x\rangle |y\rangle = |x\rangle |y \oplus f_s(x)\rangle, \quad x \in \{0,1\}^n,\ y \in \{0,1\}.$$

The Bernstein–Vazirani algorithm uses n qubits initialized to $|0\rangle^{\otimes n}$ and one ancilla qubit initialized to $|1\rangle$:



Here U_{f_s} acts as the oracle on the n input qubits and the ancilla.

Exercises:

1. Write down the initial $(n+1)$-qubit state $|\psi_0\rangle$ before any gates are applied.
2. Write the state $|\psi_1\rangle$ explicitly as a superposition over all $x \in \{0,1\}^n$.
3. Apply the oracle U_{f_s}. Show that the state $|\psi_2\rangle$ can be written as

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{\langle s,x \rangle} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

4. Apply Hadamard gates to the first n qubits again. Show that the resulting state is

$$|\psi_3\rangle = |s\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

5. Compute the probability of measuring each of the first n qubits. Explain why the measurement directly reveals the hidden string s.
6. Work out the special case $n = 3$ and $s = 101$. Write explicitly each step of the state evolution and show that the measurement outcome of the first three qubits gives s.