Advanced Quantum Mechanics

Angelo Bassi Academic Year 2020-21

The Qubit 3.1.1 One Qubit state and *|*1⟩ to the first excited state. IN ANY CASE, we have to fix a set of basis vectors when we can set of a set of basis vectors when we can set of a set of a

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

$$
|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.
$$
 (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…. *•* In some cases, *|*0⟩ stands for a vertically polarized photon *|* ↕⟩, while as a qudit. The significance of qutrits and qudits in information processing is Dhysically a qubit can be realized in many wave; nelarization state providing, a quantitum be redirect in many ways. polarization state d photon, spin states or an electron, truncated two states from a l
.

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

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

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

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

It is therefore natural to assign a unit vector $\hat{\mathbf{n}}(\theta, \phi)$ 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 ividiti 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 2ⁿ-dimensional complex vector space. Note that $2^n \gg 2n$ for a large number *n*. The ratio $2^{n}/2n$ is ~ 6.3 × 10²⁷ 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 $\{|b_{n-1}b_{n-2}...b_0\rangle\}$, where $b_{n-1}, b_{n-2}, ..., b_0 \in$ *{*0*,* 1*}*. It is also possible to express the basis in terms of the decimal system. We write $|x\rangle$, instead of $|b_{n-1}b_{n-2}...b_0\rangle$, 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

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

Decimal expression: |x>, with $x = 1 \times 2^{1} + 0 \times 2^{0} = 2$ The set

$$
\{|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),
$$

$$
|\Psi^{+}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\}
$$
(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⟩*, |*01⟩, *|*10⟩*, |*11⟩*}* 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

$$
|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)
$$
\n(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],

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

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

Examples

Measurements [∆](*M*) = "⟨(*^M* − ⟨*M*⟩)²⟩ ⁼ "⟨*M*2⟩−⟨*M*⟩2*.* (3.14)

Let us analyze measurements in a two-qubit system in some detail. An arbitrary state is written as where α , and α and α measurement of the first qubit with respect of the first α

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

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 *a|*00⟩ + *b|*01⟩ + *c|*10⟩ + *d|*11⟩

$$
a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle
$$
\n
$$
= |0\rangle \otimes (a|0\rangle + b|1\rangle) + |1\rangle \otimes (c|0\rangle + d|1\rangle)
$$
\n
$$
= u|0\rangle \otimes \left(\frac{a}{u}|0\rangle + \frac{b}{u}|1\rangle\right) + v|1\rangle \otimes \left(\frac{c}{v}|0\rangle + \frac{d}{v}|1\rangle\right), \quad u = \sqrt{|a|^2 + |b|^2} \text{ and } v = \sqrt{|c|^2 + |d|^2}.
$$
\n
$$
\downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow \q
$$

⟨ψ*|M*0*|*ψ⟩ ⁼ *^u*² = *|a|* ² ⁺ *[|]b[|]* 2 *,* classical probabilistic case.

Quantum Computation Quantum Computation. Is a part of a p

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, $U \in U(2^n)$ 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 $\frac{1}{2}$ ¹ = $\frac{1}{2}$ antu *.* (4.1) and *Z* : *|*0⟩ → *|*0⟩*, |*1⟩→− *|*1⟩, whose matrix representations are Similarly we introduce *X* : *|*0⟩ → *|*1⟩*, |*1⟩ → *|*0⟩, *Y* : *|*0⟩→− *|*1⟩*, |*1⟩ → *|*0⟩, *<u>Single Qubit Quantum Gates</u>*

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

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

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

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

X = *|*1⟩⟨0*|* + *|*0⟩⟨1*|* = $\frac{1}{Z}$ is $\frac{1}{Z}$ the the trivial (identity) transfor *Y* = *|*0⟩⟨1*|* − *|*1⟩⟨0*|* = *s* easily verified that these σ^2 *b*^{*x*} (4.3) (4.3) (4.4) (4.3) (4.3) *The transformation I* is the trivial (identity) transforma negation (NOT), *Z* the phase shift and $Y = XZ$ the combination of them. It $_{\rm 120}$ *s* are unitary. The transformation *I* is the trivial (identity) transformation, while *X* is the The transformation I is the trivial (identity) transformation, while X is the is easily verified that these gates are unitary.

