量子計算的數學基礎 MA5501

Homework Assignment 2

Due Apr. 12. 2023

Problem 1. Grover's algorithm can be tweaked to work with probability 1 if we know the number of solutions exactly. Let $n \in \mathbb{N}$, $N = 2^n$, and $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function. Suppose that there is exactly one $x \in \{0,1\}^n$ satisfying $f(x) = 1$ (thus the Hamming weight $t = 1$).

1. Define a new function $g : \{0,1\}^{n+1} \to \{0,1\}$ by

   $$g(j_1 \cdots j_n j_{n+1}) = \begin{cases} 1 & \text{if } f(j_1 j_2 \cdots j_n) = 1 \text{ and } j_{n+1} = 0; \\ 0 & \text{otherwise.} \end{cases}$$

   Show how you can implement the following $(n+1)$-qubit unitary

   $$S_g : |a\rangle \mapsto (-1)^{g(a)} |a\rangle$$

   based on the implementation of U_f satisfying

   $$U_f : |a\rangle|b\rangle \mapsto |a\rangle|b \oplus f(a)\rangle \qquad \forall\, a \in \{0,1\}^n, b \in \{0,1\}\,.$$

2. Let $\gamma \in [0, 2\pi)$ and let U_γ be a 1-qubit rotation gate with matrix representation $\begin{bmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{bmatrix}$. Let $\mathcal{A} = \mathrm{H}^{\otimes n} \otimes U_\gamma$ be an $(n+1)$-qubit unitary. What is the probability (as a function of γ) that measuring the state $\mathcal{A}|0^{n+1}\rangle$ in the computational basis gives a solution $j \in \{0,1\}^{n+1}$ for g (that is, such that $g(j) = 1$)?

3. Give a quantum algorithm that finds the unique solution with probability 1 using $\mathcal{O}(\sqrt{N})$ queries to f.

Problem 2. Let $n \in \mathbb{N}$, $N = 2^n$, $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and t is the Hamming weight of f; that is, $t = \#\{x \in \{0,1\}^n \,|\, f(x) = 1\}$. Suppose that we know that $t \in \{1, 2, \cdots, s\}$ for some known $s \ll N$. Give a quantum algorithm that finds a solution with probability 1, using $\mathcal{O}(\sqrt{sN})$ queries to f.

Problem 3. Suppose $a \in \mathbb{R}^N$ is a vector (indexed by $\ell = 0, 1, \cdots, N-1$) which is r-periodic in the following sense: there exists an integer r such that $a_\ell = 1$ whenever ℓ is an integer multiple of r, and $a_\ell = 0$ otherwise. Compute the Fourier transform $F_N|a\rangle$ of this vector; that is, write down a formula for the entries of the vector $F_N|a\rangle$. Assuming r divides N, write down a simple closed form for the formula for the entries. Assuming also $r \ll N$, what are the entries with largest magnitude in the vector $F_N|a\rangle$?

Problem 4. The process of RSA encryption and decryption consists of the following 4 steps:

Step 1: Key generation: Choose prime numbers p and q, compute $n = pq$ and $\varphi(n) = (p-1)(q-1)$.

Step 2: Key distribution: Choose $1 < e < \varphi(n)$ so that $\gcd(e, \varphi(n)) = 1$. Compute $d \equiv e^{-1} \bmod \varphi(n)$ (using extended Euclid's algorithm). Provide (n, e) to public, and keep d privately.

Step 3: Encryption: To encode an message $m < n$, we compute $c \equiv m^e \mod n$.

Step 4: Decryption: To decode the encrypted message c, we raise c to power d and recover m since $m = c^d \mod n$.

In class I only prove that $c^d \equiv m \mod n$ as long as $\gcd(m, n) = 1$. Complete the following in order to show that $c^d = m \mod n$ for $m \in \{1, \cdots, n-1\}$ and $\gcd(m, n) = p$.

1. Show that $c^d \equiv m \mod p$.

2. Show that $c^d \equiv m \mod q$.

3. Show that $c^d \equiv m \mod n$.

Hint of 2: Since $\gcd(m, n) = p$ and $1 < m < n$, $m = pk_1$ for some $k_1 \in \{1, 2, \cdots, q-1\}$. Moreover, $ed = 1 + k_2\varphi(n) = 1 + k_2(p-1)(q-1) = 1 + k_3(q-1)$. Making use of these two facts to conclude that $c^d \equiv m \mod q$.