# CMPT 476/776: Introduction to Quantum Algorithms
# Assignment 2 - Solution

Due **February 5th, 2026 at 11:59pm on crowdmark**
Complete individually and submit in PDF format.

## Question 1 [5 points]: Entanglement

Consider the following two-qubit gate:

$$\Delta = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

A two-qubit gate is **entangling** if it maps **at least one** separable state $|\phi\rangle \otimes |\psi\rangle$ to an entangled state, and is **separable** if it can be written as a tensor product of 2x2 matrices.

1. Is the $\Delta$ gate entangling? Give a proof for your answer.
2. Is the $\Delta$ gate separable? Give a proof for your answer.
3. How might you interpret the effect of the $\Delta$ gate on a two-qubit state?

*Solution.*

1. We prove that **$\Delta$ is not entangling** by analyzing its effect on an arbitrary separable state. Consider arbitrary single-qubit states $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle, |\psi\rangle = \gamma|0\rangle + \delta|1\rangle \in \mathbb{C}^2$.
   The corresponding two-qubit product state is

   $$|\phi\rangle \otimes |\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{bmatrix}.$$

   Applying $\Delta$, we obtain

   $$\Delta(|\phi\rangle \otimes |\psi\rangle) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{bmatrix} = \begin{bmatrix} \alpha\gamma \\ \beta\gamma \\ \alpha\delta \\ \beta\delta \end{bmatrix}.$$

Since multiplication in $\mathbb{C}$ is commutative, we may rewrite this as

$$\begin{bmatrix} \alpha\gamma \\ \beta\gamma \\ \alpha\delta \\ \beta\delta \end{bmatrix} = \begin{bmatrix} \gamma\alpha \\ \gamma\beta \\ \delta\alpha \\ \delta\beta \end{bmatrix} = \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = |\psi\rangle \otimes |\phi\rangle.$$

Therefore, for every product state $|\phi\rangle \otimes |\psi\rangle$, the output is another product state, namely $|\psi\rangle \otimes |\phi\rangle$. Hence, $\Delta$ does not map any separable state to an entangled state. $\square$

2. We prove that $\Delta$ **is not separable** by contradiction.
Suppose there exist matrices $A, B \in \mathbb{C}^{2\times 2}$ such that $A \otimes B = \Delta$. Then, write

$$A = \begin{bmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{bmatrix}, \qquad B = \begin{bmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{bmatrix}.$$

Recall that the tensor product has the block form

$$A \otimes B = \begin{bmatrix} A_{00}B & A_{01}B \\ A_{10}B & A_{11}B \end{bmatrix}.$$

On the other hand,

$$\Delta = \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] = \begin{bmatrix} |0\rangle\langle 0| & |1\rangle\langle 0| \\ |0\rangle\langle 1| & |1\rangle\langle 1| \end{bmatrix}.$$

Comparing blocks gives $A_{00}B = |0\rangle\langle 0|$. Since $|0\rangle\langle 0|$ is nonzero, we must have $A_{00} \neq 0$. Therefore,

$$B = \frac{1}{A_{00}}|0\rangle\langle 0| = \frac{1}{A_{00}} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

In particular, this forces $B_{01} = B_{10} = B_{11} = 0$. Thus, for any $c \in \mathbb{C}$, the matrix $cB$ can have a nonzero entry only in its top-left position. Consequently, the block $A_{01}B$ must also have zeros everywhere except possibly in the top-left entry. However, from $\Delta$, the top-right block must equal

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

which has a nonzero entry in the bottom-left position. This contradicts with the assumption of $A \otimes B = \Delta$, therefore $\Delta$ is not separable. $\square$

3. From the first part, we showed that $\Delta$ maps any product state $|\phi\rangle \otimes |\psi\rangle$ to $|\psi\rangle \otimes |\phi\rangle$. In particular, its action on the computational basis states is

$$|00\rangle \mapsto |00\rangle, \qquad |01\rangle \mapsto |10\rangle, \qquad |10\rangle \mapsto |01\rangle, \qquad |11\rangle \mapsto |11\rangle.$$

Therefore, by linearity, for any two-qubit state (not necessarily separable), we have

$$\Delta : \sum_{i,j\in\{0,1\}} \alpha_{i,j}|i,j\rangle \mapsto \sum_{i,j\in\{0,1\}} \alpha_{i,j}|j,i\rangle.$$

Thus, it exchanges the state of two qubits. Hence, $\Delta$ is the **SWAP** gate.

