# Foundations of Quantum Computing: Assignment 2

Candidate number: 300521

03/03/2025

## Problem 1 - Week 2

Consider the operator:

$$H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix} \tag{1}$$

1. Provide a simple algebraic argument (for example, from a matrix computation) that H is a reflection of the 2D plane.
2. Provide a simple geometric argument (for example, referring to angles between lines in a 2D diagram) to determine the angle made by the axis of reflection, relative to the $|\,0\rangle$ axis. (Hint: what angle does $H\,|\,0\rangle$ make with $|\,0\rangle$?)
3. Use the above to identify the eigenvalues and orthogonal unit eigenvectors of H.
4. Use the above to describe an eigendecomposition of H.

**Solution:** Consider the operator

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}.$$

### 1. Algebraic Argument: Showing $H$ is a Reflection

A reflection matrix H in $\mathbb{R}^2$ satisfies the following algebraic properties:

- **Unitary:** $H^\dagger H = I$.
- **Hermitian:** $H^\dagger = H$.
- **Self-inverse:** $H^2 = I$.

- **Eigenvalues:** $\pm 1$.

The simplest one it is:

$$H^2 = I.$$

So if we compute:

$$H^2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}.$$

The $(1,1)$ entry is

$$\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} = \frac{1}{2} + \frac{1}{2} = 1.$$

The $(1,2)$ entry is

$$\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot \left(-\frac{1}{\sqrt{2}}\right) = \frac{1}{2} - \frac{1}{2} = 0.$$

Similarly, the $(2,1)$ entry is 0 and the $(2,2)$ entry is 1. Therefore,

$$H^2 = I,$$

confirming that $H$ is an involution, hence a reflection operator.

## 2. Geometric Argument: Determining the Reflection Axis

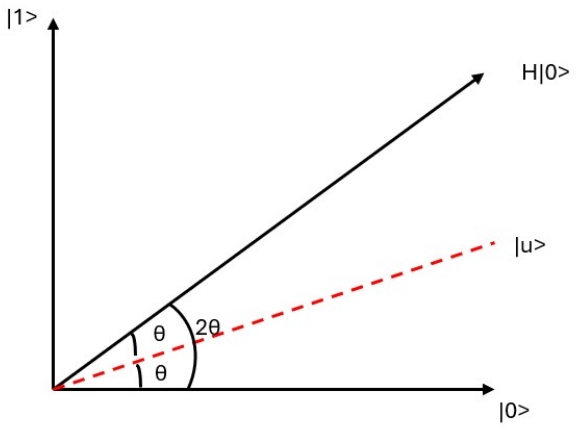


Figure 1: The effect of reflecting $|0\rangle$ over the axis of reflection $|u\rangle$

A reflection leaves vectors along its axis unchanged (eigenvalue $+1$) and flips the sign of vectors perpendicular to it (eigenvalue $-1$). Consider the state

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Then,

$$H\,|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}.$$

This vector makes an angle:

$$\theta' = \tan^{-1}\left( \frac{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}} \right) = \tan^{-1}(1) = 45^\circ$$

with the $x$-axis. In a reflection, the angle between $|0\rangle$ and the reflection axis is half of the angle between $|0\rangle$ and its image, as shown in Figure 1. Hence, if $\theta$ is the angle between the reflection axis and the $x$-axis,

$$2\theta = 45^\circ \quad \Longrightarrow \quad \theta = 22.5^\circ.$$

Thus, the reflection axis makes an angle of $22.5^\circ$ with the $|0\rangle$ (or $x$) axis.

## 3. Eigenvalues and Orthogonal Unit Eigenvectors

To find the eigenvalues, we solve

$$\det(H - \lambda I) \;=\; 0.$$

That is,

$$H - \lambda I \;=\; \begin{bmatrix} \frac{1}{\sqrt{2}} - \lambda & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} - \lambda \end{bmatrix}.$$

The determinant is

$$\det \begin{pmatrix} \frac{1}{\sqrt{2}} - \lambda & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} - \lambda \end{pmatrix} \;=\; \left(\tfrac{1}{\sqrt{2}} - \lambda\right)\left(-\tfrac{1}{\sqrt{2}} - \lambda\right) \;-\; \left(\tfrac{1}{\sqrt{2}}\right)\left(\tfrac{1}{\sqrt{2}}\right) = 0.$$

