COMS 4281 - Introduction to Quantum Computing Fall 2024

Problem Set #2 - Theory

Sally Student *Instructor: Henry Yuen*

Due date: December 4, 11:59pm. Collaboration is allowed and encouraged (teams of size at most 3). Please read the syllabus carefully for the guidelines regarding collaboration.

- Everyone must write their own solutions in their own words.
- You must also indicate who you worked with.

Write your collaborators here:

Problem 1: Uncovering Hidden Structure

We saw in class how Shor's Factoring Algorithm makes clever use of the Phase Estimation Algorithm, which in turn takes advantage of the Quantum Fourier Transform. This algorithm works and appears to get an exponential speed-up over the best possible classical algorithm because of special number-theoretic structure underlying the factoring problem.

In this problem we'll explore a slightly different context in which the Quantum Fourier Transform can be used to uncover hidden structure in a function. This exercise should remind you of Simon's Problem somewhat.

Problem 1.1

Consider the additive group $\mathbb{Z}_N$ which is the set of integers $\{0, 1, 2, \ldots, N-1\}$ equipped with binary operation which is addition modulo N (in other words, to add $x, y \in \mathbb{Z}_N$ we add them as usual, and take the remainder after dividing by N).

Let A be a set, and let $f : \mathbb{Z}_N \to A$ be a function such that for all $x, y \in \mathbb{Z}_N$, we have $f(x) = f(y)$ if and only if $x - y$ is a multiple of some secret number r that divides N.

First, show that f is a $\frac{N}{r}$-to-1 function.

Solution:

Problem 1.2

Our eventual goal is to design a quantum algorithm to discover this underlying periodicity r, given black-box access to the function.

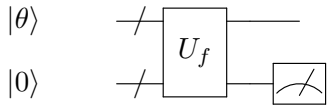
To keep things simple, let's assume that our quantum algorithm operates on two registers, one of dimension N, and one of dimension $M = |A|$ (rather than dealing with qubits, because N

and M may not be powers of 2). In other words, the oracle unitary U_f is a unitary acting on $\mathbb{C}^N \otimes C^M$ such that for all $x \in \mathbb{Z}_N$

$$U_f \left|x, 0\right\rangle = \left|x, f(x)\right\rangle$$

where 0 is some distinguished element of A.

Consider the following circuit, acting on input state $\left|\theta\right\rangle \otimes \left|0\right\rangle$ where $\left|\theta\right\rangle = N^{-1/2} \sum_{x \in \mathbb{Z}_N} \left|x\right\rangle$ is the uniform superposition over $\mathbb{Z}_N$:



What is the distribution of outcomes from measuring the second register? What is the post-measurement state of the first register conditioned on outcome $a \in A$?

Solution:

Problem 1.3

Fix a measurement outcome $a \in A$. What is the resulting state if we then apply the Quantum Fourier Transform of order N (i.e. apply the unitary F_N) to the first register of the corresponding post-measurement state?

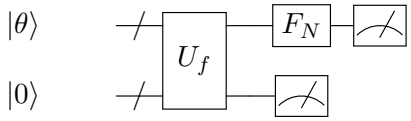
What is the distribution of outcomes $y \in \mathbb{Z}_N$ if we then measure the first register?

Hint: You may find your solutions to Worksheet 6 helpful.

Solution:

Problem 1.4

Show that, by using the following subroutine 20 times, we can obtain a random sequence of elements $y_1, y_2, \ldots, y_{20} \in \mathbb{Z}_N$ from which it is possible to recover the secret r with probability at least 99%.



Hint: Use the fact that if we sample uniformly random elements a, b from the set $\{1, 2, \ldots, k\}$, with probability at least 60% we will have $\gcd(a, b) = 1$ (this holds for any k).

Solution:

Problem 2: Grover Grover

In this problem we'll see an application of Grover's algorithm. Let $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ is a function. Suppose we want to design an algorithm that, given query access to O_f, outputs "YES" if there exists an $x \in \{0,1\}^n$ such that for all $y \in \{0,1\}^m$, we have $f(x,y) = 1$, and outputs "NO" otherwise.

Problem 2.1

Argue that any deterministic classical query algorithm that solves this problem needs to query the oracle $2^n \times 2^m$ times.

Hint: Try arguing this via contradiction: suppose there was such a deterministic classical query algorithm that made fewer than $2^n \times 2^m$ queries. Then design an f that would "trick" the algorithm in outputting the wrong answer.

Solution:

Problem 2.2

Let

$$O_f |x,y\rangle = (-1)^{f(x,y)} |x,y\rangle$$

denote the phase oracle corresponding to f. Design a quantum algorithm that, using Grover's algorithm, solves this problem with 98% by making $O(\sqrt{2^n \cdot 2^m} \cdot m)$ queries to f.

Hint: Try to first design a quantum algorithm that solves it with $O(\sqrt{2^n} \cdot 2^m)$ queries to f. Once you have that solution, try to then improve it to $O(\sqrt{2^n \cdot 2^m} \cdot m)$.

Hint: The reason for the extra m factor has to do with Problem 2 from Practice Worksheet 7.

