Quantum Computation Exercise

1 Operator Functions

Let $f : \mathbb{C} \to \mathbb{C}$ be a function and A be a normal operator on a finite-dimensional Hilbert space $\mathcal{H}$ (i.e., $AA^\dagger = A^\dagger A$). According to the Spectral Decomposition Theorem, we know that A has the form

$$A = \sum_i \lambda_i |u_i\rangle \langle u_i| ,$$

where $\{|u_i\rangle\}$ is an orthonormal basis of $\mathcal{H}$ and λ_i is the eigenvalue such that $A|u_i\rangle = \lambda_i |u_i\rangle$. We define that

$$f(A) = \sum_i f(\lambda_i) |u_i\rangle \langle u_i| .$$

Problem 1 (Unitary operators)**.** *In quantum mechanics, the solution to the Schrödinger's equation*

$$i\frac{\mathrm{d}|\psi\rangle}{\mathrm{d}t} = H|\psi\rangle$$

for a (time-independent) Hamiltonian H is

$$|\psi(t)\rangle = \exp(-iHt)|\psi(0)\rangle .$$

Show that $\exp(-iHt)$ *is a unitary operator.*

Problem 2 (Pauli operators)**.** *We recall the three Pauli operators*

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Let $\vec{v} = (x, y, z) \in \mathbb{R}^3$ be a unit vector (i.e., $\sqrt{x^2 + y^2 + z^2} = 1$) and $A = xX + yY + zZ$. Show that for every real number θ,

$$f(\theta A) = \frac{f(\theta) + f(-\theta)}{2} I + \frac{f(\theta) - f(-\theta)}{2} A.$$

Problem 3 (Rotation operators)**.** *Let A be a normal operator such that $A^2 = I$. Show that*

$$\exp(iAx) = \cos(x)I + i\sin(x)A.$$

Use this formula to find the matrix representations of the rotation operators

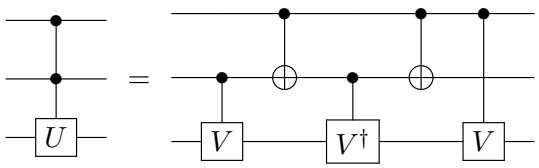
$$\begin{aligned} R_x(\theta) &= \exp(-i\theta X/2), \\ R_y(\theta) &= \exp(-i\theta Y/2), \\ R_z(\theta) &= \exp(-i\theta Z/2). \end{aligned}$$

2 Quantum Circuits and Measurements

We learned that although only a finite number of quantum gates (e.g., Pauli gates, Hadamard gate, CNOT gate, ...) can be directly implemented in current quantum experiments, other quantum unitary operators can be efficiently approximated via these elementary quantum gates. In this section, you are going to get familiar with common quantum gates and circuits.

Problem 4. *Verify that $HXH = Z$, $HYH = -Y$, and $HZH = X$. Show that $HTH = e^{i\theta}R_x(\pi/4)$ for some real number θ. Here, we call that HTH implements $R_x(\pi/4)$ up to a global phase.*

Problem 5. *Verify the equivalence of the following two quantum circuits. The following circuit implements the controlled-controlled-U gate ($\mathrm{C}^2(U)$ for short) by controlled-V, controlled-$V^\dagger$ and CNOT gates, where $V^2 = U$.*



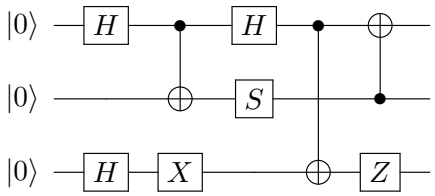
Problem 6 (Anonymous measurements)**.** *There are two quantum systems A and B. Let ρ be the (mixed) quantum state of the quantum system AB (treat the two quantum systems A and B as a whole). Bob made a measurement on quantum system B in the computational basis, that is, the measurement is $M = \{P_0, P_1\}$, where $P_0 = I_A \otimes |0\rangle_B \langle 0|$ and $P_1 = I_A \otimes |1\rangle_B \langle 1|$ are projectors. However, we do not know Bob's measurement result. Show that after the measurement, (in our view) the quantum state ρ' will be*

$$\rho' = P_0\rho P_0 + P_1\rho P_1.$$

Alice is in quantum system A and she does not know the existence of quantum system B. Show that Alice will never perceive Bob's measurement. That is, $\mathrm{tr}_B(\rho) = \mathrm{tr}_B(\rho')$. Here, $\mathrm{tr}_B(\cdot)$ is the partial trace that traces out quantum system B, defined by

$$\mathrm{tr}_B(|i\rangle_A \langle j| \otimes |k\rangle_B \langle l|) = |i\rangle_A \langle j| \,\mathrm{tr}(|k\rangle_B \langle l|).$$