## Question 2 [4 points]: Pauli operators

Recall the definition of the $I$, $X$, $Z$, and $Y$ gates:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

These are known as the *Pauli matrices* or gates.

1. Compute the matrices $X \otimes Z$ and $Z \otimes X$
2. Show that the non-identity Pauli matrices anti-commute: that is, $UV = -VU$ for every pair of $X$, $Y$, and $Z$ matrices where $U \neq V$
3. Show that the Pauli matrices $I, X, Z, Y$ are linearly independent
4. Show that the Pauli matrices form a basis for the space of $2 \times 2$ complex-valued matrices.

*Solution.*

1. $X \otimes Z = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad Z \otimes X = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$

2. It's easy to check that $X^2 = Y^2 = Z^2 = I$. Now, we find $ZX = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = iY$ and $XZ = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -iY$. Thus, $X$ and $Z$ anti-commute. Furthermore, we can now also deduce that

$$\begin{aligned} XY &= X(iXZ) = iX^2Z = iZ \quad \text{and} \quad YX = (-iZX)X = -iZX^2 = -iZ; \\ YZ &= (iXZ)Z = iXZ^2 = iX \quad \text{and} \quad ZY = Z(-iZX) = -iZ^2X = -iX \end{aligned}$$

   as required.

3. Let $\alpha, \beta, \gamma, \delta$ be scalars such that $\alpha I + \beta Z + \gamma X + \delta Y = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Thus we have

$$\begin{aligned} \alpha + \beta &= 0, \\ \gamma - i\delta &= 0, \\ \gamma + i\delta &= 0, \\ \alpha - \beta &= 0, \end{aligned}$$

   and solving these equations simultaneously gives $\alpha = \beta = \gamma = \delta = 0$. Hence the Pauli matrices are linearly independent.

4. From the previous part, we know that the four Pauli matrices are linearly independent. The vector space of $2 \times 2$ complex-valued matrices is isomorphic to $\mathbb{C}^4$ and hence has dimension 4. Thus the Pauli matrices form a minimal spanning set and are therefore a basis.

## Question 3 [9 points]: Non-local games

In this question, we're going to study another non-local game involving 3-parties, or 3 qubits. First let $|\psi\rangle = \frac{1}{2}(|000\rangle - |110\rangle - |011\rangle - |101\rangle)$.

1. Give a 3-qubit circuit $U$ consisting of $X$, $H$, and $CNOT$ gates such that

$$U\left(\frac{1}{\sqrt{2}}|000\rangle - \frac{1}{\sqrt{2}}|111\rangle\right) = |\psi\rangle.$$

2. Show that a partial measurement of any qubit of the $|\psi\rangle$ state leaves an entangled state in the remaining 2 qubits.

3. Compute the parity $a \oplus b \oplus c = a + b + c \mod 2$ of the measurement results if

   (a) All qubits are measured in the $\{0, 1\}$ basis.
   (b) Qubits 0 and 1 are measured in the $\{|+\rangle, |-\rangle\}$ basis and qubit 2 in the $\{0, 1\}$ basis.
   (c) Qubits 0 and 2 are measured in the $\{|+\rangle, |-\rangle\}$ basis and qubit 1 in the $\{0, 1\}$ basis.
   (d) Qubits 1 and 2 are measured in the $\{|+\rangle, |-\rangle\}$ basis and qubit 0 in the $\{0, 1\}$ basis.

   In the $\{|+\rangle, |-\rangle\}$ basis, interpret the measurement result "+" as 0 and "-" as 1.

4. Denote the measurement result of qubit $i$ in the $\{0, 1\}$ basis by $a_i$, and in the $\{|+\rangle, |-\rangle\}$ basis by $b_i$. Is it possible that each measurement result $a_i$ and $b_i$ has a **pre-determined** value which is **independent** of which basis the other qubits are measured in?

