M1522.002500 - 양자 컴퓨팅 및 정보의 기초

(Prof. Taehyun Kim)

Homework #4

Due date: June. 14, Sun 2020 12:00 pm

If you submit after the due date, your score will be deducted by 20%.

No more submission will be accepted after June. 16, 2020. 12:00pm

To reduce the grading burden of TA, the homework will be graded all-or-nothing style. We will grade just a few problems randomly sampled from the homework and renormalize the total grading according to the relative weight of each problem. Also, within each problem, there may be several sub-problems, but we will grade only a few sub-problems within each problem, and the score of each problem will be determined by the graded sub-problems proportionally.

For example, if problem 1 is composed of 5 sub-problems, we will decide which sub-problems will be graded later, and if you solved that sub-problems correctly, you will get the full credit of problem 1. In the worst case, you might have solved all other sub-problems correctly, but got the wrong answers in all the graded sub-problems. That is an unfortunate situation, but the score for that entire problem will become 0. Without this policy, we cannot grade so much homework efficiently.

The homework should be *hand-written*, converted into a pdf file, and uploaded to ETL. The pdf file may either be a scanned-copy or camera-taken picture of your homework. If you solve the homework problems using digital pen on a tablet, it will be considered as your hand-writing, but make sure that your hand-writing is legible. Please make sure you denote the number of the problems correctly. We will post solutions for every homework and announce the problems and sub-problems to be graded after the hard deadline.

The homework should be written with your hand-writing either on a paper or a tablet. Computer-typed homework won't be accepted!

Note)

1. Please read through chapters 1.4.3~1.4.4, 5.1 ~ 5.3 of the textbook for details if necessary.

2. Some problems contain lengthy explanation. The questions that you should answer are underlined, so please read thoroughly.

Deutsch-Josza algorithm

1. (20 points) The Deutsch-Josza problem can be stated as follows.

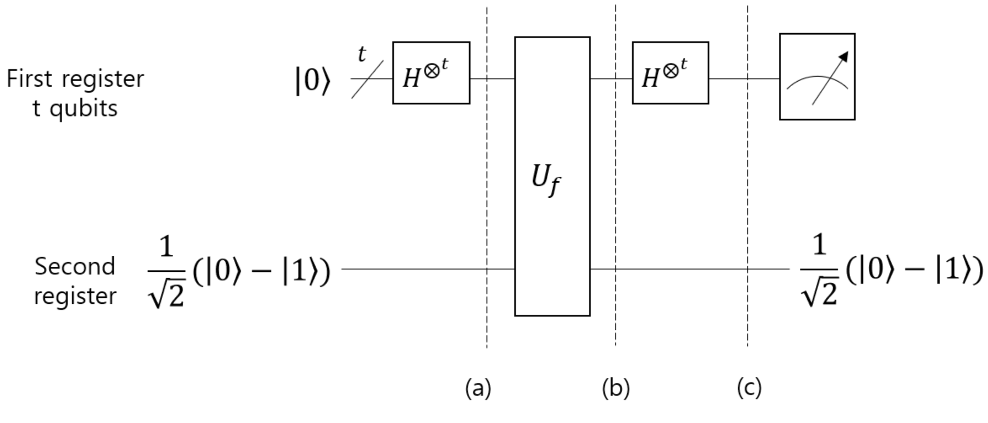
Input: A black-box for computing an unknown function $f: \{0,1\}^t \rightarrow \{0,1\}$

Constraint: f is either a constant or a balanced function

Problem: Determine whether f is either constant or balanced by making queries to f.

$\{0,1\}^t$ indicates an t-bit bit string. It is the computational basis of an t-qubit system. f is constant if f maps to either 0 or 1 for all input, whereas it is balanced if exactly half of the inputs map to 0 and the other half to 1.

Classically, we would have to make $2^{t-1}+1$ queries in order to solve this problem. The following circuit, on the other hand, requires just one query.



The slashed line indicates a multi-qubit channel. There is one Hadamard gate per one-qubit line in the first register.

The operator U_f is defined as follows.

$$U_f|j\rangle|k\rangle = |j\rangle|k \oplus f(j)\rangle$$

The indices j, k for the computational basis may either be decimal ($|0\rangle, |1\rangle, \ldots$) or binary ($|0..00\rangle, |0..01\rangle, ..$) representations depending on the context.

Show that the states at stages (a) – (c) are given as follows.

