Solutions to problem Set - 2

Introduction to quantum computing using QSim

Problem 1: Multi-qubit transformations

The following questions are based on the properties of the Kronecker (Tensor) product and transformations on multi-qubit systems.

a) If A and B are two single qubit gates, prove the following relations: [I is the 2×2 identity matrix and $\circ$ denotes matrix multiplication. All other symbols carry their usual meanings]

(This problem uses concepts discussed in slides $9-11$, Week 2 Session 1-2.)

i. $(A \otimes I) \circ (I \otimes B) = (A \otimes B)$

Solution: The aim of this problem is to prove the distributive property of the tensor product. Let the action of the A and B on the single-qubit standard basis given by the following relations:

$$A|0\rangle = |a_0\rangle \qquad B|0\rangle = |b_0\rangle$$
$$A|1\rangle = |a_1\rangle \qquad B|1\rangle = |b_1\rangle$$

The proof can be proven by showing that the action of the operators $(A \otimes I) \circ (I \otimes B)$ and $(A \otimes B)$ on the two-qubit basis is the same:
Let us first consider the action of the two operators on the basis element $|00\rangle$

$$\begin{aligned}(A \otimes I) \circ (I \otimes B)|00\rangle &= (A \otimes I) \circ (I|0\rangle \otimes B|0\rangle) \\ &= (A \otimes I)(|0\rangle \otimes |b_0\rangle) \\ &= A|0\rangle \otimes I|b_0\rangle \\ \therefore \quad (A \otimes I) \circ (I \otimes B)|00\rangle &= |a_0\rangle \otimes |b_0\rangle\end{aligned}$$

and

$$\begin{aligned}(A \otimes B)|00\rangle &= (A|0\rangle \otimes B|0\rangle) \\ &= |a_0\rangle \otimes |b_0\rangle\end{aligned}$$

Similarly, the equality can be proven for all other basis elements and this completes the proof.

ii. $(A \circ B)^{-1} = B^\dagger \circ A^\dagger$

Solution: The proof of this question is based on the fact that A and B are single qubit gates and are therefore unitary transformations.
Therefore, from the definition of matrix inverse:

$$(A \circ B)^{-1}(A \circ B) = I$$

Now, considering the product of the operators:

$$\begin{aligned}(B^\dagger \circ A^\dagger)(A \circ B) &= \left(B^\dagger \circ \left(A^\dagger A\right) \circ B\right) \\ &= \left(B^\dagger \circ B\right) \quad \because A \text{ is unitary} \\ &= I \quad \because B \text{ is unitary}\end{aligned}$$

Therefore, $B^\dagger \circ A^\dagger$ is the inverse of $A \circ B$ and the proof is complete.

b) Let U be a single qubit gate with actions on the standard basis given as follows:

$$\begin{aligned}U|0\rangle &= |a\rangle \\ U|1\rangle &= |b\rangle\end{aligned}$$

Given V be a single qubit gate related to U through the following relation: $V^\dagger X V = U$
Find the action of the following circuit (i.e. find $|\psi\rangle$), on the two-qubit computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

(There was an error in the circuit diagram for this question, the correct figure is given below:.)

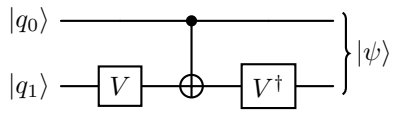

Figure 1: Circuit diagram for Problem 1 b).

Solution: Since the circuit uses a CX gate, it may be worthwhile examining the effect of the circuit in the cases, $|q_0\rangle = |0\rangle$ and $|q_0\rangle = |1\rangle$.
The matrix corresponding to the given circuit is given by:

$$M = \left(I \otimes V^\dagger\right) \circ CX \circ (I \otimes V)$$

(The method for this has been discussed in slides 11 – 13, Week 2 Session 2-3.)

When the qubit q_0 is in $|0\rangle$, the action of the above circuit is given by:

$$\begin{aligned}\left(I \otimes V^\dagger\right) \circ CX \circ (I \otimes V)\ |0\rangle \otimes |q_1\rangle &= \left(I \otimes V^\dagger\right) \circ CX\ |0\rangle \otimes V\,|q_1\rangle \\ &= \left(I \otimes V^\dagger\right)\ |0\rangle \otimes V\,|q_1\rangle\ \text{, the control qubit is set to } |0\rangle \\ &= |0\rangle \otimes V^\dagger V\,|q_1\rangle \\ &= |0\rangle \otimes |q_1\rangle\ \text{, } V \text{ is unitary.}\end{aligned}$$

When the qubit q_0 is in $|1\rangle$, the X gate is applied to second qubit. Therefore, the action of the above circuit is given by:

$$\begin{aligned}\left(I \otimes V^\dagger\right) \circ CX \circ (I \otimes V)\ |1\rangle \otimes |q_1\rangle &= \left(I \otimes V^\dagger\right) \circ CX\ |1\rangle \otimes V\,|q_1\rangle \\ &= \left(I \otimes V^\dagger\right)\ |1\rangle \otimes XV\,|q_1\rangle \\ &= |1\rangle \otimes V^\dagger XV\,|q_1\rangle \\ &= |1\rangle \otimes U\,|q_1\rangle\ \text{, from the definition of } V.\end{aligned}$$

