Advanced Quantum Mechanics

Angelo Bassi

Academic Year 2020-21

The Qubit

A qubit is a (unit) vector in the vector space $\mathbb{C}^2$, whose basis vectors are denoted as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{3.1}$$

Physically, a qubit can be realized in many ways: polarization states of a photon, spin states of an electron, truncated two states from a many level system….

It is convenient to assume the vector $|0\rangle$ corresponds to the classical value 0, while $|1\rangle$ to 1 in quantum computation. Moreover it is possible for a qubit to be in a superposition state:

$$|\psi\rangle = a|0\rangle + b|1\rangle \text{ with } a, b \in \mathbb{C}, \ |a|^2 + |b|^2 = 1. \tag{3.2}$$

It is useful, for many purposes, to express a state of a single qubit graphically. Let us parameterize a one-qubit state $|\psi\rangle$ with θ and ϕ as

$$|\psi(\theta,\phi)\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle. \tag{3.3}$$

We are not interested in the overall phase, and the phase of $|\psi\rangle$ is fixed in such a way that the coefficient of $|0\rangle$ is real. Now we show that $|\psi(\theta,\phi)\rangle$ is an eigenstate of $\hat{\boldsymbol{n}}(\theta,\phi)\cdot\boldsymbol{\sigma}$ with the eigenvalue $+1$. Here $\boldsymbol{\sigma} = (\sigma_x,\sigma_y,\sigma_z)$ and $\hat{\boldsymbol{n}}(\theta,\phi)$ is a real unit vector called the **Bloch vector** with components

$$\hat{\boldsymbol{n}}(\theta,\phi) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)^t.$$

In fact, a straightforward calculation shows that

$$\begin{aligned}\hat{\boldsymbol{n}}(\theta,\phi)\cdot\boldsymbol{\sigma}|\psi(\theta,\phi)\rangle &= \begin{pmatrix}\cos\theta & \sin\theta e^{-i\phi}\\ \sin\theta e^{i\phi} & -\cos\theta\end{pmatrix}\begin{pmatrix}\cos\frac{\theta}{2}\\ e^{i\phi}\sin\frac{\theta}{2}\end{pmatrix}\\ &= \begin{pmatrix}\cos\frac{\theta}{2}\cos\theta + \sin\frac{\theta}{2}\sin\theta\\ e^{i\phi}\left(\cos\frac{\theta}{2}\sin\theta - \cos\theta\sin\frac{\theta}{2}\right)\end{pmatrix}\\ &= \begin{pmatrix}\cos\frac{\theta}{2}\\ e^{i\phi}\sin\frac{\theta}{2}\end{pmatrix} = |\psi(\theta,\phi)\rangle.\end{aligned}$$

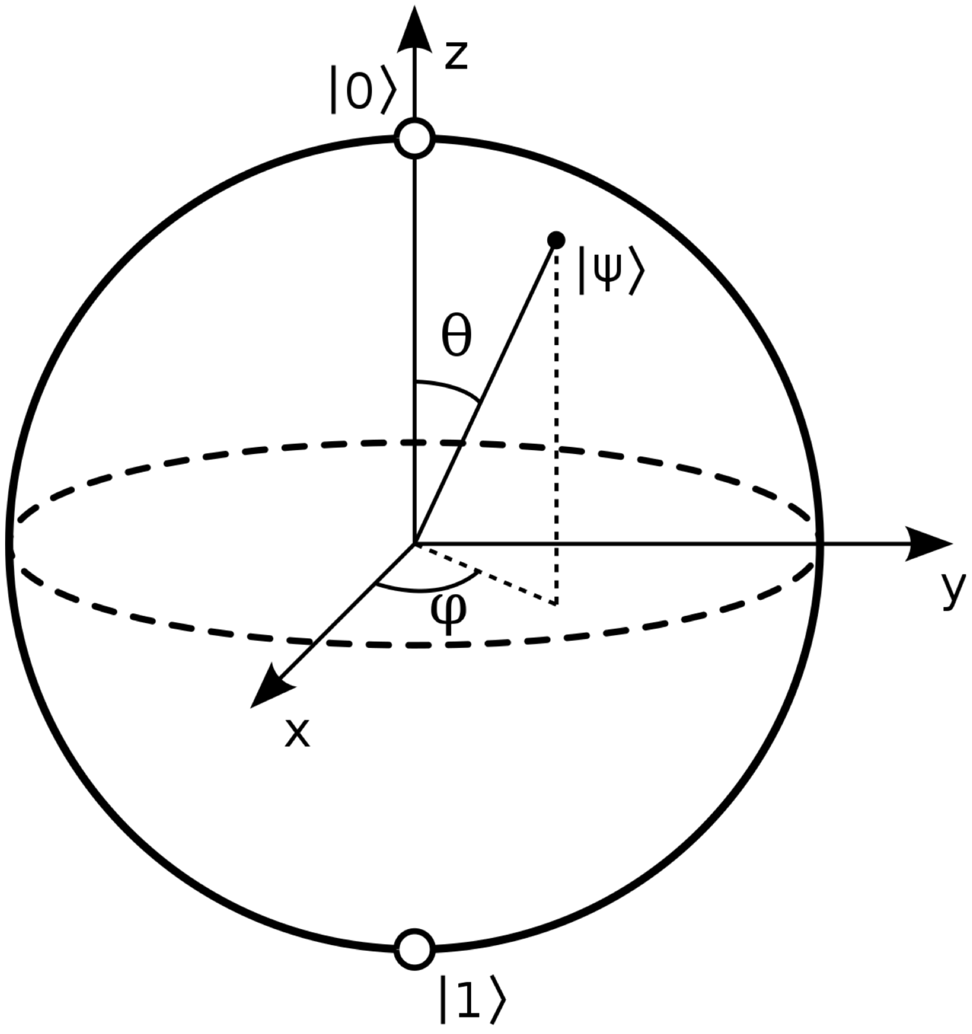
It is therefore natural to assign a unit vector $\hat{\boldsymbol{n}}(\theta,\phi)$ to a state vector $|\psi(\theta,\phi)\rangle$. Namely, a state $|\psi(\theta,\phi)\rangle$ is expressed as a unit vector $\hat{\boldsymbol{n}}(\theta,\phi)$ on the surface of the unit sphere, called the **Bloch sphere**. This correspondence is one-to-one if the ranges of θ and ϕ are restricted to $0\le\theta\le\pi$ and $0\le\phi<2\pi$.

EXERCISE 3.1 Let $|\psi(\theta,\phi)\rangle$ be the state given by Eq. (3.3). Show that

$$\langle\psi(\theta,\phi)|\boldsymbol{\sigma}|\psi(\theta,\phi)\rangle = \hat{\boldsymbol{n}}(\theta,\phi), \tag{3.4}$$

where $\hat{\boldsymbol{n}}$ is the unit vector defined above.

Bloch sphere



Multi-qubit systems

$$|\psi\rangle = \sum_{i_k=0,1} a_{i_1 i_2 \dots i_n} |i_1\rangle \otimes |i_2\rangle \otimes \dots \otimes |i_n\rangle$$

and lives in a 2^n-dimensional complex vector space. Note that $2^n \gg 2n$ for a large number n. The ratio $2^n/2n$ is $\sim 6.3 \times 10^{27}$ for $n = 100$ and $\sim 5.4 \times 10^{297}$ for $n = 1000$. These astronomical numbers tell us that most quantum states in a Hilbert space with large n are entangled, i.e., they do not have classical analogy which tensor product states have. Entangled states that have no classical counterparts are extremely powerful resources for quantum computation and quantum communication as we will show later.

Let us consider a system of two qubits for definiteness. The combined system has a basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. More generally, a basis for a system of n qubits may be taken to be $\{|b_{n-1}b_{n-2}\dots b_0\rangle\}$, where $b_{n-1}, b_{n-2}, \dots, b_0 \in \{0, 1\}$. It is also possible to express the basis in terms of the decimal system. We write $|x\rangle$, instead of $|b_{n-1}b_{n-2}\dots b_0\rangle$, where $x = b_{n-1}2^{n-1} + b_{n-2}2^{n-2} + \dots + b_0$ is the decimal expression of the binary number $b_{n-1}b_{n-2}\dots b_0$. Thus the basis for a two-qubit system may be written also as $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ with this decimal notation. Whether the binary system or the decimal system is employed should be clear from the context. An n-qubit system has $2^n = \exp(n \ln 2)$ basis vectors.

Example: two qubits

|10> $\rightarrow$ $b_0 = 0$, $b_1 = 1$

Decimal expression:

|x>, with

$x = 1 \times 2^1 + 0 \times 2^0 = 2$

The set

$$\begin{aligned} \{|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\} \end{aligned} \tag{3.8}$$

is an orthonormal basis of a two-qubit system and is called the **Bell basis**. Each vector is called the **Bell state** or the **Bell vector**. Note that all the Bell states are entangled.

EXERCISE 3.4 The Bell basis is obtained from the binary basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ by a unitary transformation. Write down the unitary transformation explicitly.

Among three-qubit entangled states, the following two states are important for various reasons and hence deserve special names. The state

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{3.9}$$

is called the **Greenberger-Horne-Zeilinger state** and is often abbreviated as the **GHZ state**[3]. Another important three-qubit state is the **W state** [4],

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle). \tag{3.10}$$

EXERCISE 3.5 Find the expectation value of $\sigma_x \otimes \sigma_z$ measured in each of the Bell states.