Expanding carefully,

$$-\tfrac{1}{2} + \lambda^2 = \tfrac{1}{2},$$

$$\lambda^2 = 1$$

Thus the characteristic equation is

$$\lambda^2 - 1 \;=\; 0 \;\Longrightarrow\; \lambda = \pm 1.$$

Hence the eigenvalues of $H$ are

$$\boxed{\lambda_1 = +1, \quad \lambda_2 = -1.}$$

Now lets find the eigenvectors:

**Eigenvector for $\lambda = +1$**

We solve

$$(H - I)|v\rangle = 0 \quad \Longrightarrow \quad \begin{bmatrix} \frac{1}{\sqrt{2}} - 1 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} - 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Focusing on the first row, we have:

$$\left(\frac{1}{\sqrt{2}} - 1\right) x + \frac{1}{\sqrt{2}}\, y = 0.$$

Rearrange to obtain:

$$\frac{1}{\sqrt{2}}\, y = \left(1 - \frac{1}{\sqrt{2}}\right) x,$$

so that

$$y = \sqrt{2}\left(1 - \frac{1}{\sqrt{2}}\right) x = (\sqrt{2} - 1)x.$$

Thus an unnormalized eigenvector is

$$|v_{+1}\rangle \propto \begin{pmatrix} 1 \\ \sqrt{2} - 1 \end{pmatrix}.$$

Notice that

$$\tan\theta = \sqrt{2} - 1 \quad \Longrightarrow \quad \theta = 22.5^\circ,$$

so we can also express the normalized eigenvector as

$$|v_{+1}\rangle = \begin{pmatrix} \cos 22.5^\circ \\ \sin 22.5^\circ \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2+\sqrt{2}}}{2} \\ \frac{\sqrt{2-\sqrt{2}}}{2} \end{pmatrix}.$$

## Eigenvector for $\lambda = -1$

Next, we solve

$$(H + I)|w\rangle = 0 \quad \Longrightarrow \quad \begin{bmatrix} \frac{1}{\sqrt{2}} + 1 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} + 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

From the first row,

$$\left(\frac{1}{\sqrt{2}} + 1\right) x + \frac{1}{\sqrt{2}}\, y = 0,$$

we rearrange:

$$\frac{1}{\sqrt{2}}\, y = -\left(\frac{1}{\sqrt{2}} + 1\right) x,$$

so that

$$y = -\sqrt{2}\left(\frac{1}{\sqrt{2}} + 1\right) x = -(1 + \sqrt{2})x.$$

Alternatively, note that since the eigenvector for $\lambda = +1$ is

$$|v_{+1}\rangle = \begin{pmatrix} \cos 22.5^\circ \\ \sin 22.5^\circ \end{pmatrix},$$

its orthogonal (and hence $-1$ eigenvector, up to a phase) is given by a rotation by 90°:

$$|v_{-1}\rangle = \begin{pmatrix} -\sin 22.5^\circ \\ \cos 22.5^\circ \end{pmatrix} = \begin{pmatrix} -\frac{\sqrt{2-\sqrt{2}}}{2} \\ \frac{\sqrt{2+\sqrt{2}}}{2} \end{pmatrix}.$$

This is consistent with the ratio obtained above because

$$\cot 22.5^\circ = \frac{1}{\tan 22.5^\circ} = \sqrt{2} + 1.$$

### 4. Eigendecomposition of $H$

The eigendecomposition of $H$ is written as

$$H = E\Lambda E^T,$$

where

$$E = \begin{bmatrix} \cos 22.5^\circ & -\sin 22.5^\circ \\ \sin 22.5^\circ & \cos 22.5^\circ \end{bmatrix}$$

is the orthogonal matrix whose columns are $|v_+\rangle$ and $|v_-\rangle$, and

$$\Lambda = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

is the diagonal matrix of eigenvalues. Equivalently, we can write:

$$H = |v_+\rangle\langle v_+| - |v_-\rangle\langle v_-|.$$

## Problem 2 - Week 3

Consider the operator SWAP $= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ discussed in the Week 3 Study materials.

1. What is the inverse operation for SWAP? From this, explain how you can infer that it has eigenvalues $\pm 1$. Hint: you can answer this by thinking of what it does to product states, or even computational basis states.