Z Z \sim *L* \sim *L* \sim *l* \sim *l* \sim *n* \sim *l* le Hamilt leme *σπ*ιατι τησε πηρισπισπευ επι
ad Evercise: Find the Hamiltonian that implements these gates and show and the view international that inprements these gates, and show
how they are implemented is that the theorem that the theorem that the that the unitary α *|*1⟩, while leaving the second bit unchanged when the first qubit state is *|*0⟩. Let *{|*00⟩*, |*01⟩*, |*10⟩*, |*11⟩*}* be a basis for the two-qubit system. In the following, *|*1⟩, while leaving the second bit unchanged when the first qubit state is *|*0⟩. 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

$$
U_{\rm H}: |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)
$$

$$
|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).
$$
 (4.9)

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

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

A Hadamard gate is depicted as

$$
\boxed{H}
$$

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 *...* 0⟩:

$$
(H \otimes H \otimes \dots \otimes H)|00\dots 0\rangle
$$

= $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
= $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n - 1} |x\rangle.$ (4.11)

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

$$
W_1 = U_H, \quad W_{n+1} = U_H \otimes W_n. \tag{4.12}
$$

Two qubit gates: CNOT Gate The transformation *I* is the trivial (identity) transformation, while *X* is the I wo qubit gates: CNOT Gate shift and *Y* the phase shift and *Y* and *Y* and *Y* the component of the is easily verified that these gates are unitary. *|*1⟩, while leaving the second bit unchanged when the first qubit state is *|*0⟩. Let *{|*00⟩*, |*01⟩*, |*10⟩*, |*11⟩*}* be a basis for the two-qubit system. In the following, we use the standard basis vectors with components with components with components with components with componen
The standard basis vectors with components with components with components with components with components wit $T \cdot h$ action of $T \cap T$ and $m \in \mathbb{N}$ *U*CNOT, is EXERCISE 4.2 Let (*a|*0⟩ + *b|*1⟩) ⊗ *|*0⟩ be an input state to a CNOT gate. **Two qubit gates: CNOT Gate** Let *{|*00⟩*, |*01⟩*, |*10⟩*, |*11⟩*}* be a basis for the two-qubit system. In the following, *|*1⟩, while leaving the second bit unchanged when the first qubit state is *|*0⟩. we yanne darco.

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 $|0\rangle$. I ¹ The left horizontal line is the input $\mathcal{L}_\mathcal{A}$ is the input $\mathcal{L}_\mathcal{A}$ is the right horizontal line in *x*¹ *m***₂ <u>***n***₁</sub> ***<i>n***₁** *n***₁</sub>** *<i>n***₁</sub>** *n***₁^{***n***}** *n***₂***n***₁^{***n***}** *n***₂***n***₁^{***n***}** *n***₂***n***₁^{***n***}** *n***₂***n***₁^{***n***}** *n***₂***n***₁***n***₂***n***₁***n***₂***n***₁***n***₂***n***₁***n***₂***n***₁***n***₂***n***₁***n***₂***n***₂***n*</u> *U*CNOT : *|*00⟩ %→ *|*00⟩*, |*01⟩ %→ *|*01⟩*, |*10⟩ %→ *|*11⟩*, |*11⟩ %→ *|*10⟩*. [|]*00⟩ = (1*,* ⁰*,* ⁰*,* 0)*^t l l n*** ***CNO[']I***'** (controlled-NO[']I') gate is a two-qu
*n*_{th} on important role in quantum computation. The ond qubit (the **target qubit**) when the first qubit (t

