# CMPT 476/776: Introduction to Quantum Algorithms
# Assignment 1 – Solutions

Due **January 22, 2026 at 11:59pm on Crowdmark**
Complete individually and submit in PDF format.

## Question 1 [6 points]: Classical circuits

The $NAND$ gate is a classical gate with the following truth table:

| $x$ | $y$ | $NAND(x,y)$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

1. Show by induction on $n$ that the gate set $\{AND, OR, NOT, FANOUT\}$ can implement any function $f : \{0,1\}^n \to \{0,1\}$. **You may find the following identity helpful:**

$$f(x_1, \ldots, x_{n-1}, x_n) = (x_n \wedge f(x_1, \ldots, x_{n-1}, 1)) \vee (\neg x_n \wedge f(x_1, \ldots, x_{n-1}, 0)).$$

2. Show that the gate set $\{NAND, FANOUT\}$ is universal for classical computation by giving implementations of each gate of the universal set $\{AND, OR, NOT, FANOUT\}$.

3. Suppose we encode the state of two classical bits $x, y \in \{0,1\}$ as 4-dimensional vectors labelled $|x, y\rangle$ with the following encoding:

$$|0,0\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad |0,1\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad |1,0\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad |1,1\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

   Give a 4x4 matrix which maps the vector $|x, y\rangle$ to $|x, NAND(x, y)\rangle$ for any $x, y \in \{0,1\}$.

4. Is the matrix you gave in part 3 invertible?

*Solution.*

1. Let $G = \{AND, OR, NOT, FANOUT\}$. We prove by induction on $n$, the number of input variables, that every Boolean function $f : \{0,1\}^n \to \{0,1\}$ can be implemented using the gate set $G$.

**Induction Base ($n = 1$):** There are $2^2 = 4$ Boolean functions $f : \{0,1\} \to \{0,1\}$. We show that each can be implemented using $G$.

- $\mathrm{id}(x) = x$: This function can be trivially implemented with no gates.
- $\mathrm{not}(x) = \neg x$: This function can be implemented using a single NOT gate.
- $\mathbf{0}(x) = 0$: Since $x \wedge \neg x = 0$, the constant-zero function can be implemented by duplicating the input $x$ using FANOUT, applying a NOT gate to one copy, and then AND-ing the two signals.
- $\mathbf{1}(x) = 1$: Since $x \vee \neg x = 1$, the constant-one function can be implemented by duplicating the input $x$ using FANOUT, applying a NOT gate to one copy, and then OR-ing the two signals.

**Induction Hypothesis ($n = k$):** Assume that every Boolean function $f : \{0,1\}^k \to \{0,1\}$ can be implemented using the gate set $G$.

**Induction Step ($n = k + 1$):** Let $f : \{0,1\}^{k+1} \to \{0,1\}$ be an arbitrary Boolean function, written as $f(x_1, \ldots, x_k, x_{k+1})$. Using the given identity, we have:

$$f(x_1, \ldots, x_k, x_{k+1}) = (x_{k+1} \wedge f(x_1, \ldots, x_k, 1)) \vee (\neg x_{k+1} \wedge f(x_1, \ldots, x_k, 0)).$$

In other words, to compute $f(x_1, \ldots, x_k, x_{k+1})$, we either have $x_{k+1} = 1$ and must compute the function $f(x_1, \ldots, x_k, 1)$, or we have $\neg x_{k+1} = 1$ and must compute $f(x_1, \ldots, x_k, 0)$. Define $f_1(x_1, \ldots, x_k) := f(x_1, \ldots, x_k, 1)$ and $f_0(x_1, \ldots, x_k) := f(x_1, \ldots, x_k, 0)$. Then $f_1$ and $f_0$ are Boolean functions of $k$ variables and, by the induction hypothesis, can be implemented using the gate set $G$.
Therefore, the function $f : \{0,1\}^{k+1} \to \{0,1\}$ can be implemented using $G$ as follows:

$$OR\big(AND(x_{k+1}, f_1(x_1, \ldots, x_k)), AND(NOT(x_{k+1}), f_0(x_1, \ldots, x_k))\big),$$

using FANOUT as needed to duplicate inputs. □

2. NOT: $NAND(x, x) = \neg(x \wedge x) = \neg x \vee \neg x = \neg x = NOT(x)$.

   FANOUT: Trivial.

   AND: $NOT(NAND(x, y)) = \neg(\neg(x \wedge y)) = x \wedge y = AND(x, y)$.

   OR: $NAND(NOT(x), NOT(y)) = \neg(\neg x \wedge \neg y) = \neg\neg x \vee \neg\neg y = x \vee y = OR(x, y)$.

3. We want the matrix of the transformation $T : \{0,1\}^2 \to \{0,1\}^2$ defined by

   $$T : |x, y\rangle \mapsto |x, NAND(x, y)\rangle.$$

   Using outer products, we can write $T = \sum_{x,y \in \{0,1\}} |x, NAND(x, y)\rangle\langle x, y|$. And by evaluating $NAND(x, y)$ on each of 4 points, we have:

   $$T = |0,1\rangle\langle 0,0| + |0,1\rangle\langle 0,1| + |1,1\rangle\langle 1,0| + |1,0\rangle\langle 1,1| = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

4. No. Since both $|0,0\rangle$ and $|0,1\rangle$ are mapped to $|0,1\rangle$, the transformation is not injective. Therefore, $T$ and hence its matrix, is not invertible.