(a) (3 points) $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=\frac{1}{\sqrt{2^t}}\sum_{j\in\{0,1\}^t}|j\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

(Hint: This is just an equally weighted superposition of the computational basis in the first register. Two equivalent expressions are presented to show how the decimal and binary representations differ.)

(b) (7 points) $\frac{1}{\sqrt{2^t}}\sum_{j\in\{0,1\}^t}(-1)^{f(j)}|j\rangle\,(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$

(Hint: First try proving this for $t=1$.)

Notice that the work that has been performed by U_f on the qubit in the second register appears to have been encoded in the phase of qubits in the first register. For this reason, this scheme is known as the *phase kick-back.* Such schemes are frequently employed throughout quantum algorithms.

(c) (7 points) $\frac{1}{2^t}\sum_{l\in\{0,1\}^t}(\sum_{j\in\{0,1\}^t}\,(-1)^{f(j)+j\cdot l})\,|l\rangle\,(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$

$j\cdot l=j_1l_1+j_1l_1+\cdots j_tl_t$ is defined as the bit-wise inner product, modulo 2.

(Hint: You may want to first prove the following identity:

$$H^{\otimes n}|j\rangle=\frac{1}{\sqrt{2^t}}\sum\nolimits_{l\in\{0,1\}^t}(-1)^{j\cdot l}|l\rangle$$

Or, to make it more transparent,

$$H^{\otimes n}|j_1j_2\ldots j_t\rangle=\frac{1}{\sqrt{2^t}}\sum\nolimits_{l\in\{0,1\}^t}(-1)^{j_1l_1+j_1l_1+\cdots j_tl_t}|l_1l_2\ldots l_t\rangle$$

Double hint: In the case of a single qubit, it is easy to show that,

$$H|j\rangle=\frac{1}{\sqrt{2}}\sum\nolimits_{l\in\{0,1\}}(-1)^{jl}|l\rangle$$

)

The state that we measure in the first register in (c) is thus a superposition of computational basis $|l\rangle$ each with coefficients $\sum_{j\in\{0,1\}^t}(-1)^{f(j)+j\cdot l}$. Consider the state $|l\rangle=|00\ldots0\rangle$. The coefficient is then $\sum_{j\in\{0,1\}^t}(-1)^{f(j)}$. If f is constant, all $(-1)^{f(j)}$ add up constructively to 2^t $(f(j)=0)$ or -2^t $(f(j)=0)$. Since the coefficient of $|00\ldots0\rangle$ is either ±1, the t-qubit state is uniquely determined as $|00\ldots0\rangle$. On the other hand, if f is balanced, $\sum_{j\in\{0,1\}^t}(-1)^{f(j)}$ sums to zero, so the coefficient of $|00\ldots0\rangle$ is exactly zero.

Based on such observations, what would your criterion be for determining whether f is constant or balanced? (3 points)

Quantum Fourier transform and phase estimation

2. (10 points) The quantum Fourier transform and its inverse are defined as follows.

$$U_{QFT}|j\rangle = \frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1} e^{2\pi ijk/N}\,|k\rangle$$

$$U_{QFT}^{-1}|j\rangle = \frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1} e^{-2\pi ijk/N}\,|k\rangle$$

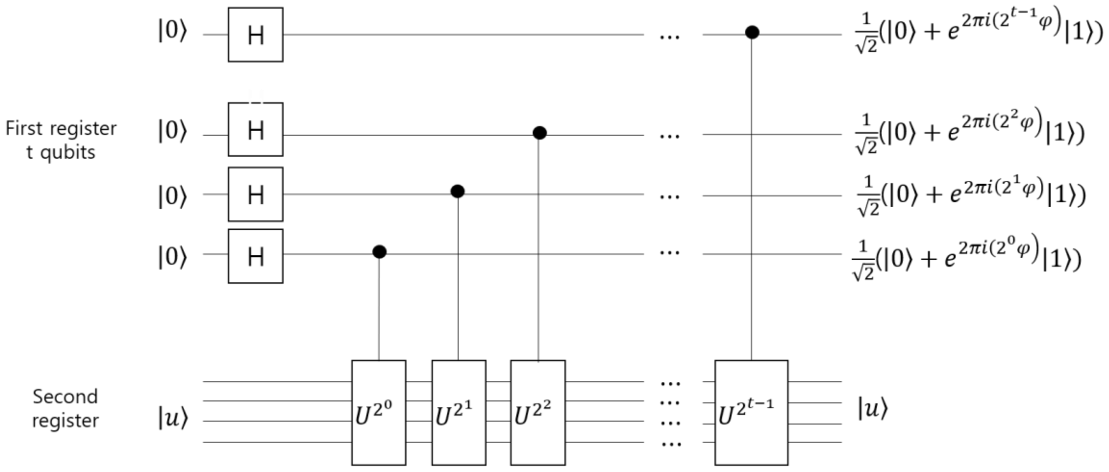
The circuit that implements U_{QFT} is given in slide 3, lecture 15. Draw the circuit that performs U_{QFT}^{-1}. (Hint: You will need the inverse of R_k)

