Assignment 3: Quantum computing

Wang Dingrui 3036196908

November 29, 2023

1 Excersice 1: quantum phase estimation

We studied quantum phase estimation as a tool to estimate the number ϕ in the eigenvalue $e^{2\pi i \phi}$ with corresponding eigenvector $|u\rangle$ of a unitary operation U. The algorithm proceeded in two steps: first, the phase factor ϕ of the eigenvalue is encoded in binary in a t-qubit quantum state. Thereafter, a measurement in the computational basis yields the t binary digits of ϕ – explicitly telling us the eigenvalue up to some precision.

1. Let us depict again the phase estimation circuit: We found that the final state of the first register at the end of the circuit is given by $\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i \phi k} |k\rangle$. Derive this state by going through the circuit step-by-step (in particular, show that the output state can be written in this exact form). (8 points)

   Solution:

   In the first step, $|0\rangle_{t-1} \ldots |0\rangle_1 |0\rangle_0 |u\rangle \rightarrow \frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + |1\rangle_0}{\sqrt{2}} |u\rangle$

   In the second step, $0th$ qbit is the applied control qbit.

   $$\frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + |1\rangle_0}{\sqrt{2}} |u\rangle$$
   $$\rightarrow \frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + |1\rangle_0}{\sqrt{2}} U^{2^0} |u\rangle$$
   $$= \frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 |u\rangle + |1\rangle_0 U^{2^0} |u\rangle}{\sqrt{2}}$$
   $$= \frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + e^{2\pi i \phi 2^0} |1\rangle_0}{\sqrt{2}} |u\rangle$$

   In the third step, $1th$ qbit is the applied control qbit.

   $$\frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + e^{2\pi i \phi 2^0} |1\rangle_0}{\sqrt{2}} |u\rangle$$
   $$\rightarrow \frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + e^{2\pi i \phi 2^0} |1\rangle_0}{\sqrt{2}} U^{2^1} |u\rangle$$
   $$= \frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + e^{2\pi i \phi 2^1} |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + e^{2\pi i \phi 2^0} |1\rangle_0}{\sqrt{2}} |u\rangle$$

   In the t+1th step, $(t-1)th$ qbit is the applied control qbit.

   $$\frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + e^{2\pi i \phi 2^1} |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + e^{2\pi i \phi 2^0} |1\rangle_0}{\sqrt{2}} |u\rangle$$
   $$\rightarrow \frac{|0\rangle_{t-1} + |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + e^{2\pi i \phi 2^1} |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + e^{2\pi i \phi 2^0} |1\rangle_0}{\sqrt{2}} U^{2^{t-1}} |u\rangle$$
   $$= \frac{|0\rangle_{t-1} + e^{2\pi i \phi 2^{t-1}} |1\rangle_{t-1}}{\sqrt{2}} \ldots \frac{|0\rangle_1 + e^{2\pi i \phi 2^1} |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + e^{2\pi i \phi 2^0} |1\rangle_0}{\sqrt{2}} |u\rangle$$

We know that $F(|j\rangle) = \frac{1}{\sqrt{2}} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{jk}{2^n}} |k\rangle$

Assume $k_t = 2^t$,

$$\frac{|0\rangle_{t-1} + e^{2\pi i \phi 2^{t-1}} |1\rangle_{t-1}}{\sqrt{2}} \cdots \frac{|0\rangle_1 + e^{2\pi i \phi 2^1} |1\rangle_1}{\sqrt{2}} \frac{|0\rangle_0 + e^{2\pi i \phi 2^0} |1\rangle_0}{\sqrt{2}} |u\rangle$$
$$= \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i \phi k} |k\rangle |u\rangle$$

So, the final state of the first register at the end of the first circuit is given by $\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i \phi k} |k\rangle$.

