CMPT 476/981: Introduction to Quantum Algorithms
Assignment 5

Due **March 28th, 2024 at 11:59pm on coursys**
Complete individually and submit in PDF format.

Question 1 [7 points]: Coset states and Generalized Simon

Recall that the dot product on the vector space $\mathbb{Z}_2^n$ is defined as $x \cdot y = x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n$ where $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_2^n$. For any subspace S of $\mathbb{Z}_2^n$, define the orthogonal complement of S with respect to the dot product as

$$S^\perp = \{z \in \mathbb{Z}_2^n \mid s \cdot z = 0 \quad \forall s \in S\}.$$

1. Let $|x + S\rangle = \frac{1}{\sqrt{|S|}} \sum_{s \in S} |x + s\rangle$ and show that

$$H^{\otimes n}|x + S\rangle = \sqrt{\frac{|S|}{2^n}} \sum_{z \in S^\perp} (-1)^{x \cdot z} |z\rangle$$

   Hint: show that for any $z \in \mathbb{Z}_2^n$, either $z \in S^\perp$ (i.e. $z \cdot s = 0$ for all $s \in S$) or $z \cdot s = 0$ for exactly **half** the elements $s \in S$.

2. Show that Simon's algorithm can be generalized to solve the *Boolean hidden subgroup problem* **with no changes to the quantum part**. That is, given a linear subspace S of $\mathbb{Z}_2^n$ and $f(x) = f(y)$ if and only if $x = y \oplus s$ for some $s \in S$, generalize Simon's algorithm to find a **basis** for S. You should sketch an algorithm in pseudo-code.

Question 2 [3 points]: Factoring, classically

In this question we will factor the number 21 classically. You do not have to show your calculations and you may find it useful to use a calculator or program to calculate the GCD. If it were me, I would probably write a program to do it.

1. Compute the period of $f(x) = 5^x \mod 21$ — that is, find the smallest integer r such that $5^r \equiv 1 \mod 21$.

2. Compute $GCD(5^{r/2} + 1, 21)$, $GCD(5^{r/2} - 1, 21)$. What's the problem?

3. Now repeat steps 1 and 2 with $f(x) = 2^x \mod 21$ to factor 21 into its prime factors.

Question 3 [3 points]: QFT or QFT^{-1}?

In lectures and in the notes we've been pretty cavalier about whether we use QFT or the $QFT^{-1} = QFT^\dagger$ in period finding and phase estimation. In this question we'll investigate why.

1. Determine what transformation is applied by $QFT_{2^n}^2$ — that is, compute $QFT_{2^n}(QFT_{2^n}|x\rangle)$ where $x \in \{0,1\}^n$.

2. Now suppose you accidentally applied QFT when you should have applied QFT^{-1} and measured the result to get a bit string $y \in \{0,1\}^n$. How could you **classically** recover from y the "correct" bit string $z \in \{0,1\}^n$ which you would have measured if you had instead applied QFT^{-1}?

Question 4 [7 points]: Qutrit quantum computing

Much of quantum computation can be generalized to higher-dimensional **qudits**. Most gates we've seen have higher-dimensional generalizations, like the **Pauli gates** X, Y, Z and the Hadamard or **Fourier** gate H. In this question we will explore this notion briefly.

Consider a **qutrit**, which is a 3-dimensional quantum state — i.e. a unit vector in $\mathbb{C}^3$. As discussed in class, we denote the computational basis of $\mathbb{C}^3$ as $\{|0\rangle, |1\rangle, |2\rangle\}$, or $|x\rangle$ where $x \in \mathbb{Z}_3$, the integers mod 3. Denote the primitive third root of unity as $\omega_3 = e^{2\pi i/3}$. The Pauli X and Z operators on a qutrit can now be defined as

$$X = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega_3 & 0 \\ 0 & 0 & \omega_3^2 \end{bmatrix}$$

Likewise, the qutrit Hadamard gate can be defined as

$$H = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \omega_3^2 \\ 1 & \omega_3^2 & \omega_3 \end{bmatrix}$$

1. Show that X and Z have order 3 (i.e. $X^3 = Z^3 = I$)

2. Show that $XZ = \omega_3^2 ZX$. Use this to calculate k (as a function of i and j) such that $X^i Z^j = \omega^k Z^j X^i$ for $i, j \in \{0,1,2\}$.

3. Show that $H^\dagger Z H = X$.

4. Compute the eigenvalues of X and give corresponding (unit) eigenvectors. Hint: recall the relationship between H and the eigenvectors of X in the qubit case.

5. Now show that Deutsch's algorithm generalizes to *qutrits*. Explicitly, given a function $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ promised to either be **constant** or **balanced** where balanced in this case means for every $y \in \mathbb{Z}_3$, there exists exactly one $x \in \mathbb{Z}_3$ such that $f(x) = y$, show that Deutsch's algorithm with the qutrit version of the H gate works the same way.

   Hint: you may want to use the fact that over qutrits, $H = QFT_3$, i.e.

$$H|x\rangle = \frac{1}{\sqrt{3}} \sum_{z \in \mathbb{Z}_3} \omega_3^{xz} |z\rangle.$$

Question 5 [2 points]: Eigenvalues of Hermitian operators

Recall that a **Hermitian** operator is an operator H such that $H = H^\dagger$. Prove that the eigenvalues of H — and hence the *energies* of a Hamiltonian $\hat{H}$ — are real numbers (i.e. have no imaginary part).

Question 6 [4 points]: A quantum algorithm for SAT?

Given a formula in propositional logic φ — that is, a logical formula over Boolean variables, constants, $\vee$, $\wedge$, $\implies$, and $\neg$ — the SAT problem is to determine whether there exists a satisfying assignment to the variables in φ. That is, when viewed as a function from the values of its n variables to $\{0,1\}$, there exists some $x_1, \ldots, x_n \in \{0,1\}$ such that $\varphi(x_1, \ldots, x_n) = 1$.

In this question we're going to investigate whether or not the type of interference we've seen so far suffices (at least, in an obvious way) to give an efficient quantum algorithm for SAT.

1. Consider the superposition

$$\sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}} (-1)^{y(1 \oplus \varphi(x))} |x\rangle.$$

   Show that the amplitude of a computational basis state $|x\rangle$ in the above is non-zero if and only if $\varphi(x) = 1$.

2. Can the transformation

$$|00\cdots0\rangle \mapsto \frac{1}{2\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}} (-1)^{y(1 \oplus \varphi(x))} |x\rangle$$

   be implemented using unitary operations? Stated more simply, is the state on the right hand side a unit vector for every φ?

3. Now consider the transformation

$$|00\cdots0\rangle \mapsto \frac{1}{2\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}} (-1)^{y(1 \oplus \varphi(x))} |x\rangle|y\rangle.$$

   This transformation is indeed unitary, but we no longer get useful interference as in part 1. Explain why.

4. Is it likely that we'll easily discover an efficient quantum algorithm for SAT knowing that an efficient algorithm for SAT would allow us to solve **any** problem in NP efficiently?

Aside: In general, given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, the phase difference $(-1)^{yf(x)}$ acts like a *filter* when the paths $y = 0$ and $y = 1$ are allowed to interfere, filtering out the unwanted values of x where $f(x) = 1$. Part of my research involves the use and generalization of interference patterns like this to allow (classical) computers to symbolically reason about quantum circuits and algorithms. One fun thing that this leads to is the classical simulation of quantum circuits via Gröbner bases and algebraic varieties, though this is not likely to be very efficient in most cases.