Raul Garcia-Patron
Stuart Ferguson

Tutorial 5

IQC 2025-26
October 29, 2025

Problem 1: SWAP Test

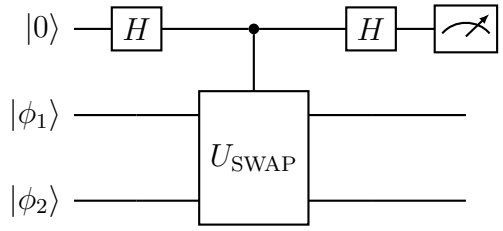
Given the two-qubit SWAP gate:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and the two single-qubit states $|\phi_1\rangle = a\,|0\rangle + b\,|1\rangle$ and $|\phi_2\rangle = c\,|0\rangle + d\,|1\rangle$.

a. Show that $U_{\text{SWAP}}\,|\phi_1\rangle \otimes |\phi_2\rangle = |\phi_2\rangle \otimes |\phi_1\rangle$

b. Consider the following SWAP test circuit acting on the two states $|\phi_1\rangle$ and $|\phi_2\rangle$.



Give the quantum state of the three qubit system at each step of the circuit.

c. Compute the probability $P(0)$ of obtaining the outcome 0 at the top qubit, the probability $P(1)$ of obtaining the outcome 1, and their bias $P(0) - P(1)$.

Problem 2: Quantum Fourier Transform

As you have seen in the lectures, we can represent any integer z in its binary form as:

$$z = z_1 z_2 \dots z_n$$

where $z_1, z_2, \dots, z_n$ are such so that:

$$z = z_1 2^{n-1} + \dots + z_{n-1} 2^1 + z_n$$

a. How many qubits at least would we need to encode the integer states $|14\rangle$ and $|9\rangle$? What is their binary representation when using qubits to encode the integers?

b. Recall that:

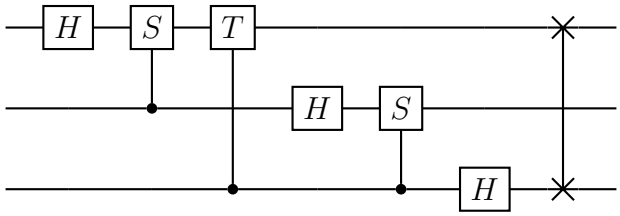
$$0.z_l z_{l+1} \dots z_m \equiv \frac{z_l}{2} + \frac{z_{l+1}}{2^2} + \dots + \frac{z_m}{2^{m-l+1}}$$

Calculate:

1. $2^3 \cdot 0.z_1 z_2 z_3$, $2^2 \cdot 0.z_1 z_2 z_3$ and $2 \cdot 0.z_1 z_2 z_3$, where $z_i \in \{0, 1\}$.

2. $e^{2\pi i \cdot 2^2 \cdot 0.j_1 j_2 j_3}$ where $j_i \in \{0, 1\}$.

c. Now consider the quantum Fourier circuit for three qubits:



with S and T being the gates:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Suppose that we input the state $|j\rangle = |j_1 j_2 j_3\rangle$. What will be the output state?

Problem 3: Order-Finding

For two positive integers x and N with $x < N$ the *order* of x modulo N is defined to be the *least positive integer* such that:

$$x^r = 1 \mod N$$

a. Show that for $x = 2$ and $N = 5$ we have $r = 4$.

b. Now consider the transformation U which acts on the computational basis states as follows:

$$U_x |y\rangle \equiv |xy \mod N\rangle$$

Prove that:

1. $U_x U_{x'} = U_{xx'}$
2. $U_{x^{-1}} = U_x^{-1} = U_x^\dagger$, using the fat that x has an inverse x^{-1} ($\mod N$) if and only if x and N are co-prime.
3. $U_x U_x^\dagger = U_x^\dagger U_x = I$, which proves it is an unitary transformation.
4. $U_x^r = I$ where r is the period of x modulo N.

