Quantum Computing - Solutions 4

Abbas Edalat

1. Show that if for a single qubit unitary operation U we have $U = V^2$ where V is another single qubit unitary operation, then the double controlled U gate, called $\mathsf{C}^2(U)$ gate, can be implemented as in Figure 1. Show that for $V = (1-i)(I + iX)/2$ this implements the Toffoli gate.

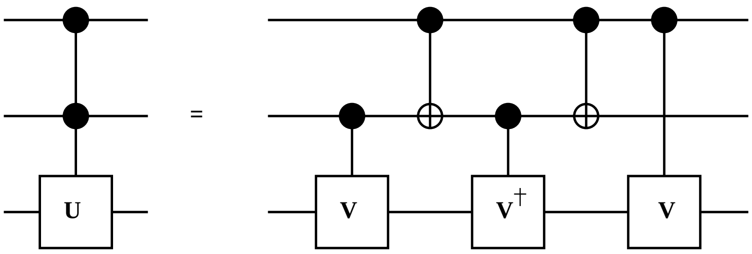

Figure 1: Implementation of $C^2(U)$

Solution: We have the following step by step transformation of the input, where x denotes the third qubit:

$$|00x\rangle \mapsto |00x\rangle \mapsto |00x\rangle \mapsto |00x\rangle \mapsto |00x\rangle \mapsto |00x\rangle.$$

$$|01x\rangle \mapsto |01Vx\rangle \mapsto |01V^\dagger Vx\rangle = |01x\rangle \mapsto |01x\rangle \mapsto |01x\rangle \mapsto |01x\rangle.$$

$$|10x\rangle \mapsto |10x\rangle \mapsto |11x\rangle \mapsto |11V^\dagger x\rangle \mapsto |10V^\dagger x\rangle \mapsto |10VV^\dagger x\rangle = |10x\rangle.$$

$$|11x\rangle \mapsto |11Vx\rangle \mapsto |10Vx\rangle \mapsto |10Vx\rangle \mapsto |11Vx\rangle \mapsto |11VVx\rangle = |11Ux\rangle.$$

Hence the network implements the $\mathsf{C}^2(\mathsf{U})$ gate. If $V = (1-i)(I + iX)/2$, then $V^2 = (1-i)^2(I - X^2 + 2iX)/4 = -2i(2iX)/4 = X$ and hence the network implements $\mathsf{C}^2(\mathsf{X}) = \mathsf{C}^2(\mathsf{NOT})$, which is the Toffoli gate.

2. Check that $XYX = -Y$ and $XZX = -Z$; then show that $XR_y(\theta)X = R_y(-\theta)$ and $XR_z(\theta)X = R_z(-\theta)$.

Solution: It is easy to check the first two equations. We now have

$$R_y(\theta) = e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y,$$

Hence $XR_y(\theta)X = \cos\frac{\theta}{2}I + i\sin\frac{\theta}{2}Y = \cos\frac{\theta}{2}I - i\sin\frac{-\theta}{2}Y$. Similarly for $XR_z(\theta)X$.

3. Assuming that the single qubit operation U is given as in the lecture notes (page 58) by $U = e^{i\alpha}AXBXC$ with $ABC = I$, show that the network in Figure 2 implements the controlled U gate, $\mathsf{C(U)}$, using the single qubit gate X the phase gate α and the single qubit gates A, B and C.

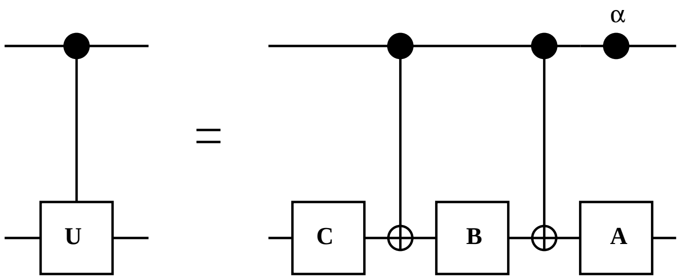

Figure 2: Implementation of $C(U)$

Solution: First recall that the phase gate α has matrix $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$ and hence it has action:

$$|0\rangle \mapsto |0\rangle, \qquad |1\rangle \mapsto e^{i\alpha}|1\rangle.$$

Therefore, we have the following input-output for the network:

$$|0\rangle \otimes |x\rangle \mapsto |0\rangle \otimes ABC|x\rangle = |0\rangle \otimes |x\rangle,$$

$$|1\rangle \otimes |x\rangle \mapsto e^{i\alpha}|1\rangle \otimes AXBXC|x\rangle = e^{i\alpha}|1\rangle \otimes e^{-i\alpha}U|1\rangle = |1\rangle \otimes U|1\rangle.$$

