M1522.002500 – 양자 컴퓨팅 및 정보의 기초

Introduction to Quantum Computing and Information (001)

(Prof. Taehyun Kim)

Final

June 12, 2019 7:00 PM ~ 9:30 PM

Write the answer under each problem.

You can also use additional answer sheet attached behind.

이름: _____

학번: _____

시험 중 부정 행위는 F 학점 **및** 징계의 사유가 됩니다.

Total: 125 points

Problem 1. OX problems (8 points, 2 points each)

(A) We can transmit information faster than light by using entangled qubits. (O / X)

(B) All the Boolean logics can be constructed by quantum gates. (O / X)

(C) Arbitrary set of positive operators that sum to identity can be used as a POVM element (O / X)

(D) The output of n-qubit QFT on input state $|000 \dots 0\rangle$ is the same as the output state generated by n-qubit Hadamard gates $H^{\otimes n}$. (O / X)

Problem 2. "Trace distance" between two quantum states represented by density matrices ρ, σ is defined as $D(\rho, \sigma) = \frac{1}{2}\text{tr}(|\rho - \sigma|)$, where $|A| \equiv \sqrt{A^\dagger A}$. Show that for single qubit case, $D(\rho_1, \rho_2) = \frac{1}{2}|\vec{r_1} - \vec{r_2}|$ when we write $\rho_i = (I + a_i\sigma_x + b_i\sigma_y + c_i\sigma_z)/2$, $i = 1,2$ & $\vec{r_i} = (a_i, b_i, c_i)$. ($\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$). (8 points)

Problem 3. Show the following properties about an arbitrary density matrix ρ. (10 points)

(A) $\mathrm{tr}(\rho^2) \leq 1$ & equality holds if and only if the state is pure. (5 points)

(B) $\mathrm{tr}(\rho^2) \geq \frac{1}{n}$, where n is the dimension of a quantum state. (5 points)

(for example, n = 3 if $|a\rangle = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$) (Hint: $\sum_{i=1}^{n} x_i^2 \geq \frac{1}{n}(\sum_{i=1}^{n} x_i)^2$)

Problem 4. E91 protocol provides means to safely distribute keys and check whether there was an eavesdropper. Figure 1 corresponds to E91 protocol and table 1 shows the measurement result. (13 points)

$$|\psi_{AB}^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$
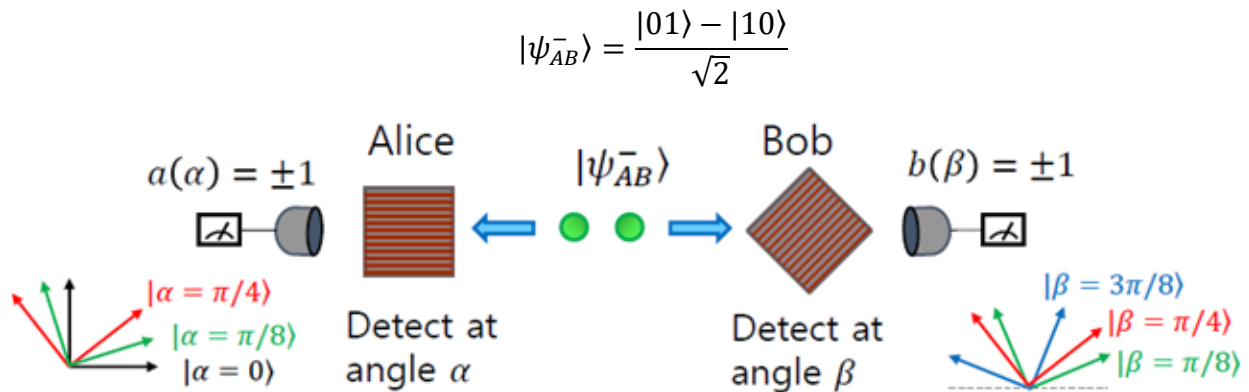
[Figure 1 & Table 1]