Problem 7. *Compute the output state of following circuit: $|\psi_{out}\rangle = U_C |000\rangle$. The result state $|\psi_{out}\rangle$ can be represented either in Dirac notation or as an 8-dimensional complex vector.*



You need to explain how your result is obtained.

3 Quantum Algorithms

We have just learned about Grover's searching algorithm, which finds a solution (if exists) among $N = 2^n$ elements using $O(\sqrt{N})$ queries to the oracle with access to the elements. Suppose the n elements are $a_0, a_1, \ldots, a_{N-1} \in \{0,1\}$, and the quantum oracle U is given by

$$U|i,j\rangle = |i, j \oplus a_i\rangle$$

for every $i \in \{0,1,\ldots,N-1\}$ and $j \in \{0,1\}$, where $\oplus$ denotes the exclusive-OR.

Problem 8 (Quantum search without a promise)**.** *The original Grover search needs $O(\sqrt{N/M})$ queries to the oracle to find a solution if it is known that there are exactly M solutions. Try to design a quantum algorithm that finds a solution when the number of solutions is not known. (Can you use only $O(\sqrt{N})$ queries to the oracle?)*

Many optimization problems need to find the maximal or minimal value with certain restrictions. In the (possibly near) future, when quantum computers are established, we are eager to solve such optimization problems using quantum computers. As a modern quantum programmer of the future, now it is your turn to solve this problem.

Problem 9 (Find the maximum)**.** *Suppose there are $N = 2^n$ non-negative integers $a_0, a_1, \ldots, a_{N-1} \in [0, 2^W - 1]$, where W is the width of unsigned integers in our quantum computer (In the current generation of classical computers, W is usually 32 or 64. So for convenience, you may assume that $N \gg W$). You are given access to the N elements by a quantum oracle U such that*

$$U|i,j\rangle = |i, j \oplus a_i\rangle$$

for $i \in \{0,1,\ldots,N-1\}$ and $j \in \{0,1,\ldots,2^W-1\}$, where $\oplus$ denotes bitwise exclusive-OR. Note that U is an $(n+W)$-qubit quantum unitary operator. You are asked to design a quantum algorithm that finds the maximum among the n integers.

Hint: $W = 1$ degenerates to the quantum search problem (the maximum is 1 if we find a 1, and 0 otherwise). Either (or both) of the ideas may work:

1. If we have an integer comparator (which returns $a < b$, $a > b$ or $a = b$ given two integers a and b), the integer a_i is not maximum if there is an index j such that $a_j > a_i$.
2. Consider to first determine the most significant bit of the maximal value in the binary form. And then the second most significant bit, the third, the fourth, ..., and at last the least (i.e., W-th) significant bit.

DO NOT forget to prove the complexity of the quantum algorithms you designed.

Problem 10 (**Bonus**)**.** *Suppose a function $f : \{0,1\}^4 \to \{0,1\}$ is defined by:*

$$f(x) = \begin{cases} 1, & x = 7 \\ 0, & x \neq 7 \end{cases}$$

where $0 \leq x < 16$. Let O_f be the oracle operator with respect to f:

$$O_f|i\rangle|j\rangle = |i\rangle|j \oplus f(i)\rangle\,.$$

Here, O_f is a 5-qubit unitary operator ($0 \leq x < 16$ and $j \in \{0,1\}$).

Write a quantum program on the isQ platform (`http://124.16.138.151/`). You need to

1. *implement O_f, and*

2. *write a Grover search program which finds the answer by making queries to O_f.*

You can submit your code online to check the correctness. However, you should attach your program to this problem and write a short report (it is okay in Chinese) explaining your code. We will then check the correctness of your code.

Hints: You can construct the oracle O_f by:

- directly defining a 32×32 complex matrix in the Gate Definition Part;
- or constructing a quantum circuit that implements O_f.

We mainly care about the final Print result, which is expected to be 0111 with high probability. Please FEEL FREE to ask the TAs if you have any doubts.