4. Show that the $\mathsf{C^n(U)}$ gate, where U is single qubit unitary operation, can be implemented using $n-1$ work qubits with input $|0\rangle$ as in the network in Figure 3, depicted for $n = 5$. Deduce that any such $\mathsf{C^n(U)}$ gate can be implemented by $O(n)$ single qubit and CNOT gates.

Solution: If all of the controlled qubits are $|1\rangle$ then the all the $|0\rangle$ inputs of the work qubits are flipped and hence the control is set for the controlled U gate. Therefore in this case for the target qubit we get: $|\psi\rangle \mapsto U|\psi\rangle$; the work qubits are then flipped back to $|0\rangle$ (and the control bits are clearly intact). If on the other hand, any of the controlled qubits is $|0\rangle$, then the input $|0\rangle$ to the connected work qubit and all its underneath work qubits go through intact and hence the control qubit on the controlled U gate is not set. Therefore in this case for the target qubit we get: $|\psi\rangle \mapsto |\psi\rangle$; the flipped work qubits are then flipped back to $|0\rangle$ (and the control bits are again clearly intact).

Each Toffoli gate can be implemented by $O(1)$ CNOT and single qubit gates. The $\mathsf{C(U)}$ gate also needs $O(1)$ CNOT and single qubit gates. Hence the

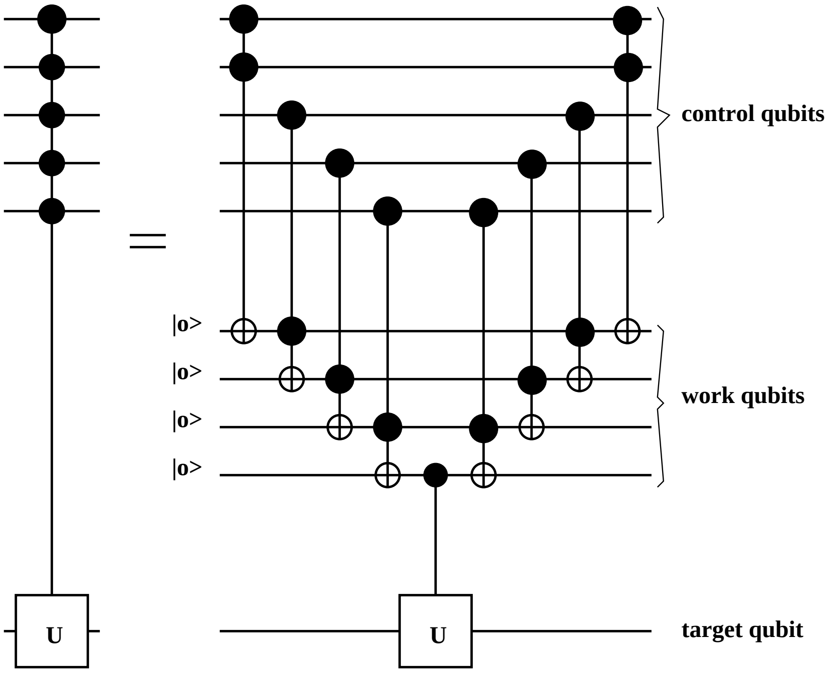

Figure 3: Implementation of $C^n(U)$

$2(n-1)$ Toffoli gates in the network and the $\mathsf{C(U)}$ gate can be implemented using $O(n)$ CNOT and single qubit gates.

5. Let U be the two-level matrix

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}$$

Then the the non-trivial levels correspond to $s = 000$ and $t = 111$.

(i) Check that if we use the Gray Code sequence $000 \to 001 \to 011 \to 111$, then from Algorithm 4.9 in the notes (page 54), we obtain the network in Figure 4.

(ii) Check directly that the network in Figure 4 actually implements U.