Examples

Measurements

Let us analyze measurements in a two-qubit system in some detail. An arbitrary state is written as

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \quad |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1,$$

where $a, b, c, d \in \mathbb{C}$. We make a measurement of the first qubit with respect to the basis $\{|0\rangle, |1\rangle\}$. To this end, we rewrite the state as

$$\begin{aligned}
&a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \\
&= |0\rangle \otimes (a|0\rangle + b|1\rangle) + |1\rangle \otimes (c|0\rangle + d|1\rangle) \\
&= u|0\rangle \otimes \underbrace{\left(\frac{a}{u}|0\rangle + \frac{b}{u}|1\rangle\right)}_{\text{normalized}} + v|1\rangle \otimes \underbrace{\left(\frac{c}{v}|0\rangle + \frac{d}{v}|1\rangle\right)}_{\text{normalized}}, \quad u = \sqrt{|a|^2 + |b|^2} \text{ and } v = \sqrt{|c|^2 + |d|^2}.
\end{aligned}$$

$|u|^2$ = probability

$|v|^2$ = probability

Compare with the calculation we did in the classical probabilistic case.

Quantum Computation

DEFINITION 4.1 (**Quantum Computation**) A quantum computation is a collection of the following three elements:

(1) A register or a set of registers,

(2) A unitary matrix U, which is taylored to execute a given quantum algorithm, and

(3) Measurements to extract information we need.

More formally, we say a quantum computation is the set $\{\mathcal{H}, U, \{M_m\}\}$, where $\mathcal{H} = \mathbb{C}^{2^n}$ is the Hilbert space of an n-qubit register, $U \in \mathrm{U}(2^n)$ represents the quantum algorithm and $\{M_m\}$ is the set of measurement operators.

The hardware (1) along with equipment to control the qubits is called a quantum computer.

Single Qubit Quantum Gates

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$$Y = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\sigma_y,$$

$$X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x,$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z.$$

The transformation I is the trivial (identity) transformation, while X is the negation (NOT), Z the phase shift and $Y = XZ$ the combination of them. It is easily verified that these gates are unitary.

Exercise: Find the Hamiltonian that implements these gates, and show how they are implemented.

Hadamard Gate

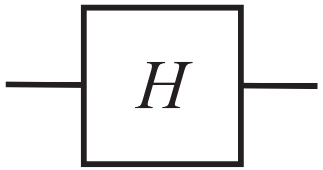
The **Hadamard gate** or the **Hadamard transformation** H is an important unitary transformation defined by

$$\begin{aligned} U_{\mathrm{H}} : |0\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{4.9}$$

It is used to generate a superposition state from $|0\rangle$ or $|1\rangle$. The matrix representation of H is

$$U_{\mathrm{H}} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{4.10}$$

A Hadamard gate is depicted as



Hadamard Gate

There are numerous important applications of the Hadamard transformation. All possible 2^n states are generated, when U_{H} is applied on each qubit of the state $|00\ldots0\rangle$:

$$\begin{aligned}
&(H \otimes H \otimes \ldots \otimes H)|00\ldots0\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \ldots \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \qquad (4.11)
\end{aligned}$$

Therefore, we produce a superposition of all the states $|x\rangle$ with $0 \leq x \leq 2^n - 1$ simultaneously. This action of H on an n-qubit system is called the **Walsh transformation**, or **Walsh-Hadamard transformation**, and denoted as W_n. Note that

$$W_1 = U_{\mathrm{H}}, \quad W_{n+1} = U_{\mathrm{H}} \otimes W_n. \qquad (4.12)$$

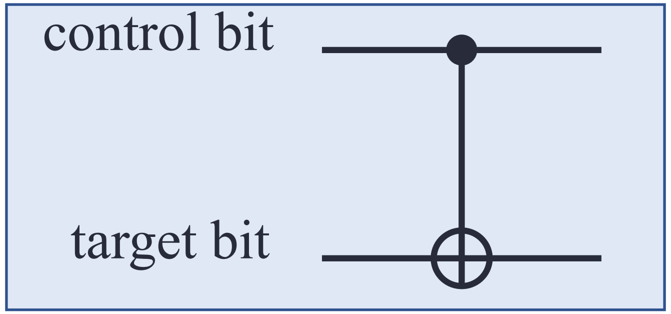
Two qubit gates: CNOT Gate

The **CNOT** (**controlled-NOT**) gate is a two-qubit gate, which plays quite an important role in quantum computation. The gate flips the second qubit (the **target qubit**) when the first qubit (the **control qubit**) is $|1\rangle$, while leaving the second bit unchanged when the first qubit state is $|0\rangle$.

$$U_{\text{CNOT}} : |00\rangle \mapsto |00\rangle,\ |01\rangle \mapsto |01\rangle,\ |10\rangle \mapsto |11\rangle,\ |11\rangle \mapsto |10\rangle.$$

$$U_{\text{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X,$$

$$U_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$



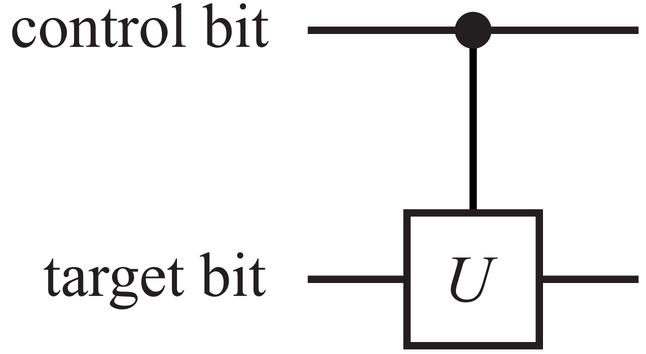
Let $\{|i\rangle\}$ be the basis vectors, where $i \in \{0,1\}$. The action of CNOT on the input state $|i\rangle|j\rangle$ is written as $|i\rangle|i \oplus j\rangle$, where $i \oplus j$ is an addition mod 2, that is, $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1$ and $1 \oplus 1 = 0$.

Control-U Gate

More generally, we consider a controlled-U gate,

$$V = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U, \tag{4.7}$$

in which the target bit is acted on by a unitary transformation U only when the control bit is $|1\rangle$. This gate is denoted graphically as



Swap Gate

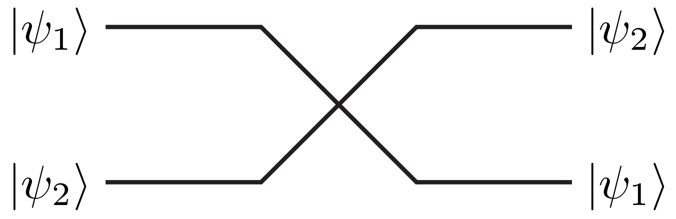
The SWAP gate acts on a tensor product state as

$$U_{\text{SWAP}}|\psi_1, \psi_2\rangle = |\psi_2, \psi_1\rangle. \tag{4.14}$$

The explict form of U_{SWAP} is given by

$$\begin{aligned} U_{\text{SWAP}} &= |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \end{aligned} \tag{4.15}$$

Needless to say, it works as a linear operator on a superposition of states. The SWAP gate is expressed as



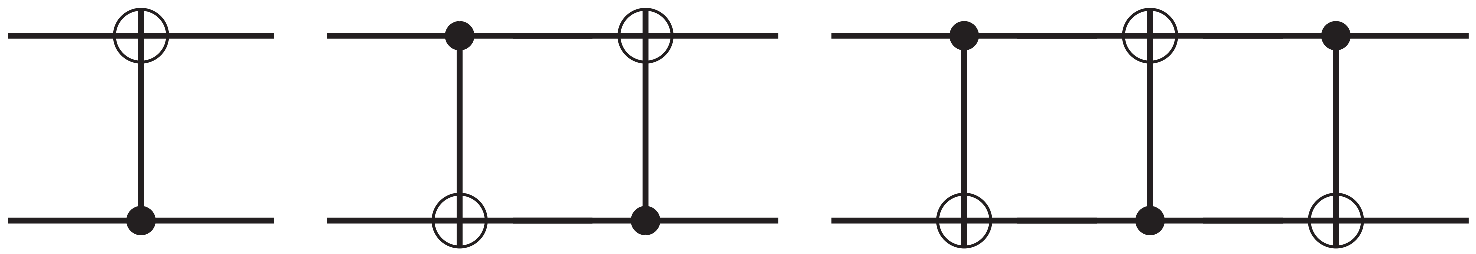
Note that the SWAP gate is a special gate which maps an arbitrary tensor product state to a tensor product state. In contrast, most two-qubit gates map a tensor product state to an entangled state.

Exercise

EXERCISE 4.1 Show that the U_{CNOT} cannot be written as a tensor product of two one-qubit gates.

EXERCISE 4.2 Let $(a|0\rangle + b|1\rangle) \otimes |0\rangle$ be an input state to a CNOT gate. What is the output state?

EXERCISE 4.3 (1) Find the matrix representation of the "upside down" CNOT gate (a) in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

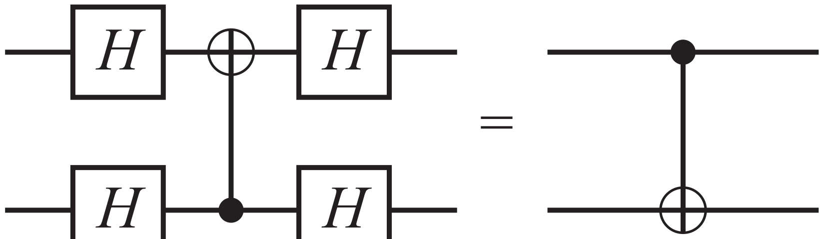


(a) (b) (c)

(2) Find the matrix representation of the circuit (b).
(3) Find the matrix representation of the circuit (c). Find the action of the circuit on a tensor product state $|\psi_1\rangle \otimes |\psi_2\rangle$.

