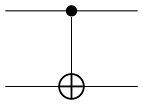
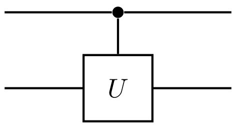
Universal set of gates

In this chapter we will show the basic principle of the construction of the quantum computer, namely the fact that any unitary operator can be constructed with the help of one-cubit operators and a single two-cubit CNOT operator, that is, the controlled negation, which we denote



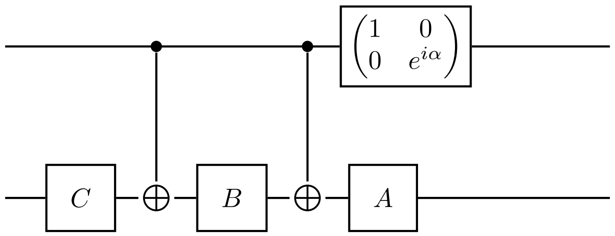
Controlled single-qubit operators. The first step is the construction of arbitrary controlled single-qubit operators. These correspond to the conditional construction “if the first qubit is one, perform the operation U on the second qubit”, schematically:



The key to the construction is to decompose any operator using X and some operators A, B and C such that

$$U = e^{i\alpha} AXBXC, \qquad\qquad ABC = E.$$

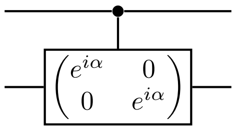
Thanks to this decomposition, we get the controlled operator U using the circuit



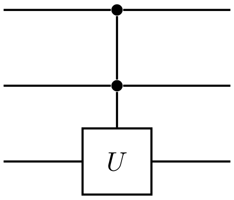
It is straightforward to verify that $|0\rangle \otimes |\varphi\rangle$ maps toa $|0\rangle \otimes |\varphi\rangle$ and $|1\rangle \otimes |\varphi\rangle$ maps to $|1\rangle \otimes U|\varphi\rangle$. Note that the matrix

$$\begin{pmatrix}1 & 0\\ 0 & e^{i\alpha}\end{pmatrix}$$

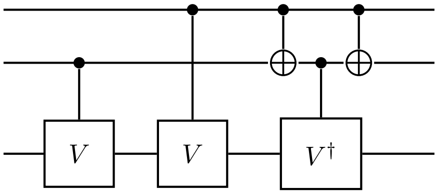
applied to the first qubit is equivalent to the controlled multiplication of the scalar matrix $e^{i\alpha}$:


$\begin{pmatrix}e^{i\alpha} & 0\\ 0 & e^{i\alpha}\end{pmatrix}$

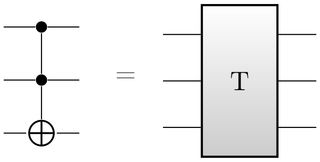
Two-controlled single-qubit operators. Next important step is the construction of two-checked operators, that is, operators that are executed just when both controlling values are one. Schematically:



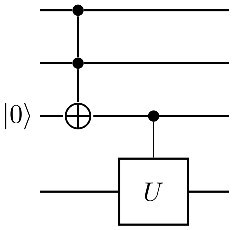
This requires the square root of the operator U, that is, an operator $V = \sqrt{U}$, such that $V^2 = U$ (see below). Two-controlled operator U is then implemented by the circuit



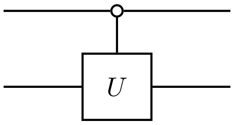
Two-controlled operator is actually an operator controlled by the conjunction of two values. Therefore, we would not need to emphasize its construction if we could implement an AND circuit, which, as we know, is possible in a reversible way using the Toffoli gate. But this is actually itself a double-checked negation (and therefore sometimes also referred to as CCNOT): :



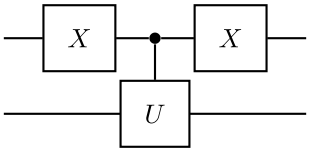
The Toffoli gate is therefore a special case of this construction and thanks to it we have all Boolean functions available, because the Toffoli gate is universal. Thus, the two-checked operator U could also be expressed by a more complex circuit with one auxiliary cubit as:



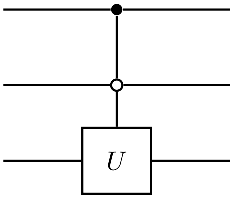
Similarly, operators controlled by any Boolean function can be constructed. If we want the operator to be applied if the value of the controlling cubite is zero, not one, then we will write schematically



which, in fact, is a shortcut for



The two options can also be combined, for instance as



On the example of the Toffoli gate, we shall show the construction of the operator V, that is, a "square root" of negation. Finding such an operator is a special case of application of a function to a normal operator. For any function $f : \mathbb{R} \to \mathbb{C}$ and a normal operator A we defined $f(A)$ as an operator satisfying

$$f(A)|u_\lambda\rangle = f(\lambda)|u_\lambda\rangle$$

for each eigenvector u_λ of the operator A, where λ is the corresponding eigenvalue. The negation is given by the Pauli operator

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

which can be written by projections on eigenvectors as

$$X = |+\rangle\langle+| - |-\rangle\langle-|,$$

where

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

From here we have

$$V = \sqrt{1}|+\rangle\langle+| + \sqrt{-1}|-\rangle\langle-|\,.$$

We have four options for choosing the pair of square roots. For $\sqrt{1} = 1$ a $\sqrt{-1} = i$ we get

$$V = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{i}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1-i}{2}\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}.$$

Conversion of two-level operators to single-qubit controlled operators. Consider the unitary operator U on a four-dimensional space given by the matrix