## Question 2 [4 points]: Dirac notation

Let $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{-i}{\sqrt{2}}|2\rangle$, $|\phi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{i}{\sqrt{3}}|1\rangle + \frac{-1}{\sqrt{3}}|2\rangle$ be two states of a **qutrit** (i.e. a three-level or three-dimensional system).

1. Write $|\psi\rangle$ and $|\phi\rangle$ explicitly as column vectors
2. Calculate the following:
   - $\langle\psi|\psi\rangle$
   - $\langle\psi|\phi\rangle$
   - $|\psi\rangle\langle\phi|$
   - $|\psi\rangle \otimes |\phi\rangle$
3. Is the vector $|\psi\rangle + |\phi\rangle$ a unit vector? If not, normalize it to get a unit vector.

*Solution.*

1. $$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\-i\end{bmatrix}, \quad |\phi\rangle = \frac{1}{\sqrt{3}}\begin{bmatrix}1\\i\\-1\end{bmatrix}$$

2. $\langle\psi|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & i\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\-i\end{bmatrix} = \frac{1}{2}(1 + i\cdot(-i)) = \frac{1}{2}\cdot 2 = 1$

   $\langle\psi|\phi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & i\end{bmatrix}\frac{1}{\sqrt{3}}\begin{bmatrix}1\\i\\-1\end{bmatrix} = \frac{1-i}{\sqrt{6}}$

   $|\psi\rangle\langle\phi| = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\-i\end{bmatrix}\frac{1}{\sqrt{3}}\begin{bmatrix}1 & -i & -1\end{bmatrix} = \frac{1}{\sqrt{6}}\begin{bmatrix}1 & -i & -1\\0 & 0 & 0\\-i & -1 & i\end{bmatrix}$

   $$|\psi\rangle \otimes |\phi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\cdot|\phi\rangle\\0\cdot|\phi\rangle\\-i\cdot|\phi\rangle\end{bmatrix} = \frac{1}{\sqrt{6}}\begin{bmatrix}1\\i\\-1\\0\\0\\0\\-i\\1\\i\end{bmatrix}$$

3. Let $|\theta\rangle = |\phi\rangle + |\psi\rangle = \frac{1}{\sqrt{3}}\begin{bmatrix}1\\i\\-1\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\-i\end{bmatrix} = \frac{1}{\sqrt{6}}\begin{bmatrix}\sqrt{2}+\sqrt{3}\\i\sqrt{2}\\-\sqrt{2}-i\sqrt{3}\end{bmatrix}$

Then,

$$\langle\theta|\theta\rangle = \frac{1}{6}\left[(2+3+2\sqrt{6})+2+(2+3)\right] = \frac{12+2\sqrt{6}}{6} = \frac{6+\sqrt{6}}{3},$$

so $|\theta\rangle$ is not a unit vector. Normalizing, we get

$$\frac{|\theta\rangle}{\sqrt{\langle\theta|\theta\rangle}} = \frac{\sqrt{3}}{\sqrt{6}\sqrt{6+\sqrt{6}}}\begin{bmatrix}\sqrt{2}+\sqrt{3}\\ i\sqrt{2}\\ -\sqrt{2}-i\sqrt{3}\end{bmatrix} = \frac{1}{\sqrt{6+\sqrt{6}}}\begin{bmatrix}\frac{3+\sqrt{6}}{\sqrt{6}}\\ i\\ \frac{-\sqrt{6}-3i}{\sqrt{6}}\end{bmatrix} = \frac{1}{\sqrt{6}\sqrt{6+\sqrt{6}}}\begin{bmatrix}3+\sqrt{6}\\ i\sqrt{6}\\ -\sqrt{6}-3i\end{bmatrix}.$$

## Question 3 [6 points]: Qubits, gates, and measurement

Suppose we have a qubit initially in the state $\frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle$ for some $\theta \in \mathbb{R}$.

1. Calculate the probabilities of receiving result "0" or "1" if the qubit is measured.
2. Recall the definition of the Hadamard gate, which is the change of basis matrix for the $\{|+\rangle, |-\rangle\}$ basis:

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

   If we first apply the Hadamard gate to the initial state $\frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle$ and then measure in the computational basis, what are the probabilities of receiving the "0" and "1" results as **(simplified)** functions of $\theta$?
3. Using computational basis measurement, $H$ gates, and *phase gates*

   $$P(\theta) = \begin{bmatrix}1 & 0\\ 0 & e^{i\theta}\end{bmatrix}$$

   for any $\theta \in \mathbb{R}$, give a protocol to distinguish with 100% accuracy between the states

   $$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle), \qquad |\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i3\pi/4}|1\rangle)$$

4. Suppose you are given $k$ identical copies of the state $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle$ where $\theta \in [0, \pi]$ is unknown. Using only $H$ gates and computational basis measurements, give a procedure to estimate the value of $\theta$. Your method should converge to the correct value of $\theta$ as $k \to \infty$.