2. Write three independent product states which are +1-eigenvectors, in ket notation.

3. Suppose $|\psi\rangle = u_{00}|00\rangle + u_{01}|01\rangle + u_{10}|10\rangle + u_{11}|11\rangle$ is a -1-eigenvector of SWAP. Express $|\psi\rangle$ explicitly, as a unit vector in ket notation (and with at least one positive real-valued coefficient). Hint: what constraints does being a -1-eigenvector of SWAP impose on the coefficients?

4. Because SWAP has eigenvalues $\pm$ 1, it is also Hermitian, and can be treated as a measurement observable. If you were to perform a SWAP-measurement on the state $|\ 01\rangle$, what would be the probability of the outcome -1? What is the post-measurement state in this case?

5. Write a matrix for a three-qubit coherently controlled operation, CSWAP, in analogy to the operators C$U$ on two qubits. Then write a more-condensed algebraic representation for CSWAP, using projectors.

**Solution:**
We are given the operator

$$\text{SWAP} \;=\; \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

This operator swaps the two qubits:

$$\text{SWAP}\ |a\,b\rangle = |b\,a\rangle\,, \quad \text{for } a, b \in \{0, 1\}.$$

## 1. Inverse of SWAP and Its Eigenvalues

Note that applying SWAP twice returns the system to its original state:

$$\text{SWAP}^2\ |a\,b\rangle = \text{SWAP}\ |b\,a\rangle = |a\,b\rangle\,.$$

Thus,

$$\text{SWAP}^2 = I \quad \Longrightarrow \quad \text{SWAP}^{-1} = \text{SWAP}.$$

An operator that is its own inverse is an involution. For any eigenvector $|\psi\rangle$ with eigenvalue $\lambda$ we have

$$\text{SWAP}^2\,|\psi\rangle = \text{SWAP}(\lambda\,|\psi\rangle) = \lambda(\text{SWAP}\,|\psi\rangle) = \lambda^2\,|\psi\rangle = |\psi\rangle\,,$$

which implies

$$\lambda^2 = 1 \quad \Longrightarrow \quad \lambda = \pm 1.$$

Thus, the eigenvalues of SWAP are $\pm 1$.

## 2. Three Independent Product States with Eigenvalue $+1$

A state $|\psi\rangle$ is a $+1$-eigenvector of SWAP if

$$\text{SWAP}\,|\psi\rangle = |\psi\rangle.$$

In particular, any product state of the form

$$|\phi\rangle \otimes |\phi\rangle$$

is invariant under swapping the two factors:

$$\text{SWAP}\,(|\phi\rangle \otimes |\phi\rangle) = |\phi\rangle \otimes |\phi\rangle.$$

Thus, three independent product states that are $+1$-eigenvectors are:

1. $|0\rangle \otimes |0\rangle = |00\rangle$,
2. $|1\rangle \otimes |1\rangle = |11\rangle$,
3. $|+\rangle \otimes |+\rangle$, where
$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

## 3. Explicit Form of a $-1$-Eigenvector

Let

$$|\psi\rangle = u_{00}\,|00\rangle + u_{01}\,|01\rangle + u_{10}\,|10\rangle + u_{11}\,|11\rangle$$

be a $-1$-eigenvector, so that

$$\text{SWAP}\;|\psi\rangle = -\,|\psi\rangle\,.$$

Since

$$\begin{aligned}
\text{SWAP}\;|00\rangle &= |00\rangle\,,\\
\text{SWAP}\;|11\rangle &= |11\rangle\,,\\
\text{SWAP}\;|01\rangle &= |10\rangle\,,\\
\text{SWAP}\;|10\rangle &= |01\rangle\,,
\end{aligned}$$

the eigenvalue equation becomes:

$$u_{00}\,|00\rangle + u_{01}\,|10\rangle + u_{10}\,|01\rangle + u_{11}\,|11\rangle = -\Big(u_{00}\,|00\rangle + u_{01}\,|01\rangle + u_{10}\,|10\rangle + u_{11}\,|11\rangle\Big).$$

Equate coefficients for each computational basis state:

$$\begin{cases}
u_{00} = -u_{00} \quad\Longrightarrow\quad u_{00} = 0,\\
u_{11} = -u_{11} \quad\Longrightarrow\quad u_{11} = 0,\\
u_{01} = -u_{10},\\
u_{10} = -u_{01}.
\end{cases}$$

Thus, we must have $u_{01} = -u_{10}$. Choosing $u_{01} = \frac{1}{\sqrt{2}}$ (a positive real number) and $u_{10} = -\frac{1}{\sqrt{2}}$, we obtain the normalized $-1$-eigenvector:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big).$$