2. Show that the phase estimation algorithm does not only apply to one single eigenvector $|u\rangle$, but also to a superposition of eigenvectors $\sum_i P_i |u_i\rangle$. (6 points)

2 Exercise 2: controlled gates

In the lectures, we saw controlled gates $c^- L$, which applied a gate L to a system state $|\psi\rangle$ if the control state $|\sigma_c\rangle$ is in state $|1\rangle$, and leaves $|\psi\rangle$ invariant if $|\sigma_c\rangle = |0\rangle$.

1. Let us look now at doubly-controlled gates. Here, we have two control states $|\sigma_1\rangle$ and $|\sigma_2\rangle$. Then, $c^- c^- L$ is the gate which applies L to a system state $|\psi\rangle$ if both $|\sigma_1\rangle = |1\rangle$ and $|\sigma_2\rangle = |1\rangle$, and leaves it invariant otherwise.

   Solution:

   $c - cLX |\sigma_1\rangle_{c1} |\sigma_2\rangle_{c2} |\psi\rangle_t =$
   $|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
   $|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
   $|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
   $|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle L_3 |\psi\rangle_3$

   DRAW A PICTURE

2. We encountered anti-controlled gates in the lectures. Here, for a gate $ac^- L$, the gate L was applied to a system state $|\psi\rangle$ if the control state $|\sigma\rangle_c$ is in state $|0\rangle$, and $|\psi\rangle$ was left invariant for $|\sigma\rangle_c = |1\rangle$. Then, combining control and anti-control, there are four possible ways for a doubly-controlled gate. Write all four ways in ket-bra notation and draw the corresponding circuits. (6 points)

   Solution:

   If the first gate is anti-control, the second gate is anti-control:

   $ac - ac - L |\sigma_1\rangle_{c1} |\sigma_2\rangle_{c2} |\psi\rangle_t =$
   $|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle L_3 |\psi\rangle_3 +$
   $|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
   $|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
   $|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3$

   If the first gate is anti-control, the second gate is control:

   $ac - c - L |\sigma_1\rangle_{c1} |\sigma_2\rangle_{c2} |\psi\rangle_t =$
   $|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$

$|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle L_3 |\psi\rangle_3 +$
$|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
$|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3$

If the first gate is control, the second gate is anti-control:

$c - ac - L |\sigma_1\rangle_{c1} |\sigma_2\rangle_{c2} |\psi\rangle_t =$
$|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
$|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
$|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle L_3 |\psi\rangle_3 +$
$|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3$

If the first gate is control, the second gate is control:

$c - cLX |\sigma_1\rangle_{c1} |\sigma_2\rangle_{c2} |\psi\rangle_t =$
$|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
$|0\rangle \langle 0|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
$|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |0\rangle \langle 0|_{c_2} |\sigma_2\rangle I_3 |\psi\rangle_3 +$
$|1\rangle \langle 1|_{c_1} |\sigma_1\rangle |1\rangle \langle 1|_{c_2} |\sigma_2\rangle L_3 |\psi\rangle_3$

3 Exercise 3: quantum neural networks

In the lectures, we studied classical binary feedforward neural networks and saw how to generalize them to quantum neural networks. To make this step, we formalized the classical neuron in the gate model. In the lectures, we identified the classical bit value -1 with the state $|0\rangle$ and value $+1$ with $|1\rangle$. We use the same mapping here in this exercise.

1. Inside a classical binary neuron, the edge weight w first gets multiplied with the input a to obtain the value $w \cdot a$. Show that the multiplication of the weight with the input can be realized by the XNOR gate. (4 points)

   Solution:

   To a classical neuron, the table of $w \cdot a$ is:

w	a	$w \cdot a$
-1	-1	$+1$
-1	$+1$	-1
$+1$	-1	-1
$+1$	$+1$	$+1$

   In quantum computing, the XNOR gate is defined as:

w	a	$w \cdot a$
$|0\rangle$	$|0\rangle$	$|1\rangle$
$|0\rangle$	$|1\rangle$	$|0\rangle$
$|1\rangle$	$|0\rangle$	$|0\rangle$
$|1\rangle$	$|1\rangle$	$|1\rangle$

$|0\rangle$ is corresponding to -1, $|1\rangle$ is corresponding to $+1$.