meas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Alice	-1	-1	1	1	1	1	-1	1	-1	-1	1	1	-1	-1	-1	-1
α	0	0	$\pi/8$	0	$\pi/8$	$\pi/8$	0	$\pi/8$	$\pi/4$	0	$\pi/4$	$\pi/8$	0	$\pi/4$	0	$\pi/8$
Bob	1	1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1
β	0	$\pi/8$	$3\pi/8$	$3\pi/8$	$\pi/8$	$\pi/4$	$3\pi/8$	$\pi/8$	$\pi/8$	$\pi/8$	$\pi/4$	$\pi/4$	$3\pi/8$	$\pi/4$	$\pi/8$	$\pi/8$

(A) Find the key that Alice and Bob will share assuming that there was no attempt to eavesdrop. Alice and Bob agreed that if Alice has measurement result of '-1, 1, 1' while Bob measured '1, -1, -1', then the shared key will be 011. (5 points)

(B) Calculate CHSH parameter $S = E\left(0, \frac{\pi}{8}\right) + E\left(\frac{\pi}{4}, \frac{\pi}{8}\right) + E\left(\frac{\pi}{4}, \frac{3\pi}{8}\right) - E\left(0, \frac{3\pi}{8}\right)$ based on the table given below and give a possible explanation of why S is different from its ideal value. (8 points)

*The expectation value for measurement angle (α, β) is defined as

$$E(\alpha, \beta) = \frac{\text{\# of same result} - \text{\# of different result}}{\text{\# of total measurement with } \alpha, \beta}$$

Alice (α)	Bob (β)	Same	Different
0	$\pi/8$	400	2100
$\pi/4$	$\pi/8$	200	800
0	$3\pi/8$	2000	500
$\pi/4$	$3\pi/8$	150	850

Problem 5. Shannon entropy provides the lower bound of the length of string for data encoding. Answer the questions about encoding 5 symbols 'A', 'B', 'C', 'D', 'E'. (10 points)

(A) Suppose we don't know the probability distribution of occurrence of each symbol. What is the minimum number of bits to encode 5 symbols? (3 points)

(B) Suppose the probability of 'A' is 1/2, 'B' is 1/4, 'C' is 1/8, 'D' is 1/16, and 'E' is 1/16. Find the Shannon entropy of this information source. (3 points)

(C) What kind of encoding scheme can be used to achieve minimal average bit length? Give an example and calculate the average length of the code per symbol. (4 points)

Problem 6. Answer the questions about a circuit given below. Assume that the input state is a mixed state with probability of p_1 for $|0\rangle$ state and p_2 for $|1\rangle$ state. w_0 is a positive constant. (12 points)

$$U_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, U(t) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-iw_0 t} \end{pmatrix}$$

$|0\rangle: p_1$

$|1\rangle: p_2$ ——$\boxed{U_1}$——$\boxed{U(t)}$——$\boxed{U_1}$——

$p_1 + p_2 = 1$
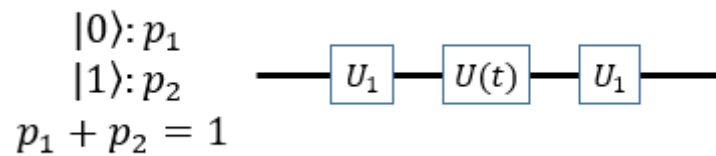
(A) Find the probability to measure $|0\rangle$ state at the end of the given circuit. (6 points)

(B) Plot probability to measure $|0\rangle$ state as a function of time with meaningful values. (peak, period, etc.) You need to give two plots: one for general p_1, p_2 value with $p_1 > p_2$ & the other for $p_1 = p_2 = \frac{1}{2}$. (6 points)

Problem 7. Shor's algorithm requires "modular exponentiation" circuit. The following circuits are circuit diagrams for basic components for modular exponentiation with mod 15, i.e., circuits for multiplying positive integers A (left) and B (right) with mod 15. Guess A & B from the circuits. (10 points)