## 4. SWAP-Measurement on $|01\rangle$

Since SWAP is Hermitian with eigenvalues $\pm 1$, it can be treated as an observable. We can express $|01\rangle$ as a sum of the symmetric $(+1)$ and antisymmetric $(-1)$ eigenstates. The normalized symmetric eigenstate is

$$|v_+\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big),$$

and the antisymmetric eigenstate is

$$|v_-\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big).$$

We can write:

$$|01\rangle = \frac{1}{\sqrt{2}}\,|v_+\rangle + \frac{1}{\sqrt{2}}\,|v_-\rangle\,.$$

The probability of obtaining the outcome $-1$ (i.e. measuring the state $|v_-\rangle$) is given by the square of the amplitude:

$$P(-1) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}.$$

If the measurement yields $-1$, the state collapses to the corresponding eigenstate:

$$|v_-\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big).$$

## 5. Matrix and Condensed Representation of CSWAP

The CSWAP operator acts on three qubits. Taking the first qubit as the control and the second and third as the targets, its action is defined as follows:

- If the control qubit is in the state $|0\rangle$, then the target qubits are left unchanged.
- If the control qubit is in the state $|1\rangle$, then the target qubits are swapped.

## Matrix Representation

Assuming the computational basis ordered as

$$|000\rangle,\ |001\rangle,\ |010\rangle,\ |011\rangle,\ |100\rangle,\ |101\rangle,\ |110\rangle,\ |111\rangle,$$

the CSWAP operator is an $8 \times 8$ matrix. For the states with control qubit $|0\rangle$ (the first four basis states), the operator is the identity; for states with control $|1\rangle$ (the last four basis states) it applies the SWAP on the target qubits. The SWAP on two qubits is given by

$$\mathrm{SWAP}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Thus, the full matrix for CSWAP is

$$\mathrm{CSWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

In this matrix, note that for the lower block (corresponding to control $|1\rangle$):

- $|100\rangle \to |100\rangle$,
- $|101\rangle \to |110\rangle$,
- $|110\rangle \to |101\rangle$,
- $|111\rangle \to |111\rangle$.

## Algebraic Representation Using Projectors

A compact way to represent CSWAP is by writing it in terms of projectors on the control qubit:

$$P_0 = |0\rangle\langle 0|, \quad P_1 = |1\rangle\langle 1|.$$

Then we have

$$\mathrm{CSWAP} = P_0 \otimes I_4 \ + \ P_1 \otimes \mathrm{SWAP}_2,$$

where $I_4$ is the $4 \times 4$ identity operator on the space of the two target qubits, and $\mathrm{SWAP}_2$ is the SWAP operator acting on those qubits.

# Problem 3 - Week 4

Suppose that Alice and Bob share two qubits a and b in the Bell state $|\Phi^+\rangle$. Suppose also that Alice has a qubit `p` and Bob has a qubit `q` , which are in a joint state $|\psi\rangle = u_{00}|0,0\rangle + u_{01}|0,1\rangle + u_{10}|1,0\rangle + u_{11}|1,1\rangle \in \mathbb{C}^4$ that Alice and Bob don't precisely know - and which may even be entangled.

1. Write a state-vector for the joint state of `p, a, b, q` (with the qubits in that order), in ket notation.

2. Suppose that Alice and Bob perform the following operations on their qubits:

```
\# Alice and Bob each prepare some classical memory
\# to store measurement outcomes
bit r       \# for Alice
bit s       \# for Bob
            \# What Alice does
CX p, a
Mz a -> r
            \# What Bob does
CX b, q
Mx b -> s
```

   Describe the effect of this procedure, for all possible outcomes of the measurements performed.

3. Describe what information Alice and Bob must send to one another and what operations they must do, in order for the final state of `p, q` to be $|\psi'\rangle = \texttt{CX}\,|\psi\rangle$.