So, the multiplication of the weight with the input can be realized by the XNOR gate.

2. Assume now we have two inputs a_1, a_2 to the neuron. After multiplying the inputs with the weights, we defined the resulting values as $s_1 = w_1 a_1$ and $s_2 = w_2 a_2$. The values s_1 and s_2 were summed up and forwarded to the Heaviside activation function. The Heaviside function H then outputs the value $+1$ if the sum $s_1 + s_2$ is above a certain threshold α, i.e. $H(s) = +1$ if $s_1 + s_2 \geq \alpha$ and $H(s) = -1$ if $s < \alpha$. Find a quantum circuit that takes the states $|s_1\rangle$, $|s_2\rangle$ and an ancilla $|0\rangle$, and implements the Heaviside function as:

$$|s_1\rangle|s_2\rangle|0\rangle \rightarrow |s_1\rangle|s_2\rangle|H(s)\rangle \tag{1}$$

for the case $\alpha = +1$. Hint: make sure that the neuron is activated also in case $s_1 = s_2 = +1$. (8 points)

Solution: $c - c - X\,|s_1\rangle\,|s_2\rangle\,|0\rangle$

3. Find a circuit that transforms $|s_1\rangle|s_2\rangle|0\rangle$ to $|s_1\rangle|s_2\rangle|H(s)\rangle$, where $\alpha = -1$. (8 points)

$ac - ac - X\,|s_1\rangle\,|s_2\rangle\,|0\rangle$

Then X on the third qbit.

We identify now the value $+1$ with the state $|0\rangle$ and value -1 with the state $|1\rangle$.

4. Show that multiplication between input and weight can be written as $|s_1\rangle = |a_1 \oplus w_1\rangle$ and $|s_2\rangle = |a_2 \oplus w_2\rangle$, meaning that we simply need to perform an addition (modulo 2) between the input a_i and corresponding weight w_i. (4 points)

Solution:

In classical, the truth table of $a_i \oplus w_i$ is:

a_i	w_i	$a_i \cdot w_i$
-1	-1	$+1$
-1	$+1$	-1
$+1$	-1	-1
$+1$	$+1$	$+1$

In quantum, the truth table of $a_i \oplus w_i$ is:

a_i	w_i	$a_i \oplus w_i$
$|1\rangle$	$|1\rangle$	$|0\rangle$
$|1\rangle$	$|0\rangle$	$|1\rangle$
$|0\rangle$	$|1\rangle$	$|1\rangle$
$|0\rangle$	$|0\rangle$	$|0\rangle$

The two tables are the same.

$|0\rangle$ is corresponding to $+1$, $|1\rangle$ is corresponding to -1. So, multiplication between input and weight can be written as $|s_1\rangle = |a_1 \oplus w_1\rangle$ and $|s_2\rangle = |a_2 \oplus w_2\rangle$.

4 Exercise 4: quantum dot product

Distances can be evaluated more efficiently on a quantum computer compared to a classical computer. Assume we are given two quantum states $|\vec{x}_i\rangle$ and $|\vec{x}_j\rangle$ encoding the vectors $\vec{x}_i = (x_{i,0}, x_{i,1}, ..., x_{i,n-1})^T$ and $\vec{x}_j = (x_{j,0}, x_{j,1}, ..., x_{j,n-1})^T$.