Let *{|*00⟩*, |*01⟩*, |*10⟩*, |*11⟩*}* be a basis for the two-qubit system. In the following, $U_{\text{CNOT}}: |00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, |10\rangle \mapsto |11\rangle, |11\rangle \mapsto |10\rangle.$ = *|*0⟩⟨0*|* ⊗ *I* + *|*1⟩⟨1*|* ⊗ *X,* (4.5) is the output qubit state. Therefore the time flows from the left to the right. U CNOT : $|UU\rangle \mapsto |UU\rangle$, $|U1\rangle \mapsto |U1\rangle$, $|1U\rangle \mapsto |11\rangle$, $|11\rangle \mapsto$ U_{CNOT} : $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle$

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

*[|]*00⟩ = (1*,* ⁰*,* ⁰*,* 0)*^t*

Let $\{|i\rangle\}$ be the basis vectors, where $i \in \{0, 1\}$. The action of CN that is, $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0$ $1 \oplus 0 = 1$ and $1 \oplus$ $\begin{array}{c} 0 & \text{if } \\ \text{if } \\ \text{if } \\ \text{if } \\ \end{array}$ \overline{a} \overline{b} $1 = 0.$ The second expression of the RHS in Eq. (4.5) shows that the action of *U*CNOT 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 $1 \oplus 1 = 0$. $w_i \in (0, 1]$ The cotion of CNOT on basis vectors, where $i \in \{0,1\}$. The action of CNOT on $\frac{1}{\pi}$ be the base $\frac{1}{\pi}$ is writ sis vectors, where $i \in \{0, 1\}$. The
s written as $|i\rangle|i \oplus j\rangle$, where $i \oplus j$: having a matrix form $1=1,$ $1 \oplus 0 = 1$ and $1 \oplus 1 = 0$.

Control-U Gate

More generally, we consider a controlled-*U* gate,

$$
V = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U, \qquad (4.7)
$$

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

Swap Gate outputs for the inputs *|*00⟩*, |*01⟩*, |*10⟩ and *|*11⟩?

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

$$
U_{\text{SWAP}} = |00\rangle\langle00| + |01\rangle\langle10| + |10\rangle\langle01| + |11\rangle\langle11|
$$

=
$$
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.
$$
 (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 Let *{|i*⟩*}* be the basis vectors, where *i* ∈ *{*0*,* 1*}*. The action of CNOT on Exercise the contract of the c

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 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

(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 4.4 Show that *Wⁿ* is unitary.

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

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 circuit on a tensor product state *|*ψ1⟩ ⊗ *|*ψ2⟩.

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⟩. The explicit form of the CCNOT gate is

 $U_{\text{CCNOT}} = (|00\rangle\langle00| + |01\rangle\langle01| + |10\rangle\langle10|) \otimes I + |11\rangle\langle11| \otimes X.$ (4.8)

This gate is graphically expressed as

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

Fredkin Gate is in the Swandale (*|*0⟩⟨0*|* ⊗ *I* + *|*1⟩⟨1*|* ⊗ *X*)*.* (4.16)

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⟩. 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 product state to a tensor product state to a tensor product state \mathcal{L}

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

$$
U_{\text{SWAP}} = (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|)
$$

$$
(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X).
$$
 (4.16)

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

Recovering classical Gates Recovering classical Gates When the input is *|*0⟩, the output is *|*1⟩ and the measurement gives the value $A = \frac{1}{2}$ *M*¹ has eigenvalues 0 and 1 with the eigenvectors *|*0⟩ and *|*1⟩, respectively. Recovering CI

The (classical) Toffoli gate is universal, therefore it reproduces all reversible and irreversible classical gates. Its quantum version generalizes the
and irreversible classical gates. Its quantum version generalizes the classical gates into quantum gates. ciassical gates into quantum gates. In this sense, q where *interviewed* or *account gaves the quantum reference* of *account control* and control the classical gates into quantum gates. *|*0⟩*,* 1 ↔ *|*1⟩, we have already seen in Eq. (4.2) that the gate *X* negates the and irreversible classical gates. Its quantum version generalizes the
classical gates into quantum gates ciassical gales into quantum gales. I ne (classical) 10 froll gate is universal, therefore it reproduc classical gates into quantum gates. This operator operation may be made reverse. τ and the construction gate has to be reversible, we can not construct a unitary gate τ corresponding to the classical XOR gate is universal, therefore it reproduces all reversion is and irreversible classical σ and irreversible classical σ and irreversible classical σ and σ

NOT Gate
$$
X|x\rangle = |\neg x\rangle = |\text{NOT}(x)\rangle
$$
, $(x = 0, 1)$.
 $U_{\text{CCNOT}}|1, 1, x\rangle = |1, 1, \neg x\rangle$.