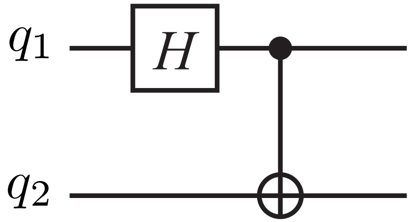
Exercise

EXERCISE 4.5 Show that the two circuits below are equivalent:



This exercise shows that the control bit and the target bit in a CNOT gate are interchangeable by introducing four Hadamard gates.

EXERCISE 4.6 Let us consider the following quantum circuit



(4.13)

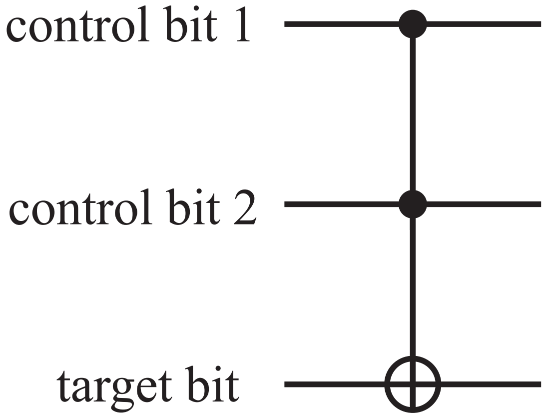
where q_1 denotes the first qubit, while q_2 denotes the second. What are the outputs for the inputs $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$?

Three qubit gate: CCNOT (Toffoli) Gate

The **CCNOT** (**Controlled-Controlled-NOT**) gate has three inputs, and the third qubit flips when and only when the first two qubits are both in the state $|1\rangle$. The explicit form of the CCNOT gate is

$$U_{\mathrm{CCNOT}} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes X. \qquad (4.8)$$

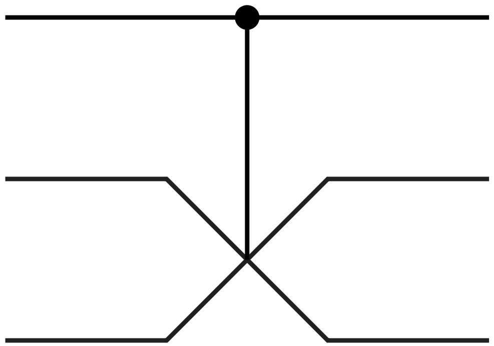
This gate is graphically expressed as



The CCNOT gate is also known as the **Toffoli gate**.

Fredkin Gate

The controlled-SWAP gate



is also called the **Fredkin gate**. It flips the second (middle) and the third (bottom) qubits when and only when the first (top) qubit is in the state $|1\rangle$. Its explicit form is

$$U_{\text{Fredkin}} = |0\rangle\langle 0| \otimes I_4 + |1\rangle\langle 1| \otimes U_{\text{SWAP}}. \tag{4.17}$$

Exercise

EXERCISE 4.7 Show that the above U_{SWAP} is written as

$$U_{\mathrm{SWAP}} = (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|) \\ (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X). \tag{4.16}$$

This shows that the SWAP gate is implemented with three CNOT gates as given in Exercise 4.3 (3).

Recovering classical Gates

The (classical) Toffoli gate is universal, therefore it reproduces all reversible and irreversible classical gates. Its quantum version generalizes the classical gates into quantum gates.

NOT Gate $$X|x\rangle = |\neg x\rangle = |\mathrm{NOT}(x)\rangle, \;\; (x = 0, 1).$$

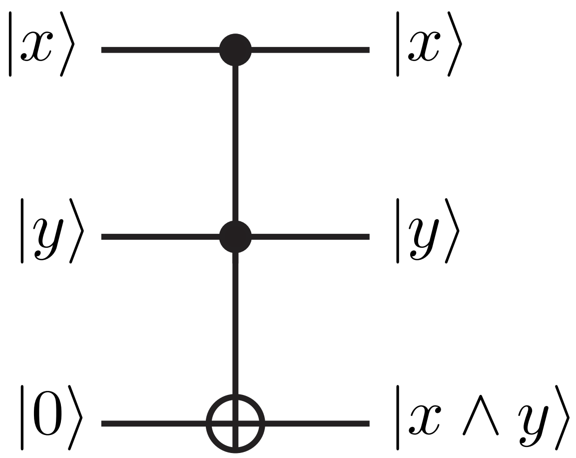
$$U_{\mathrm{CCNOT}}|1, 1, x\rangle = |1, 1, \neg x\rangle.$$

XOR Gate $$U_{\mathrm{XOR}} = U_{\mathrm{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X.$$

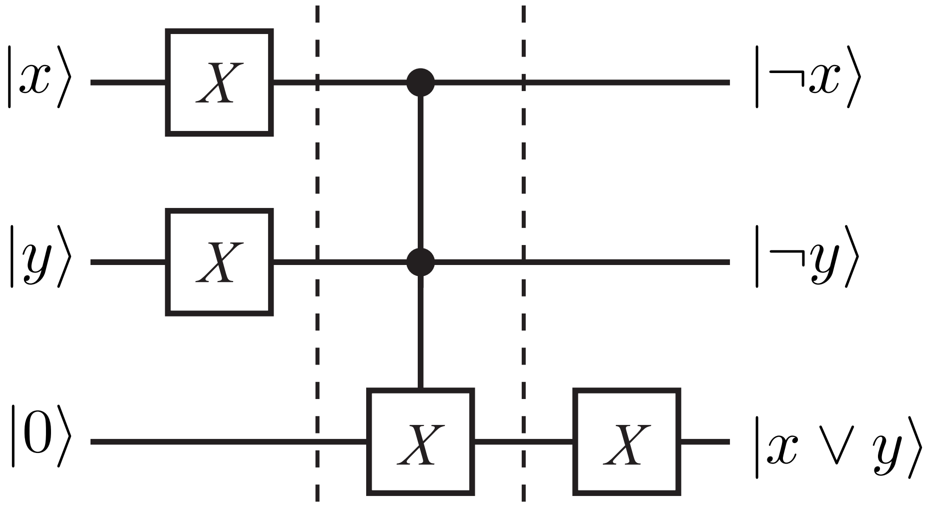
$$U_{\mathrm{CCNOT}}|1, x, y\rangle = |1, x, x \oplus y\rangle.$$

Recovering classical Gates

AND Gate



OR Gate



How to recover classical gates

1. Take a classical gate. If irreversible, consider its reversible variant.
2. Define the quantum counterpart so that on the computational basis it acts as the reversible classical gate.
3. Extend it by linearity to the whole space.

The gate thus obtained is the quantum generalization of the classical gate.

Summary

In summary, we have shown that all the classical logic gates, NOT, AND, OR, XOR and NAND gates, may be obtained from the CCNOT gate. Thus all the classical computation may be carried out with a quantum computor. Note, however, that these gates belong to a tiny subset of the set of unitary matrices.

Universal Quantum Gates

Like in the classical case, there exist a **universal set of quantum gates**.

We will now show that

- Single qubit gates
- CNOT gate

are universal for quantum computation.

Two-level unitary matrix

We will prove the following Lemma before stating the main theorem. Let us start with a definition. A **two-level unitary matrix** is a unitary matrix which acts non-trivially only on two vector components. Suppose V is a two-level unitary matrix. Then V has the same matrix elements as those of the unit matrix except for certain four elements V_{aa}, V_{ab}, V_{ba} and V_{bb}. An example of a two-level unitary matrix is

$$V = \begin{pmatrix} \alpha^* & 0 & 0 & \beta^* \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\beta & 0 & 0 & \alpha \end{pmatrix}, \quad (|\alpha|^2 + |\beta|^2 = 1),$$

where $a = 1$ and $b = 4$.

LEMMA 4.1 Let U be a unitary matrix acting on $\mathbb{C}^d$. Then there are $N \leq d(d-1)/2$ two-level unitary matrices $U_1, U_2, \ldots, U_N$ such that

$$U = U_1 U_2 \ldots U_N. \tag{4.46}$$

Proof of lemma: d = 3

Proof. The proof requires several steps. It is instructive to start with the case $d = 3$. Let

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

be a unitary matrix. We want to find two-level unitary matrices U_1, U_2, U_3 such that

$$U_3 U_2 U_1 U = I.$$

Then it follows that

$$U = U_1^\dagger U_2^\dagger U_3^\dagger.$$

(Never mind the daggers! If U_k is two-level unitary, $U_k^\dagger$ is also two-level unitary.)

Proof of lemma: d = 3

We prove the above decomposition by constructing U_k explicitly.

(i) Let

$$U_1 = \boxed{\begin{pmatrix} \frac{a^*}{u} & \frac{b^*}{u} & 0 \\ -\frac{b}{u} & \frac{a}{u} & 0 \\ 0 & 0 & 1 \end{pmatrix}},$$

where $u = \sqrt{|a|^2 + |b|^2}$. Verify that U_1 is unitary. Then we obtain

$$U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix},$$

where $a', \ldots, j'$ are some complex numbers, whose details are not necessary. Observe that, with this choice of U_1, the first component of the second row vanishes.