4. Summarise, in your own words, why the previous answer is significant.

**Solution:** In this problem, Alice and Bob share a Bell state on qubits `a` and `b`,

$$|\Phi^+\rangle_{ab} = \frac{1}{\sqrt{2}}\Big(|0\rangle_a\,|0\rangle_b + |1\rangle_a\,|1\rangle_b\Big),$$

while an additional two-qubit state on qubits `p` and `q` is given by

$$|\psi\rangle_{pq} = u_{00}\,|0\rangle_p\,|0\rangle_q + u_{01}\,|0\rangle_p\,|1\rangle_q + u_{10}\,|1\rangle_p\,|0\rangle_q + u_{11}\,|1\rangle_p\,|1\rangle_q\,.$$

## 1. Joint State of `p,a,b,q`

Since the two pairs are initially uncorrelated, the joint state is the tensor product

$$|\Psi\rangle_{pabq} = |\psi\rangle_{pq} \otimes |\Phi^+\rangle_{ab}\,.$$

Inserting the expressions and writing the qubits in the order $\mathtt{p}, \mathtt{a}, \mathtt{b}, \mathtt{q}$, we have

$$\begin{aligned}|\Psi\rangle_{pabq} &= \Big(u_{00}\,|0\rangle_p\,|0\rangle_q + u_{01}\,|0\rangle_p\,|1\rangle_q + u_{10}\,|1\rangle_p\,|0\rangle_q + u_{11}\,|1\rangle_p\,|1\rangle_q\Big) \\ &\quad\otimes \frac{1}{\sqrt{2}}\Big(|0\rangle_a\,|0\rangle_b + |1\rangle_a\,|1\rangle_b\Big) \\ &= \frac{1}{\sqrt{2}} \sum_{i,j\in\{0,1\}} u_{ij}\;|i\rangle_p \Big[\,|0\rangle_a\,|0\rangle_b + |1\rangle_a\,|1\rangle_b\Big]\,|j\rangle_q\,.\end{aligned}$$

This is the required state-vector in ket notation.

## 2. Effect of the Local Operations and Measurements

Alice and Bob now perform the following operations:

```
# Alice's operations:
CX p, a         % Controlled-NOT with control p and target a
Mz a -> r       % Measurement of qubit a in the Z-basis yielding bit r

# Bob's operations:
CX b, q         % Controlled-NOT with control b and target q
Mx b -> s       % Measurement of qubit b in the X-basis yielding bit s
```

Let us describe the effect step by step.

**Alice's Operations:**

1. **Apply** $\mathrm{CX}_{p,a}$**:** The CNOT with control `p` and target `a` acts as follows:

   $$|i\rangle_p\,|x\rangle_a \mapsto |i\rangle_p\,|x \oplus i\rangle_a\,,$$

   where $\oplus$ denotes addition modulo 2.

   In the two terms of the Bell state:

   - For the component $|0\rangle_a\,|0\rangle_b$: if $i = 0$ then $|0\rangle_a$ remains; if $i = 1$ then $|0\rangle_a$ flips to $|1\rangle_a$.
   - For the component $|1\rangle_a\,|1\rangle_b$: if $i = 0$ then $|1\rangle_a$ remains; if $i = 1$ then $|1\rangle_a$ flips to $|0\rangle_a$.

   Thus the state becomes a superposition where the state of qubit `a` now depends on the value of `p`.

2. **Measure qubit `a` in the Z-basis:** The measurement result $r \in \{0,1\}$ projects the state onto the subspace where qubit `a` is in $|r\rangle$. Consequently, two branches arise:

$$\textbf{If } r = 0: \quad \text{only the terms with } |0\rangle_a \text{ survive,}$$

$$\textbf{If } r = 1: \quad \text{only the terms with } |1\rangle_a \text{ survive.}$$

**Bob's Operations:**

1. **Apply** $\mathrm{CX}_{b,q}$**:** Here the CNOT with control `b` and target `q` acts as:

$$|j\rangle_b |y\rangle_q \mapsto |j\rangle_b |y \oplus j\rangle_q .$$

Thus, in each branch of the state, the state of `q` is flipped whenever qubit `b` is $|1\rangle$.

2. **Measure qubit `b` in the X-basis:** The X-basis states are

$$|+\rangle_b = \frac{1}{\sqrt{2}}\Big(|0\rangle_b + |1\rangle_b\Big) \quad \text{and} \quad |-\rangle_b = \frac{1}{\sqrt{2}}\Big(|0\rangle_b - |1\rangle_b\Big).$$

The measurement yields an outcome $s$ (which may be recorded as a classical bit corresponding to the eigenvalue $+1$ or $-1$). This further projects the state.

### 3. Communication and Corrections to Obtain $\mathrm{CX}\,|\psi\rangle$

I leave this question blank as I was not able to understand and develop an answer.

### 4. Significance of the Protocol

I leave this question blank as I was not able to understand and develop an answer.