(iii) What is the matrix for the change of basis corresponding to the two controlled gates in the network in Figure 4?

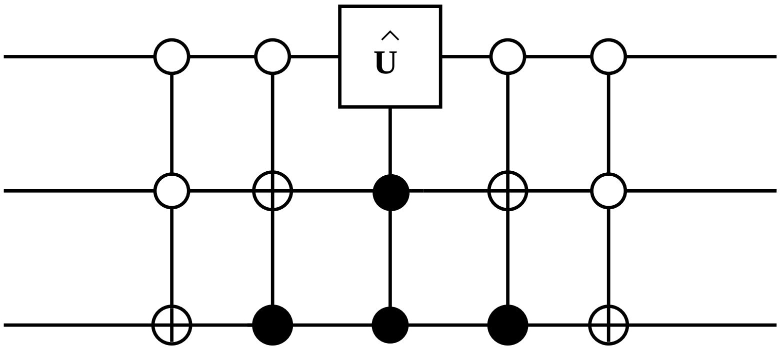

Figure 4: Network for a two-level unitary operation

Solution: (i) The $\mathsf{C}^2(\mathsf{NOT})$ gate corresponding to the first transition $000 \to 001$ flips the third qubit conditioned on the first two qubits to have value 0, whereas the $\mathsf{C}^2(\mathsf{NOT})$ gate corresponding to the second transition $001 \to 011$ flips the second qubit conditioned on the first and the third qubits to have value 0 and 1 respectively. Finally, in the last transition $011 \to 111$, the first qubit is flipped which tells us that the controlled U gate has the first qubit as target. Hence, we obtain Figure 4.

(ii) We have

$$\hat{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix},$$

so that $\hat{U}|0\rangle = a|0\rangle + b|1\rangle$ and $\hat{U}|1\rangle = c|0\rangle + d|1\rangle$. Then the step by step transformation of the input is given by:

$$|000\rangle \mapsto |001\rangle \mapsto |011\rangle \mapsto (a|0\rangle + b|1\rangle)|11\rangle \mapsto a|001\rangle + b|111\rangle \mapsto a|000\rangle + b|111\rangle.$$

$$|001\rangle \mapsto |000\rangle \mapsto |000\rangle \mapsto |000\rangle \mapsto |000\rangle \mapsto |001\rangle.$$

$$|010\rangle \mapsto |010\rangle \mapsto |010\rangle \mapsto |010\rangle \mapsto |010\rangle \mapsto |010\rangle.$$

$$|011\rangle \mapsto |011\rangle \mapsto |001\rangle \mapsto |001\rangle \mapsto |011\rangle \mapsto |011\rangle.$$

$$|100\rangle \mapsto |100\rangle \mapsto |100\rangle \mapsto |100\rangle \mapsto |100\rangle \mapsto |100\rangle.$$

$$|101\rangle \mapsto |101\rangle \mapsto |101\rangle \mapsto |101\rangle \mapsto |101\rangle \mapsto |101\rangle.$$

$$|110\rangle \mapsto |110\rangle \mapsto |110\rangle \mapsto |110\rangle \mapsto |110\rangle \mapsto |110\rangle.$$

$$|111\rangle \mapsto |111\rangle \mapsto |111\rangle \mapsto (c|0\rangle + d|1\rangle)|11\rangle \mapsto (c|0\rangle + d|1\rangle)|11\rangle \mapsto c|001\rangle + d|111\rangle.$$

This is precisely the action of U on the basis elements.

(iii) Recall that the matrix for the change of basis B induces: $U = B^{-1}VB$ where V is the matrix representation in the new basis. In our example, V is the controlled $\hat{U}$ gate and B is the composition of the first two controlled flip operations. Hence, B has action:

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

Or:

$$|0\rangle \mapsto |3\rangle$$
$$|1\rangle \mapsto |0\rangle.$$
$$|2\rangle \mapsto |2\rangle.$$
$$|3\rangle \mapsto |1\rangle.$$
$$|4\rangle \mapsto |4\rangle.$$
$$|5\rangle \mapsto |5\rangle.$$
$$|6\rangle \mapsto |6\rangle.$$
$$|7\rangle \mapsto |7\rangle$$

Hence,

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