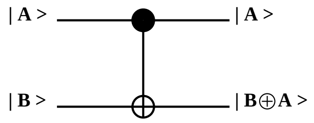
Quantum Computing - Solutions 3

Abbas Edalat

1. Check that the matrix representing CNOT in the standard computational basis is the one given in Figure 1 and that it is unitary.



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Figure 1: The CNOT gate

Solution: The action of CNOT is:

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

In terms of numerical indices:

$$|0\rangle \mapsto |0\rangle,\ |1\rangle \mapsto |1\rangle,\ |2\rangle \mapsto |3\rangle,\ |3\rangle \mapsto |2\rangle.$$

The matrix corresponding to this is therefore as given above. Since its rows form an orthonormal basis, this matrix is unitary.

2. Show that the circuit on the left in Figure 2, swaps the two qubits. It is denoted by the figure on the right.

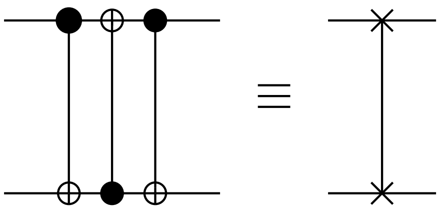


Figure 2: Swapping Gate

Solution: We have:

$$\begin{array}{l} |00\rangle \mapsto |00\rangle \mapsto |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \mapsto |11\rangle \mapsto |10\rangle \\ |10\rangle \mapsto |11\rangle \mapsto |01\rangle \mapsto |01\rangle \\ |11\rangle \mapsto |10\rangle \mapsto |10\rangle \mapsto |11\rangle \end{array}$$

Hence, with numerical indices we have:

$$
\begin{aligned}
|0\rangle &\mapsto |0\rangle \\
|1\rangle &\mapsto |2\rangle \\
|2\rangle &\mapsto |1\rangle \\
|3\rangle &\mapsto |3\rangle
\end{aligned}
$$

Therefore the matrix is:

$$
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
$$

3. There is nothing special about the control bit in the CNOT gate to take value one. The control gate in Figure 3 flips the target bit if the control bit is zero. This is represented pictorially by a hollow circle instead of the filled circle on the top line. What is its matrix representation?

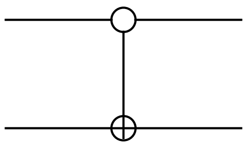


Figure 3: A variation of CNOT

Solution:

$$
\begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
$$

4. Check that the Toffoli gate (Figure 4) transformation is unitary, and thus can be implemented as a quantum gate.

IN			OUT		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

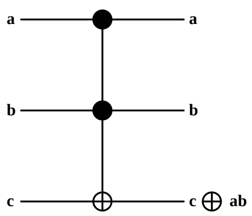


Figure 4: The Toffoli gate

Solution: We have: $|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto |1\rangle$, $|2\rangle \mapsto |2\rangle$, $|3\rangle \mapsto |3\rangle$, $|4\rangle \mapsto |4\rangle$, $|5\rangle \mapsto |5\rangle$, $|6\rangle \mapsto |7\rangle$, $|7\rangle \mapsto |6\rangle$. Hence the map is a simple permutation of basis vectors and is thus unitary as its rows form an orthonormal basis.

5.

(i) Show the bilinearity property: $(\alpha v + \alpha' v') \otimes (\beta w + \beta' w') =$
$\alpha\beta v \otimes w + \alpha\beta' v \otimes w' + \alpha'\beta v' \otimes w + \alpha'\beta' v' \otimes w'$,
where $\alpha, \alpha', \beta, \beta' \in \mathbb{C}$, $v, v' \in \mathbb{C}^k$, $w, w' \in \mathbb{C}^l$.

(ii) Show that $b_i^k \otimes b_j^l = b_{(i-1)l+j}^{kl}$.

(iii) Show that for $v, v' \in \mathbb{C}^k$ and $w, w' \in \mathbb{C}^l$ we have: $\langle v \otimes w | v' \otimes w' \rangle = \langle v|v'\rangle\langle w|w'\rangle$.

