UCInetID:

(This is your uci email address without the @uci.edu part)

Name:_____

(Please write clearly and use the same name as your gradescope account.)

Midterm 3

Practice

CS 166

Winter 2024

March 15, 2024

Instructor: Shion Fukuzawa

Instructions

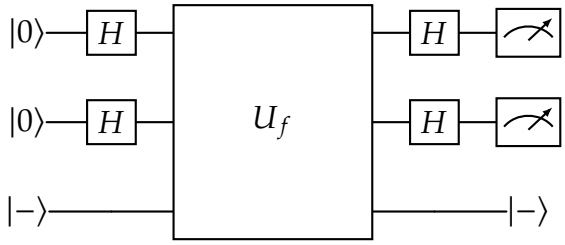
- Wait until instructed to turn over the cover page.
- There are 4 questions on the test. Select 3 questions to attempt, and indicate this by circling the problem number at the start of each problem. Each problem has 2 pages.
- For every question, simplify your answer as much as possible. We will accept your answer if we are able to plug it into a graphing calculator.
- Please write your final answer in the boxes provided. Use the extra scratch paper or the back of the exam pages for your work.
- When asked for measurement results, clearly indicate what the possible outcomes are, as well as the other information the problem is asking for.
- When drawing circuits, you may use extra qubits initialized to $|0\rangle$, as well as the † shorthand for the adjoint operator.

❖ Problem 1: Querying a unitary encoding a function. [10 minutes]

Consider the following function $f : \{0,1\}^2 \to \{0,1\}$

$$f(00) = 1 \tag{1}$$
$$f(01) = 0 \tag{2}$$
$$f(10) = 0 \tag{3}$$
$$f(11) = 1 \tag{4}$$

The unitary gate U_f in the circuit below maps $|x\rangle\,|y\rangle$ to the state $|x\rangle\,|y \oplus f(x)\rangle$, where x is a 2 bit string and y is 1 bit. In this question, you should evaluate the function $f(x)$ in your analysis whenever possible. That is, your final solution **should not** contain terms that are in the form $f(x)$.



1. What is the state of the system right after the U_f gate is applied.

2. What is the probability that we measure $|00\rangle$ at the end?

❖ Problem 2: Grover's Algorithm [15 minutes]

For this problem, we will assume that we black box access to a function $f : \{0,1\}^n \to \{0,1\}$ in the form of the gate U_f. This gate U_f is defined in the usual sense, such that if it acts on the state $|x\rangle\,|y\rangle$, the resulting state is $|x\rangle\,|y \oplus f(x)\rangle$.

We will also assume that **there is exactly one string** $a \in \{0,1\}^n$ such that $f(a) = 1$, and for any other string $x \neq a$, $f(x) = 0$. Here, we will use the following short hands:

- $|\psi\rangle = H^{\otimes n}\,|0\cdots0\rangle$
- $|e\rangle = \frac{1}{\sqrt{N-1}} \sum_{x\neq a} |x\rangle$

1. Suppose we started with n qubits and applied Hadamard gates to each of them. If we measure this state, what is the probability that we see $|a\rangle$?

2. The above probability can be written in the form $\sin\theta$. Using the fact that $\sin\theta \approx \theta$ for small θ, express an approximation to θ using N.

3. Grover's algorithm repeatedly applies the following two operations. We will call one cycle of the following procedure a **Grover step**.

   (a) Reflect the current state $|v\rangle$ over the state $|e\rangle$ to get $|v'\rangle$.

   (b) Reflect the state $|v'\rangle$ over the state $|\psi\rangle$ to get $|v''\rangle$.

   In the figure in the following page, draw $|v'\rangle$ and $|v''\rangle$.

4. If λ is the angle between $|e\rangle$ and $|v\rangle$, what is the angle formed between $|e\rangle$ and $|v''\rangle$?