   **Hint: Add up the 4 cases in the previous question mod 2. Is anything wrong?**

5. Give a **perfect** quantum strategy (i.e. a strategy involving a shared pre-entangled state which **wins 100% of the time**) for the following 3 player game.

   - Alice, Bob, and Charlie are each given one bit $x$, $y$, and $z$ respectively with the constraint that $x \oplus y \oplus z = 0$.
   - Alice, Bob, and Charlie each return a single bit $a$, $b$, $c$ respectively, and they win if $a \oplus b \oplus c = x \vee y \vee z$.

   To get you started, use the state $|\psi\rangle$ from the first part of this question as the initial shared state.

*Solution.*

1. Working backwards, we have $|\psi\rangle = \frac{1}{2}\big(|0\rangle(|00\rangle - |11\rangle) - |1\rangle(|10\rangle + |01\rangle)\big)$. Applying $\mathrm{CNOT}_{12}$ (i.e. control on qubit 1 and target on qubit 2) we get

$$\begin{aligned}\tfrac{1}{2}\big(|0\rangle(|00\rangle - |10\rangle) - |1\rangle(|11\rangle + |01\rangle)\big) &= \tfrac{1}{2}\big(|0\rangle(|0\rangle - |1\rangle)|0\rangle - |1\rangle(|1\rangle + |0\rangle)|1\rangle\big) \\ &= \tfrac{1}{\sqrt{2}}(|0\rangle|-\rangle|0\rangle - |1\rangle|+\rangle|1\rangle),\end{aligned}$$

   so we can now reach our initial state by applying $H_1$ followed by $X_1$. Thus by reversing this circuit we get that

$$\begin{aligned}U &= (X_1 H_1 \mathrm{CNOT}_{12})^\dagger \\ &= \mathrm{CNOT}_{12} H_1 X_1 \quad \text{(all these gates are hermitian).}\end{aligned}$$

2. Suppose we measure qubit 0. If we obtain an outcome of 0, the resulting state is $\frac{1}{\sqrt{2}}(|000\rangle - |011\rangle)$. If the outcome is 1, the resulting state is (proportional to) $\frac{1}{\sqrt{2}}(|110\rangle + |101\rangle)$. By inspecting qubits 1 and 2, it's easy to check that both of these states are entangled.

   If instead we measure qubit 1 or 2, we note that $|\psi\rangle$ is symmetric under permuting qubits. We can rewrite the state by swapping the qubit we're measuring with qubit 0 and proceed exactly as before.

3. (a) We can either use part 2 as a starting point, or alternatively we can consider measuring the entire system in the 3-qubit computational basis $\{|000\rangle, |001\rangle, \ldots, |111\rangle\}$. In either case, we find that the possible measurement outcomes are $abc = 000$, 110, 011 or 101. Each of these outcomes has parity $a \oplus b \oplus c = 0$.

   (b) Note that $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$. Thus we have

$$\begin{aligned}
|000\rangle &= \tfrac{1}{2}(|{+}{+}\rangle + |{+}{-}\rangle + |{-}{+}\rangle + |{-}{-}\rangle)|0\rangle, \\
|110\rangle &= \tfrac{1}{2}(|{+}{+}\rangle - |{+}{-}\rangle - |{-}{+}\rangle + |{-}{-}\rangle)|0\rangle, \\
|011\rangle &= \tfrac{1}{2}(|{+}{+}\rangle - |{+}{-}\rangle + |{-}{+}\rangle - |{-}{-}\rangle)|1\rangle, \\
|101\rangle &= \tfrac{1}{2}(|{+}{+}\rangle + |{+}{-}\rangle - |{-}{+}\rangle - |{-}{-}\rangle)|1\rangle,
\end{aligned}$$

   so $|\psi\rangle = \frac{1}{2}(-|{+}{+}1\rangle + |{+}{-}0\rangle + |{-}{+}0\rangle + |{-}{-}1\rangle)$.
   Measuring in the joint basis $\{|{+}{+}0\rangle, |{+}{+}1\rangle, \ldots, |{-}{-}1\rangle\}$, we see that the parity of any measurement result is 1.