Solution:

(i) Assume $- \otimes - : \mathbb{C}^k \times \mathbb{C}^l \to \mathbb{C}^{kl}$. Then there are k blocks of l-column vectors in $v \otimes w$ for any $v \in \mathbb{C}^k$ and $w \in \mathbb{C}^l$. We show that the jth column in $(\alpha v + \alpha' v') \otimes (\beta w + \beta' w')$ is equal to the jth column in $\alpha\beta v \otimes w + \alpha\beta' v \otimes w' + \alpha'\beta v' \otimes w + \alpha'\beta' v' \otimes w'$ are equal:

$$(\alpha v + \alpha' v')_j(\beta w + \beta' w') = (\alpha v_j + \alpha' v'_j)(\beta w + \beta' w')$$

$$= \alpha\beta v_j w + \alpha\beta' v_j w' + \alpha'\beta v'_j w + \alpha'\beta' v'_j w'.$$

(ii) This follows easily by induction on i. For $i = 1$, the statement is clear. Assuming the statement to be true for i, we have $b_i^k \otimes b_l^l = b_{(i-1)l+l}^{kl} = b_{il}^{kl}$. Hence $b_{i+1}^k \otimes b_j^l = b_{il+j}^{kl}$.

(iii) The contribution to $\langle v \otimes w | v' \otimes w' \rangle$ from the jth blocks in $v \otimes w$ and $v' \otimes w'$ is $v_j^* v'_j \langle w|w'\rangle$. Hence the sum of contributions from all blocks is $\sum_{j=1}^k v_j^* v'_j \langle w|w'\rangle = \langle v|v'\rangle\langle w|w'\rangle$.

6.

(i) Show that:
$$(M \otimes N)(v \otimes w) = (Mv) \otimes (Nw).$$

(ii) Show the bilinearity property:

$$(\alpha M + \alpha' M') \otimes (\beta N + \beta' N') =$$

$$\alpha\beta M \otimes N + \alpha\beta' M \otimes N' + \alpha'\beta M' \otimes N + \alpha'\beta' M' \otimes N'.$$

(iii) Show that:
$$(M \otimes N)(M' \otimes N') = (MM') \otimes (NN').$$

(iv) Show that

$$\begin{aligned}(M \otimes N)^* &= M^* \otimes N^*,\\ (M \otimes N)^T &= M^T \otimes N^T\\ (M \otimes N)^\dagger &= M^\dagger \otimes N^\dagger.\end{aligned}$$

(v) Show that $M \otimes N$ is unitary (invertible) if M and N are unitary (invertible).

Solution:

(i) The coefficient of the ith Nw block of $Mv) \otimes (Nw)$ is $(Mv)_i = \sum_{j=1}^k M_{ij} v_j$ and the coefficient of the ith Nw block of $(M \otimes N)(v \otimes w)$ is $\sum_{j=1}^k M_{ij} v_j$.

(ii) The the $l \times l$ matrix of the ij block on the left hand side is equal to: $(\alpha M_{ij} + \alpha' M'_{ij})(\beta N + \beta' N')$ which is also the $l \times l$ matrix of the ij block on right left hand side.

(iii) The coefficient of the ij block of the NN' matrix on both sides are equal: $\sum_t M_{it} N_{tj} = (MN)_{ij}$.

(iv)
- This follows from the fact that for any two complex numbers u and v we have: $(uv)^* = u^* v^*$. In fact, the ij block of $M \otimes N$ is $M_{ij} N$ which implies that the ij block of $(M \otimes N)^*$ is $M_{ij}^* N^*$ which is the ij block of $M^* \otimes N^*$.
- The ij block of $(M \otimes N)^T$ is $M_{ji} N^T$ which is the ij block of $M^T \otimes N^T$.
- This follows from the last two parts as $M^\dagger = (M^*)^T$.

(v) If M and N are invertible then by part(iii), we have: $(M \otimes N)(M^{-1} \otimes N^{-1}) = (MM^{-1}) \otimes (NN^{-1}) = I \otimes I = I$. Hence $M \otimes N$ is invertible with inverse $M^{-1} \otimes N^{-1}$. Next suppose, M and N are unitary. Then M and N are invertible with inverses $M^\dagger$ and $N^\dagger$ respectively. Hence, $M \otimes N$ is invertible and, by part (iv), $(M \otimes N)^\dagger = M^\dagger \otimes N^\dagger = M^{-1} \otimes N^{-1} = (M \otimes N)^{-1}$.