Proof of lemma: d = 3

(ii) Let

$$U_2 = \begin{pmatrix} \frac{a'^*}{u'} & 0 & \frac{c'^*}{u'} \\ 0 & 1 & 0 \\ -\frac{c'}{u'} & 0 & \frac{a'}{u'} \end{pmatrix} = \boxed{\begin{pmatrix} a'^* & 0 & c'^* \\ 0 & 1 & 0 \\ -c' & 0 & a' \end{pmatrix}},$$

where $u' = \sqrt{|a'|^2 + |c'|^2} = 1$. Then

$$U_2 U_1 U = \begin{pmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix},$$

where the equality $d'' = g'' = 0$ follows from the fact that $U_2 U_1 U$ is unitary, and hence the first row must be normalized.

Proof of lemma: d = 3

(iii) Finally let

$$U_3 = (U_2 U_1 U)^\dagger = \boxed{\begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{pmatrix}}.$$

Then, by definition, $U_3 U_2 U_1 U = I$ is obvious. This completes the proof for $d = 3$.

The moral of the lemma is that with N two-level unitary matrices there are enough degrees of freedom to play with, to reproduce any unitary matrix of dimension d.

Proof of lemma: any d

Suppose U is a unitary matrix acting on $\mathbb{C}^d$ with a general dimension d. Then by repeating the above arguments, we find two-level unitary matrices $U_1, U_2, \ldots, U_{d-1}$ such that

$$U_{d-1} \ldots U_2 U_1 U = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & * & * & \ldots & * \\ 0 & * & * & \ldots & * \\ & & \ldots\ldots & & \\ 0 & * & * & \ldots & * \end{pmatrix},$$

namely the $(1,1)$ component is unity and other components of the first row and the first column vanish. The number of matrices $\{U_k\}$ to achieve this form is the same as the number of zeros in the first column, hence $(d-1)$.

We then repeat the same procedure to the $(d-1) \times (d-1)$ block unitary matrix using $(d-2)$ two-level unitary matrices. After repeating this, we finally decompose U into a product of two-level unitary matrices

$$U = V_1 V_2 \ldots V_N,$$

where $N \leq (d-1) + (d-2) + \ldots + 1 = d(d-1)/2$. ∎

Exercise

EXERCISE 4.12 Let U be a general 4×4 unitary matrix. Find two-level unitary matrices U_1, U_2 and U_3 such that

$$U_3 U_2 U_1 U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix}.$$

EXERCISE 4.13 Let

$$U = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \tag{4.47}$$

Decompose U into a product of two-level unitary matrices.

Universality theorem

THEOREM 4.2 (Barenco *et al.*) The set of single qubit gates and CNOT gate are universal. Namely, any unitary gate acting on an n-qubit register can be implemented with single qubit gates and CNOT gates.

Proof. Thanks to the previous lemma, it suffices to prove the theorem for a **two-level unitary matrix**, acting non trivially on two qubits s and t.

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}, \quad (a, b, c, d \in \mathbb{C})$$

In the example (2^3 dim matrix):
s = 000 and t = 111

$$s = s_{n-1}2^{n-1} + \ldots + s_1 2 + s_0 \qquad t = t_{n-1}2^{n-1} + \ldots + t_1 2 + t_0$$

Universality theorem: step 1

Step 1. The two-level unitary matrix U can be reduced to a 2x2 unitary matrix.

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

Universality theorem: Gray code

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

Define the **Gray code** connecting s and t. It is a sequence of binary numbers such that adjacent numbers differ only by one bit. In our case s = 000 and t = 111; an example of Gray code is

$$\begin{array}{cccc} & q_1 & q_2 & q_3 \\ g_1 = & 0 & 0 & 0 \\ g_2 = & 1 & 0 & 0 \\ g_3 = & 1 & 1 & 0 \\ g_4 = & 1 & 1 & 1 \end{array}$$

If s and t differ in p bits, the shortest Gray code is made of p+1 elements

Universality theorem: the strategy

The strategy now is to find gates providing the sequence of state changes

$$|s\rangle = |g_1\rangle \rightarrow |g_2\rangle \rightarrow \ldots \rightarrow |g_{m-1}\rangle$$

Then g_{m-1} and g_m differ only in one bit, which is identified with the single qubit on which $\tilde{U}$ acts. After having applied the $\tilde{U}$ gate, we bring things back. In our example:

$$|s\rangle = \underbrace{|000\rangle \longrightarrow |100\rangle \longrightarrow |110\rangle}_{\text{DO the Gary code}} = |11\rangle \otimes |0\rangle$$