3. (15 points) Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$. For simplicity, let $\varphi = 0.\varphi_1\varphi_2 \ldots \varphi_t$ in binary representation. We would like to construct a circuit that can measure φ exactly. It can be easily shown that $U^m|u\rangle = e^{2\pi i(m\varphi)}|u\rangle$. The gates U^{2^j} represent an operator that act U on an input qubit state 2^j times. Show that the circuit below produces the states,

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle = \frac{1}{\sqrt{2^t}}(|0\rangle + e^{2\pi i(2^{t-1}\varphi)}|1\rangle)\otimes(|0\rangle + e^{2\pi i(2^{t-2}\varphi)}|1\rangle)\otimes\cdots\otimes(|0\rangle + e^{2\pi i(2^{0}\varphi)}|1\rangle)$$

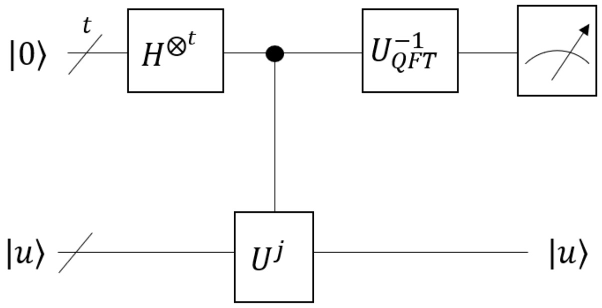
$$= \frac{1}{\sqrt{2^t}}(|0\rangle + e^{2\pi i(0.\varphi_t)}|1\rangle)\otimes(|0\rangle + e^{2\pi i(0.\varphi_{t-1}\varphi_t)}|1\rangle)\otimes\cdots\otimes(|0\rangle + e^{2\pi i(0.\varphi_1\varphi_2\ldots\varphi_t)}|1\rangle)$$

for an input t-qubit state $|00\cdots 0\rangle$ in the first register. The first equality has been covered in class.


First register
t qubits
Second register
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|u\rangle$
H
H
H
H
U^{2^0}
U^{2^1}
U^{2^2}
$U^{2^{t-1}}$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(2^{t-1}\varphi)}|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(2^{2}\varphi)}|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(2^{1}\varphi)}|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(2^{0}\varphi)}|1\rangle)$
$|u\rangle$

Notice that the eigenvalues of U have been encoded into the relative phases of the qubits in the first register using the *phase kick-back* scheme.

4. (10 points) Now we act U_{QFT}^{-1} on the t-qubit output state derived in problem 3. That is, the total circuit looks like the following.



The operator U^j represents the series of operations U^{2^j} in problem 3. Show that the t-qubit state in the first register just before measurement is, $|\tilde{\varphi}\rangle \equiv |\varphi_1\varphi_2 \ldots \varphi_t\rangle$. The tilde denotes that it is an estimator. That is, we measure a bit string $\varphi_1\varphi_2 \ldots \varphi_t$ and recover $\varphi = 0.\varphi_1\varphi_2 \ldots \varphi_t$.

This circuit allows us to exactly measure the eigenvalue of the U. But since we read the information encoded in the phases of the qubits in the first register, it is often known as the circuit for *phase estimation*. Note that the result would not be exact if the expression for the true value of φ requires more than t bits in binary representation. In that case, we would have to increase the number of qubits in the first register.

Typically, how we choose t depends on 1) the number of digits of accuracy we wish to have in our estimate for φ, and 2) with what probability we wish the phase estimation procedure to be successful.

The circuit can easily be extended to the case where U has multiple eigenvalues. In that case, the input state of the second register would be a superposition of the eigenstates of U, and the output in the first register will contain a superposition of the estimates for each eigenvalue.

Factorization and Shor's algorithm

Definitions: GCD – greatest common divisor, LCM – least common multiplier, order – the smallest period r that satisfies $x^r \equiv 1\, mod\, N$ for a given x and N.