SWAP gate

$$|p_3 p_2 p_q p_0\rangle = |A * q_3 q_2 q_1 q_0 \; mod \; 15\rangle$$
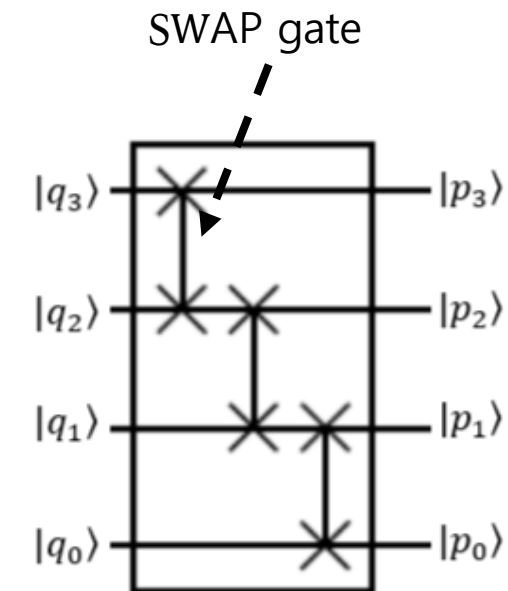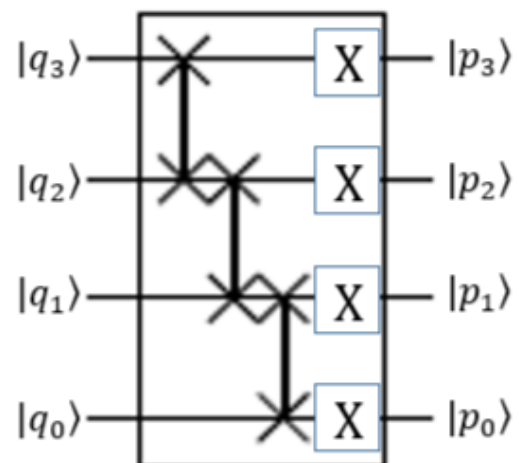
$$|p_3 p_2 p_q p_0\rangle = |B * q_3 q_2 q_1 q_0 \; mod \; 15\rangle$$

Problem 8. (Single bit–flip error correction code) Assume that unitary type error $U_{err} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$ might flip a single qubit with $\theta \ll 1$. The circuit for single bit flip error correcting code is as following and the input state is given as arbitrary quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. (17 points)

(A)