## Problem 4 - Week 5

Let $f : \{0,1\}^2 \to \{0,1\}$ be a function such that $f(x) = 1$ only for one value of $x$. (For concreteness, you may consider the function $f(x_1, x_2) = x_1 \wedge x_2$).

Let $\mathtt{O}_f$ be a unitary oracle on three qubits, computing

$$\mathtt{O}_f |x_1 x_2, t\rangle = |x_1 x_2, t \oplus f(x_1, x_2)\rangle .$$

Perform a complete analysis of the effect of Grover's algorithm using this oracle, with the minor detail of performing exactly $T = 1$ application of the Grover iterate (rather than $T = \lfloor \frac{\pi}{4} \cdot 2^1 - 1 \rfloor$ applications).

What is the probability of finding the marked element in this case?

**Solution:**

We are given a function

$$f : \{0,1\}^2 \to \{0,1\},$$

with the property that $f(x) = 1$ for only one value of $x$. For concreteness, we may take

$$f(x_1, x_2) = x_1 \wedge x_2,$$

so that $f(1,1) = 1$ and $f(x) = 0$ for $x \neq (1,1)$. The oracle $\mathsf{O}_f$ acts on three qubits (the two data qubits and one target qubit) as

$$\mathsf{O}_f \ |x_1 x_2, t\rangle = |x_1 x_2,\ t \oplus f(x_1, x_2)\rangle \, .$$

By initializing the target qubit in the state

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

the oracle acts as a phase oracle:

$$\mathsf{O}_f \ |x\rangle \ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \ (-1)^{f(x)} \, |x\rangle \ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Thus, only the marked state (here, $|11\rangle$) acquires a phase of $-1$.

## Initialization

The search space is the two-qubit space, with $N = 4$ elements. We start with the uniform superposition over the data qubits:

$$|s\rangle = \frac{1}{2}\Big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\Big).$$

Including the target qubit prepared in

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

the overall initial state is

$$|\psi_0\rangle = |s\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

## Oracle Application

After applying the oracle, the state becomes

$$\begin{aligned}|\psi_1\rangle &= \mathtt{O}_f\ |\psi_0\rangle \\ &= \frac{1}{2\sqrt{2}}\Big[\,|00\rangle + |01\rangle + |10\rangle + (-1)\,|11\rangle\Big] \otimes (|0\rangle - |1\rangle).\end{aligned}$$

That is, in the data register the amplitude of $|11\rangle$ is flipped:

$$a(|00\rangle) = a(|01\rangle) = a(|10\rangle) = \frac{1}{2}, \quad a(|11\rangle) = -\frac{1}{2}.$$

## Diffusion Operator (Inversion about the Mean)

The Grover diffusion operator is defined as

$$D = 2\,|s\rangle\,\langle s| - I,$$

where $I$ is the identity on the two-qubit space. It acts by reflecting each amplitude about the average.

The initial amplitudes (after the oracle) are:

$$a(\text{marked}) = -\frac{1}{2}, \quad a(\text{unmarked}) = \frac{1}{2}.$$

The average amplitude is

$$\bar{a} = \frac{3 \cdot \frac{1}{2} + \left(-\frac{1}{2}\right)}{4} = \frac{1}{4}.$$

Under the reflection

$$a' = 2\bar{a} - a,$$

we obtain:

$$a'(|11\rangle) = 2\left(\frac{1}{4}\right) - \left(-\frac{1}{2}\right) = \frac{1}{2} + \frac{1}{2} = 1,$$

and for any unmarked state (say $|00\rangle$):

$$a'(|00\rangle) = 2\left(\frac{1}{4}\right) - \frac{1}{2} = \frac{1}{2} - \frac{1}{2} = 0.$$

Thus, after one iteration, the state of the data register is

$$|\psi_{\text{final}}\rangle = |11\rangle\,.$$

### Probability of Finding the Marked Element

Since the final state is exactly $|11\rangle$, the probability of measuring the marked element is

$$P(11) = |1|^2 = 1.$$

## Problem 5 - Week 6

Factorize $N = 143$, using the reduction from integer factorization to order finding (taking $a = 2$ rather than selecting $a$ at random), and the reduction from order finding to phase estimation.

For this exercise, you do not have to check that $a$ is relatively prime to $N$, or test multiple values of $a$.

