量子計算的數學基礎 MA5501

Homework Assignment 3

Due May. 15. 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 $\mathrm{R}_y(2\gamma)$ be the reflection about y-axis with angle 2γ so that $\mathrm{R}_y(2\gamma)$ has the matrix representation $\begin{bmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{bmatrix}$. Let $\mathcal{A} = \mathrm{H}^{\otimes n} \otimes \mathrm{R}_y(2\gamma)$ 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, $t = \#\big\{x \in \{0,1\}^n \,\big|\, f(x) = 1\big\}$. 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. In this problem we talked about modified Grover algorithm for unknown cardinality of $f^{-1}(\{1\})$, where $f : \{0,1\}^n \to \{0,1\}$ is the function for which we look for objects whose function value is 1. We assume that $S = f^{-1}(\{1\})$ is non-empty and $t \equiv \#S \ll N$ (in fact, it requires that $t \leqslant \frac{3}{4}N$ for the following quantum algorithm to work). Let $J = \lfloor \sqrt{N} \rfloor + 1$. Randomly select $j \in \{0, 1, \cdots, J-1\}$ with equal probability $1/J$. Apply j-times the Grover iterate $\mathcal{G} = \mathrm{H}^{\otimes n}\mathrm{R}\mathrm{H}^{\otimes n} U_{f,\pm}$ to $|\psi_0\rangle$ to transform the state $|\psi_0\rangle$ to the state

$$|\psi_j\rangle = \mathcal{G}^j |\psi_0\rangle\,.$$

Here R is the reflection about zero state, and U_f is the $(n+1)$-qubit oracle satisfying

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle\,, \qquad \forall\, x \in \{0,1\}^n, y \in \{0,1\}\,.$$

Measure the final quantum state and obtain $x \in \{0,1\}^n$.

1. Show that the probability of obtaining $x \in S$ is not less than $\frac{1}{4}$.

2. Figure out an algorithm for general that gives an $x \in S$ with probability not less than $\frac{1}{4}$ if t is not necessary satisfying $t \leqslant \frac{3}{4}N$.

Hint of 1: Let $\sin^2\theta = \frac{t}{N}$. Then (show that) $\frac{1}{\sin 2\theta} \leqslant J$ and then apply the result in Problem 5 of the midterm exam.

Problem 4. In this problem you are asked to provide matlab® codes for the last step in the Shor algorithm. Let $N \in \mathbb{N}$ be a (large) number taking the form $N = pq$, where p, q are prime numbers, and $L \in \mathbb{N}$ satisfy $N^2 < 2^L \leqslant 2N^2$. Let $x \in \mathbb{Z}_N^*$ be given (so you also have the function $f(a) = x^a \mod N$). Suppose that the quantum part of the Shor algorithm provides $b \in \{0,1\}^L$ upon measurement (so b is also given). Write a program to produces irreducible fractions $\frac{n}{m}$ satisfying

$$\left|\frac{b}{2^L} - \frac{n}{m}\right| < \frac{1}{2m^2} \qquad \text{and} \qquad m < 2^{L/2}$$

and check whether the denominator of these irreducible fractions are the period of the function $f(a) = x^a \mod N$ (for given x).

Problem 5. Let $\mathbb{V}$ be the vector space spanned by three monomials 1, x and x^2, and let $\langle \cdot, \cdot \rangle : \mathbb{V} \times \mathbb{V} \to \mathbb{R}$ be an inner product on $\mathbb{V}$ given by

$$\langle f, g \rangle = \int_{-1}^{1} f(x)g(x)\,dx\,.$$

1. Use the Gram-Schmidt process to find an orthonormal basis of $\mathbb{V}$.

2. Let $L : \mathbb{V} \to \mathbb{R}$ be defined by

$$L(p) = p'(0)\,,$$

   where p' is the derivative of p. Show that $L \in \mathbb{V}^*$.

3. Find $q \in \mathbb{V}$ satisfying $L(p) = \langle q, p \rangle$ for all $p \in \mathbb{V}$.

Problem 6. For matrices $A = [a_{k\ell}]$ and $B = [b_{k\ell}]$ of the same size $m \times n$, define the Hadamard product of A and B, denoted by $A \odot B$, as an $m \times n$ matrix whose (k, ℓ)-entry is give by $a_{k\ell}b_{k\ell}$; that is,

$$C = A \odot B\,, \quad C = [c_{k\ell}]\,, \quad c_{k\ell} = a_{k\ell}b_{k\ell}\,. \tag{0.1}$$

In matlab®, the Hadamard product of A and B can be computed by $A \odot B = A .* B$. **In the following, we will always use $.*$ to denote the Hadamard product.**

Let H_n be the **unnormalized** Hadamard matrix whose (k, ℓ)-entry is given by $(-1)^{(k-1)\bullet(\ell-1)}$, and $\boldsymbol{r}_j$ be the $(j+1)$-th row of H_n. Define $\varphi : \{0,1\}^n \to \{\boldsymbol{r}_0, \boldsymbol{r}_1, \cdots, \boldsymbol{r}_{2^n-1}\}$ by

$$\varphi(j_1, j_2, \cdots, j_n) = \boldsymbol{r}_j \quad \text{if } j = (j_1 j_2 \cdots j_n)_2\,.$$

For example, for the case $n = 2$ the map φ is given by

$$\varphi : \left\{ \begin{array}{lcl} (0,0) & \mapsto & \boldsymbol{r}_0 = \\ (0,1) & \mapsto & \boldsymbol{r}_1 = \\ (1,0) & \mapsto & \boldsymbol{r}_2 = \\ (1,1) & \mapsto & \boldsymbol{r}_3 = \end{array} \right. \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \equiv \mathrm{H}_2\,. \tag{$\star$}$$

Show that $\varphi : (\{0,1\}^n, \oplus) \to \big(\{\boldsymbol{r}_0, \boldsymbol{r}_1, \cdots, \boldsymbol{r}_{2^n-1}\},\ .*\ \big)$ is a group isomorphism, where $\oplus$ is the element-wise addition in $\mathbb{Z}_2$; that is,

$$(x_1, x_2, \cdots, x_n) \oplus (y_1, y_2, \cdots, y_n) = (x_1 \oplus y_1, x_2 \oplus y_2, \cdots, x_n \oplus y_n)\,.$$

In other words, show that $\varphi : \{0,1\}^n \to \{\boldsymbol{r}_0, \boldsymbol{r}_1, \cdots, \boldsymbol{r}_{2^n-1}\}$ defined above is a bijection and

$$\varphi\big((k_1, \cdots, k_n) \oplus (\ell_1, \cdots, \ell_n)\big) = \boldsymbol{r}_k \,.*\, \boldsymbol{r}_\ell \qquad \forall\, k = (k_1 k_2 \cdots k_n)_2 \text{ and } \ell = (\ell_1 \ell_2 \cdots \ell_n)_2\,. \tag{$\diamond$}$$

For example, in the example above $(\star)$ implies that

$$\varphi\big((0,1) \oplus (1,1)\big) = \varphi(1,0) = \boldsymbol{r}_2$$

while

$$\varphi(0,1).*\varphi(1,1) = \boldsymbol{r}_1.*\boldsymbol{r}_3 = \begin{bmatrix}1 & -1 & 1 & -1\end{bmatrix}.*\begin{bmatrix}1 & -1 & -1 & 1\end{bmatrix} = \begin{bmatrix}1 & 1 & -1 & -1\end{bmatrix} = \boldsymbol{r}_2$$

so that $\varphi\big((0,1) \oplus (1,1)\big) = \varphi(0,1).*\varphi(1,1)$.