(B)
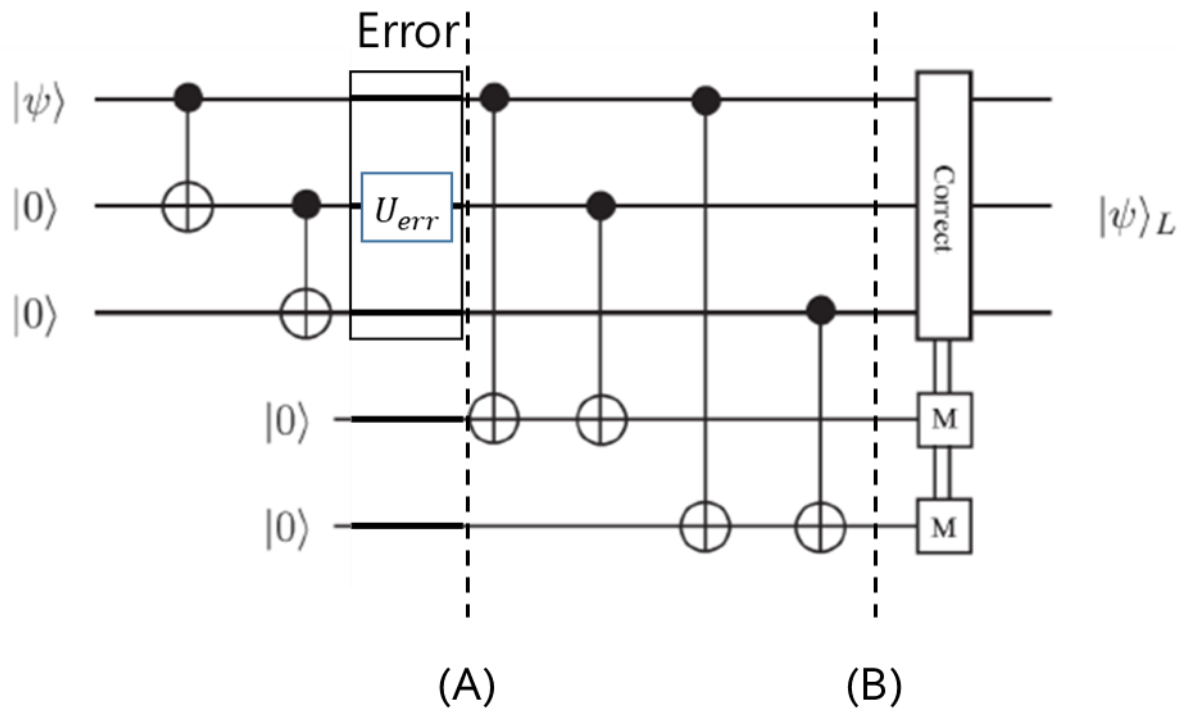
(A) What is the qubit state right after the error? (3 points)

(B) What is the overall quantum state before the measurement? (3 points)

(C) What is the probability to get correct output state? (3 points)

(Hint: Probability to get $|0\rangle$ from $|\psi\rangle = \alpha|A\rangle|0\rangle + \beta|B\rangle|1\rangle$ is $|\alpha|^2\langle A|A\rangle$.)

(D) What is the probability to get flipped output state? (3 points)

(E) What gates should be applied according to each syndrome measurement result? For this, assume U_{err} can be applied to one of the three qubits, not only to the second qubit and we already know the type of error as U_{err}. (5 points)

Problem 9. Gate identities might induce convenience in implementing quantum circuits. Answer the questions. (20 points)
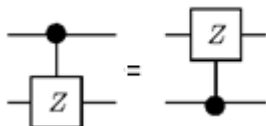
(A) Prove following circuit identity. (3 points)
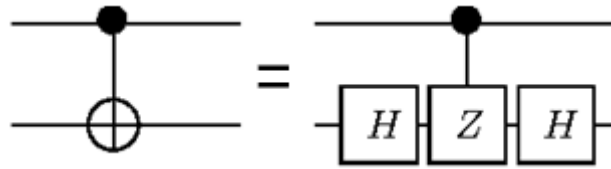
(B) Prove following circuit identity. (3 points)
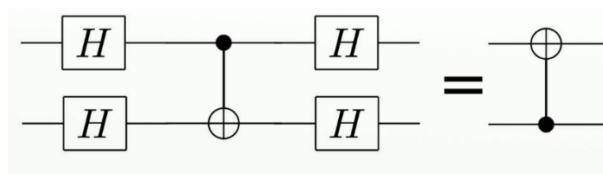
(Hint: Note that Controlled-Z is symmetric between control bit and target bit)