Therefore, the action of the circuit on the two-qubit standard basis is given by;

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \xrightarrow{M} \{|00\rangle, |01\rangle, |1\rangle \otimes |a\rangle, |1\rangle \otimes |b\rangle\}$$

The above circuit is therefore a representation of the controlled U gate.

c) Show that there <u>exists no</u> pair of single qubit gates, A, B that satisfy the following relation:

$$A \otimes B = \text{CNOT}_1^0$$

Solution: Assuming that it is possible to write CNOT_1^0 in the form $A \otimes B$. Where A and B are single qubit gates given by the matrices:

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

Therefore the expansion of CNOT_1^0 may be expressed as:

$$\begin{aligned} A \otimes B &= \begin{bmatrix} A_{00}\begin{bmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{bmatrix} & A_{01}\begin{bmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{bmatrix} \\ A_{10}\begin{bmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{bmatrix} & A_{11}\begin{bmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{bmatrix} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \end{aligned}$$

This further implies that the following relations are true:

$$
\begin{aligned}
& A_{00}\begin{bmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
\Rightarrow\ & A_{00}B_{01} = A_{00}B_{10} = 0 \\
\Rightarrow\ & A_{00}B_{00} = A_{00}B_{11} = 1 \\
\therefore\ & B_{01} = B_{10} = 0 \\
\text{and}\ & B_{00} = B_{11} \neq 0
\end{aligned}
\qquad
\begin{aligned}
& A_{11}\begin{bmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
\Rightarrow\ & A_{11}B_{01} = A_{00}B_{10} = 1 \\
\Rightarrow\ & A_{11}B_{00} = A_{00}B_{11} = 0 \\
\therefore\ & B_{01} = B_{10} \neq 0 \\
\text{and}\ & B_{00} = B_{11} = 0
\end{aligned}
$$

The above results are a contradiction, therefore it is impossible to express CNOT_1^0 as $A \otimes B$.

d) If a two-qubit gate has the following action on the two-qubit standard basis:

$$
\begin{aligned}
U\left|00\right\rangle &= \left|v_0\right\rangle \\
U\left|01\right\rangle &= \left|v_1\right\rangle \\
U\left|10\right\rangle &= \left|v_2\right\rangle \\
U\left|11\right\rangle &= \left|v_3\right\rangle
\end{aligned}
$$

i. Prove the following relation:

$$
\left|v_0\right\rangle\!\left\langle 00\right| + \left|v_1\right\rangle\!\left\langle 01\right| + \left|v_2\right\rangle\!\left\langle 10\right| + \left|v_3\right\rangle\!\left\langle 11\right| = U
$$

Solution: This relation can be verified by multiplying the left hand side of the above equation with elements of the two-qubit standard basis. As an example, the product with $\left|00\right\rangle$ is shown.

$$
\begin{aligned}
\left(\left|v_0\right\rangle\!\left\langle 00\right| + \left|v_1\right\rangle\!\left\langle 01\right| + \left|v_2\right\rangle\!\left\langle 10\right| + \left|v_3\right\rangle\!\left\langle 11\right|\right)\left|00\right\rangle &= \left|v_0\right\rangle\left\langle 00|00\right\rangle + \left|v_1\right\rangle\left\langle 01|00\right\rangle \\
&\quad + \left|v_2\right\rangle\left\langle 10|00\right\rangle + \left|v_3\right\rangle\left\langle 11|00\right\rangle \\
&= \left|v_0\right\rangle
\end{aligned}
$$

The other terms vanish because of the orthonormality of the two-qubit standard basis. working out the expression for the other elements of the basis will complete the proof.

ii. Using the above relation, find the matrix form of CNOT_0^1.

Solution: The action of CNOT_0^1 on the two-qubit standard basis is given as:

$$
\begin{aligned}
\text{CNOT}_0^1\left|00\right\rangle &= \left|00\right\rangle \\
\text{CNOT}_0^1\left|01\right\rangle &= \left|11\right\rangle \\
\text{CNOT}_0^1\left|10\right\rangle &= \left|10\right\rangle \\
\text{CNOT}_0^1\left|11\right\rangle &= \left|01\right\rangle
\end{aligned}
$$

The operator form of CNOT_0^1 is given by:

$$\text{CNOT}_0^1 = |00\rangle\langle 00| + |11\rangle\langle 01| + |10\rangle\langle 10| + |01\rangle\langle 11|$$

if one were to try to expand this to the matrix form, we get the following result.

$$\text{CNOT}_0^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Problem 2: Boolean functions and quantum gates

The following questions are based on quantum implementations of Boolean functions.

a) Find the quantum circuits (bit oracles) for the following Boolean functions: [$\oplus$ - XOR, $\vee$ - OR, $^-$ - NOT]

i. $F(x_0, x_1) = x_0 \oplus x_1$

Solution: This is a two variable function. Therefore the bit oracle requires a 3-qubit operation and is represented by the following circuit:

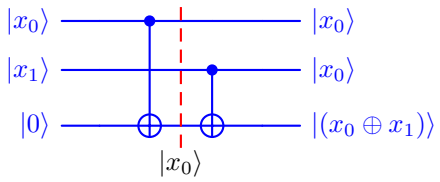

Figure 2: Circuit diagram for Problem 2 a) i.

