Quantum Computing (CS5100) : Problem Set 3

Department of Computer Science and Engineering
IIT Hyderabad

Deadline: Nov. 25, 2024 before 17:00PM

Please read the following comments before you work on the problems.

- Plagiarism leads to **F** grade and a meeting with disciplinary committee!
- Assignments after the deadline will not be accepted at any cost. So plan for your internet outages etc. beforehand. You may submit a hard copy as well. There won't be any extension.
- All problems builds on what has been taught in the class. Try to attempt them all.
- Please mention in case you collaborate with other students or look up a source (other than the class notes or materials mentioned on the course webpage). If you don't acknowledge and get caught, you will be severely penalised.

---

1. The *total variation distance* between two probability distributions P and Q on the same set $\mathcal{A}$, is defined as $d_{TV}(P,Q) = 1/2 \sum_{i\in\mathcal{A}} |P(i) - Q(i)|$. An equivalent alternative way to define this: $d_{TV}(P,Q)$ is the maximum, over all events $E \subseteq \mathcal{A}$, of $|P(E) - Q(E)|$. Hence $d_{TV}(P,Q)$ is small iff all events have roughly the same probability under P and under Q.

   The *Euclidean distance* between two states $|\phi\rangle = \sum_i \alpha_i |i\rangle$ and $|\psi\rangle = \sum_i \beta_i |i\rangle$ is defined as $\||\phi\rangle - |\psi\rangle\| = \sqrt{\sum_i |\alpha_i - \beta_i|^2}$. Assume the two states are unit vectors. Suppose the Euclidean distance is small: $\||\phi\rangle - |\psi\rangle\| = \varepsilon$. If we measure $|\phi\rangle$ in the computational basis then the probability distribution over the outcomes is given by the $|\alpha_i|^2$, and if we measure $|\psi\rangle$ then the probabilities are $|\beta_i|^2$. Show that these distributions are close in total variation distance, i.e., $1/2 \sum_i ||\alpha_i|^2 - |\beta_i|^2|$ is $\leq \varepsilon$. **(6 marks)**

2. Suppose $a \in \mathbb{R}^N$ is a vector (indexed by $\ell = 0, \ldots, N-1$) 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 $F_N a$ of this vector, i.e., write down a formula for the entries of the vector $F_N a$. Assuming r divides N, write down a simple closed form for the formula for the entries. Which are the nonzero entries in the vector $F_N a$, and what is their magnitude? **(5 marks)**

3. (a) The squared Fourier transform, F_N^2, turns out to map computational basis states to computational basis states. Describe this map, i.e., determine to which basis state a basis state $|k\rangle$ gets mapped for each $k \in \{0, 1, \ldots, N-1\}$. **(5 marks)**

   (b) Show that $F_N^4 = I$. What can you conclude about the eigenvalues of F_N? **(4 marks)**

4. Consider the task of constructing a quantum circuit to compute $|x\rangle \mapsto |x + y \bmod N\rangle$, where y is a fixed constant, and $0 \leq x < N$. Show that one efficient way to do this, for values of y such as 1, is to first perform a quantum Fourier transform, then to apply single qubit phase shifts, then an inverse Fourier transform. What values of y can be added easily this way, and how many operations are required? **(10 marks)**

5. Construct a quantum circuit that computes the Hamming weight of a given string $x \in \{0,1\}^n$. That is, it performs the following transformation: $|x\rangle|0\rangle \mapsto |x\rangle|hw(x)\rangle$, where $hw(x)$ is the Hamming weight of x. What is the size of your circuit? **(10 marks)**

6. In the lectures we claimed without proof that Grover's algorithm can be tweaked to work *with probability* 1 if we know the number of solutions exactly. For $N = 2^n$, this question asks you to provide such an exact algorithm for an $x \in \{0,1\}^n$ with a unique solution (so we are promised that there is exactly one $i \in \{0,1\}^n$ with $x_i = 1$, and our goal is to find this i).

   (a) Define a new $2N$-bit string $y \in \{0,1\}^{2N}$, indexed by $(n+1)$-bit strings $j = j_1 \ldots j_n j_{n+1}$, by setting

   $$y_j = \begin{cases} 1 & \text{if } x_{j_1 \cdots j_n} = 1 \text{ and } j_{n+1} = 0, \\ 0 & \text{otherwise.} \end{cases}$$

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

   $$S_y \colon |j\rangle \mapsto (-1)^{y_j}|j\rangle,$$

   using one query to x (of the usual form $O_x \colon |i, b\rangle \mapsto |i, b \oplus x_i\rangle$) and a few elementary gates. **(5 marks)**

   (b) Let $\gamma \in [0, 2\pi)$ and let $U_\gamma = \begin{pmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{pmatrix}$ be the corresponding rotation matrix. Let $\mathcal{A} = H^{\otimes n} \otimes U_\gamma$ 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 y (i.e., such that $y_j = 1$)? **(5 marks)**

   (c) Give a quantum algorithm that finds the unique solution in string x with probability 1 using $O(\sqrt{N})$ queries to x. **(10 marks)**