The *generic algorithm* for factorizing a product of two prime numbers $N = p_1 p_2$ developed in number theory may be listed as follows. They are presented without proof.

1. Select a number $x < N$ at random and verify if $GCD(x, N) = 1$.

2. Find the order r of $x\, mod\, N$.

3. Check if r is even, and $x^{r/2} + 1 \not\equiv 0\, mod\, N$. If not, go back to step 1.

4. Compute $p_1 = GCD\left(x^{\frac{r}{2}} - 1, N\right), p_2 = GCD\left(x^{\frac{r}{2}} + 1, N\right)$

Steps 1, 3, 4 are best processed through classical computers. Especially, step 4 is efficiently implemented by the *extended Euclidean algorithm*. It is step 2 for which no efficient classical algorithm is known to exist.

The insight in Shor's algorithm contrived in 1994 was to apply the *quantum Fourier transform* and the *phase estimation* scheme in order to achieve exponential speedup in the sampling of orders in the modular arithmetic of step 2. Although we work with a quantum circuit based on the textbook which is slightly different from that of the original circuit invented by Peter Shor, we emphasize that they share the same spirit.

5. (5 points) Factor $N = 21$ using the *generic algorithm* (in the classical way).

6. (21 points) We define the unitary operator U_{mod} and its eigenstate $|u_s\rangle$ as follows.

$$U_{mod}|y\rangle \equiv |xy \quad mod\ N\rangle \quad (0 \le y \le N-1)$$

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^k \quad mod\ N\rangle$$

where r is the order that we wish to estimate and s is an integer and $0 \le s < r$. x is randomly chosen in step 1. Prove the following.

(a) (7 points)

$$U_{mod}|u_s\rangle = e^{\frac{2\pi i s}{r}} |u_s\rangle$$

(Hint: $e^{-\frac{2\pi i s}{r} r} |x^r \quad mod\ N\rangle = e^{-\frac{2\pi i s}{r} 0} |x^0 \quad mod\ N\rangle$)

(b) (3 points) $\sum_{s=0}^{r-1} e^{-\frac{2\pi i s n}{r}} = r\delta_{n0}$.

(Hint: Geometric series. To get an intuitive understanding for this, try drawing a unit circle in the complex plane and represent the complex numbers as vectors on the unit circle. The angle or phase will determine the spacing of these vectors. Summation of the complex numbers is just the summation of these vectors. You will notice that they add up only when they are in phase. This means that they point towards the same direction or have an angular spacing that is a multiple of 2π. Otherwise, they cancel to zero.)

(c) (7 points)

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} e^{\frac{2\pi i s j}{r}} |u_s\rangle = |x^j \quad mod\ N\rangle$$

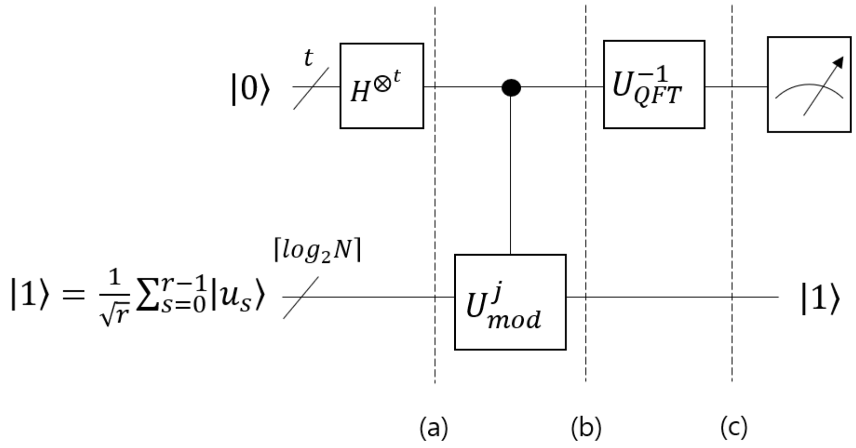
(Hint: Use (b))

(c) (4 points)

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

Note, (c) is an important identity in that, which will become clear in problem 7, it does not require knowledge about r in order to prepare such a state. The state $|1\rangle$ will simply be a superposition of r-$|u_s\rangle$ states.

7. (10 points) Recall the circuit for phase estimation in problem 4. To construct the *order-finding* circuit, we simply replace the unitary operator U^j with U_{mod}^j, which is basically a series of U_{mod}^{2j} operators as in problem 3. We also substitute $|1\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle$ for $|u\rangle$ in the second register.



