QML SoC
Evaluation for Quantum Computing

Siddhant Midha & Vedang Asgaonkar

Note You are supposed to submit only `.ipynb` files, answer the questions as markdown boxes in these files. Submit one file for each question, with appropriate file names.

1 Quantum SWAP Test

In this question, you will learn about and implement `Quantum SWAP Test`. Given two states $|\phi\rangle$ and $|\psi\rangle$, the `Quantum SWAP Test` is a way of experimentally measuring the (magnitude of the) inner product $\langle\phi|\psi\rangle$. The following circuit does that via measuring the topmost qubit in the eigenbasis of the Z operator.

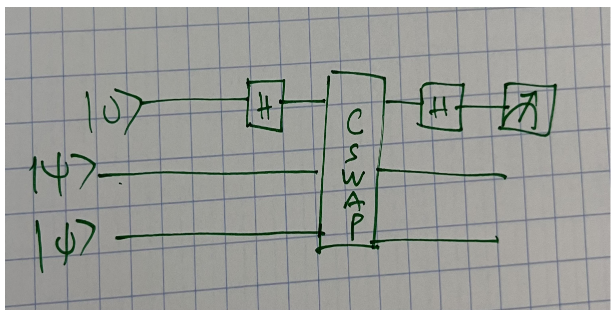

Figure 1: The Circuit

For the state $|xyz\rangle$ for $x, y, z \in \{0, 1\}$ the `CSWAP` operator exchanges y and z iff $x = 1$. For general states, linear superposition carries over.

1. How do you implement the `CSWAP` operation?

2. How is the inner product estimated? (Hint: Look at the probabilities. You might note a lack of formalism for describing such a situation. Density Operators are needed here to formally describe the probabilities. Refer to pages 98 to 108 of `QCQI`).

3. Implement the `Quantum SWAP Test` in Qiskit for some $|\phi\rangle$ and $|\psi\rangle$ of your choice, and experimentally verify the operation.

4. (#)There is a way of doing this without using an ancilla qubit. This is done simply by a measurement in the bell basis. How? (Hint: Again, the probabilities) Code up both in Qiskit and experimentally verify.

2 Quantum 3 SAT

We will explore the application of Grover's search to the satisfiability problem. Given a boolean function $F : \{0,1\}^n \to \{0,1\}$, the SAT problem seeks to find an input vector x such that $F(x) = 1$. If such a vector is absent then it tells us so. For example consider the boolean function $F((x_1, x_2, x_3)) = (x_1 \wedge x_2) \vee x_3$, then **a** solution to the SAT problem for this could be $(x_1, x_2, x_3) = (1, 0, 1)$. The SAT problem is known to be NP hard i.e. it is believed that there is no *efficient algorithm* to solve it on a classical computer. We will explore a quantum way of solving this efficiently.

In particular, we will solve a reduction of the SAT problem called the 3 SAT problem where we have functions which are of the form:

$$F(x) = C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

where each of the C_i's are formed by taking $\vee$ over at most 3 variables or their negations. An example of such a formula would be:

$$F^*((x_1, x_2, x_3, x_4, x_5)) = (x_1 \vee \neg x_2) \wedge (x_3 \vee x_4 \vee \neg x_1) \wedge (x_2 \vee \neg x_5)$$

1. How would you pose the 3 SAT problem for F^* mentioned above as a Grover's search problem? Specify how you would encode the variables into qubits and what the Grover oracle is supposed to do?

2. Given the above encoding of the variables into qubits, how would you implement the NOT, OR and AND operators? Use this implementation to create the Grover's oracle for 3 SAT for F^* in Qiskit. Note that the exact oracle will depend on the specific F^*, but the procedure for making it will be fixed.

3. Implement Grover's search to solve the 3 SAT problem for F^* in Qiskit. How many Grover iterations do you need to do?

3 Quantum Channels

This question will involve some research on your part, and will give you a flavour of quantum information. Good to go through the density operator formalism before attempting.
The most general state of a quantum system S with the hilbert space $\mathcal{H}_S$ can be described by a *density operator* $\rho \in L(\mathcal{H}_s)$ (where, $L(V)$ is the set of all linear operators on the space V). We know that the density operator formalism is more general than the pure state formalism. Hence, we would expect that density operators might undergo evolution which is more general than unitary evolution[1]! These evolutions are called *quantum channels*. There are a lot of ways of representing these channels, and we shall focus on what is called the *kraus representation*. Formally, we say that the channel $\mathcal{E}$ has the kraus[2] representation given by $K(\mathcal{E}) \equiv \{E_i | E_i \in L(\mathcal{H}_S)\}$ if

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$$

With this in mind, answer the following questions.

- What conditions must the set $\{E_i\}$ satisfy in order to be a valid quantum operators? (That is, it should map density operators to density operators – recall what a valid density operator is).

- How would one go about *implementing* a quantum channel on a gate based quantum circuit model? Concretely, code up a circuit in Qiskit to construct the single qubit state

  $$\frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

  starting from the initial state

  $$|0\rangle \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

- Represent both the states on the bloch sphere. (How do you represent density matrices on the bloch sphere?)

[1] refer to the standard postulates of QM

[2] I assure you that a finite number of kraus operators are enough for a finite dimensional system. Can you find a proof?

- Read about the Von-Neumann Entropy. Comment about the differece in von-neumann entropy of initial and final state. Does it say anything about entanglement, and/or motivate why we need the density operator formalism at all? Can you think of any other reasons?
- (*Optional*) Take the states $|0\rangle$, $|1\rangle$, and the ensemble[3] $\{(|0\rangle, \frac{1+p}{2}), (|1\rangle, \frac{1-p}{2})\}$. Vary p from -1 to $+1$ and plot the evolution on the bloch sphere.

4 Non-local games

Consider the following game, called the GHZ game. There are three players, Alice, Bob, and Charlie, and a Referee who mediates the game. The Referee will give one bit each to the players such that even number of 1 are given. Let us call the bits given to Alice, Bob, and Charlie as r, s, t respectively. Then each of the 3 players must give one bit back to the Referee, call the bits given by them as a, b, c respectively. Then Alice, Bob and Charlie win if $a \oplus b \oplus c = r \vee s \vee t$, else the Referee wins.

- **Classical Case**: Alice, Bob and Charlie get to discuss their strategy beforehand. They are not allowed to communicate during the game. Show that the best strategy for them is able to win $\frac{3}{4}^{th}$ of the time, and they can not do better.
- **Quantum Case**: Alice, Bob and Charlie are allowed to discuss and share qubits beforehand. During the game they can not communicate with each other, but they can perform operations on their own qubits. Find a strategy that allows them to always win the game. Here are some hints for the same:
  - They have to share entangled qubits, non-entangled qubits would be useless. In particular the GHZ state.
  - They must perform some operation in case they get a 1 from the referee. They must not do this operation if they get a 0.
  - Once everyone is done performing/not performing their operation, they must all measure and tell the referee three bits a, b, c based on the measurement

  Find the operation they must perform and show that the strategy always works.

[3] That is, the system is in $|0\rangle$ with probability $(1+p)/2$ and $|1\rangle$ with probability $(1-p)/2$.