(C) For three-qubit phase flip code given in lecture, we can apply similar but slightly different circuit to perform syndrome measurement. Draw a circuit for syndrome measurement on the blank in the figure below. (Hint: phase error can be detected by converting $|+\rangle$, $|-\rangle$ state to $|1\rangle$, $|0\rangle$.) (7 points)
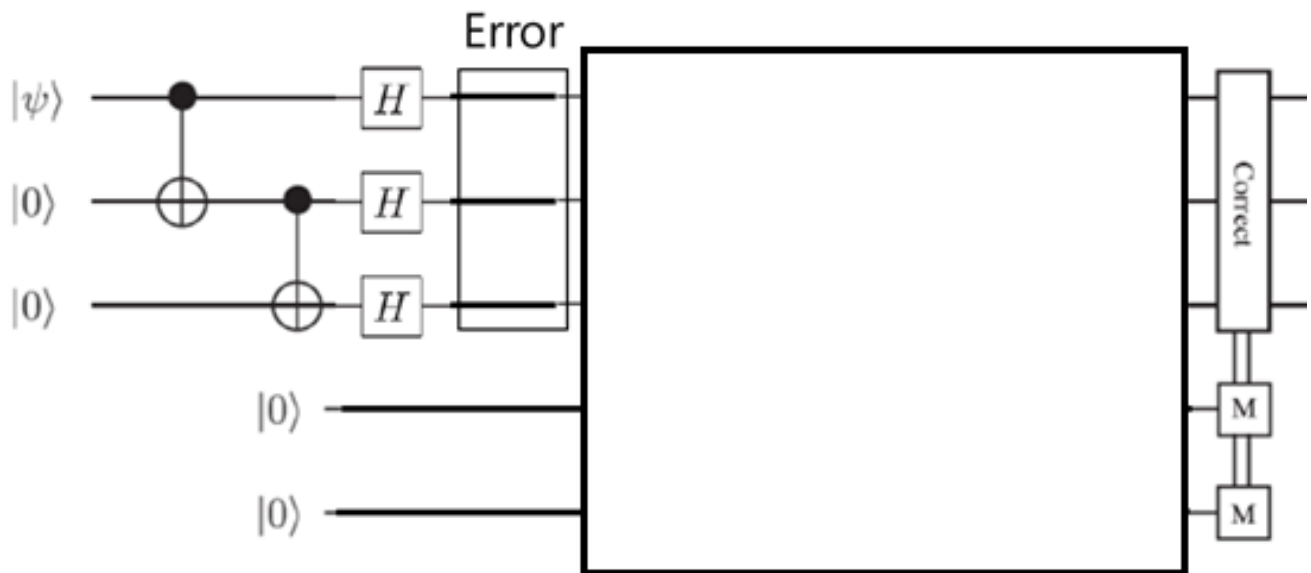

(D) Modify the circuit you gave in (C) by using the identity shown in (B) to remove all the Hadamard gate on the first 3 qubits. (encoding qubits) (7 points)

(Intentionally left blank for continued answer)

Problem 10. (Phase estimation algorithm) Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{i2\pi\varphi}$, where the value of φ is unknown. The goal of the phase estimation algorithm is to estimate φ. To perform the estimation, we assume that we are given the black boxes (or oracle) that can prepare the state $|u\rangle$ and perform the controlled-U^{2^j} operation, for suitable non-negative integers j as shown in the circuit below.

The quantum phase estimation procedure uses two registers. The first register contains t qubits initially in the state $|0\rangle$. The second register begins in the eigenstate $|u\rangle$ with eigenvalue $e^{i2\pi\varphi}$, and this register contains as many qubits as is necessary to store $|u\rangle$. Phase estimation is performed in two stages, and the following circuit shows the first stage.