 $I_{x\circ p} = I_{\text{error}} - |0\rangle/|0| \otimes I + |1\rangle/|1| \otimes Y$ **XOR Gate** $U_{\text{XOR}} = U_{\text{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X.$ 4.3.2 XOR Gate 4.3.2 XOR Gate

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

Recovering classical Gates *U*CCNOT*|*1*, x, y*⟩ = *|*1*, x, x* ⊕ *y*⟩*.* (4.24) +*|*11⟩⟨11*|*⊗ *X.* (4.27) It is readily verified that EXERCISE 4.8 Verify that the above matrix *U*OR indeed satisfies

AND Gate Observe that the third qubit in the RHS is 1 if and only if *x* = *y* = 1 and 0

OR Gate. Ω is obvious why negative Ω

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 λ *n* λ *y* = λ *x* λ *y* = λ *y* λ *x* λ *y* = λ *y* λ *x* λ *y* λ *x* λ *y* λ *x* λ *x*

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 (1) the set of single qubit gates and single qubit gates and wo-leve form a universal set of quantum circuits (universality theorem).

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 twolevel 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 $U = U_1 U_2 ... U_N.$ (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

$$
U_3U_2U_1U=I.
$$

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: $d = 3$

(Never mind the daggers! If *U^k* is two-level unitary, *U† ^k* is also two-level We prove the above decomposition by constructing U_k explicitly. (Never mind the daggers! If *U^k* is two-level unitary, *U†* We prove the above decomposition by constructing U_k explicitly.

(i) Let
\n
$$
U_{1} = \begin{bmatrix} \frac{a^{*}}{u} & \frac{b^{*}}{u} & 0 \\ -\frac{b}{u} & \frac{a}{u} & 0 \\ 0 & 0 & 1 \end{bmatrix},
$$

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

$$
U_1U=\left(\begin{matrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{matrix}\right),
$$

 ω ¹ vitation that the first component of the first component of the second view ω' 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 where *a*′ *,...,j*′ are some complex numbers, whose details are not necessary. Proof of lemma: $d = 3$

(ii) Let

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

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 $Proof$ of lemma: $d = 3$

(iii) Finally let

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

Then, by definition, $U_3U_2U_1U = I$ is obvious. This completes the proof for $d = 3$.

Suppose *U* is a unitary matrix acting on C*^d* with a general dimension *d*.

U₂, u₂, u₂, u₂ d₀, u₂, u₂, u₂, u₂ enough degrees of freedom to play with, to reproduce any unitary matrix 0 ∗ ∗ *...* ∗ The moral of the lemma is that with N two-level unitary matrices there are of dimension d.

Proof of lemma: any d Then, by definition, *U*3*U*2*U*1*U* = *I* is obvious. This completes the proof for

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

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

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

$$
U=V_1V_2\ldots V_N,
$$

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

Exercise where *N* ≤ (*d* − 1) + (*d* − 2) + *...* +1= *d*(*d* − 1)*/*2.

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 ²*ⁿ*−¹(2*ⁿ* [−] 1) two-level unitary matrices. Now we are in a position to state Universality theorem. **In the state of sequence (4.13 Let 1011)**.