$$|t\rangle \qquad |11\rangle \otimes |1\rangle$$

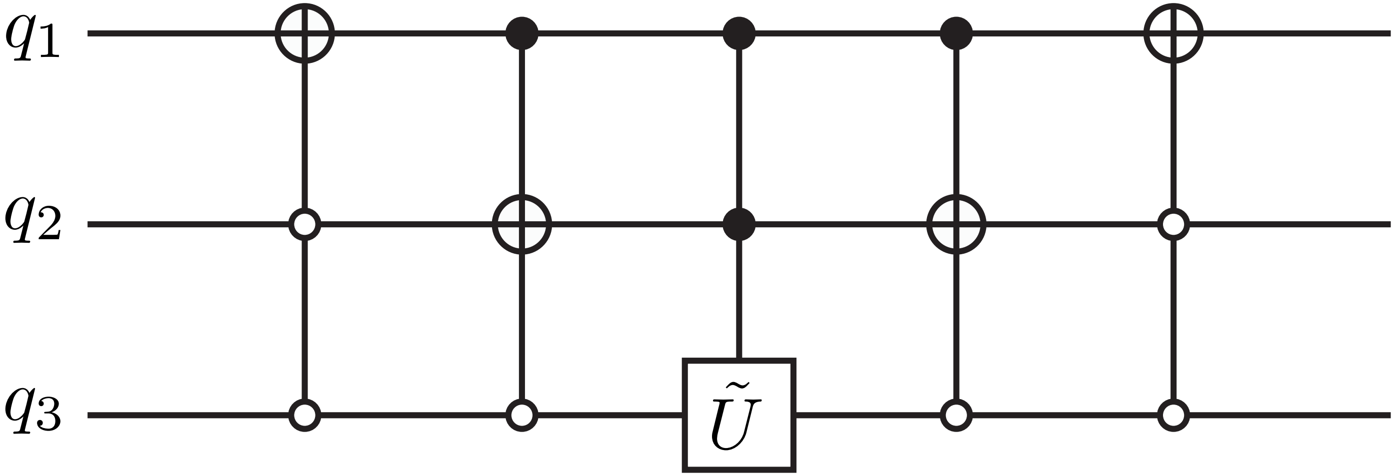
Act with the 2x2 gate $\tilde{U}$

UNDO the Gary code

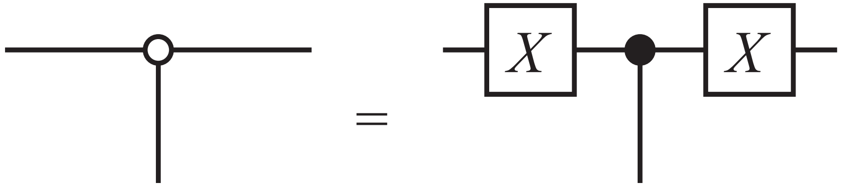
Universality theorem: d = 3 example

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

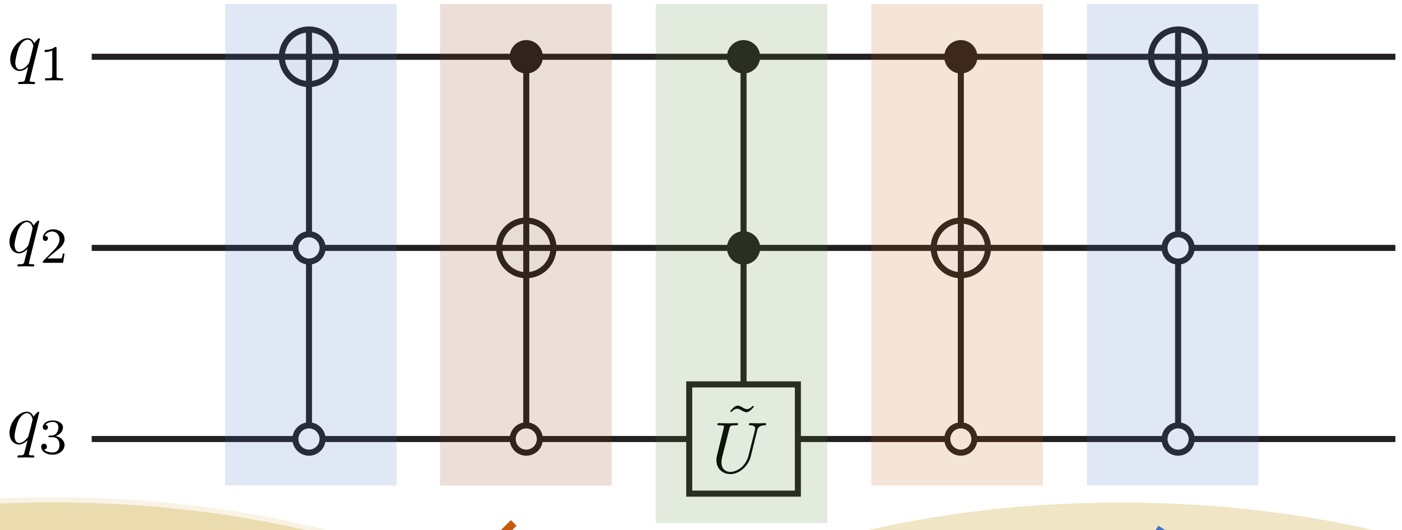
=



Where we defined



Universality theorem: d = 3 example



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

It changes
$|x00\rangle \rightarrow |\bar{x}00\rangle$

It changes
$|1x0\rangle \rightarrow |1\bar{x}0\rangle$

DO

It changes
$|1x0\rangle \rightarrow |1\bar{x}0\rangle$

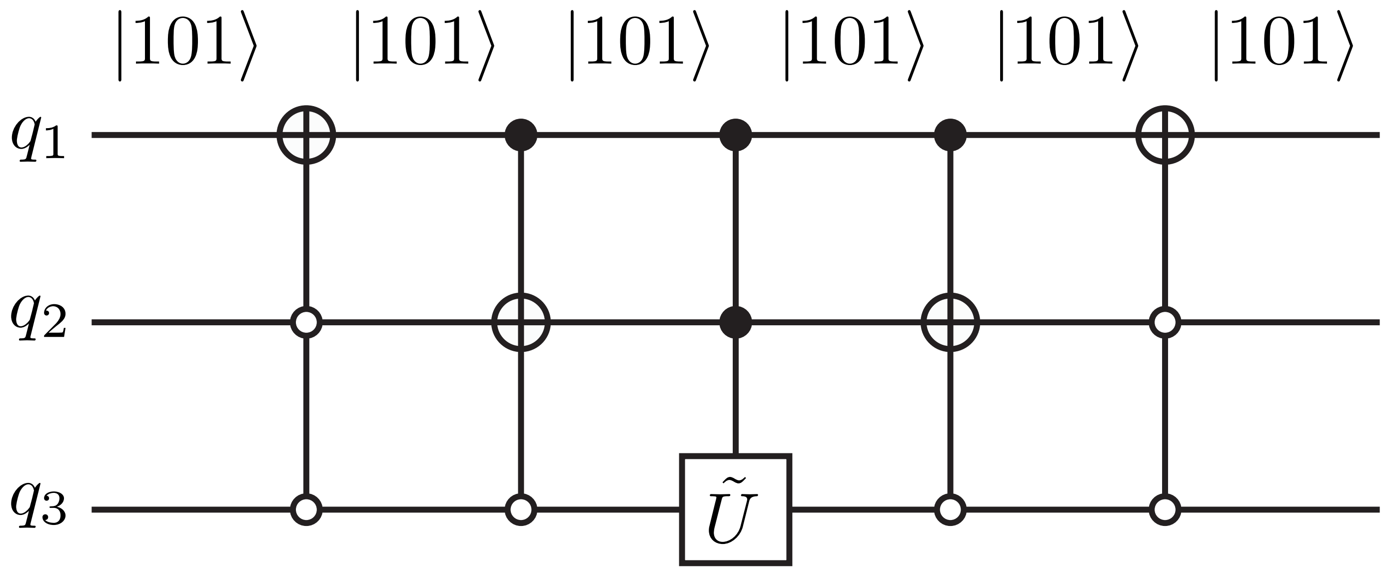
It changes
$|1x0\rangle \rightarrow |1\bar{x}0\rangle$

UNDO

	q_1	q_2	q_3
$g_1 =$	0	0	0
$g_2 =$	1	0	0
$g_3 =$	1	1	0
$g_4 =$	1	1	1

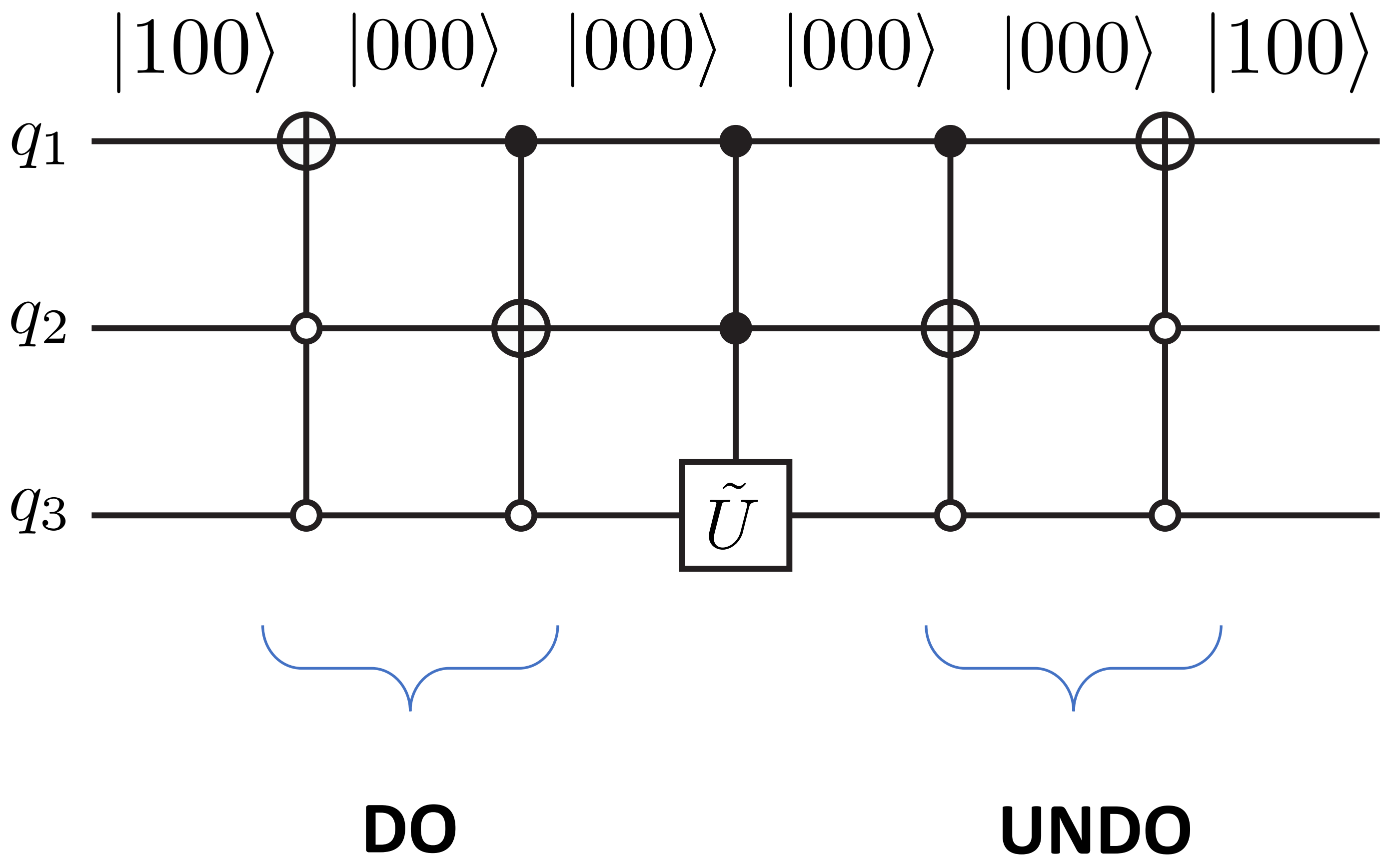
Universality theorem: d = 3 example

Let us consider the effect on a qubit different from |s> and |t>, for example the qubit |101>



