QOSF : Task 3 - Decompose

Ankit Kumar Jha

Contents

1 The U and the X gate

The U gate as given is :

$$U(\theta,\phi,\lambda) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda}\sin\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) & e^{i(\phi+\lambda)}\cos\left(\frac{\theta}{2}\right) \end{bmatrix} \tag{1}$$

It basically rotates a vector in the block sphere by the Eulerian angles θ, λ and ϕ.

Similarly, we have the X gate given by :

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2}$$

Since, $|0\rangle = [1 \quad 0]^\dagger$ and $|1\rangle = [0 \quad 1]^\dagger$, we can also write :

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{3}$$

Let us look at its action on $|0\rangle$ and $|1\rangle$:

$$\begin{aligned} X|0\rangle &= |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle = |1\rangle \\ X|1\rangle &= |0\rangle\langle 1|1\rangle + |1\rangle\langle 0|1\rangle = |0\rangle \end{aligned} \tag{4}$$

Thus, the first term $|0\rangle\langle 1|$ becomes $|0\rangle$ when the acting on $|1\rangle$ while the second term goes to 0. When input is $|0\rangle$, the first term goes to 0 while the second term $|1\rangle\langle 0|$ takes $|0\rangle$ to $|1\rangle$. Its utility is thus just to flip the bit of the qubit from 0 to 1 and vice versa.

We start by noting that $U(0,0,0) = I$, where I is the identity gate :

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{5}$$

2 The CX gate from U and X gates

The CX gate is given by :

$$CX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{6}$$

We see that this is equivalent to writing :

$$CX = \begin{bmatrix} I & O_{2\times 2} \\ O_{2\times 2} & X \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes I + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes X \tag{7}$$

In terms of $|0\rangle$ and $|1\rangle$ this gives :

$$CX = \begin{bmatrix} I & O_{2\times 2} \\ O_{2\times 2} & X \end{bmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \tag{8}$$

Let us try to understand this structure by again looking at its action to various systems :

$$\begin{aligned} CX|00\rangle &= |0\rangle\langle 0|0\rangle \otimes I|0\rangle + |1\rangle\langle 1|0\rangle \otimes X|0\rangle = |00\rangle \\ CX|01\rangle &= |0\rangle\langle 0|0\rangle \otimes I|1\rangle + |1\rangle\langle 1|0\rangle \otimes X|1\rangle = |01\rangle \\ CX|10\rangle &= |0\rangle\langle 0|1\rangle \otimes I|0\rangle + |1\rangle\langle 1|1\rangle \otimes X|0\rangle = |11\rangle \\ CX|11\rangle &= |0\rangle\langle 0|1\rangle \otimes I|1\rangle + |1\rangle\langle 1|1\rangle \otimes X|1\rangle = |10\rangle \end{aligned} \tag{9}$$

What we notice is that the first-system (the single-qubit operator before the kronecker product) controls which gate will be operated on the second qubit while keeping the first-qubit intact. When first qubit is $|0\rangle$ the second term vanishes and hence I gate acts on the second qubit thereby resulting in no-change in the inputs. When first qubit is $|1\rangle$, the first term vanishes and the X gate operates on the second qubit thereby resulting in the flip. This is how the control bit-flip is obtained.

We can already see a pattern emerging but let us keep going.

3 The CCX gate from U and X gates

The CCX gate is given by :

$$\text{CCX} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{10}$$

This can equivalently be written as :

$$CCX = \begin{bmatrix} I & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} \\ O_{2\times 2} & I & O_{2\times 2} & O_{2\times 2} \\ O_{2\times 2} & O_{2\times 2} & I & O_{2\times 2} \\ O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \otimes I + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \otimes X \tag{11}$$

We can simplify this by decomposing the 4×4 matrices further :

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes I + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes |0\rangle\langle 0| \tag{12}$$

Similarly,

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = |1\rangle\langle 1| \otimes |1\rangle\langle 1| \tag{13}$$

Thus,

$$\text{CCX} = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes X \tag{14}$$

The three terms can be interpreted as follows :

- If the first qubit is $|0\rangle$ then we want the operator to return the 3 qubits unchanged. This is done by the first term while the rest of the terms vanish.
- If the first qubit is $|1\rangle$ then we check the second qubit. If it is $|0\rangle$ then we do not want a bit-flip on the third qubit. This is done by the second term while the other two terms vanish.
- If both first and second qubit are $|1\rangle$, then we do want a bit-flip on the third qubit. This is done by the third term while the rest vanish.

Thus again, the first two single-qubit operators check the first two-qubits and decide the gate acting on the third-qubit. Only when both the first two qubits are $|1\rangle$ does X act on the third qubit. Otherwise I acts on the third qubit. We now have a concrete pattern which we will use to construct CCCX.

4 CCCX gate for U and X gates

The terms we expect are as follows :

- if the first qubit is $|0\rangle$, return everything as it is. Then first term must look like

$$|0\rangle\langle 0| \otimes I \otimes I \otimes I$$

- if the first qubit is $|1\rangle$, look at the second qubit. If it is $|0\rangle$, then again return everything as it is. This term must look as follows :

$$|1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I \otimes I$$

- if the second qubit is also $|1\rangle$. Check for the third qubit. If it is $|0\rangle$, return everything as it is. This term must look like :

$$|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I$$

- if all first three qubits are $|1\rangle$ then flip the last qubit. This term looks like :

$$|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes X$$

Hence, adding these terms together we have,

$$\text{CCCX} = |0\rangle\langle 0| \otimes I \otimes I \otimes I + |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes X \tag{15}$$

In the matrix representation this is given in the decomposed form as :

$$\text{CCCX} = \begin{bmatrix} I & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} \\ O_{2\times 2} & I & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} \\ O_{2\times 2} & O_{2\times 2} & I & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} \\ O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & I & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} \\ O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & I & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} \\ O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & I & O_{2\times 2} & O_{2\times 2} \\ O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & I & O_{2\times 2} \\ O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & O_{2\times 2} & X \end{bmatrix} \tag{16}$$

where, the first term is responsible for the first 4 Is on the diagonal, the second term is responsible for the next 2 Is, the third term for the last I on the diagonal whereas the last term adds the X.

$$\text{CCCX} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}$$

5 Generalization

As such, the general $C^n X$ gate looks is given by :

$$\text{C}^n\text{X} = \sum_{i=0}^{n-1} |1\rangle\langle 1|^{\otimes i} \otimes |0\rangle\langle 0| \otimes I^{\otimes(n-i)} + |1\rangle\langle 1|^{\otimes n} X \tag{17}$$

The corresponding matrix decomposition will be of the form (16) but size $2^{n+1} \times 2^{n+1}$ where ith term in the sum in Eq. (17) adds I to 2^{n-2i} of the diagonals sequentially until all diagonals except the last one is filled with Is. The last diagonal is then filled with X through the last term. This is the general decomposition of any $C^n X$ operator.

5.1 Additional remarks

If one observes, this general way of building higher qubit controlled operators is independent of X. In fact replace X with any single qubit gate in 17 and you will have the corresponding single-qubit gate controlled by n other qubits.