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. so that *|g^m*−¹⟩ → *|g^m*−²⟩ → *...* → *|g*1⟩ = *|s*⟩. Each of these steps can be (Barenco *et al.*) The set of single qubit gates and $\frac{1}{2}$ Nemetre previously previously gate parties on an a qubit $\frac{1}{1}$ 1 $\mathcal{S}^{\text{avco}}$ and $\mathcal{S}^{\text{avco}}$ Let us consider a unitary matrix acting on an *n*-qubit system. Then this

Proof. Thanks to the previous $\int a 0 0 0 0 0 c$ lemma, it suffices to prove the $\left(\begin{array}{cc} a & b & c & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$ theorem for a two-level unitary $\left[\begin{array}{cc} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right]$ $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ **THERE** IS A GUITTLE CONTINUES INTEREST ELEMENT IN THE UPPER CONTROLS IN THE UPPER CONTROLS (0) **matrix**, acting non trivially on two qubits s and t. $\mathcal{C} = \left[\begin{array}{cc} 0 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right]$ the main theorem.

unitary submatrix of *U*. *U* a single $(2^3$ dim matrix): In the example (2^3 dim matrix): $\begin{pmatrix} b & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $s = 000$ and $t = 111$ $\sum_{n=0}^{n}$ is sufficiently matrix.

those of the unit matrix, while all the others are the same, where *|s*⟩ stands for *|sⁿ*−¹⟩*|sⁿ*−²⟩*... |s*0⟩, for example. We can construct *U* ˜, the non-trivial 2 [×] ² ˜ may be thought of as a unitary matrix acting on *U* = ⎛ ⎜⎜⎜⎜⎜⎜⎜⎜⎜⎜⎝ *a* 000000 *c* 01000000 00100000 00010000 00001000 00000100 00000010 *b* 000000 *d* ⎞ ⎟⎟⎟⎟⎟⎟⎟⎟⎟⎟⎠ *,* (*a, b, c, d* ∈ C) (4.49) be a two-level unitary matrix which we wish to implement. Note that *U* acts non-trivially only in the subspace spanned by *|*000⟩ and *|*111⟩. The unitarity CNOT gate are universal. Namely, any unitary gate acting on an *n*-qubit register can be implemented with single qubit gates and CNOT gates. sis vectors of an *n*-qubit system, where *s* = *sⁿ*−¹2*ⁿ*−¹ + *...* + *s*12 + *s*⁰ and ²*ⁿ*−¹(2*ⁿ* [−] 1) two-level unitary matrices. Now we are in a position to state the main theorem. THEOREM 4.2 (Barenco *et al.*)[14] 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*. We closely follow [1] for the proof here. Thanks to the previous Lemma, it suffices to prove the theorem for a two-level unitary matrix. Let *U* be a two-level unitary matrix acting nontrivially only on *|s*⟩ and *|t*⟩ basis vectors of an *n*-qubit system, where *s* = *sⁿ*−¹2*ⁿ*−¹ + *...* + *s*12 + *s*⁰ and *t* = *tⁿ*−¹2*ⁿ*−¹ +*...*+*t*12+*t*⁰ are binary expressions for decimal numbers *s* and

Universality theorem: step 1 it acts on a two-dimensional subspace of the total Hilbert subspace of the total Hilbert space, in which the total Hilb **UNIVE IS ALLET FIRST FIRST FIRST FIRST FIRST FIRST FIRST PIPE I**

 $\frac{1}{2}$ and $\frac{1}{2}$ interpretations in $\frac{1}{2}$ interpretations of $\frac{1}{2}$ \blacksquare **Step 1.** The two-level unitary matrix U can be reduced to a 2x2 unitary matrix. FIGURE 4.5

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

 $\tilde{U} =$ $\left(\begin{array}{cc} a & c \\ b & d \end{array}\right)$

Universality theorem: Gray code Example of circuit implementing the gate *U*.

 $U =$ ⎛ *a* 000000 *c* \blacksquare $\overline{0}$ 1 0 0 0 0 $\overline{0}$ 00100000 00010000 00001000 00000100 00000010 *b* 000000 *d* $\sqrt{2}$ ⎟⎟⎟⎟⎟⎟⎟⎟⎟⎟⎠

our case s = 000 and t = 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 of *U* ensures that the matrix ary
.... <mark>umb</mark>
er onl</mark> $\frac{1}{2}$ out case s = 000 and $\frac{1}{2}$ = 111, an example of