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

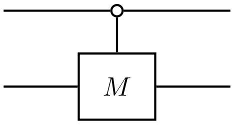
The operator acts non-identically only on the basis vectors $|00\rangle$ and $|01\rangle$, as follows:

$$|0\rangle \otimes |0\rangle \mapsto |0\rangle \otimes (a|0\rangle + c|1\rangle), \qquad |0\rangle \otimes |1\rangle \mapsto |0\rangle \otimes (b|0\rangle + d|1\rangle).$$

If we denote

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

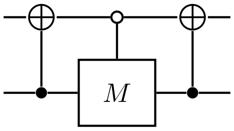
it is therefore possible to construct U as



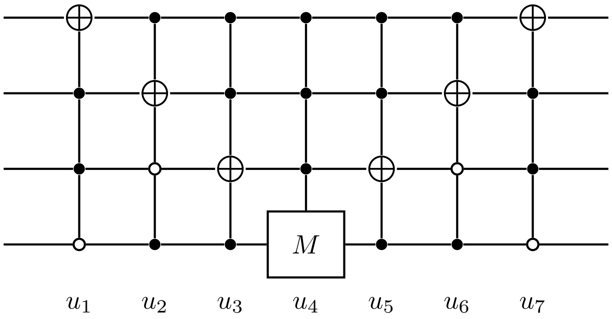
Operators acting non-identically on only two base vectors are called two-level. However, not every two-level operator has such a simple circuit as the U operator above. E.g., the operator

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

acts non-identically on the basis vectors $|00\rangle$ a $|11\rangle$, which differ in more than one place, and therefore cannot be simply written as a controlled matrix M. It is necessary to first change the basis so that the non-identically mapped vectors differ only in one place. We therefore perform a permutation that swaps $|11\rangle$ and $|01\rangle$, which is the CNOT on the first qubit controlled by the second one. Then we can proceed as in the case of U and then swap back $|11\rangle$ and $|01\rangle$. The whole circuit looks like this



n the case of a general two-level matrix acting non-identically on basis vectors $\mathbf{b} = |k_{n-1}k_{n-2}\dots k_0\rangle$ and $\mathbf{b}' = |\ell_{n-1}\ell_{n-2}\dots\ell_0\rangle$, we have to map these vectors to basis elements that differ only in one cubit. We then perform the controlled operation on it and convert the base back to its original form. In total, this means a series of operations controlled by all but one qubit that varies. Suppose, for example, that the matrix M acts non-identically on qubits $\mathbf{b} = |0110\rangle$ and $\mathbf{b}' = |1001\rangle$. We can choose base vectors, differing in only one cubit, on which we will perform the controlled operation M; for example, choose $|1110\rangle$ and $|1111\rangle$. So we have to change the first three cubits: the first in the base vector $\mathbf{b}$, the second and the third in the base vector $\mathbf{b}'$. The circuit will look like this



- u_1 and u_7: transposition $|0110\rangle \leftrightarrow |1110\rangle$
- u_2 and u_6: transposition $|1001\rangle \leftrightarrow |1101\rangle$
- u_3 and u_5: transposition $|1101\rangle \leftrightarrow |1111\rangle$
- u_4: transformation $|1110\rangle \mapsto a|1110\rangle + b|1111\rangle$; $|1111\rangle \mapsto c|1110\rangle + d|1111\rangle$

Decomposition into two-level operators. It remains to show that any unitary operator can be decomposed into unitary two-level operators. The process of such decomposition is similar to the Gaussian elimination, and the two-level matrices sought are matrices of the corresponding elementary transformations. These are always two-level: they only manipulate two lines. Unlike the classical Gaussian elimination, however, we still have to ensure that they are unitary. This is certainly true if we only swap lines (to get a non-zero element on the diagonal). Let's study the case when we want to subtract an element outside the diagonal. Let the matrix to be modified be of the form

$$U = \begin{pmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix},$$

where $U_{1,1} = a \neq 0$ and $U_{j,1} = b \neq 0$ and other elements are arbitrary. We may have ensured that a is non-zero by a permutation of rows, if needed. We now want to get rid of the element b, i.e. to set the position $(j, 1)$ to zero. We can do this by adding an appropriate multiple of the first line to the j-th line. In the case of classical Gaussian elimination we would use the matrix of elementary transformation

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ -b/a & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that if we want to avoid division (e.g. when manipulating an integer matrix), we can also use the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ b & 0 & 0 & -a & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Although neither of these matrices is unitary, it is not difficult to complete it to a unitary one by normalizing j-th row and changing the first line to a orthogonal unit vector:

$$U_1 = \begin{pmatrix} a^*/c & 0 & 0 & b^*/c & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ b/c & 0 & 0 & -a/c & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where $c = \|(a,b)\| = \sqrt{aa^* + bb^*}$. Multiplying we obtain

$$U_1 \cdot U = \begin{pmatrix} c & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} .$$

In this way we gradually convert the matrix U to

$$U' = \begin{pmatrix} a' & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} .$$

Since the resulting matrix is still unitary (we multiplied it by unitary matrices), we have $|a'| = 1$. In addition, it is clear from the last step of the elimination that $a' = 1$. Because also the rows of a unitary matrix have the norm of one, U' is actually of the form

$$U' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} .$$

Repeating the procedure for the smaller matrix, we finally get the identity matrix. We then have

$$U_k \cdots U_2 U_1 \cdot U = I \,,$$

where U_i are two-level unitary operators (some of them may be permutation matrices swapping rows). Thus we have the desired decomposition of U into two-level operators

$$U = U_1^\dagger U_1^\dagger \cdots U_k^\dagger \,.$$