7. Let $N = 2^n$ and $x = x_0 \dots x_{N-1}$ be a sequence of distinct integers such that each x_i can be written exactly using b bits. We can query these in the usual way, i.e., we can apply $(n+b)$-qubit unitary $O_x\colon |i, 0^b\rangle \mapsto |i, x_i\rangle$, as well as its inverse. The *minimum* of x is defined as $\min\{x_i \mid 0 \le i \le N-1\}$. Give a quantum algorithm that finds (with probability $\ge 2/3$) an index acheiving the minimum, using at most $O(\sqrt{N}\log N)$ queries to the input. **(10 marks)**

8. Let $x = x_0 \dots x_{N-1}$, where $N = 2^n$ and $x_i \in \{0,1\}^n$, be an input that we can query in the usual way. We are promised that this input is 2-to-1: for each i there is exactly one other j such that $x_i = x_j$. Such an (i,j)-pair is called a *collision*. Give a quantum algorithm that finds a collision (with probability $\ge 2/3$) using $O(N^{1/3})$ queries. **(10 marks)**

9. Consider an undirected graph $G = (V, E)$, where $V = \{1, \dots, n\}$. Let M be the adjacency matrix of G. Suppose we are given input graph G in the form of a unitary that allows us to query whether an edge (i,j) is present in G or not:

$$O_M\colon |i, j, b\rangle \mapsto |i, j, b \oplus M_{ij}\rangle.$$

   (a) Assume G is connected. Suppose we have a set A of edges which we already know to be in the graph (so $A \subseteq E$; you can think of A as given classically, you don't have to query it). Let $G_A = (V, A)$ be the subgraph induced by only these edges , and suppose G_A is not connected, so it consists of $c > 1$ connected components. Call an edge $(i,j) \in E$ "good" if it connects two of these components. Give a quantum algorithm that finds a good edge with an expected number of $O(n/\sqrt{c-1})$ queries to M. **(10 marks)**

   (b) Give a quantum algorithm that uses at most $O(n^{3/2})$ queries to M and decides (with success probability $\ge 2/3$) whether G is connected or not. **(10 marks)**

10. Consider a 2-bit input $x = x_0x_1$ with phase-oracle $O_{x,\pm}\colon |i\rangle \mapsto (-1)^{x_i}|i\rangle$. Write out the final state of the following 1-query quantum algorithm: $HO_{x,\pm}H|0\rangle$. Give a degree 2-polynomial $p(x_0, x_1)$ that equals the probability that this algorithm outputs 1 on this input x. **(5 marks)**

11. Let $f\colon \{0,1\}^N \to \{0,1\}$ be the N-bit Parity function, which is 1 iff its input $x \in \{0,1\}^N$ has odd Hamming weight.

   (a) Give a quantum algorithm that computes Parity with success probability 1 on every input x, using $N/2$ queries (assume N is an even number). **(5 marks)**

   (b) Show that this is optimal, even for quantum algorithms that have error probability $\le 1/3$ on every input. **(10 marks)**

12. Suppose we have a T-query quantum algorithm that computes the N-bit OR function with success probability 1 on all inputs $x \in \{0,1\}^N$. Show that $T \ge N$. **(10 marks)**

13. For a partial function $f\colon \{0,1\}^N \to \{0,1,*\}$, let $Y \subseteq f^{-1}(1)$ and $Z \subseteq f^{-1}(0)$. Let $R \subseteq Y \times Z$ be a set of pairs and for each coordinate $j \in [N]$, define $R_j = \{(y,z) \in R \mid y_j \neq z_j\}$. Now suppose that

    - for each $y \in Y$, there are at least m_1 strings $z \in Z$ with $(y,z) \in R$;
    - for each $z \in Z$, there are at least m_0 strings $y \in Y$ with $(y,z) \in R$;
    - for each $y \in Y$ and $j \in [N]$, there are at most ℓ_1 strings $z \in Z$ with $(y,z) \in R_j$;
    - for each $z \in Z$ and $j \in [N]$, there are at most ℓ_0 strings $y \in Y$ with $(y,z) \in R_j$.

    Then show that $Q(f) \geq \Omega(\sqrt{m_0 m_1/\ell_0 \ell_1})$, where $Q(f)$ denotes the quantum query complexity of computing f with success probability at least $2/3$. **(10 marks)**

14. Show a quantum query lower bound of $\Omega(\sqrt{N/k})$ for computing the following partial function with error probability $\leq 1/3$: output 1 if the input string $x \in \{0,1\}^N$ has at least k 1's; output 0 if $x = 0^N$. Be explicit about what relations R, R_j you are using, and about the values of the parameters m_0, m_1, ℓ_0, ℓ_1. **(4 marks)**

15. Let k be an odd natural number and $N = k^2$. Define $f\colon \{0,1\}^N \to \{0,1\}$ such that $f(x) = \mathsf{Maj}_k(\mathsf{OR}_k(x^{(1)}), \ldots, \mathsf{OR}_k(x^{(k)}))$ where $x = x^{(1)} \ldots x^{(k)}$ with each $x^{(i)} \in \{0,1\}^k$, Maj_k is the k-bit majority function and OR_k is the k-bit OR function. Show that $Q(f) = \Omega(N^{3/4})$. Be explicit about what relations R, R_j you are using, and about the values of the parameters m_0, m_1, ℓ_0, ℓ_1. **(6 marks)**