Do not actually simulate any quantum computations. Instead, assume that the outcomes of the phase estimation process provide you with the following two samples of values of $x$ (for eigenvalues $e^{2\pi ix}$ of the unitary $U_a$):

$$x_1 = \frac{3}{4}, \qquad x_2 = \frac{4}{15}. \tag{2}$$

Use these to compute a candidate value for the order of $a$ modulo $N$, and use this information to find factors of $N$. (To compute greatest common divisors, you may use whatever tools you wish, or present a line of reasoning using whatever relevant information you have available.)

Show your workings.

**Solution:**

We are given:

$$N = 143, \quad a = 2,$$

and two samples from the phase estimation process:

$$x_1 = \frac{3}{4}, \qquad x_2 = \frac{4}{15}.$$

These samples are assumed to be exact and represent fractions of the form $\frac{s}{r}$ where $r$ is the order of $a$ modulo $N$; that is, $r$ is the smallest positive integer satisfying:

$$2^r \equiv 1 \pmod{143}.$$

### Determining the Order $r$

Each measured eigenphase gives a fraction in lowest terms:

$$x_1 = \frac{3}{4} \implies \text{candidate denominator } r_1 = 4,$$

$$x_2 = \frac{4}{15} \implies \text{candidate denominator } r_2 = 15.$$

Since the true order $r$ must be consistent with both measurements, a natural candidate is the least common multiple of these denominators:

$$r = \operatorname{lcm}(4, 15) = 60.$$

## Using the Order $r$ to Factorize $N$

Shor's algorithm shows that if $r$ is even and

$$2^{r/2} \not\equiv -1 \pmod{143},$$

then a nontrivial factor of $N$ can be obtained by computing the greatest common divisors:

$$\gcd\left(2^{r/2} - 1,\, 143\right) \quad \text{and} \quad \gcd\left(2^{r/2} + 1,\, 143\right).$$

For $a = 2$ and $r = 60$, we have:

$$r/2 = 30.$$

Thus, we need to analyze $2^{30}$ modulo 143.

Since $143 = 11 \times 13$, it is convenient to consider the computations modulo 11 and 13 separately.

**Note:** At this point we are using already the factorization for demonstration purposes. In an actual execution of Shor's algorithm on a large number $N$, one does not know the factorization of $N$ in advance. The modular exponentiation $a^{r/2} \mod N$ would be computed directly using efficient classical algorithms without decomposing $N$ into its prime factors. Thus, while it may appear circular to use the factorization $143 = 11 \times 13$ in our demonstration, this is simply a pedagogical tool. In the practical algorithm, the reduction from order finding to factorization does not assume prior knowledge of the factors, but here we use it to show clearly how the candidate order yields the factors.

### Modulo 11

By Fermat's Little Theorem, since 11 is prime:

$$2^{10} \equiv 1 \pmod{11}.$$

Thus,

$$2^{30} = \left(2^{10}\right)^3 \equiv 1^3 \equiv 1 \pmod{11}.$$

### Modulo 13

Similarly, by Fermat's Little Theorem for the prime 13:

$$2^{12} \equiv 1 \pmod{13}.$$

Write:

$$2^{30} = 2^{12 \cdot 2 + 6} = \left(2^{12}\right)^2 \cdot 2^6 \equiv 1^2 \cdot 2^6 \equiv 2^6 \pmod{13}.$$

Since $2^6 = 64$ and

$$64 \equiv 64 - 52 = 12 \equiv -1 \pmod{13},$$

we obtain:

$$2^{30} \equiv -1 \pmod{13}.$$

## Computing the Greatest Common Divisors

From the above results:

$$2^{30} \equiv 1 \pmod{11} \implies 2^{30} - 1 \equiv 0 \pmod{11},$$

so 11 divides $2^{30} - 1$.

Similarly,

$$2^{30} \equiv -1 \pmod{13} \implies 2^{30} + 1 \equiv 0 \pmod{13},$$

so 13 divides $2^{30} + 1$.

Thus, we can compute:

$$\gcd(2^{30} - 1, 143) = 11, \qquad \gcd(2^{30} + 1, 143) = 13.$$

## Conclusion

The candidate order obtained from the phase estimation samples is $r = 60$. Using this order and computing the greatest common divisors, we have:

$$\gcd(2^{30} - 1, 143) = 11, \qquad \gcd(2^{30} + 1, 143) = 13.$$

Therefore, the factors of $N = 143$ are:

$$143 = 11 \times 13.$$