*Solution.*

1. $\mathbb{P}(0) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$.

   $\mathbb{P}(1) = |\frac{e^{i\theta}}{\sqrt{2}}|^2 = \frac{e^{i\theta}e^{-i\theta}}{2} = \frac{1}{2}$
2. Let $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle$

   Then

   $$H|\psi\rangle = \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ e^{i\theta}\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1+e^{i\theta}\\ 1-e^{i\theta}\end{bmatrix} = \frac{e^{i\theta/2}}{2}\begin{bmatrix}e^{-i\theta/2}+e^{i\theta/2}\\ e^{-i\theta/2}-e^{i\theta/2}\end{bmatrix} = e^{i\theta/2}\begin{bmatrix}\cos(\theta/2)\\ -i\sin(\theta/2)\end{bmatrix}$$

using the identites $\cos\alpha = \frac{e^{i\alpha}+e^{-i\alpha}}{2}$, $\sin\alpha = \frac{e^{i\alpha}-e^{-i\alpha}}{2i}$. We can read off the probabilities of measurement as $\mathbb{P}(0) = \cos^2\frac{\theta}{2}$, $\mathbb{P}(1) = \sin^2\frac{\theta}{2}$.

3. If we apply $T = P(\pi/4)$ to each state, we get

$$T|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \quad T|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle.$$

Thus applying H after gives

$$HT|\psi\rangle = H|+\rangle = |0\rangle, \quad HT|\phi\rangle = H|-\rangle = |1\rangle.$$

Measuring in the computational basis after applying $HT$ distinguishes the two states with certainty.

4. From part 2, we know that after applying $H$ to $|\psi\rangle$, the probability of measuring 0 and 1 in the computational basis are $\cos^2\frac{\theta}{2}$, $\sin^2\frac{\theta}{2}$ respectively. After measuring $k$ states in this manner, $\cos^2\frac{\theta}{2}$ is estimated by the fraction of states which resulted in a 0 measurement. Thus we can estimate $\theta$ as

$$\hat{\theta} = 2 \cdot \cos^{-1}\left(\sqrt{\frac{\#\text{ of 0's measured}}{k}}\right).$$

## Question 4 [4 points]: Eigenvectors

1. Let $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$. Find two **unit** vectors $|+_Y\rangle$, $|-_Y\rangle$ such that

$$Y|+_Y\rangle = |+_Y\rangle$$
$$Y|-_Y\rangle = -|-_Y\rangle$$

2. Let $U$ be the 2 by 2 matrix with columns $|+_Y\rangle$ and $|-_Y\rangle$. Is $U$ unitary?

3. Calculate $U^\dagger Y U$. What do you notice?

*Solution.*

1. •

$$Y\begin{bmatrix} a \\ b \end{bmatrix} = \mathbb{I}\begin{bmatrix} a \\ b \end{bmatrix}$$
$$\begin{bmatrix} -1 & -i \\ i & -1 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = 0$$

Using row operations to reduce $\begin{bmatrix} -1 & -i \\ i & -1 \end{bmatrix}$ we get the matrix $\begin{bmatrix} 1 & i \\ 0 & 0 \end{bmatrix}$, hence we have

$$\begin{bmatrix} 1 & i \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = 0 \implies a + ib = 0.$$

This is solved by $a = 1, b = i$ and normalizing gives $|+_Y\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ i \end{bmatrix}$.

- $$Y\begin{bmatrix}c\\d\end{bmatrix} = -\mathbb{I}\begin{bmatrix}c\\d\end{bmatrix}$$
$$\begin{bmatrix}1 & -i\\ i & 1\end{bmatrix}\begin{bmatrix}c\\d\end{bmatrix} = 0$$
$$\begin{bmatrix}1 & -i\\ 0 & 0\end{bmatrix}\begin{bmatrix}c\\d\end{bmatrix} = 0$$
$$\implies a - ib = 0$$

  This is solved by $a = 1, b = -i$ and normalizing gives $|-_Y\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$.

2. $$U = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ i & -i\end{bmatrix}$$
$$UU^\dagger = \frac{1}{2}\begin{bmatrix}1 & 1\\ i & -i\end{bmatrix}\begin{bmatrix}1 & -i\\ 1 & i\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & i-i\\ i-i & 2\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$
$$U^\dagger U = \frac{1}{2}\begin{bmatrix}1 & -i\\ 1 & i\end{bmatrix}\begin{bmatrix}1 & 1\\ i & -i\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1+i\cdot(-i) & 1+(-i)^2\\ 1+i^2 & 1+i\cdot(-i)\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$
   Hence $U$ is unitary.

3. $$U^\dagger Y U = \frac{1}{2}\begin{bmatrix}1 & -i\\ 1 & i\end{bmatrix}\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\begin{bmatrix}1 & 1\\ i & -i\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$
   Notice that $U^\dagger Y U$ is diagonal (in the $|0\rangle, |1\rangle$ basis), and that the entries on the diagonal are exactly the eigenvalues of $Y$.