   For parts (c) and (d), we can simply use the symmetry of $|\psi\rangle$ to immediately deduce that the parity is 1 in each of these cases.

4. We can show that the values of $a_i$ and $b_i$ can't have predetermined values by way of a parity argument. The previous question showed that for the 4 measurement bases in that question, we get the series of constraints on the values of $a_i$ and $b_i$:

$$\begin{aligned}
a_0 \oplus a_1 \oplus a_2 &= 0 \\
b_0 \oplus b_1 \oplus a_2 &= 1 \\
b_0 \oplus a_1 \oplus b_2 &= 1 \\
a_0 \oplus b_1 \oplus b_2 &= 1
\end{aligned}$$

   Now suppose each $a_i$ and $b_i$ is pre-determined and independent of the measurement performed on the other qubits. Then each $a_i$ and $b_i$ has a definite value and in particular must simultaneously satisfy *all* the above constraints. We can show that the above constraint system is inconsistent and hence can't be simultaneously satisfied by summing up both sides mod 2:

$$\begin{array}{c|c|c}
 & a_0 \oplus a_1 \oplus a_2 & 0 \\
 & b_0 \oplus b_1 \oplus a_2 & 1 \\
 & b_0 \oplus a_1 \oplus b_2 & 1 \\
 & a_0 \oplus b_1 \oplus b_2 & 1 \\
\hline
+ & = 0 \quad \text{mod } 2 & = 1 \quad \text{mod } 2
\end{array}$$

5. Part 3 gives us a clue for a potential strategy. Let Alice, Bob and Charlie share the state $|\psi\rangle$ such that Alice can only perform local operations and measurements on qubit 0, Bob on qubit 1, and Charlie on qubit 2. Each player performs a measurement on their qubit as follows: if the bit they are given is 0, they measure in the computational basis; if the bit is 1, they measure in the $\{|+\rangle, |-\rangle\}$ basis. They each return a bit corresponding to their measurement outcome.

   By symmetry, and after imposing the additional constraint that $x \oplus y \oplus z = 0$, we only need to check what happens in two cases: $x, y, z$ are all 0; two of $x, y, z$ are 1. In the case where $x, y, z$ are all 0, part 3(a) tells us that the returned bits satisfy $a \oplus b \oplus c = 0$, which is equal to $x \vee y \vee z$. Similarly, in the case where two of $x, y, z$ are 1, parts 3(b)–(d) tell us that the returned bits satisfy $a \oplus b \oplus c = 1$, which is equal to $x \vee y \vee z$. Hence this strategy succeeds with 100% probability.

## Question 4 [4 points]: Partial measurement and mixed states

Let

$$|\psi\rangle = \frac{i\sqrt{2}}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}\sqrt{2}}|01\rangle + \frac{\sqrt{2}}{2\sqrt{3}}|10\rangle.$$

1. Calculate the probabilities of measuring 0 or 1 in the first qubit, and the resulting normalized state vector in each case.
2. Write the mixed state obtained after measuring the first qubit as a density matrix $\rho$.
3. Compute the partial trace $\mathrm{Tr}_A(\rho)$ obtained by tracing out the first qubit of $\rho$.
4. Compute the partial trace $\mathrm{Tr}_B(\rho)$ obtained by tracing out the second qubit of $\rho$.

*Solution.*

1. The probability of measuring 0 in the first qubit is $(\frac{\sqrt{2}}{\sqrt{3}})^2 + (\frac{1}{\sqrt{3}\sqrt{2}})^2 = \frac{2}{3} + \frac{1}{6} = \frac{5}{6}$. The resulting normalized state becomes

$$\frac{1}{\sqrt{p(0)}}\left(\frac{i\sqrt{2}}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}\sqrt{2}}|01\rangle\right) = \frac{2i}{\sqrt{5}}|00\rangle + \frac{1}{\sqrt{5}}|01\rangle.$$