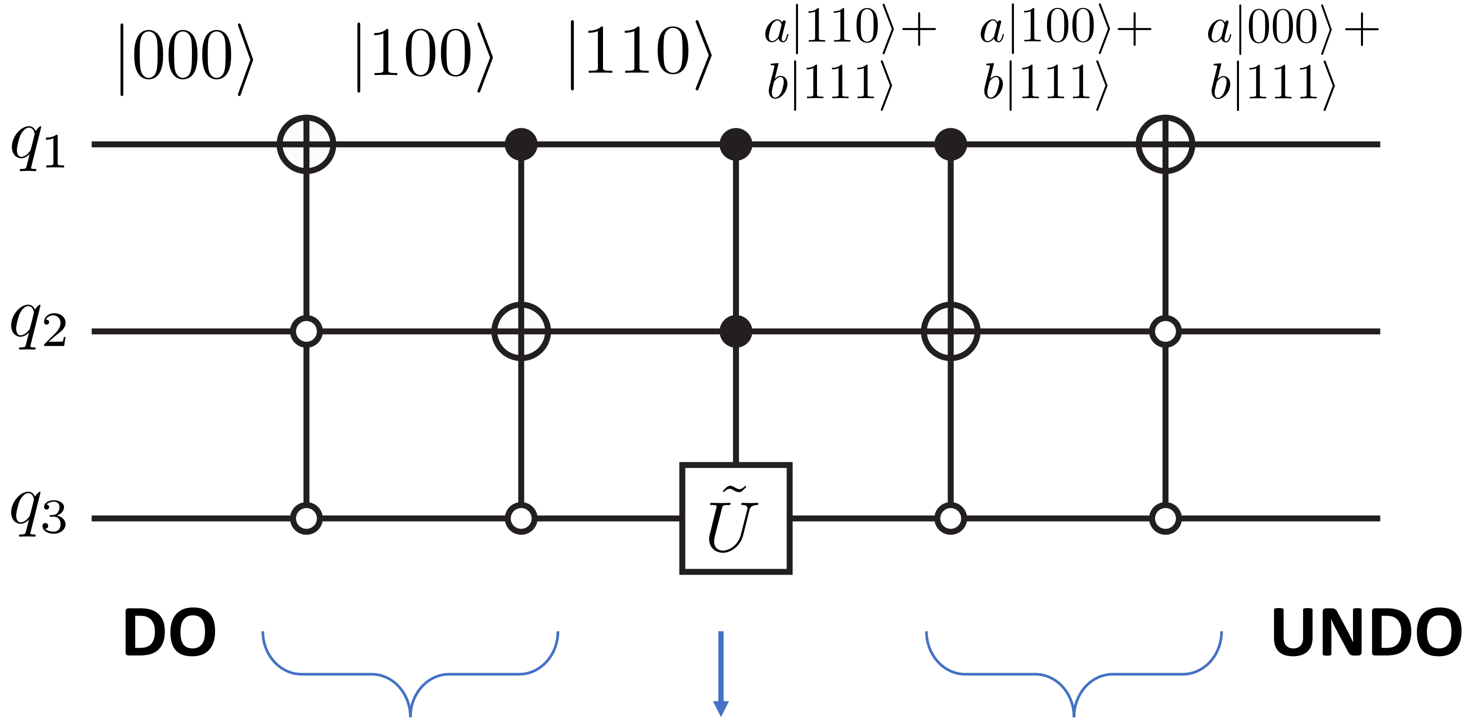
Universality theorem: d = 3 example

Or the qubit|100>



Universality theorem: d = 3 example

While on |000>



The gate acts only on the third qubit

Exercises

EXERCISE 4.14 (1) Find the shortest Gray code which connects 000 with 110.
(2) Use this result to find a quantum circuit, such as Fig. 4.5, implementing a two-level unitary gate

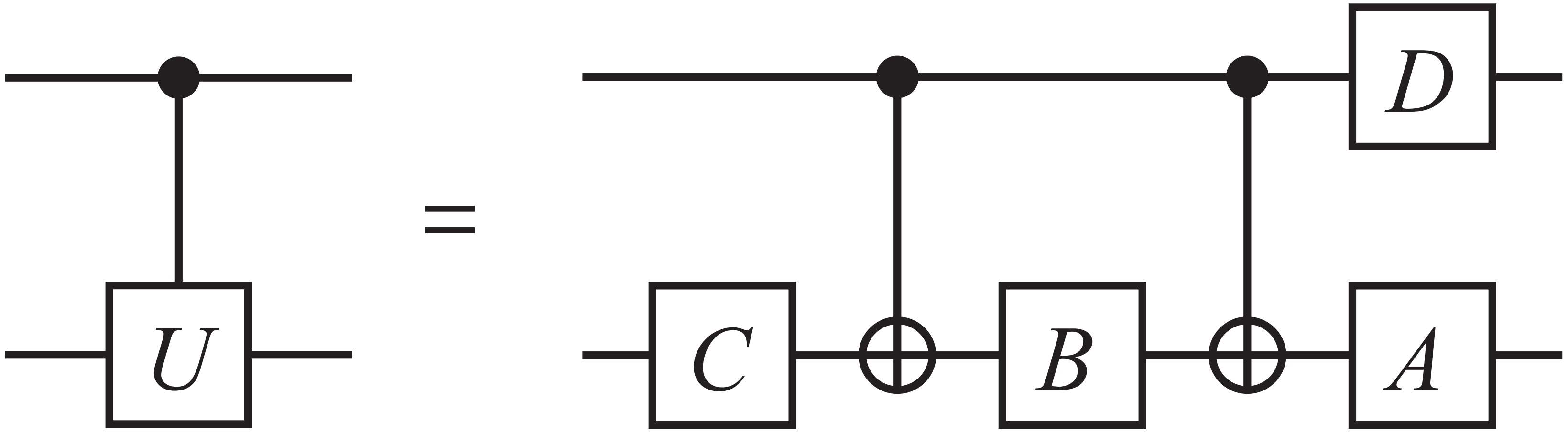
$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & c & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & d & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \tilde{U} \equiv \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in U(2).$$

Next step

It will be shown next that all the gates in the above circuit can be implemented with single-qubit gates and CNOT gates, which proves the universality of these gates.

Universality theorem: step 2

Step 2. The controlled-U gate is decomposed in the CNOT gate and single qubit gates



Decomposition of SU(2) gates

LEMMA 4.2 Let $U \in \mathrm{SU}(2)$. Then there exist $\alpha, \beta, \gamma \in \mathbb{R}$ such that $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$, where

$$R_z(\alpha) = \exp(i\alpha\sigma_z/2) = \begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix},$$

$$R_y(\beta) = \exp(i\beta\sigma_y/2) = \begin{pmatrix} \cos(\beta/2) & \sin(\beta/2) \\ -\sin(\beta/2) & \cos(\beta/2) \end{pmatrix}.$$

Proof. After some calculation, we obtain

$$R_z(\alpha)R_y(\beta)R_z(\gamma) = \begin{pmatrix} e^{i(\alpha+\gamma)/2}\cos(\beta/2) & e^{i(\alpha-\gamma)/2}\sin(\beta/2) \\ -e^{i(-\alpha+\gamma)/2}\sin(\beta/2) & e^{-i(\alpha+\gamma)/2}\cos(\beta/2) \end{pmatrix}. \quad (4.53)$$

Any $U \in \mathrm{SU}(2)$ may be written in the form

$$U = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} = \begin{pmatrix} \cos\theta e^{i\lambda} & \sin\theta e^{i\mu} \\ -\sin\theta e^{-i\mu} & \cos\theta e^{-i\lambda} \end{pmatrix}, \quad (4.54)$$

where we used the fact that $\det U = |a|^2 + |b|^2 = 1$. Now we obtain $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$ by making identifications

$$\theta = \frac{\beta}{2}, \lambda = \frac{\alpha+\gamma}{2}, \mu = \frac{\alpha-\gamma}{2}. \quad (4.55)$$

∎

Decomposition of SU(2) gates

LEMMA 4.3 Let $U \in \mathrm{SU}(2)$. Then there exist $A, B, C \in \mathrm{SU}(2)$ such that $U = AXBXC$ and $ABC = I$, where $X = \sigma_x$.

Proof. Lemma 4.2 states that $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$ for some $\alpha, \beta, \gamma \in \mathbb{R}$. Let

$$A = R_z(\alpha)R_y\left(\frac{\beta}{2}\right), B = R_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right), C = R_z\left(-\frac{\alpha-\gamma}{2}\right).$$

Then

$$\begin{aligned}
AXBXC &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)XR_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)XR_z\left(-\frac{\alpha-\gamma}{2}\right) \\
&= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)\left[XR_y\left(-\frac{\beta}{2}\right)X\right]\left[XR_z\left(-\frac{\alpha+\gamma}{2}\right)X\right]R_z\left(-\frac{\alpha-\gamma}{2}\right) \\
&= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)R_y\left(\frac{\beta}{2}\right)R_z\left(\frac{\alpha+\gamma}{2}\right)R_z\left(-\frac{\alpha-\gamma}{2}\right) \\
&= R_z(\alpha)R_y(\beta)R_z(\gamma) = U,
\end{aligned}$$

where use has been made of the identities $X^2 = I$ and $X\sigma_{y,z}X = -\sigma_{y,z}$.

It is also verified that

$$\begin{aligned}
ABC &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)R_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)R_z\left(-\frac{\alpha-\gamma}{2}\right) \\
&= R_z(\alpha)R_y(0)R_z(-\alpha) = I.
\end{aligned}$$

This proves the Lemma. ∎

Controlled-U gate with U in SU(2)

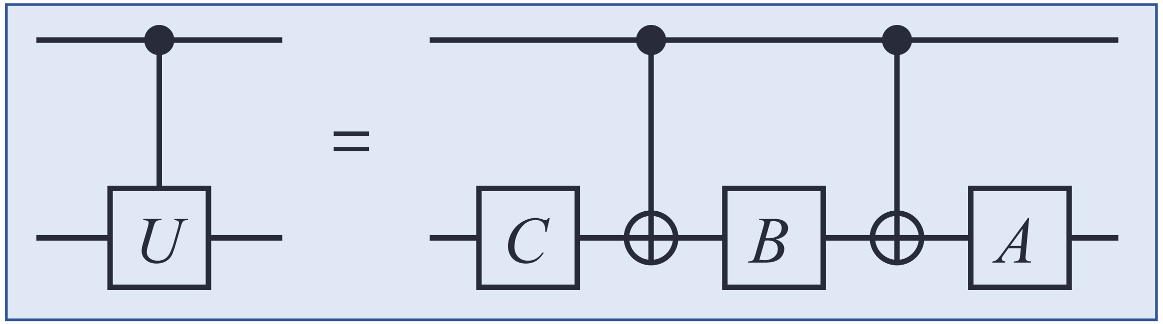
LEMMA 4.4 Let $U \in \mathrm{SU}(2)$ be factorized as $U = AXBXC$ as in the previous Lemma. Then the controlled-U gate can be implemented with at most three single-qubit gates and two CNOT gates (see Fig. 4.8).

Proof. The proof is almost obvious. When the control bit is 0, the target bit $|\psi\rangle$ is operated by C, B and A in this order so that

$$|\psi\rangle \mapsto ABC|\psi\rangle = |\psi\rangle,$$

while when the control bit is 1, we have

$$|\psi\rangle \mapsto AXBXC|\psi\rangle = U|\psi\rangle.$$



From SU(2) to (2)

So far, we have worked with $U \in \mathrm{SU}(2)$. To implement a general U-gate with $U \in \mathrm{U}(2)$, we have to deal with the phase. Let us first recall that any $U \in \mathrm{U}(2)$ is decomposed as $U = e^{i\alpha}V,\ V \in \mathrm{SU}(2), \alpha \in \mathbb{R}$.