1. The vectors $\vec{x}_i$ and $\vec{x}_j$ do not need to be normalized - they can, in general, have arbitrary norms $\|\vec{x}_i\|$ and $\|\vec{x}_j\|$. Show that the encodings $|\vec{x}_i\rangle = \frac{1}{\|\vec{x}_i\|} \sum_{m=0}^{n-1} x_{i,m}|m\rangle$ and $|\vec{x}_j\rangle = \frac{1}{\|\vec{x}_j\|} \sum_{k=0}^{n-1} x_{j,k}|k\rangle$ are indeed normalized correctly. (3 points)

   Solution:

   $$\|\frac{1}{\|\vec{x}_i\|} \sum_{m=0}^{n-1} x_{i,m} |m\rangle\|^2 = \frac{\sum_{m=0}^{n-1} x_{i,m}^2}{\|\vec{x}_i\|^2} = \frac{\sum_{m=0}^{n-1} x_{i,m}^2}{\sum_{m=0}^{n-1} x_{i,m}^2} = 1$$

   $$\|\frac{1}{\|\vec{x}_j\|} \sum_{k=0}^{n-1} x_{j,k} |k\rangle\|^2 = \frac{\sum_{k=0}^{n-1} x_{j,k}^2}{\|\vec{x}_j\|^2} = \frac{\sum_{k=0}^{n-1} x_{j,k}^2}{\sum_{k=0}^{n-1} x_{j,k}^2} = 1$$

   So, the encodings are normalized correctly.

In the following, we assume the sum of the vector norms $Z = \|\vec{x}_i\|^2 + \|\vec{x}_j\|^2$ to be known. Further, let us assume we are given the states $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|\vec{x}_i\rangle_2 + |1\rangle_1|\vec{x}_j\rangle_2)$ and $|\phi\rangle = \frac{1}{\sqrt{Z}}(\|\vec{x}_i\||0\rangle_1 - \|\vec{x}_j\||1\rangle_1)$.

2. Compute the overlap $(\langle\phi|_1 \otimes I_2)|\psi\rangle_{12}$ between the states. (3 points)

   Solution:

   $$\langle\phi|_1 = \frac{1}{\sqrt{Z}}(\|\vec{x}_i\| \langle0|_1 - \|\vec{x}_j\| \langle1|_1)$$

   $$(\langle\phi|_1 \otimes I_2)|\psi\rangle_{12} = \frac{1}{\sqrt{2Z}}(\|\vec{x}_i\|^2 |\vec{x}_i\rangle_2 - \|\vec{x}_j\|^2 |\vec{x}_j\rangle_2)$$

The goal of this exercise is to show that we can compute the distance between the vectors $\vec{x}_i$ and $\vec{x}_j$ by performing a swap-test on the states $|\psi\rangle$ and $|\phi\rangle$.

3. Begin with the initial state $|0\rangle|\psi\rangle|\phi\rangle$ and compute the state before the final measurement. Do so by doing a step-by-step calculation for each operation in the circuit. The operation after the first Hadamard gate is a controlled swap gate: for two states $|a\rangle$ and $|b\rangle$, a swap gate acts as $\text{SWAP}(|a\rangle_1|b\rangle_2) = |b\rangle_1|a\rangle_2$. (6 points)

   Solution:

   In the first step: $|0\rangle_0 |\psi\rangle_1 |\phi\rangle_2$

   In the second step: $\frac{1}{\sqrt{2}}(|0\rangle_0 + |1\rangle_0) |\psi\rangle_1 |\phi\rangle_2$

   In the third step: $\frac{1}{\sqrt{2}}(|0\rangle_0 |\psi\rangle_1 |\phi\rangle_2 + |1\rangle_0 |\phi\rangle_1 |\psi\rangle_2)$

   In the fourth step: $\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0\rangle_0 + |1\rangle_0) |\psi\rangle_1 |\phi\rangle_2 + \frac{1}{\sqrt{2}}(|0\rangle_0 - |1\rangle_0) |\phi\rangle_1 |\psi\rangle_2)$
   $= \frac{1}{2}(|0\rangle_0 |\psi\rangle_1 |\phi\rangle_2 + |1\rangle_0 |\psi\rangle_1 |\phi\rangle_2 + |0\rangle_0 |\phi\rangle_1 |\psi\rangle_2 - |1\rangle_0 |\phi\rangle_1 |\psi\rangle_2)$

We want to show that the final measurement gives insight to the distance $\|\vec{x}_i - \vec{x}_j\|$ between the vectors $\vec{x}_i$ and $\vec{x}_j$. We do so by showing the following steps.