(This is also explained in the python notebook titled, "2.Boolean function oracles.ipynb".)

ii. $F(x_0, x_1) = x_0 \vee x_1$

Solution: This is a two variable function. Therefore the bit oracle requires a 3-qubit operation. It will also be of benefit to represent the OR gate in terms of the AND gate.

$$x_0 \vee x_1 = \overline{\overline{x}_0 \wedge \overline{x}_1}$$

This is due to the De Morgan's law.
The bit oracle of the AND gate can be represented by a single Toffoli (CCX) gate. Additionally, the negation of the bit value stored in any qubit can be performed using the Pauli X gate.
Therefore, the circuit for this function is as shown below:

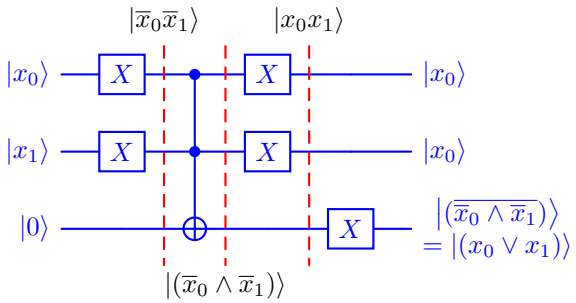

Figure 3: Circuit diagram for Problem 2 a) ii.

iii. $F(x) = \overline{x}$

Solution: It should be remembered that what is required for this question is a bit oracle, which will be a two-qubit circuit. This circuit will be given by:

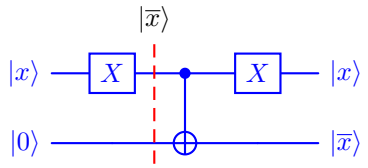

Figure 4: Circuit diagram for Problem 2 a) iii.

b) Prove the following statements for a n-bit Boolean function bit oracle: ['+' denotes the XOR operation]

$$U_F \underset{n\text{-qubit}}{|\mathbf{x}\rangle} \underset{1\text{-qubit}}{|y\rangle} \rightarrow |\mathbf{x}\rangle\,|F(\mathbf{x}) + y\rangle$$

i. The bit oracle causes entanglement between the input qubits, $|\mathbf{x}\rangle$ and the target qubit, $|y\rangle$.

Solution: To prove this statement, we can consider two distinct input values $\mathbf{x}_1$ and $\mathbf{x}_2$ for the Boolean function such that:

$$F(\mathbf{x}_1) \neq F(\mathbf{x}_2)$$

The action of the the bit-oracle U_F on the state, $|\mathbf{x}_1\rangle + |\mathbf{x}_2\rangle$ is given by:

$$U_F(|\mathbf{x}_1\rangle + |\mathbf{x}_2\rangle)\,|0\rangle = |\mathbf{x}_1\rangle\,|F(\mathbf{x}_1)\rangle + |\mathbf{x}_2\rangle\,|F(\mathbf{x}_2)\rangle$$

In the above expression, normalization has been temporarily disregarded. Now since it is known that $\mathbf{x}_1 \neq \mathbf{x}_2$ and $F(\mathbf{x}_1) \neq F(\mathbf{x}_2)$. It is impossible to separate the target qubit from the n-qubit input states. This implies that there is entanglement between the input qubits and the target qubit. The following statement is a property of all Boolean function oracles.

"As long as the Boolean function $F(\mathbf{x})$ **is not constant** the quantum bit oracle U_F causes entanglement between the input and the output qubits."

(This was also discussed in slides $11 - 12$*, Week 3 Session 2-3.)*

ii. $U_F^\dagger = U_F$

Solution: The proof of this statement involves applying the bit oracle of the Boolean function twice. This is done as shown below:

$$|\mathbf{x}\rangle |y\rangle \xrightarrow{U_F} |\mathbf{x}\rangle |y + F(\mathbf{x})\rangle \xrightarrow{U_F} |\mathbf{x}\rangle |y + F(\mathbf{x}) + F(\mathbf{x})\rangle$$

Using the property of the XOR gate, $y + y = 0$, the resultant state of of the above equation can be written as:

$$|\mathbf{x}\rangle |y + F(\mathbf{x}) + F(\mathbf{x})\rangle = |\mathbf{x}\rangle |y + 0\rangle = |\mathbf{x}\rangle |y\rangle$$

This implies that applying the Boolean function bit oracle, U_F twice is the same as applying the identity gate (or no gate). This implies that:

$$U_F^{-1} = U_F$$

and since, U_F is also unitary (as it is a quantum gate), $U_F^{-1} = U_F^\dagger$, this when used with the previous result proves the statement.

$$U_F^\dagger = U_F$$