

Assignment 3

Due: 11:59pm, October 19, 2026

1. Action of unitary operations on the Bloch sphere [12 points].

It turns out that, for every 2×2 unitary matrix U , the effect of applying U on a qubit can be viewed as a rotation of the states in the Bloch sphere. For example, it can be shown that

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

corresponds to rotation by angle 2θ along the axis specified by states $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$. In each case below, determine the axis of rotation as well as the angle of rotation (each of which can depend on the parameter θ):

(a) $\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$

(b) $\begin{pmatrix} \cos \theta & i \sin \theta \\ i \sin \theta & \cos \theta \end{pmatrix}$

(c) $\begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}.$

- 2. Function $f : \{00, 01, 10\} \rightarrow \{0, 1\}$ with an even number of 1s [12 points].** Suppose that you are given a black-box that computes a function $f : \{00, 01, 10\} \rightarrow \{0, 1\}$ such that the number of inputs where the function takes the value 1 is *even*. The function takes two bits as input and if it is queried at the “out of range” point 11 then it takes the value 0. In summary, there are four possible functions with this property:

x	$f_{000}(x)$
00	0
01	0
10	0
11	0

x	$f_{110}(x)$
00	1
01	1
10	0
11	0

x	$f_{101}(x)$
00	1
01	0
10	1
11	0

x	$f_{011}(x)$
00	0
01	1
10	1
11	0

Your goal is to determine which of the four functions your black-box is, where you are allowed to query f at any point in $\{00, 01, 10, 11\}$.

- How many classical queries are there needed for this problem? Justify your answer.
- Give a quantum algorithm that solves this problem making one query to the function and explain why it works.

3. **Modulo 3 version of constant vs. balanced [12 points]**. Let $f : (\mathbb{Z}_3)^n \rightarrow \mathbb{Z}$ have the property that, *either* f is “constant” (meaning that there exists an $c \in \mathbb{Z}_3$ such that, for all $a \in (\mathbb{Z}_3)^n$, it holds that $f(a) = c$), *or* f is “balanced,” in the sense that it takes on all three values in an equal number of places. In other words, balanced means:

$$|\{a \in (\mathbb{Z}_3)^n : f(a) = 0\}| = |\{a \in (\mathbb{Z}_3)^n : f(a) = 1\}| = |\{a \in (\mathbb{Z}_3)^n : f(a) = 2\}| = 3^{n-1}.$$

You are promised that f is either constant or balanced and your goal is to distinguish between the two cases.

- (a) [4 points] Explain the number of classical f -queries necessary for this problem.
- (b) [8] A quantum f -query is the unitary operation U_f acting on $n+1$ qutrits such that, for all $a \in (\mathbb{Z}_3)^n$ and $b \in \mathbb{Z}_3$, $U_f|a_1, \dots, a_n\rangle|b\rangle = |a_1, \dots, a_n\rangle|b+f(a_1, \dots, a_n) \bmod 3\rangle$.

Give a quantum algorithm that solves this problem making one f -query and explain in detail why it works. You may assume that, in addition to an f -query gate, the algorithm can apply Fourier transform gates, F_3 , inverse Fourier transform gates, F_3^* , and measurements in the computational basis.

4. **Generalized form of period-finding by quantum algorithms [12 points]**. Let $\sigma : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a bijection (i.e., a one-to-one and onto function on the set $\{0, 1\}^n$). Let $z \in \{0, 1\}^n$. Then the sequence of iterates of σ , starting with z , which is

$$z, \sigma(z), \sigma(\sigma(z)), \sigma(\sigma(\sigma(z))), \dots = \sigma^{(0)}(z), \sigma^{(1)}(z), \sigma^{(2)}(z), \sigma^{(3)}(z), \dots$$

eventually comes back to z .

Define $\text{size}(z)$ as the *size of the cycle of iterates of σ starting at z* . In other words, $\text{size}(z)$ is the minimum $r > 0$ such that $\sigma^{(r)}(z) = z$.

Define the n -qubit unitary operation U as $U|x\rangle = |\sigma(x)\rangle$, for all $x \in \{0, 1\}^n$.

Suppose that we are given a black box implementation of the unitary operation

$$V_\sigma : |x\rangle|y\rangle \mapsto |x\rangle|\sigma^{(x)}(y)\rangle$$

for all $x, y \in \{0, 1\}^n \equiv \{0, 1, 2, \dots, 2^n - 1\}$. (Note that $V_\sigma(|x\rangle|y\rangle) = |x\rangle U^x|y\rangle$.)

Our goal is to determine $r = \text{size}(z)$, where we are promised that $r \leq 2^{n/2}$, but otherwise r is unknown to us.

Let $\omega = e^{2\pi i/r}$, and $|\phi\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \omega^{-s} |\sigma^{(s)}(z)\rangle$.

- (a) Show that $U|\phi\rangle = \omega|\phi\rangle$.
- (b) Show that $V_\sigma\left(\sum_{x=0}^{2^n-1} |x\rangle|\phi\rangle\right) = \left(\sum_{x=0}^{2^n-1} \omega^x |x\rangle\right)|\phi\rangle$.

CONTINUED ON NEXT PAGE

- (c) Show that there is a quantum circuit that, given the additional help of one copy of the state $|\phi\rangle$, determines r with success probability $\geq 1/4$, making one single query to the black box for V_σ , plus an additional number of 1- and 2-qubits gates that is polynomial in n .

(Note: r can also be determined with a constant number of queries to the black box *without* being provided with the special quantum state $|\phi\rangle$; however, you are not asked to show this here.)

5. **(This is an optional challenge question)**

Function $f : \{00, 01, 10\} \rightarrow \{0, 1\}$ with an even number of 1s revisited [0 points].

As in question 2, you are given a black-box computing a function $f : \{00, 01, 10\} \rightarrow \{0, 1\}$ such that the number of inputs where the function has value 1 is even. However, now the value at the “out of range” point 11 is *arbitrary*. Now there are these four possibilities

x	$f_{000}(x)$
00	0
01	0
10	0
11	*

x	$f_{110}(x)$
00	1
01	1
10	0
11	*

x	$f_{101}(x)$
00	1
01	0
10	1
11	*

x	$f_{011}(x)$
00	0
01	1
10	1
11	*

where * means that the bit could be *either* 0 *or* 1 *and you don't know which it is*. Is there a quantum algorithm that solves *this* version of the problem (determining which of the four cases) with one single query? If your answer is yes then you must give the quantum algorithm. If your answer is no then you must prove that there is no one-query quantum algorithm.

There is a solution that can be explained in less than one page. If you submit a solution to this question, then please do not exceed two pages.