Controlled-phase gate

LEMMA 4.5 Let

$$\Phi(\phi) = e^{i\phi} I = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

and

$$D = R_z(-\phi)\Phi\left(\frac{\phi}{2}\right) = \begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix} \begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}.$$

Then the controlled-$\Phi(\phi)$ gate is expressed as a tensor product of single qubit gates as

$$U_{\mathrm{C}\Phi(\phi)} = D \otimes I. \tag{4.56}$$

.

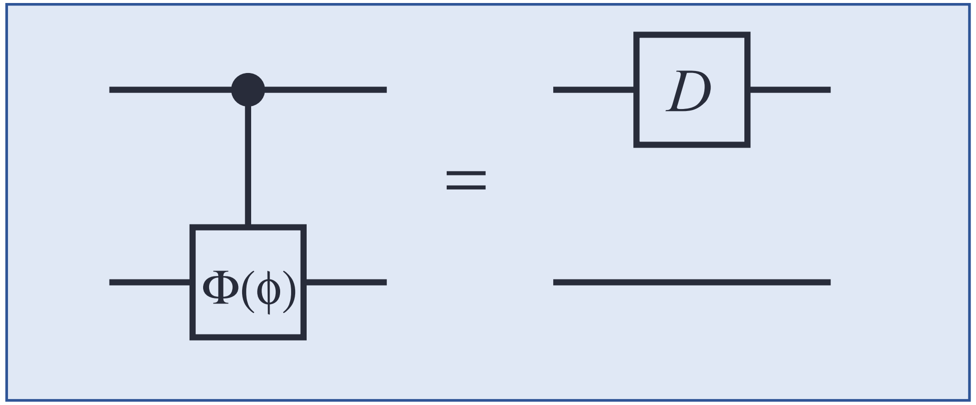
Proof. The LHS is

$$\begin{aligned} U_{\mathrm{C}\Phi(\phi)} &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \Phi(\phi) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{i\phi} I \\ &= |0\rangle\langle 0| \otimes I + e^{i\phi}|1\rangle\langle 1| \otimes I, \end{aligned}$$

while the RHS is

$$\begin{aligned} D \otimes I &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \otimes I \\ &= \left[|0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|\right] \otimes I = U_{\mathrm{C}\Phi(\phi)}, \end{aligned}$$

which proves the lemma. ∎



Exercise

EXERCISE 4.15 Let us consider the controlled-V_1 gate U_{CV_1} and the controlled-V_2 gate U_{CV_2}. Show that the controlled-V_1 gate followed by the controlled-V_2 gate is the controlled-V_2V_1 gate $U_{C(V_2V_1)}$ as shown in Fig. 4.10.

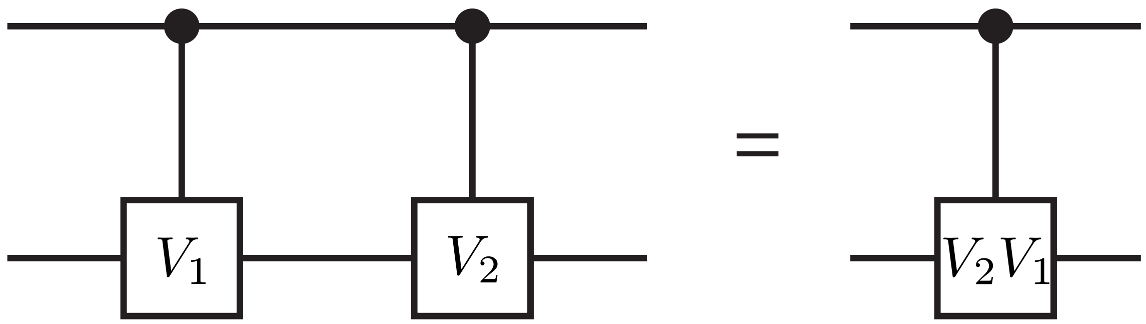


FIGURE 4.10
Equality $U_{CV_2}U_{CV_1} = U_{C(V_2V_1)}$.

Controlled-U gate with U in U(2)

PROPOSITION 4.1 Let $U \in \mathrm{U}(2)$. Then the controlled-U gate $U_{\mathrm{C}U}$ can be constructed by at most four single-qubit gates and two CNOT gates.

Proof. Let $U = \Phi(\phi)AXBXC$. According to the exercise above, the controlled-U gate is written as a product of the controlled-$\Phi(\phi)$ gate and the controlled-$AXBXC$ gate. Moreover, Lemma 4.5 states that the controlled-$\Phi(\phi)$ gate may be replaced by a single-qubit phase gate acting on the first qubit. The rest of the gate, the controlled-$AXBXC$ gate is implemented with three SU(2) gates and two CNOT gates as proved in Lemma 4.3. Therefore we have the following decomposition:

$$U_{\mathrm{C}U} = (D \otimes A)U_{\mathrm{CNOT}}(I \otimes B)U_{\mathrm{CNOT}}(I \otimes C), \tag{4.57}$$

where

$$D = R_z(-\phi)\Phi(\phi/2)$$

and use has been made of the identity $(D \otimes I)(I \otimes A) = D \otimes A$. ∎

Controlled-U gate with U in U(2)

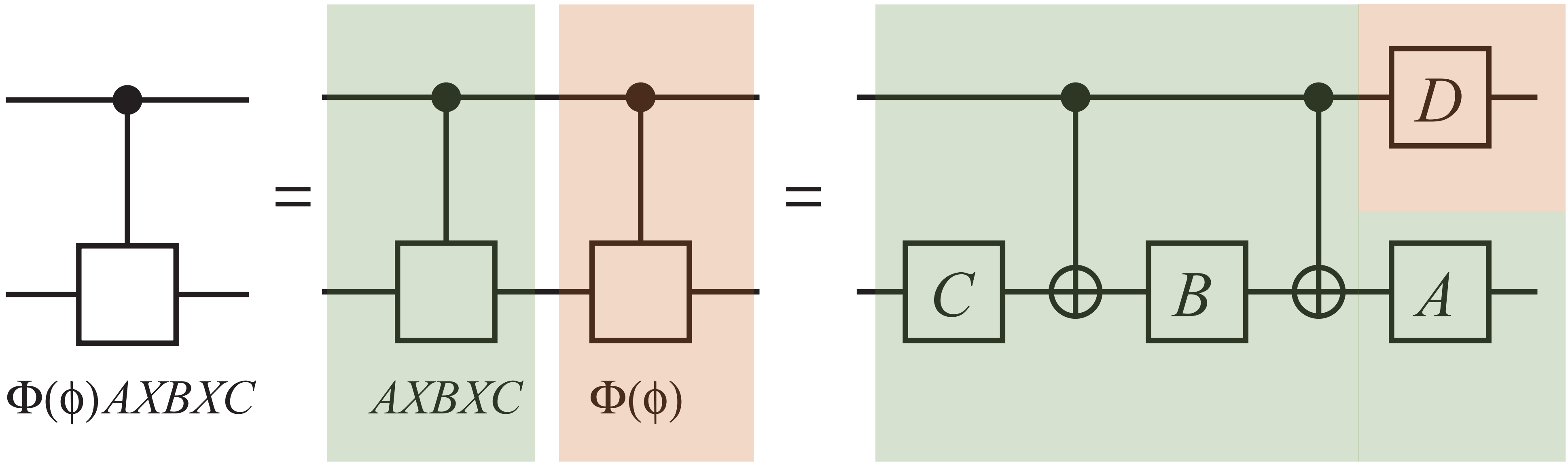
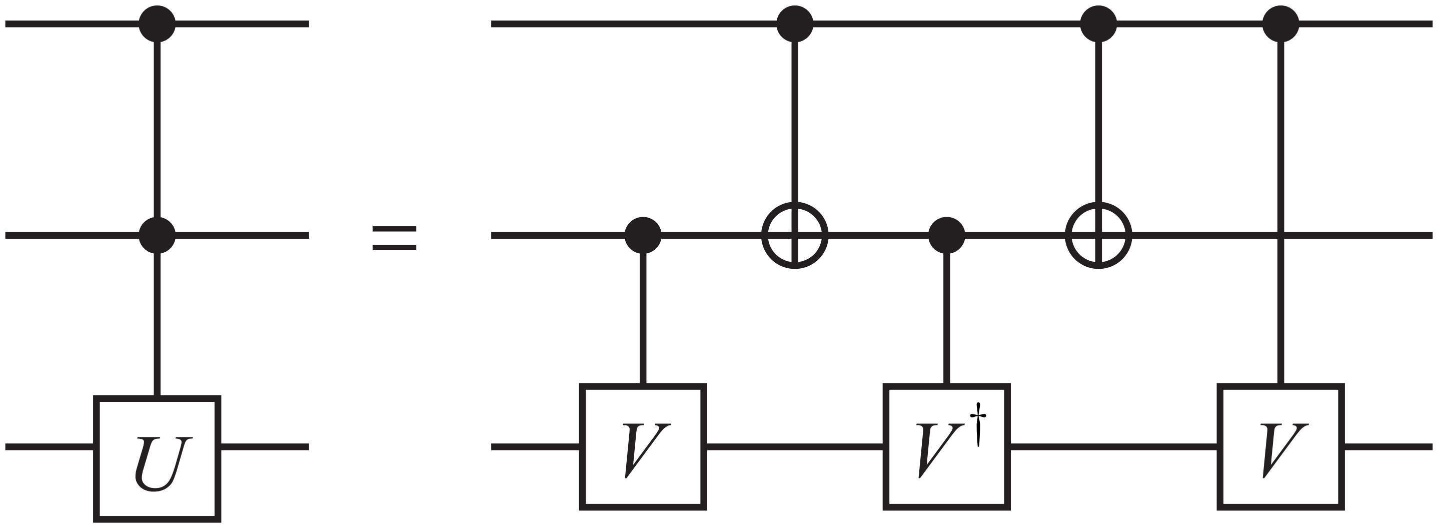


FIGURE 4.11

Controlled-U gate is implemented with at most four single-qubit gates and two CNOT gates.