This circuit performs order-finding for step 2 in the generic factorization algorithm. At (a), the state is just a uniform superposition of the computational basis in the first register.

(a) $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|1\rangle$

Assuming that 2^t is a multiple of r, show that the states at the stages (b) and (c) are as follows.

(b) (5 points) $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \mod N\rangle = \frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1} e^{\frac{2\pi isj}{r}}|j\rangle|u_s\rangle$

(Hint: Use the identities proven in problem 6. This equality is exact because we have assumed that 2^t is a multiple of r. This simplifies our estimation. In general, this will not be the case and lead to more complicated number theoretical analysis regarding the accuracy of estimation, such as the *continued fractions algorithm* etc. We will not go into that here.)

(c) (5 points) $\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left|2^t\frac{s}{r}\right\rangle|u_s\rangle$

(Hint: Use the definition of the quantum Fourier transform in slide 4, lecture 15)

Note that we can define $\left|\widetilde{\frac{s}{r}}\right\rangle \equiv \left|2^t\frac{s}{r}\right\rangle$ as the estimator for a multiple of $\frac{1}{r}$ in the sense that when we measure $\left|2^t\frac{s}{r}\right\rangle$, we obtain a number $k = 2^t\frac{s}{r}$ from which we can compute $\frac{k}{2^t} = \frac{s}{r}$ and obtain a sample of r.

It can be observed in (c) that we perform measurements on states that are in a uniform superposition of r-states with each state containing partial or complete information about the value r, or the order. We can repeat measurements and keep a list of the estimated orders $\{r_1, r_2, r_3, \ldots\}$ where the subscript denotes the repetition number. When we have found a r_i that satisfies $x^{r_i} \equiv 1 \mod N$, we can move on to step 3 in the factorization algorithm. This will make more sense once we have gone through a specific example in the following problem.

8. (15 points) In class we have applied the *order-finding* circuit to factor $N = 15$. Here we repeat the problem using a different x. We pick $x = 8$. It can be easily shown that the order is $r = 4$. That is, $8^4 \equiv 1 \mod 15$. Let us see how this value is returned to us by the circuit. We use $t = 11$ qubits.

The state in stage (b) in the circuit will be,

$$\frac{1}{\sqrt{2^{11}}}\sum_{j=0}^{2^{11}-1}|j\rangle|8^j \mod 15\rangle = \frac{1}{\sqrt{4\cdot 2^{11}}}\sum_{s=0}^{3}\sum_{j=0}^{2^{11}-1} e^{\frac{2\pi isj}{4}}|j\rangle|u_s\rangle$$

In stage (c) the state is,

$$\frac{1}{\sqrt{4}}\sum_{s=0}^{3}\left|2^{11}\frac{s}{4}\right\rangle|u_s\rangle = \frac{1}{\sqrt{4}}(|0\rangle|u_0\rangle + |512\rangle|u_1\rangle + |1024\rangle|u_2\rangle + |1536\rangle|u_3\rangle)$$

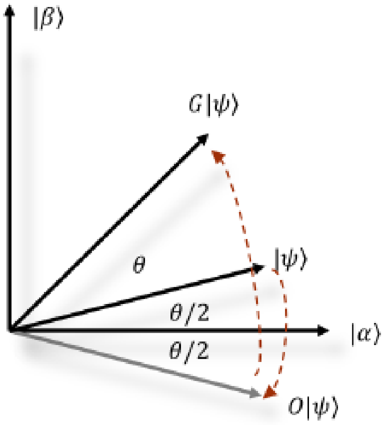
Measurement on the first register will yield the numbers $0, 512, 1024, 1536$ with uniform probability. Based on these measurements, we compute $\frac{0}{2048} = 0$, $\frac{512}{2048} = \frac{1}{4}$, $\frac{1024}{2048} = \frac{1}{2}$, $\frac{1536}{2048} = \frac{3}{4}$ from which we obtain the list of sampled $r's$ for each number, $\{undetermined, 4, 2, 4\}$. From this list we can choose the largest number 4 as the estimator for the order and check if $8^4 \equiv 1\, mod\, 15$. If it is true, then we can move onto step 3.

When the period is so large that we are uncertain that we have sampled the largest r, we can also try estimating the order as $LCM(r_1, r_2)$ for two different r_1, r_2. In our simple example, suppose we have performed two measurements and obtained $\{2, 4\}$. Then $LCM(2, 4) = 4$ is a strong candidate for r.