 $b_3 = 1$ $g_4 = 1$ *q*¹ *q*² *q*³ $g_1 = 0 \ 0 \ 0$ $g_2 = 1 \ 0 \ 0$ $g_3 = 1 \; 1 \; 0$ $g_4 = 1 \; 1 \; 1$

> $\frac{1}{2}$ the chartect Gray code is made of n+1 elements , the shortest oray code is made or p+1 elements If s and t differ in p bits, the shortest Gray code is made of p+1 elements

Universality theorem: the strategy *s* and *t* differ at most in *n* bits. Universality theorem: the strategy $\frac{1}{2}$ and $\frac{1}{2}$ $\frac{1}{2}$ code connecting *s* and *t* is

The strategy now is to find gates providing the sequence of state changes With these preparations, we consider the implementation of *U*. The strat-The strategy now is to find gates providing the sequence The strategy now is to find gates providing the sequence o *g*² = 1ˆ10101 $\boldsymbol{\mathsf{g}}$ the seque

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

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: it acts on a two-dimensional subspace of the total Hilbert space, in which the Then *g^m*−¹ and *g^m* differ only in one bit, which is identified with the single Then g_{m-1} and g_m differ only in one bit, wh Then *g^m*−¹ and *g^m* differ only in one bit, which is identified with the single n g_{m-1} and g_m differ only in one bit, which is identified with the single

¹ \mathbf{r} as a has been renewed. It is constructed renewed. It is constructed by it is construction to the construction of \mathbf{r} that g_m differ only in one bit, which is identified with the single \sim

$$
|s\rangle = |000\rangle \longrightarrow |100\rangle \longrightarrow |110\rangle = |11\rangle \otimes |0\rangle
$$

$$
|t\rangle
$$

DO the Gary code
Act with the 2x2 gate \tilde{U}
UNDO the Gary code

Universality theorem: d = 3 example *g*² =1 0 0 **g**3 $\frac{1}{2}$

 $\sqrt{2}$ \blacksquare *a* 000000 *c* 01000000 00100000 00010000 00001000 00000100 00000010 *b* 000000 *d* $\sqrt{2}$ ⎟⎟⎟⎟⎟⎟⎟⎟⎟⎟⎠

 $U =$

Universality theorem: d = 3 example easily implemented using simple gates that have been introduced previously amnle Let us consider the following example of a three-qubit system, whose basis 86 *QUANTUM COMPUTING*

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 bring *g*¹ to *g*³ and then operate *U*˜ on the qubit *q*³ provided that the first and Universality theorem: d = 3 example bring *g*¹ to *g*³ and then operate *U*˜ on the qubit *q*³ provided that the first and Universality theorem: d = 3 example bring *g*¹ to *g*³ and then operate *U*˜ on the qubit *q*³ provided that the first and Universality theorem: d = 3 example bring *g*¹ to *g*³ and then operate *U*˜ on the qubit *q*³ provided that the first and Universality theorem: d = 3 example

Or the qubit | 100> with the target bit *q*³ and the control bits *q*¹ and *q*2.) After this controlled with the target bit *q*³ and the control bits *q*¹ and *q*2.) After this controlled with the target bit *q*³ and the control bits *q*¹ and *q*2.) After this controlled with the target bit *q*³ and the control bits *q*¹ and *q*2.) After this controlled

Universality theorem: $d = 3$ example *b* 000000 *d*

While on |000> in Fig. 4.7 in Fig. 4.7

U-gate acts only on the third qubit $\frac{1}{2}$ (*b*α + *d*β)*|*111⟩. *U*-gate acting on α*|*000⟩ + β*|*111⟩ yields the desired output (*a*α + *c*β)*|*000⟩ + (*b*α + *d*β)*|*111⟩. The gate acts only on the third qubit

Exercises be implemented with single-qubit gates, which proves the contract gates and CNOT gates, which proves the contract of \mathcal{L}

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

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

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 *ABC* = *Rz*(α)*R^y* \overline{c} *R*
R
R^y 2 $\overline{}$ = *Rz*(α)*Ry*(0)*Rz*(−α) = *I.*

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

Decomposition of SU(2) gates A controlled-*U* gate can be constructed from at most four single-qubit gates Decomposition of SU(2) gates several Lemmas before we prove this statement.