   The probability of measuring 1 in the first qubit is $(\frac{\sqrt{2}}{2\sqrt{3}})^2 = \frac{1}{6}$. The resulting normalized state becomes

$$\frac{1}{\sqrt{p(1)}}\frac{\sqrt{2}}{2\sqrt{3}}|10\rangle = |10\rangle.$$

2. 

$$\begin{aligned}
\rho &= (|0\rangle\langle 0| \otimes I)\rho_i(|0\rangle\langle 0| \otimes I) + (|1\rangle\langle 1| \otimes I)\rho_i(|1\rangle\langle 1| \otimes I) \\
&= (\frac{i\sqrt{2}}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}\sqrt{2}}|01\rangle)(\frac{-i\sqrt{2}}{\sqrt{3}}\langle 00| + \frac{1}{\sqrt{3}\sqrt{2}}\langle 01|) + (\frac{\sqrt{2}}{2\sqrt{3}}|10\rangle)(\frac{\sqrt{2}}{2\sqrt{3}}\langle 10|) \\
&= \frac{2}{3}|00\rangle\langle 00| + \frac{1}{6}|01\rangle\langle 01| + \frac{i}{3}|00\rangle\langle 01| - \frac{i}{3}|01\rangle\langle 00| + \frac{1}{6}|10\rangle\langle 10|
\end{aligned}$$

3.

$$\begin{aligned}\mathrm{Tr}_A(\rho) &= \frac{2}{3}|0\rangle\langle 0| + \frac{1}{6}|1\rangle\langle 1| + \frac{i}{3}|0\rangle\langle 1| - \frac{i}{3}|1\rangle\langle 0| + \frac{1}{6}|0\rangle\langle 0| \\ &= \frac{5}{6}|0\rangle\langle 0| + \frac{i}{3}|0\rangle\langle 1| - \frac{i}{3}|1\rangle\langle 0| + \frac{1}{6}|1\rangle\langle 1|.\end{aligned}$$

4.

$$\begin{aligned}\mathrm{Tr}_B(\rho) &= \frac{2}{3}|0\rangle\langle 0| + \frac{1}{6}|0\rangle\langle 0| + \frac{1}{6}|1\rangle\langle 1| \\ &= \frac{5}{6}|0\rangle\langle 0| + \frac{1}{6}|1\rangle\langle 1|.\end{aligned}$$

## Question 5 [8 points]:

In this question you're going to write a tiny simulator for quantum circuits, which explicitly performs — on a classical computer such as yours — the linear algebraic calculations that quantum circuits represent. We'll use Python with Numpy to provide some data structures and randomization routines. Starter code and some simple sanity checks are provided in the file `simulator.py`, along with the constant and function stubs you are tasked with filling in.

Tasks:

1. Fill out the definitions of the `ket0` and `ket1` states.
2. Fill out the defintions of the `X`, `Y`, `Z`, `H`, and `CNOT` gates.
3. Fill out the definitions of the `normalize` and `tensor` operators. **You may not use numpy's `normalize` or `kron` functions**. `tensor` should allow tensor products of vectors and matrices of arbitrary dimensions.
4. Fill out the definition of `measure`, which takes a state vector and measures the indicated qubit number (starting from 0), and returns a pair $(result, |\psi\rangle)$ consisting of the numerical result of the measurement, $result$, and the resulting (normalized) state vector $|\psi\rangle$.
5. Test it out on some larger circuits, e.g. by applying some gates to a large state like $|+\rangle^{\otimes 20}$, the tensor product of 20 copies of $|+\rangle$. What do you notice? Do you think classical computers can efficiently simulate arbitrary quantum circuits? How can you make this simulation more scalable?

Notes:

- Represent the computational basis in big-endian (most significant bit first). A helper function, `toBits` is provided which decomposes an integer $i$ into a length $n$ list of bits in big-endian.
- Vectors are most conveniently represented as matrices (i.e. 2d arrays) where there is only a single column. You may use a 1d array instead, but `tensor` becomes slightly more involved.

- `numpy.random` has a function, `choice`, which allows specification of a probability distribution for the random choice and will hence be helpful.
- The conjugate of a complex number `c` can be obtained by `c.conjugate()`
- Part of your mark will be auto-graded, so test your code thoroughly.