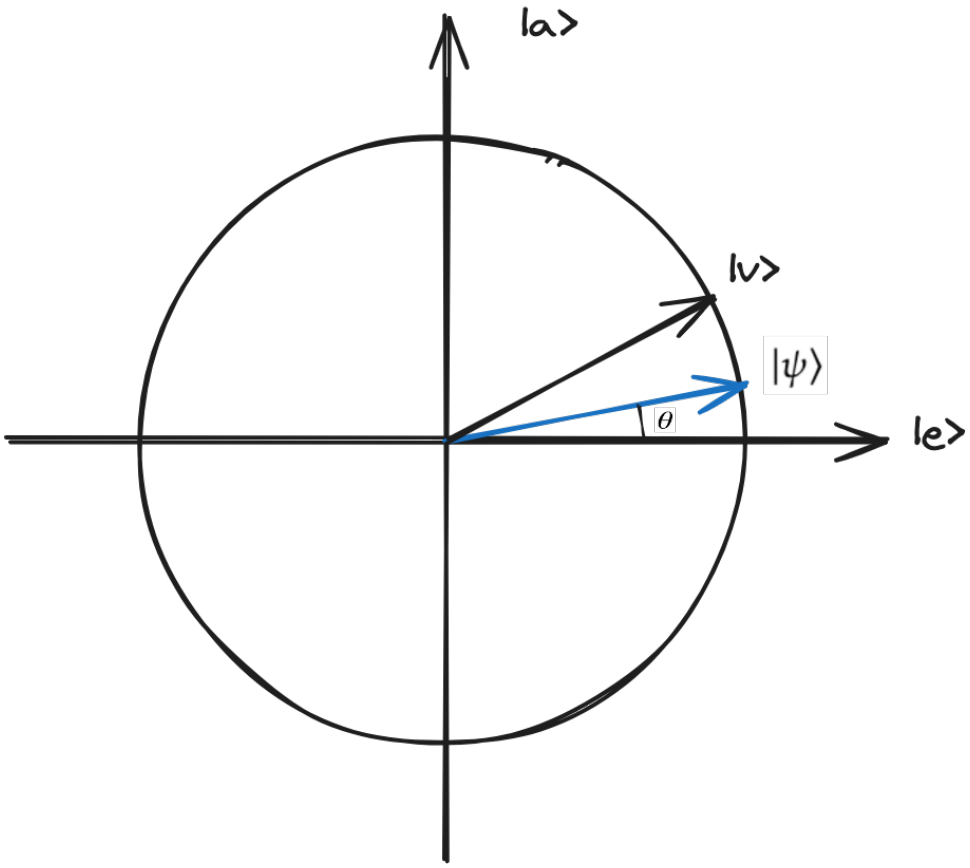


Figure 1: Caption

5. We will start the algorithm from the state $|\psi\rangle$. How many times should we repeat the Grover step to maximize the probability that we measure $|a\rangle$?

❖ Problem 3: Shor's Algorithm [25 minutes]

In this section, we will analyze one instance of Shor's algorithm, so each part will depend on previous parts. Suppose we are trying to factor the integer 33. For the analysis, we will use the notation $M = 33$, $n = 6$, and $N = 64$.

1. Suppose we sampled $x = 7$ in step 1. Given this, what is the function $f(s)$ that the unitary encodes in the Period Finding subroutine of step 5?

2. Below is part of the table for the function you stated above. Fill out the empty cells.

s	0	1	2	3	4	5	6	7	8	9	10	11	12
f(s)	1		16	13	25	10		28	31	19			

3. Consider the period finding algorithm applied to this instance of the problem. Write down the first 5 terms in the state of the system after the U_f gate is applied. That is, your answer should be in the form

$$\frac{1}{\sqrt{?}}(|?\rangle\,|?\rangle + |?\rangle\,|?\rangle + |?\rangle\,|?\rangle + |?\rangle\,|?\rangle + |?\rangle\,|?\rangle + \cdots) \tag{5}$$

   Do not use summation notation, and write the states explicitly.

4. Suppose we measure $|16\rangle$ in the second register at step 4 of the algorithm. The state after this measurement can be written in the form $\frac{1}{\sqrt{s}} \sum_{j=0}^{s-1} |jr + l\rangle\,|16\rangle$.

   What is r and l?

5. What is $QFT_N\,|32\rangle$? Use summation notation.

6. Suppose that at the measurement in step 6, we measure $|45\rangle$. Write down $\frac{45}{64}$ as a continued fraction using a_1, a_2, a_3, and a_4. That is, your solution should be in the form

$$\frac{45}{64} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \frac{p}{q}}}}} \tag{6}$$

   where p and q are also integers.

7. Ignore p and q from above to get an approximation for $\frac{45}{64}$. Let's call the denominator of this approximation be r. The Period Finding subroutine in step 5 of Shor's algorithm returns this value of r. What is $f(r/2)$?

8. Let's call the answer of your previous answer z. Write down $\gcd(z-1, M)$ and $\gcd(z+1, M)$. Your solutions should be multiples of or equal to the factors of M.

❖ Alice, Bob, and Frankie [50 minutes]

If you have time, draw a picture of Frankie using Shor's algorithm to read a message Alice sent to Bob.

Or use this page as extra workspace.