Universality theorem: step 3

Step 3. The CCNOT gate and its variants are implemented with CNOT gates and its variants



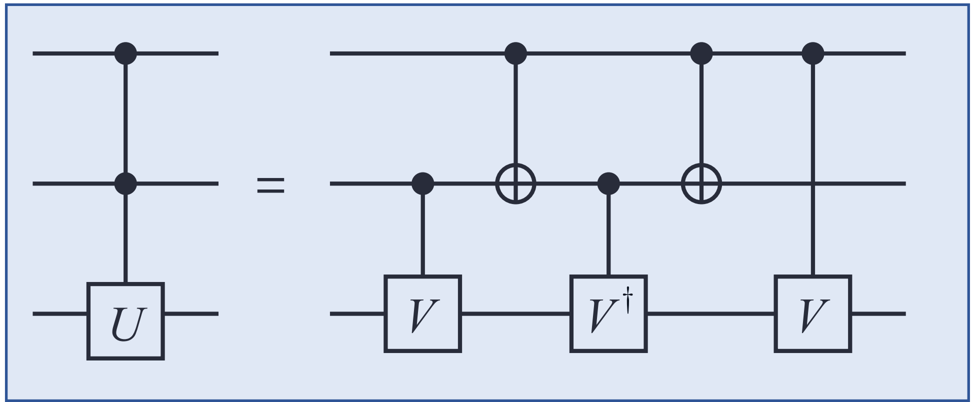
LEMMA 4.6 The two quantum circuits in Fig. 4.12 are equivalent, where $U = V^2$.

CC-U gate

Proof. If both the first and the second qubits are 0 in the RHS, all the gates are ineffective and the third qubit is unchanged; the gate in this subspace acts as $|00\rangle\langle 00| \otimes I$. In case the first qubit is 0 and the second is 1, the third qubit is mapped as $|\psi\rangle \mapsto V^\dagger V|\psi\rangle = |\psi\rangle$; the gate is then $|01\rangle\langle 01| \otimes I$. When the first qubit is 1 and the second is 0, the third qubit is mapped as $|\psi\rangle \mapsto VV^\dagger|\psi\rangle = |\psi\rangle$; hence the gate in this subspace is $|10\rangle\langle 10| \otimes I$. Finally let both the first and the second qubits be 1. Then the action of the gate on the third qubit is $|\psi\rangle \mapsto VV|\psi\rangle = U|\psi\rangle$; namely the gate in this subspace is $|11\rangle\langle 11| \otimes U$. Thus it has been proved that the RHS of Fig. 4.12 is

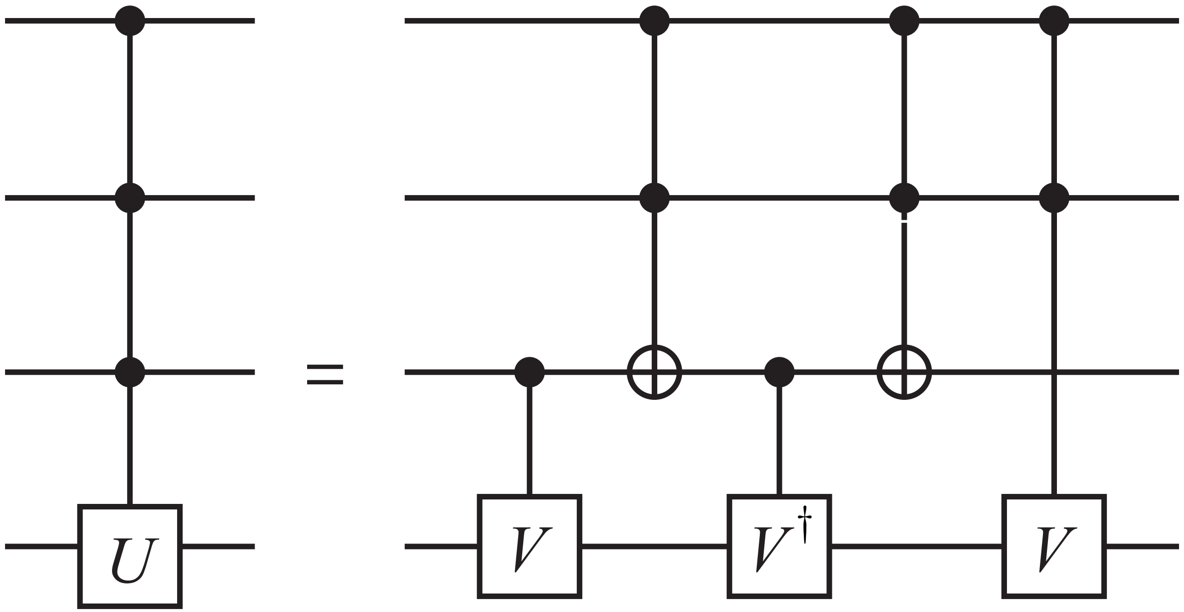
$$(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes U, \tag{4.58}$$

namely the controlled-controlled-U gate.



C^3-U gate

EXERCISE 4.17 Show that the circuit in Fig. 4.13 is a controlled-U gate with three control bits, where $U = V^2$.

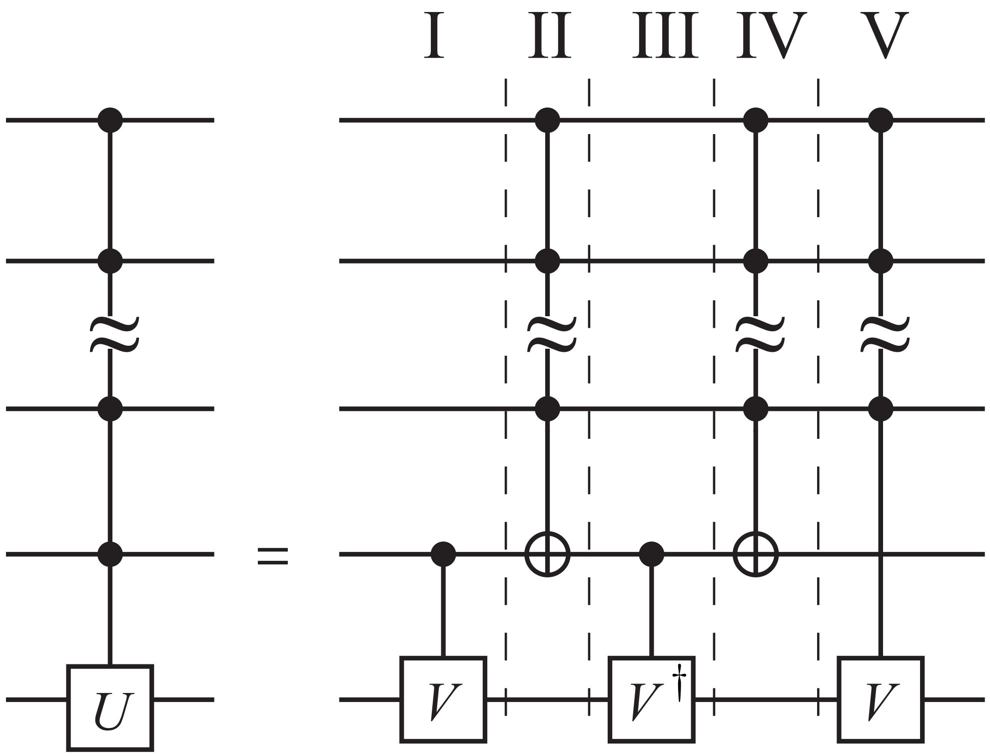


C^n-U gate

PROPOSITION 4.2 The quantum circuit in Fig. 4.14 with $U = V^2$ is a decomposition of the controlled-U gate with $n-1$ control bits.

The proof of the above proposition is very similar to that of Lemma 4.6 and Exercise 4.17 and is left as an exercise to the readers.

Theorem 4.2 has been now proved.



Comment

The above controlled-U gate with $(n-1)$ control bits requires $\Theta(n^2)$ elementary gates.*† Let us write the number of the elementary gates required to construct the gate in Fig. 4.14 by $C(n)$. Construction of layers I and III requires elementary gates whose number is independent of n. It can be shown that the number of the elementary gates required to construct the controlled NOT gate with $(n-2)$ control bits is $\Theta(n)$ [14]. Therefore layers II and IV require $\Theta(n)$ elementary gates. Finally the layer V, a controlled-V gate with $(n-2)$ control bits, requires $C(n-1)$ basic gates by definition. Thus we obtain a recursion relation

$$C(n) - C(n-1) = \Theta(n). \tag{4.59}$$

The solution to this recursion relation is

$$C(n) = \Theta(n^2). \tag{4.60}$$

Therefore, implementation of a controlled-U gate with $U \in \mathrm{U}(2)$ and $(n-1)$ control bits requires $\Theta(n^2)$ elementary gates.