4. Assume the final measurement on the uppermost wire is performed in the computational basis $\{|0\rangle, |1\rangle\}$. Compute the corresponding probability $p(0)$ of obtaining outcome "0" from the measurement. (8 points)

   Solution: $p(0)$
   $= |\langle 0| \frac{1}{2}(|0\rangle_0 |\psi\rangle_1 |\phi\rangle_2 + |1\rangle_0 |\psi\rangle_1 |\phi\rangle_2 + |0\rangle_0 |\phi\rangle_1 |\psi\rangle_2 - |1\rangle_0 |\phi\rangle_1 |\psi\rangle_2)|^2$
   $= \frac{1}{4} | |\psi\rangle_1 |\phi\rangle_2 + |\phi\rangle_1 |\psi\rangle_2 |^2$
   $= \frac{1}{4} | |\vec{x_i}\rangle_1 |\vec{x_j}\rangle_2 + |\vec{x_j}\rangle_1 |\vec{x_i}\rangle_2 |^2$

5. Use the expression for the overlap $\langle \psi | \phi \rangle$ from part 2 to show that the probability $p(0)$ can be written as
   $$p(0) = \frac{1}{2}\left(1 + \frac{\|\vec{x_i} - \vec{x_j}\|^2}{2Z}\right)$$
   (6 points) Hint: note, that $\|\vec{x_i}\| |\vec{x_i}\rangle = \vec{x_i}$.

   Solution:

   $p(0)$
   $= (\langle 0|_0 \otimes I_1 \otimes I_2)\frac{1}{2}(|0\rangle_0 |\psi\rangle_1 |\phi\rangle_2 + |1\rangle_0 |\psi\rangle_1 |\phi\rangle_2 + |0\rangle_0 |\phi\rangle_1 |\psi\rangle_2 - |1\rangle_0 |\phi\rangle_1 |\psi\rangle_2)$
   $=$

5 Exercise 5: quantum causality (26 points)

The last part of the lectures discussed the possibility of exotic causal scenarios in quantum mechanics. One concrete example of indefinite causality that was considered is the quantum switch. The quantum switch, denoted as S, is a map that takes two channels, A and B, as inputs and creates a coherent superposition, S(A, B), of the two classical causal orders: B ∘ A and A ∘ B.

1. The orders in the quantum switch are determined by a control qubit, which can be in a quantum superposition. We observed that even though the channels in both arms of the quantum switch completely erase any information, Bob can still receive information about Alice's input state . Instead of transmitting her information through the information-erasing channels in the switch, why doesn't Alice encode her information into the control qubit? This way, the information would not be erased, and Bob could extract by measuring the control qubit and the output of the switch, just like he did in the communication protocol discussed in the lectures. (3 points) **Solution:**

   - Interference with the control qubit: The control qubit may be in a quantum superposition, and measuring it to extract the information introduces uncertainty and reduces the reliability of the communication.

   - Efficiency of bit transmission: Directly encoding the information into transmission bits, rather than using the control qubit, allows for more efficient and faster communication. It reduces the need for additional bits and operations.

   - Information confidentiality: Encoding the information into the control qubit may reveal information about Alice's input state when Bob measures the control qubit.

This can lead to information leakage and security issues. Encoding the information directly into the transmission bits provides better control over information confidentiality.

We saw in the lectures that the quantum switch can help with certain tasks. One example was communication. Here, we look at another example: channel discrimination. Most generally, channel discrimination is the following task. Given a black box which executes one of two channels C_1 and C_2, find out which channel it is. Clearly, we need some information about the channels to be successful. Depending on the information, there are many variations of the task. Here, we look at the following instance: given channel $C_1 = U \otimes U$ and $C_2 = U \otimes V$, with U and V unitary channels, do we have C_1 or C_2?