Introduction to Quantum Computing
Fall 2024, Peking University

Due: 1 pm on Wednesday, October 23
Submit by sending to: PKU.Quantum-Computing@outlook.com

Assignment 2

1 Qubit rotations and the Hadamard gate

1) Suppose that $(n_x, n_y, n_z) \in \mathbb{R}^3$ is a unit vector and $\theta \in \mathbb{R}$. Show that
$$e^{-i\frac{\theta}{2}(n_x X + n_y Y + n_z Z)} = \cos(\theta/2)I - i\sin(\theta/2)(n_x X + n_y Y + n_z Z).$$

2) Find a unit vector $(n_x, n_y, n_z) \in \mathbb{R}^3$ and numbers $\phi, \theta \in \mathbb{R}$ such that
$$H = e^{i\phi} e^{-i\frac{\theta}{2}(n_x X + n_y Y + n_z Z)},$$
where H denotes the Hadamard gate. What does this mean in terms of the Bloch sphere?

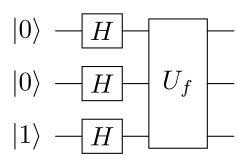
3) Write the Hadamard gate as a product of rotations about the x and y axes. In particular, find $\alpha, \beta, \gamma, \phi \in \mathbb{R}$ such that $H = e^{i\phi} R_y(\gamma) R_x(\beta) R_y(\alpha)$.

2 One-out-of-four search

Let $f\colon \{0,1\}^2 \to \{0,1\}$ be a black-box function taking the value 1 on exactly one of the four inputs. The goal of the one-out-of-four search problem is to find the unique $(x_1, x_2) \in \{0,1\}^2$ such that $f(x_1, x_2) = 1$.

1) How many classical queries are needed to solve one-out-of-four search?

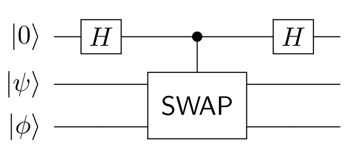
2) Suppose f is given as a quantum black box U_f acting as
$$|x_1, x_2, y\rangle \xmapsto{U_f} |x_1, x_2, y \oplus f(x_1, x_2)\rangle.$$
Determine the output of the following quantum circuit for each possible black-box function f:



3) Show that the four possible outputs obtained in the previous part are pairwise orthogonal. What can you conclude about the quantum query complexity of one-out-of-four search?

3 Swap test

1) Let $|\psi\rangle$ and $|\phi\rangle$ be arbitrary single-qubit states (not necessarily computational basis states), and let SWAP denote the 2-qubit gate that swaps its input qubits (i.e., $\mathsf{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$ for any $x, y \in \{0,1\}$). Compute the output of the following quantum circuit:



2) Suppose the top qubit in the above circuit is measured in the computational basis. What is the probability that the measurement result is 0?

3) If the result of measuring the top qubit in the computational basis is 0, what is the (normalized) post-measurement state of the remaining two qubits?

4) How do the results of the previous parts change if $|\psi\rangle$ and $|\phi\rangle$ are n-qubit states, and SWAP denotes the $2n$-qubit gate that swaps the first n qubits with the last n qubits?

4 The Bernstein-Vazirani problem

1) Suppose $f\colon \{0,1\}^n \to \{0,1\}$ is a function of the form

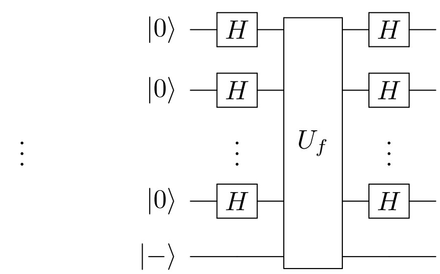
$$f(x) \equiv x_1 s_1 + x_2 s_2 + \cdots + x_n s_n \mod 2$$

for some $s \in \{0,1\}^n$. Given a black box for f, how many classical queries are required to learn s with certainty?

2) Prove that for any n-bit string $u \in \{0,1\}^n$,

$$\sum_{v \in \{0,1\}^n} (-1)^{u \cdot v} = \begin{cases} 2^n & \text{if } u = 00\cdots 0 \\ 0 & \text{otherwise} \end{cases}.$$

3) Let U_f denote a quantum black box for f, acting as $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ for any $x \in \{0,1\}^n$ and $y \in \{0,1\}$. Show that the output of the following circuit is the state $|s\rangle|-\rangle$.



4) What can you conclude about the quantum query complexity of learning s?

5 A fast approximate QFT

In class, we stated that the QFT uses $O(n^2)$ gates. Here we consider a fast approximate version of QFT.

1) Let $\mathsf{c}R_k$ denote the controlled-R_k gate, with $\mathsf{c}R_k|x,y\rangle = e^{2\pi i x y/2^k}|x,y\rangle$ for $x,y \in \{0,1\}$. Show that

$$E(\mathsf{c}R_k, I) \le 2\pi/2^k,$$

where I denotes the 4×4 identity matrix, and recall $E(U,V) = \max_{|\psi\rangle} \|U|\psi\rangle - V|\psi\rangle\|$.

2) Let F denote the exact QFT on n qubits. Suppose that for some constant c, we delete all the controlled-R_k gates with $k > \log_2 n + c$ from the QFT circuit, giving a circuit for another unitary operation, $\tilde{F}$. Show that $E(F,\tilde{F}) \le \epsilon$ for some ϵ that is independent of n, where ϵ can be made arbitrarily small by choosing c arbitrarily large.

3) For a fixed c, how many gates are used by the circuit implementing $\tilde{F}$? It is sufficient to give your answer using the big-O notation.