For the simplicity, we assume that $\varphi < 1$ and it can be represented by t binary digits like $\varphi = 0.\varphi_1\varphi_2 \ldots \varphi_t$ in binary format (for example, $1/2 = 0.1_2$, $3/4 = 0.11_2$) . (?? points)
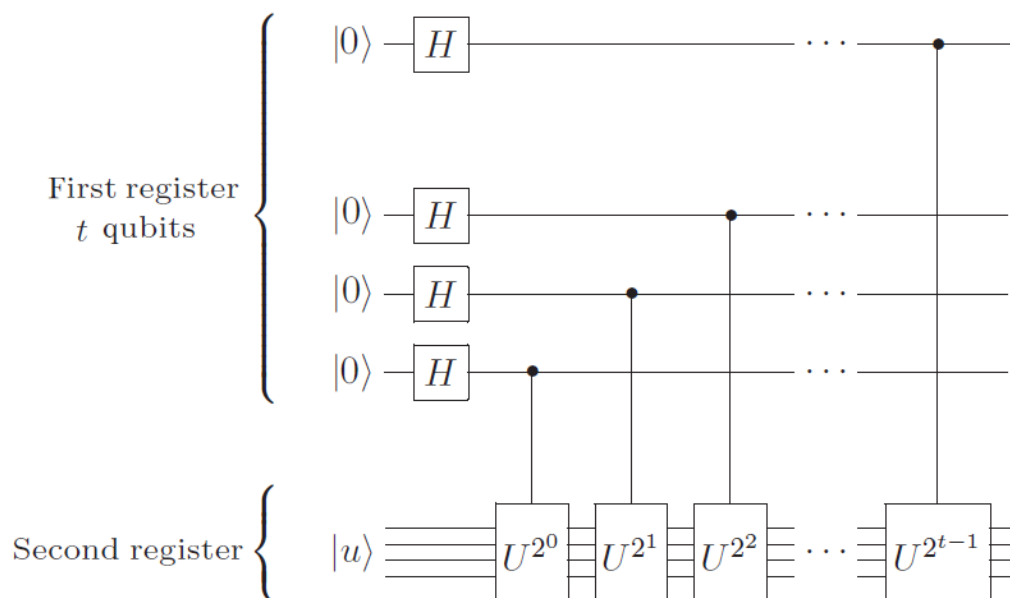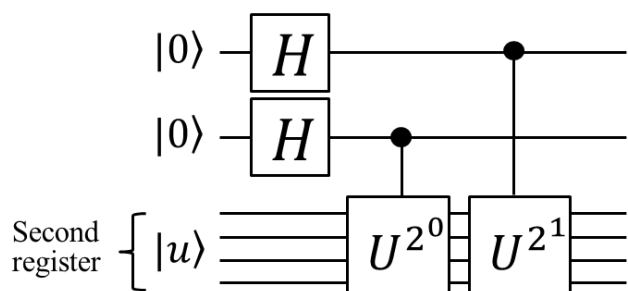

First stage circuit for the phase estimation algorithm

We want to find out the output quantum state of the above circuit.

(A) First, find out the output state of the following circuit. (Hint: even if the second qubit register seems to be affected by the controlled-U gate, the quantum state of the second register won't be entangled with the control qubit.) (3 point)
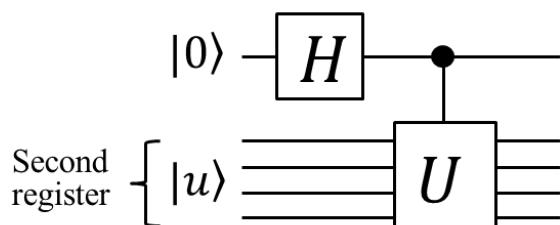
(B) What is the state of the m-th qubit from the top in the register, at the end of the first stage circuit? Try to write the phase of the qubit in terms of $\varphi_1, \varphi_2, \ldots, \varphi_t$. For example, $|0\rangle + e^{2\pi i\, 0.\varphi_n \cdots \varphi_l}|1\rangle$ (Hint: consider the output state of the following circuit, and generalize it to t qubits.) (6 points)

(C) Note that the goal of phase estimation algorithm is to obtain the value of φ. From the output of the above first stage circuit, how can we obtain the binary digits of $\varphi_1, \varphi_2, \ldots, \varphi_t$? (Hint: we already saw the output state with the similar pattern during the derivation of QFT circuit.) Answer this question by <u>showing the circuit</u> and <u>finding the final state and measurement result</u> with specific example of t = 3, $U = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi*1/8} \end{pmatrix}$, $|u\rangle = |1\rangle$.

(8 points)