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

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

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

Proof. After some calculation, we obtain

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

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

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

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

.

LEMMA 4.3 Let $U \in SU(2)$. Then there exist $A, B, C \in SU(2)$ 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

$$
AXBXC = R_z(\alpha)R_y\left(\frac{\beta}{2}\right)XR_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)XR_z\left(-\frac{\alpha-\gamma}{2}\right)
$$

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

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

$$
ABC = R_z(\alpha)R_y\left(\frac{\beta}{2}\right)R_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)R_z\left(-\frac{\alpha-\gamma}{2}\right)
$$

= $R_z(\alpha)R_y(0)R_z(-\alpha) = I.$

This proves the Lemma.

Decomposition of SU(2) gates

\overline{z} = *Rz*(α)*R^y* " | Z *R^y* Controlled-U gate with U in SU(2) gates for any *U* ∈ SU(2).

most three single-qubit gates and two CNOT gates (see Fig. 4.8). \overline{P} *AYRY*(*C*) es in the Γ can be implemented with at *I a*nd *X* = *I* and *X* = *I* a \int atch (bcc 1 ig. 4.0). **LEMMA 4.4** Let $U \in SU(2)$ 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 *ABC* = *Rz*(α)*R^y*

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

while when the control bit is 1, we have

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

From $SU(2)$ to (2) *|*ψ⟩ "→ *AXBXC|*ψ⟩ = *U|*ψ⟩*.*

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

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

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

Proof. The LHS is

 $U_{\mathbf{C}\Phi(\phi)} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \Phi(\phi) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{i\phi}I$ $= |0\rangle\langle 0| \otimes I + e^{i\phi} |1\rangle\langle 1| \otimes I,$

while the RHS is

$$
D \otimes I = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \otimes I
$$

= $[|0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|] \otimes I = U_{\mathcal{C}\Phi(\phi)},$

which proves the lemma.

Controlledphase gate

Exercise $w = \frac{1}{2}$ Figure 4.9 shows the statement of the statement of the above lemma.

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) Now we are ready to prove the main proposition.

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

Proof. Let $U = \Phi(\phi) A X B X C$. 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:

$$
U_{\text{CU}} = (D \otimes A)U_{\text{CNOT}}(I \otimes B)U_{\text{CNOT}}(I \otimes C), \qquad (4.57)
$$

 \blacksquare

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 **Exercise is implemented** with a most four single-qubit gate α

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

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 $|00\rangle\langle00| \otimes I$. 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 $|01\rangle\langle01| \otimes I$. When the first qubit is 1 and the second is 0, the third qubit is mapped as $|\psi\rangle \mapsto V V^{\dagger} |\psi\rangle = |\psi\rangle$; 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 $|11\rangle\langle11| \otimes U$. Thus it has been proved that the RHS of Fig. 4.12 is ence gave in this subspace

$(|00\rangle\langle00| + |01\rangle\langle01| + |10\rangle\langle10|) \otimes I + |11\rangle\langle11| \otimes U,$ (4.58) two CNOT gates.

namely the controlled-controlled-*U* gate.

CC-U gate

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

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 Commented with single-qubit gates and the top denotes the lay CNOT gates. See Barenco *et al.* [14] for further details. A few remarks are in CONTILICTI

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 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 $\frac{1}{2}$ $\frac{1}{2}$ require $\Theta(n)$ elementary gates. Finally the layer V, a controlled-*V* gate with to construct the gate in Fig. 4.14 by $C(n)$. Construction of layers I and III $(n-2)$ 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 $U \in U(2)$ and $(n-1)$ control bits requires $\Theta(n^2)$ elementary gates. $\frac{1}{\sqrt{1+\frac{1}{2}}}\left(\frac{1}{\sqrt{1+\frac{1}{2}}}\right)$ (*n* − 2) control bits, requires *C*(*n* − 1) basic gates by definition. Thus we