c. Show that the states:

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^k \mod N\rangle$$

for integer $0 \leq s \leq r-1$ are eigenstates of U_x. What is their corresponding eigenvalues?

d. As you can see preparing the state $|u_s\rangle$ requires that we know r in advance. Fortunately there is clever observation which circumvents the problems of preparing $|u_s\rangle$. Show that:

1.
$$\sum_{s=0}^{r-1} e^{-2\pi isk/r} = r\delta_{k,0}$$

2.
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi isk/r} |u_s\rangle = |x^k \mod N\rangle$$

which has as special case when $k = 0$:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle ,$$

which is a trivial state to generate. This opens the door to applying quantum phase-estimation to sample from $\varphi = s/r$, which later leads to a guess of r as explained in the lecture on Shor's algorithm.

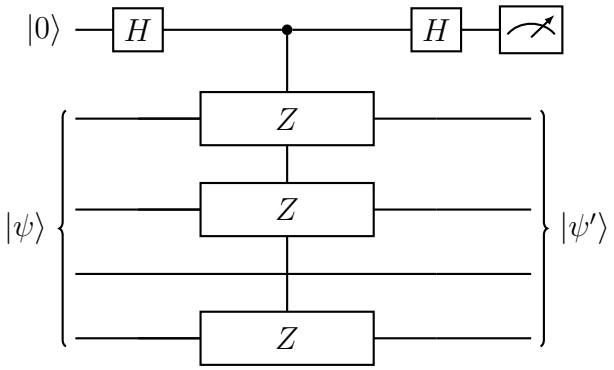
e. If we wanted to apply a phase estimation procedure we must have efficient procedures to implement a controlled-U^{2^j} operation for any integer j. Given an integer number x, propose a technique to compute x^{2^k} that scales linearly in k.

f. Assuming that we are given an unitary S such that implements $S|x\rangle = |x^2 \mod N\rangle$ that needs $O(L^2)$ gates, where $L = \lceil \log N \rceil$, i.e., the size of the register. How many gates we will be needed to implement $|x\rangle \to |x^{2^k} \mod N\rangle$?

Extra problem: Three-Qubit Parity Check

We want to perform an even/odd parity check on qubits $1, 2, 4$. It's easy to see that the parity operator $P = Z \otimes Z \otimes I \otimes Z$ is both Hermitian and Unitary, so that it can both be regarded as an observable and a quantum gate. Suppose we wish to measure the observable P. That is, we desire to obtain a measurement result indicating one of the two eigenvalues, and leaving an updated state after the measurement that is projected to its corresponding eigenspace. We are going to show that the following circuit implements a measurement of P:

Tutorial 5

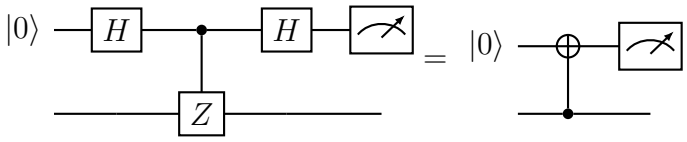


a. Derive the action of the three-qubit parity operator $P = Z \otimes Z \otimes I \otimes Z$ on the computational basis state $|x_1 x_2 x_3 x_4\rangle$. What are the eigenvalues of the operator P?

b. Derive the global state right before the measurement of the upper-qubit when the input state reads $|0\rangle \otimes |\psi\rangle$, where $|\psi\rangle = \sum_{x \in \{0,1\}^4} \gamma_x |x\rangle$ is a four qubit arbitrary input state and x is a four bit string.

c. Using the rules of partial measurement, show that the measurement of the upper-qubit projects the state of the lower four qubits to its odd or even parity subspaces, depending on the outcome being 0 or 1.

d. Prove that the two circuits below are equivalent:



e. Prove that we can achieve the same result with the circuit: