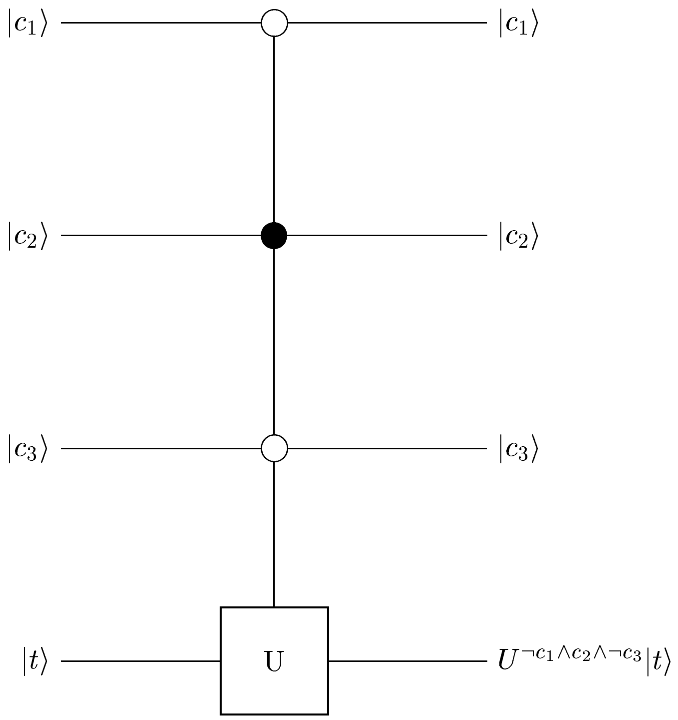
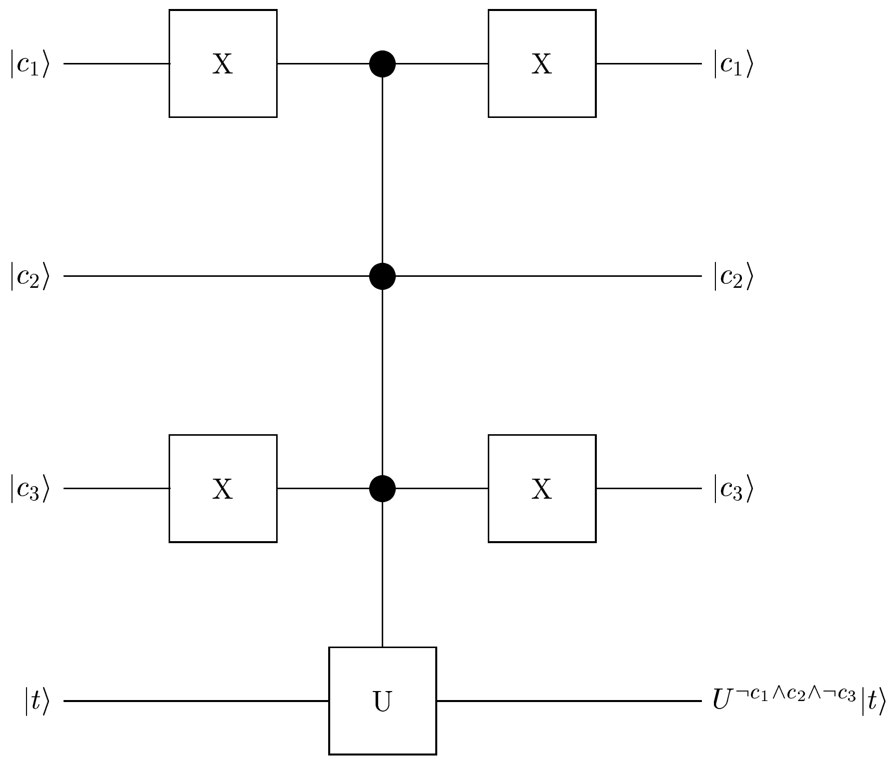
2.5.1 General Controlled Operations

In a general controlled operation, we may condition on an arbitrary combination of truth values of the control qubits as shown below. The black junction dots connecting a control variable to the box U indicate that the control is effective when the control has value 1; open dots indicate effectiveness when the value is 0.



The above controlled operation can be implemented using a standard $C^n(U)$ operation with the aid of pre- and post-X operations, as shown below.



2.6 Universality

Goal: To show that any unitary operation U acting on arbitrary number of qubits can be approximated to any desired degree of accuracy by using CNOT, Hadamard, and $\pi/8$ gates.

Measure of accuracy: Probabilities of measurement outcomes.

Steps of argument:

- Any unitary U acting on a d-dimensional Hilbert space can be written as $U = U_1 \cdots U_n$ where U_i are unitary operators acting non-trivially only on one or two-dimensional subspaces.
- Any unitary U acting non-trivially only on a subspace spanned by two measurement basis vectors can be implemented using only CNOT and and single-qubit gates.
- Any single qubit unitary operator U can be approximated arbitrarily closely by using Hadamard and $\pi/8$ gates.

2.6.1 Two-Level Decompositions

Let U be a unitary operator acting on a 3-dimensional Hilbert space with the following matrix representation in some basis $|e_1\rangle$, $|e_2\rangle$, $|e_3\rangle$:

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}.$$

Our goal is to find unitary $V_1, \ldots, V_n$ acting non-trivially only on two basis vectors at a time such that

$$V_n \cdots V_1 U = I.$$

By setting $U_i = V_i^\dagger$, we will then have the desired decomposition:

$$U = U_1 \cdots U_n.$$

The first phase of transformations will turn the first column of U into $(1,0,0)^T$.

$$\begin{aligned}
U &= \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix} \\
&\xrightarrow{V_1} \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c & f & j \end{bmatrix} \\
&\xrightarrow{V_2} \begin{bmatrix} a'' & d'' & g'' \\ 0 & e' & h' \\ 0 & f' & j' \end{bmatrix} \\
&\overset{(1)}{=} \begin{bmatrix} a'' & 0 & 0 \\ 0 & e' & h' \\ 0 & f' & j' \end{bmatrix} \\
&\xrightarrow{V_3} \begin{bmatrix} 1 & 0 & 0 \\ 0 & e' & h' \\ 0 & f' & j' \end{bmatrix}
\end{aligned}$$

Equality (1) above follows by unitarity: d'', g'' must be zero, because the columns are orthogonal.

Now, we specify the individual transformations. If $b = 0$, take $V_1 = I$. If $b \neq 0$, set

$$V_1 = \begin{bmatrix} a^*/r & b^*/r & 0 \\ b/r & -a/r & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where

$$r = \sqrt{|a|^2 + |b|^2}.$$

It is readily observed that V_1 is a rotation in $|e_1\rangle$-$|e_2\rangle$ plane.

Next, if $c = 0$, take $V_2 = I$. If $c \neq 0$, set

$$V_2 = \begin{bmatrix} a'^*/r & 0 & c'^*/r \\ 0 & 1 & 0 \\ c'/r & 0 & -a'/r \end{bmatrix}$$

where

$$r = \sqrt{|a'|^2 + |c'|^2}.$$

V_2 is a rotation in the $|e_1\rangle$-$|e_3\rangle$ plane. It should be clear how the remaining transformations are specified.

In general, for a d-dimensional unitary U, it takes at most $d-1$ two-level operations and 1 one-level operation to transform U into the following form:

$$\begin{bmatrix} a_{11} & a_{12} & \cdot & \cdot & \cdot & a_{1d} \\ a_{21} & a_{22} & \cdot & \cdot & \cdot & a_{2d} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{d1} & a_{d2} & \cdot & \cdot & \cdot & a_{dd} \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & a'_{22} & \cdot & \cdot & \cdot & a'_{2d} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & a'_{d2} & \cdot & \cdot & \cdot & a'_{dd} \end{bmatrix}.$$

By induction, it takes at most $(d-1)+(d-2)+\cdots+1 = d(d-1)/2$ two-level operations and d one-level operations to transform U to identity I. Thus, complexity of this procedure is $O(d^2)$ one or two-level operations.

2.6.2 Two-Level vs. Single-Qubit Transformations

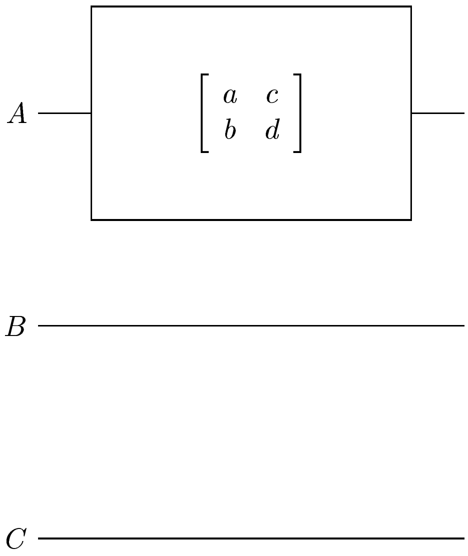
Consider the following unitary U on a 3-qubit system, expressed in the measurement basis:

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

This is a two-level operation acting non-trivially only on $|000\rangle$ and $|111\rangle$. But it is a 3-qubit operation. Can we implement U in terms of single-qubit operations? If U were

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

it would then be a two-level transformation acting on $|011\rangle$ and $|111\rangle$, i.e., only on the first qubit. Labeling the qubits as $|ABC\rangle$, this operation could be implemented as follows:



Returning to the original example, the action

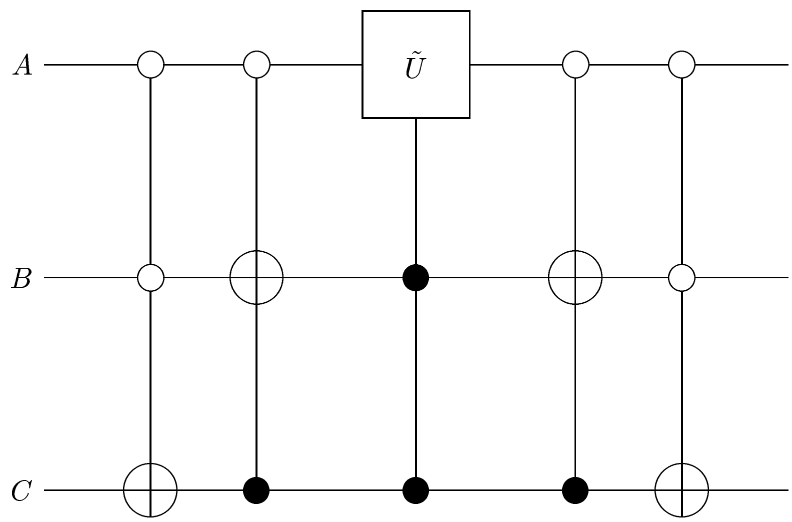
$$\begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} ax_0 + cx_7 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ bx_0 + dx_7 \end{bmatrix}$$

can be broken into single-qubit steps

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \to \begin{bmatrix} x_1 \\ x_0 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \to \begin{bmatrix} x_1 \\ x_3 \\ x_2 \\ x_0 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \to \begin{bmatrix} x_1 \\ x_3 \\ x_2 \\ ax_0 + cx_7 \\ x_4 \\ x_5 \\ x_6 \\ bx_0 + dx_7 \end{bmatrix}$$

$$\to \begin{bmatrix} x_1 \\ ax_0 + cx_7 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ bx_0 + dx_7 \end{bmatrix} \to \begin{bmatrix} ax_0 + cx_7 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ bx_0 + dx_7 \end{bmatrix}.$$

This sequence of operations can be implemented using the following circuit using only standard qubit operations that we have discussed above.



In the above diagram, $\tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$.

In general, for a two-level unitary operation affecting measurement basis states $|s\rangle$ and $|t\rangle$, we need a sequence of swap operations each affecting a single qubit that carries $|s\rangle$ to a neighbor of $|t\rangle$. This can be done using a common procedure known as Gray coding. An example suffices to illustrate this. For example, if $|s\rangle = |0000\rangle$ and $|t\rangle = |1111\rangle$, the steps of Gray coding are:

$$\begin{aligned} |s\rangle &= |0000\rangle \\ &\to |0001\rangle \\ &\to |0011\rangle \\ &\to |0111\rangle \end{aligned}$$

We now estimate the complexity of an arbitrary two-level operation in a $d = 2^n$-dimensional space consisting of n qubits. The complexity measure is how many single-qubit gates are required. We saw that in the worst case $n-1$ swap operations are required and each such operation requires n single-qubit gates. There is one controlled-U operation which also requires $O(n)$ single-qubit operations (not counting how many gates may be required for approximating U if that is necessary). The worst-case complexity is therefore $O(n^2)$.

We saw earlier that an arbitrary d-dimensional operation can be carried out as a sequence of $O(d^2)$ two-level operations. So, the worst case complexity of implementing an arbitrary $d = 2^n$-dimensional unitary operator is $O(4^n n^2)$ single-qubit operations. arbitrary $d = 2^n$ dimensional operator. It turns out this exponential complexity cannot be materially improved because it can be proven that there are operations that require a number of gates of this exponential order.