Using the values x and r that you found in problem 5 with $N = 21$, show how the order-finding circuit would return r. Write down what the states would look like through steps (a) – (c) as in the explanation above. You may choose your own qubit number t. (This may be awkward, since we already know r, but hopefully it will helpful in emulating the inner workings of the circuit for a particular example.)

Quantum search and Grover's algorithm

In the below problems, $|\psi\rangle = H^{\otimes n}|0\rangle$



9. (15 points) Consider the Grover search algorithm in the lecture.

Prove the followings.

(a) (5 points) For $O|x\rangle = (-1)^{f(x)}|x\rangle$, $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$ (which means O is reflection about $|\alpha\rangle$)

(b) (5 points) $H^{\otimes n}(2|0\rangle\langle 0| - I)\, H^{\otimes n}$ is reflection about $|\psi\rangle$

(c) (5 points) For $N \gg M$, $\theta \simeq 2\sqrt{\frac{M}{N}}$

10. (10 points) Consider $f: \{0,1\}^2 \to \{0,1\}, f(x) = \begin{cases} 1, & x = 10_2 \\ 0, & otherwise \end{cases}$.

Calculate (in the computational basis) the followings.

(a) (2 points) $|x\rangle \equiv H^{\otimes 2}|00\rangle$

(b) (2 points) $|y\rangle \equiv O|x\rangle$

(c) (2 points) $|z\rangle \equiv (2|\psi\rangle\langle\psi| - I)|y\rangle$

(d) (4 points) Probability distribution of measurement of $|z\rangle$ (in computational basis).

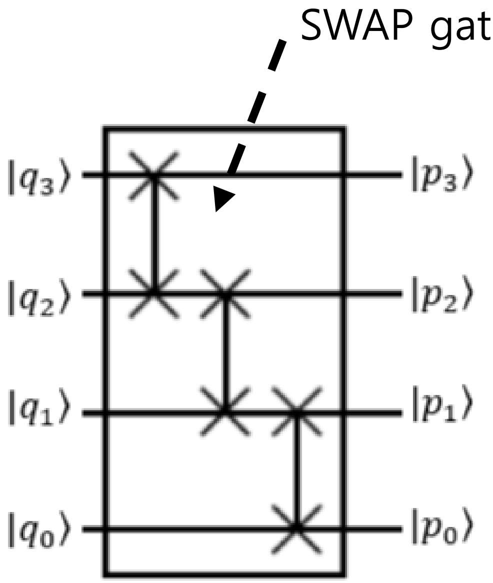
11. (10 points) Show that the operation $(2|\psi\rangle\langle\psi| - I)$ applied to a general state $\sum_k \alpha_k |k\rangle$ produces

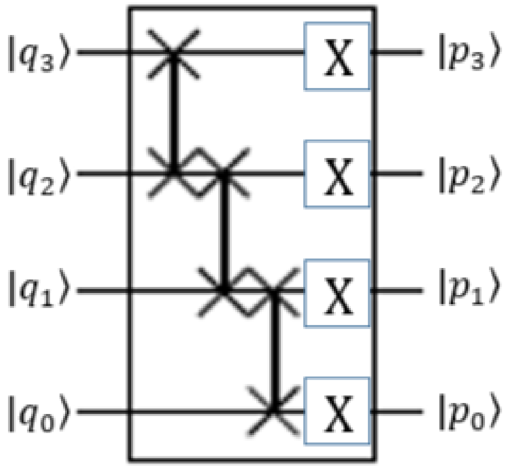
$$\sum_k (-\alpha_k + 2\langle\alpha\rangle)|k\rangle,$$

where $\langle\alpha\rangle \equiv \sum_k \alpha/N$ is the mean value of the α_k. For this reason, $(2|\psi\rangle\langle\psi| - I)$ is sometimes referred to as the inversion about mean operation.

Example of modular exponentiation

12. (10 points) Shor's algorithm requires a "*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.





$|p_3p_2p_qp_0\rangle = |A * q_3q_2q_1q_0\ mod\ 15\rangle$ $|p_3p_2p_qp_0\rangle = |B * q_3q_2q_1q_0\ mod\ 15\rangle$

Note, here $p_3p_2p_qp_0$ and $q_3q_2q_1q_0$ are binary representations of some integers. You must convert them to decimal values to make the arithmetic make sense.