Solution:

Problem 3: 1D Ising model

Let n be odd. Recall the 1-dimensional Ising model, which is a Hamiltonian describing a bunch of magnets on a line:

$$H = \sum_{j=1}^{n-1} Z_j \otimes Z_{j+1} + \mu \sum_{i=1}^{n} Z_i$$

where $\mu \in \mathbb{R}$ is a real parameter that represents the strength of the global magnetic field relative to the interactions between neighboring magnets.

Problem 3.1

Fix a string $x \in \{0,1\}^n$ and consider the corresponding n-qubit basis state $|x\rangle = |x_1, \ldots, x_n\rangle$. Give a formula for the energy $\langle x| H |x\rangle$ in terms of the strings x and the parameter μ.

Solution:

Problem 3.2

Using the previous subproblem, deduce the spectral decomposition (i.e. find its eigenvectors and eigenvalues) of H, as a function of μ.

Solution:

Problem 3.3

Suppose $\mu = 0$. What is the minimum energy of H and what are the ground states of H? What is the maximum energy of H and what states achieve the maximum energy?

Solution:

Problem 3.4

Suppose $\mu = 1$. What is the ground energy and ground states of H? What about when $\mu = -1$?

Solution:

Problem 3.5

Give a qualitative description of what the ground states of H are, depending on μ. What happens as $\mu \to \infty$ or $\mu \to -\infty$? Are there "critical points" of μ where the behavior of the ground states seem to change?

Solution:

Problem 4: Quantum error correction

Problem 4.1: Going beyond 1 correctable error

In the next few subproblems we will improve Shor's code so that it can correct errors on more than 1 qubit.

Recall that Shor's code is comprised of a three-qubit bitflip code (which corrects up to one X error) and a three-qubit phaseflip code (which corrects up to one Z error).

First, generalize the three-qubit bitflip code to one where it can correct k bitflip errors. Choose an integer m, and write down m-qubit states $\left|\overline{0}\right\rangle, \left|\overline{1}\right\rangle$. Then argue that there do not exist two k-qubit bitflip errors E_0, E_1 such that

$$E_0 \left|\overline{0}\right\rangle = E_1 \left|\overline{1}\right\rangle \ .$$

In other words, by bit-flipping k qubits of either $\left|\overline{0}\right\rangle$ or $\left|\overline{1}\right\rangle$, it is always possible to tell which codeword you started from.

Solution:

Problem 4.2: Correction circuits

Describe a circuit for correcting any k bitflip errors: it should take in m input qubits, and output an m-qubit state (plus ancillas) that is a superposition of $\left|\overline{0}\right\rangle$ and $\left|\overline{1}\right\rangle$.

Your description can be in a Qiskit-like, high-level pseudocode. Note that you will need to introduce ancilla qubits to compute your syndromes; be sure to explain the role of each ancilla qubit and whether it gets reset back to zero at the end of the decoding circuit.

(Just describe the circuit for now; you will explain why this works in the next subproblem.)

Solution:

Suppose you measure the ancilla/syndrome qubits in the standard basis at the end of the correction circuit. What are all the possible measurement outcomes of the ancilla/syndrome qubits? Explain how there is a one-to-one mapping between the measurement outcomes and the set of possible k-qubit bitflip errors.

Solution:

Let $\left|\overline{\psi}\right\rangle = \alpha \left|\overline{0}\right\rangle + \beta \left|\overline{1}\right\rangle$ be a codeword and let $X^{\otimes S}$ denote bitflips on a subset $S \subseteq [m]$ of at most k qubits. Analyze the correction circuit when given $X^{\otimes S} \left|\overline{\psi}\right\rangle$ as input: show the relevant intermediate states, and show that the the circuit produces $\left|\overline{\psi}\right\rangle$ in the end.

Hint: You can analyze the how the circuit behaves on $\left|\overline{0}\right\rangle$ and $\left|\overline{1}\right\rangle$ and use linearity to conclude for the superposition $\left|\overline{\psi}\right\rangle = \alpha \left|\overline{0}\right\rangle + \beta \left|\overline{1}\right\rangle$. Watch out and make sure that the ancilla qubits don't entangle themselves with each branch of the superposition!

Solution:

Problem 4.3: Generalized phaseflip code

Now describe how you would adapt your generalization of the bitflip code to get a code that can correct k qubit *phaseflip* errors.

Write down what the $\left|\overline{0}\right\rangle$ and $\left|\overline{1}\right\rangle$ codewords are.

Solution:

Describe the correction circuit.

Solution:

Explain why your phaseflip code works.

Solution:

Problem 4.4: Putting everything together

Now combine your solutions to the generalized bitflip and generalized phaseflip codes to obtain a quantum error-correcting code that encodes 1 logical qubit, but can handle arbitrary k-qubit errors.

First, write down the codewords $\left|\overline{0}\right\rangle$ and $\left|\overline{1}\right\rangle$ that logical $|0\rangle, |1\rangle$ map to. How many physical qubits are used?

Solution:

Describe the correction circuit using your previous bitflip and phaseflip decoding circuits as subroutines. You should start and end with m^2 physical qubits.

Solution:

Explain why your code can correct *any* k-qubit error (not just bitflip or phaseflip).

Solution: