QIQC: Assignment #3

Due Sunday, November 7 24: 00

1 Lecture review

(1) **Prove** (5') the inequality used in the lecture note on Quantum Phase Estimation

$$\frac{2}{\pi}|\theta| \leqslant |1-e^{i\theta}| \leqslant |\theta|, \forall\theta \in [-\pi,\pi]. \tag{1}$$

(2) Period finding algorithm find the smallest order r satisfying

$$a^r \bmod N = 1 \tag{2}$$

for given positive integers a and N. It relies on the construction of unitary operator U defined by

$$U|y\rangle \equiv |ay \bmod N\rangle, \tag{3}$$

which has eigenvectors read

$$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-i\frac{2\pi sk}{r}} \left|a^k \bmod N\right\rangle, \quad s = 0,1,\dots r-1. \tag{4}$$

Prove (5') the computational basis state $|1\rangle \equiv \left|a^0 \bmod N\right\rangle$ is a superposition of all the eigenvectors $|u_s\rangle$, i.e.,

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle. \tag{5}$$

2 Quantum adder

How do we construct the unitary operator U mentioned in the question (1) utilizing quantum gates implemented on qubits? As we have known in computer class, all the arithmetic operations can be reduced into adding and bit shifting. So we can simplify the problem into constructing a quantum adder.

Design (10') a binary 3 qubits quantum adder with elementary quantum gates we learned on the class (single-qubit gates, CNOT, and Toffoli gate) as well as some ancilla qubits (with initial state $|0\rangle$. Ancilla qubits are **not** required to be recovered to initial state in this homework. Sometimes, it is necessary to avoid entanglement) . The quantum adder has input and output as follows.

Given one addend qubit $|a = 0/1\rangle$ and three summand qubits $|s_2s_1s_0\rangle$. The circuit should change the summand qubits into $|s_2's_1's_0' = s_2s_1s_0 + a\rangle$ remaining the addend qubit unchanged. The possible overflow can be simply discarded.

e.g. Given input $|a\rangle = |1\rangle$, $|s_2s_1s_0\rangle = |011\rangle$. Output $|s_2's_1's_0'\rangle = |100\rangle$. i.e. $4 = 3 + 1$.

3 Period finding and Quantum mechanics

Quantum mechanics describes all the objects in the real world from elementary particles like electrons to humans ourselves and huge planets. For simplicity, we call all the objects "particles". In this

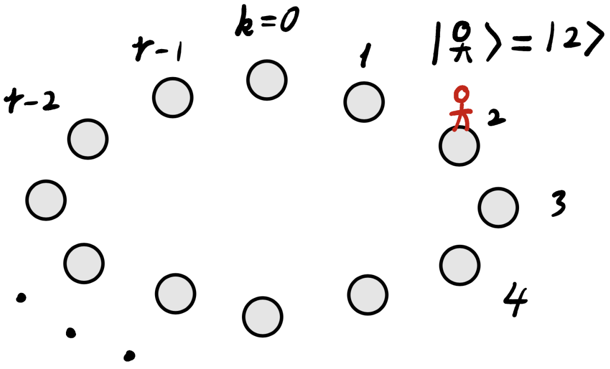

Figure 1: Discretized 1-dimensional world with periodic boundary condition.

question, we will find the wave functions used in the question (1) $\left|a^k \bmod N\right\rangle$ can describe particles living on a 1-dimensional lattice with periodic boundary condition and learn the physical implication of unitary operator U.

(1) The elementary observables in quantum mechanics are position and momentum. They are operators (which can be represented by matrices as long as we choose some basis) in Hilbert space $\mathcal{H}$ denoted by $\hat{X}$ and $\hat{P}$ which satisfy elementary commutation relation

$$[\hat{X}, \hat{P}] = i. \tag{6}$$

where i is the unit complex number. We can represent Hilbert space $\mathcal{H}$ in terms of either position basis $\{|x\rangle\}$ or momentum basis $\{|p\rangle\}$ which are eigenvector of $\hat{X}$ and $\hat{P}$ respectively

$$\hat{X}\,|x\rangle = x\,|x\rangle\,, \quad \hat{P}\,|p\rangle = p\,|p\rangle\,. \tag{7}$$

Prove (5') the commutation relation

$$[\hat{X}, e^{-i\hat{P}}] = e^{-i\hat{P}} \tag{8}$$

according to elementary commutation relation Eq. (6) .
(Hint. The operator function $e^{-i\hat{P}}$ is defined by its Taylor expansion.)

(2) For simplicity, we denote the wave function by $|k\rangle \equiv \left|a^k \bmod N\right\rangle, k = 0, 1 \ldots r-1$.They can be viewed as the position wave functions which are eigenvectors of position operator $\hat{X}$

$$\hat{X}\,|k\rangle = k\,|k\rangle\,. \tag{9}$$

The corresponding Hilbert space in this complete basis describe one particle (such as a human) living on discretized lattice (see Figure (1)) .
Prove (5') the operator $e^{-i\hat{P}}$ is a translation operator which translate the particle by one unit through showing

$$e^{-i\hat{P}}\,|k\rangle = |k+1\rangle\,. \tag{10}$$

We see that the translation operator is exactly U in Eq. (3)

(3) Finding this relation between U and $\hat{P}$ helps us to derive the eigenvector of U (which is also eigenvector of $\hat{P}$) in quantum mechanical way. Noting that in discretized world with lattice size r and periodic boundary condition, the momentum can only take discretized value $p = -\frac{2\pi s}{r}, s = 0, 1 \ldots r-1$.
Show (5') the momentum eigenvectors can be expanded by

$$\left|p = -\frac{2\pi s}{r}\right\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i\frac{2\pi s k}{r}}\,|k\rangle\,, \quad s = 0, 1, \ldots r-1, \tag{11}$$

which is exactly $|u_s\rangle$ in Eq. (4) .
(Hint. plane wave function $\left\langle x = k \middle| p = -\frac{2\pi s}{r}\right\rangle = \frac{1}{\sqrt{r}} e^{-i\frac{2\pi s}{r}k}$)

4 Trotterization

For an n-qubit system, consider the following Hamiltonian

$$H = \sum_{i=0}^{n-2} X_i X_{i+1} + \sum_{i=0}^{n-1} Z_i,$$

where X_i and Z_i are the Pauli X and Z operator on the ith qubit, respectively.
(1) Consider the time evolution $U = e^{-iHT}$ with time T, use the Trotterization method to **approximate**(5') the time evolution with single and two-qubit gates.
(2) Suppose the Trotter step is L, **count** the number of gates and **analyze**(5') the Trotter error as functions of n, L, and T.
(3) Consider the special case $n = 6$, $T = 10$, numerically **calculate**(10') the trotter errors with different L and compare the result with the analytical one.

5 Circuit design: QPE

Modern quantum computers can only realize all single qubit gates and one two qubits gate (We choose CNOT in this homework) . **Design** (20') a Quantum Phase Estimation circuit evaluating eigenvalues of a given exact eigenvector $|\psi\rangle$ of Hermitian operator $H = X_1X_0 + Z_1 + Z_0$ with following requirements:

- Gates should be chosen from gate set {single qubit gates, CNOT}. (No Toffoli gate)
- Require measured qubits number $n = 4$ for precision.
- Show both the **primitive** version and the **iterative** version.

Remarks.
1. Ancilla qubits with initial state $|0\rangle$ are available and recovering to initial state is **not** required.
2. For clarity, the whole main circuit is recommended to be expressed by sub-circuit blocks. Just like we write sub-function in main function of c++. See Figure (2) .
3. Optimization of the circuit is **not** required.

6 Circuit design: Grover

In this question, we construct the circuit of one Grover iteration G for the 3-qubit popcount function $f(x)$. The gate set available is the same as in question (5) . The Grover iteration mainly consists of an oracle and a phase reflection. Firstly, we try to construct the oracle of the popcount function.

6.1 Compute popcount function for n = 3 qubits

Popcount, also known as the Hamming weight or simply weight, is a popular instruction in classical computing that is utilized in certain implementations of quantum algorithms. For the Boolean n-tuple $(x_{n-1}, \dots x_1, x_0)$, popcount tell us how many inputs are $|1\rangle$

$$f(x_{n-1}, \dots x_1, x_0) = (y_{m-1}, \dots y_1, y_0) = x_{n-1} + \dots + x_1 + x_0, \tag{12}$$

e.g. if we input $|x_2x_1x_0\rangle = |110\rangle$ with 2 $|1\rangle$s, the output is $|y_1y_0\rangle = |10\rangle$ (larger index means higher weight)
(1) **Design** (5') the quantum circuit with input $|x_2x_1x_0, 0\rangle$ and output $|x_2x_1x_0, y_0\rangle$.
(2) **Design** (10') the quantum circuit with input $|x_2x_1x_0, 0\rangle$ and output $|x_2x_1x_0, y_1\rangle$.

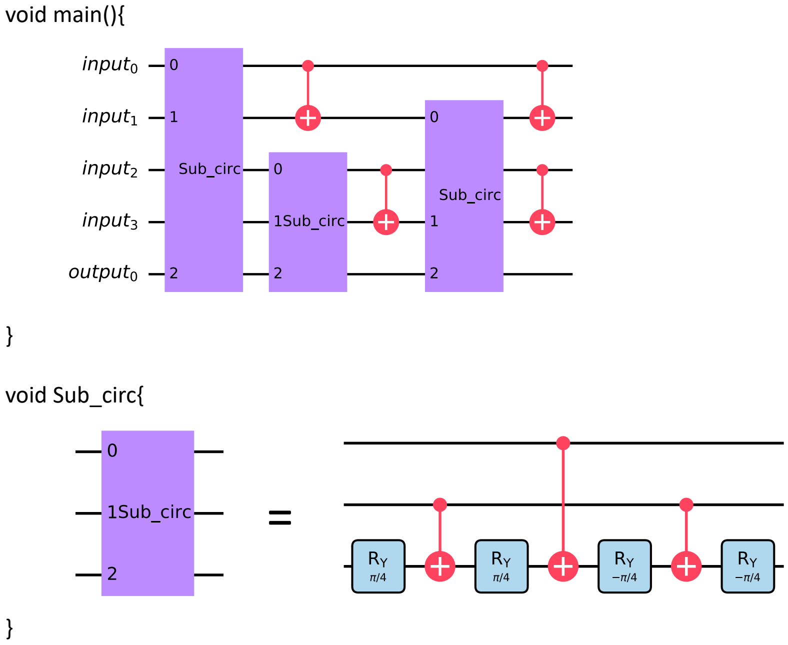

Figure 2: Main circuit and sub-circuit

Remarks.

1. **Try** to optimize the above circuit, i.e., optimize the cost function

$$\mathrm{cost}(C, A) = C + A, \tag{13}$$

where C is the total number of CNOT gates and A is the number of ancilla qubits in your circuit. Single qubit gates are free. Please **write** the total cost of your design.

2. Ancilla qubits with initial state $|0\rangle$ are available and recovering to initial state is **not** required.

3. For clarity, the whole main circuit is recommended to be expressed by sub-circuit blocks. Just like we write sub-function in the main function of c++. See Figure (2) .

6.2 Grover

Design (10') the Grover iteration G searches for the space with number of $|1\rangle$s larger than 1 in $|x_2x_1x_0\rangle$ utilizing the constructed popcount function y_1.