# Quantum Computing 4 – Qubits & Gates

Angelo Bassi

# The Qubit **The most part we track and real systems is made.** The most part we treat abstract mathematical objects. The beauty of treating  $\alpha$

The bit is the fundamental concept of classical computation and classical inc bit is the rundamental concept or classical computation and classical<br>information. Just as a classical bit has a state – either 0 or 1 – a qubit also has a state. Two possible states for a qubit are the states  $|0\rangle$  and  $|1\rangle$ , which as you might areas correspond to the states 0 and 1 for a classical bit. The as you might guess correspond to the states 0 and 1 for a classical bit. The as you might guess correspond to the states 0 and 1 for a classical bit. Th<br>difference between bits and qubits is that a qubit can be in a state other than  $|0\rangle$  or  $|1\rangle$ . It is also possible to form linear combinations of states, often called superpositions: *Dirac notation*, and we'll be seeing it often, as it's the standard notation for states in often take superpositions. lost by thinking of them as real numbers. Put another way, the state of a qubit is a vector *computational basis states*, and form an orthonormal basis for this vector space. ubit can be in a state other ar combinations of states, we

> $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ ,  $|\alpha|^2 + |\beta|^2 = 1$ either the result 0, with probability *|*α*|*

The special states (0) and (1) are known as computational basis states, *ine special states | 0, and | 1, are known as sompleted in secio 3.<br>and form an orthonormal basis for this vector space . computational basis states*, and form an orthonormal basis for this vector space.  $\overline{\phantom{a}}$  state is a unit vector in a two-dimensional complex vector space. or space  $\mathbf r$ Because *|*α*|* <sup>2</sup> <sup>+</sup> *<sup>|</sup>*β*<sup>|</sup>* pecial states 10) and 11) are known as comp e known as computational pasis states,<br>ōr this v<u>e</u>ctor space .  $\epsilon$  proposition in this vector space .

 $\mathbb{R}$  can examine a bit to determine whether it is in the state of the state  $\mathbb{R}$ Because  $|\alpha|^2 + |\beta|^2 = 1$ , we may rewrite the above relation as where **d**,  $\frac{1}{2}$  and  $\frac{1}{2}$  we will see that we can ignore that we can ignore that we can ignore the factor the factor the factor that we can ignore the factor that we can ignore the factor that we can ignore the fa  $\log |\alpha|^2 + |\beta|^2 = 1$ , we may rewrite the above relation as

<sup>2</sup> = 1, we may rewrite Equation (1.1) as

The numbers  $\overline{\phantom{a}}$  are complex numbers a and  $\overline{\phantom{a}}$  are complex numbers, although for much is much

$$
|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle.
$$

either the result 0, with probability *|*α*|* 2, or the result 1, with probability *<sup>|</sup>*β*<sup>|</sup>* . Naturally, 2 op to an giobal phase factor, which has no physical significance. The probability of the probability of the present such as the probability of t  $\alpha$  indiffusition that  $\alpha$  define a point on the differential consequences,  $\alpha$ often called the **bloch sphere.** which leads which distinctly on the different on the distinctly on the differ Up to an global phase factor, which has no physical significance. The numbers  $\theta$  and  $\phi$  define a point on the unit three-dimensional sphere, often called the Bloch sphere.<br>
picture. que describe later with which sphere.  $\sigma$ ers wand  $\phi$  denne a point on the dint three-dimensional no simple generalization of the Bloch sphere known for multiple qubits.



Figure 1.3. Bloch sphere representation of a qubit.

### Multiple Qubits ple Qubits a powerful tool for information processing  $\mathcal{L}$  $\frac{1}{\sqrt{2}}$  with for much of this book, and which lies at this book, and which lies at the heart of what makes  $\frac{1}{\sqrt{2}}$

Suppose we have two qubits. If these were two classical bits, then there would be four possible states, 00, 01, 10, and 11. Correspondingly, a two qubit system has four computational basis states denoted<br>
Heal leal leal leal basis is a big place would be four-|00), |01), |10), |11). A pair of qubits can also exist in superpositions of these four states, so the quantum state of two qubits involves associating a these four states, so the quantum state of two qubits involves associating a<br>complex coefficient – sometimes called an amplitude – with each computational basis state, such that the state vector describing the two qubits is *Hilbert space is a big place.* we have two qubits. If these were two classical bits, then there possible states, 101, 11, and 11. Corresponding to the second in **11.** Corresponding to the second integrating system has four *community* system in the system of the supply complex community superpositions of the state of the modern state of two states of the two quantum states associations associations at the state of th computational basis state, such that the state vector aesembing the two state, such that the state vector describing the two qubits is al basis state, such that the state vector describing the two  $\overline{\phantom{a}}$ possible states, 00, 01, 10, and 11. Correspondingly, a two qubit system has four *com-*

 $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$ 

Similar to the case for a single qubit, the measurement result x (= 00, 01, 10 or 11) occurs with probability  $|\alpha_x|^2$ , with the state of the qubits after the measurement being  $|x\rangle$ . The condition that probabilities sum to one is therefore expressed by the normalization condition of the incasurement being  $\beta$ , the condition that probabilities sum to one  $S_{\text{max}}$  or  $\frac{1}{2}$  ( $\frac{1}{2}$   $\frac{1}{2}$   $\frac{1}{2}$  expressed by the normalization condition with probability *|*α*x|* 2, with the state of the qubits after the measurement being *<sup>|</sup>x*!. The

> ! <sup>=</sup> <sup>α</sup>00*|*00! <sup>+</sup> <sup>α</sup>01*|*01!  $\sum_{x \in \{0,1\}^2} |\alpha_x|^2 = 1$ of length two with each letter being either zero or one'. For a two qubit system, we could

More generally, we may consider a system of n qubits. The computational basis states of this system are of the form  $|x_1x_2...x_n\rangle$ , and so a quantum state of such a system is specified by  $2^n$  amplitudes. "*|*α00*|* <sup>2</sup> + *|*α01*|* measure just a subset of the qubits, say the first qubit, and you can probably guess how this we may consider a system of h qubits. The com<u>putational strategive</u><br>| of this system are of the form ly y = = x \ and so a quantum

Two ways of denoting the qubits  $\frac{1}{\sqrt{2}}$ 

Binary basis: sequence of 0 and 1, i.e.  $|x_{n-1}x_{n-2}...x_0\rangle$ **Decimal basis:**  $|x\rangle$ , with  $x = x_{n-1} 2^{n-1} + x_{n-2} 2^{n-2} + ... + x_0$ *|*00! + *|*11!

Examples  $|10\rangle = | 1 \times 2^{1} + 0 \times 2^{0} \rangle = | 2 \rangle$  $|101\rangle = | 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 \rangle = |6 \rangle$  α00*|*00! + α01*|*01!

<sup>2</sup> + *|*α01*|*

"*|*α00*|*

*|*00! + *|*11! √

2

<sup>2</sup> *.* (1.6)

The set employed should be clear from the context. An *n*-qubit system has 2*<sup>n</sup>* = the basis for a two-qubit system may be written also as *{|*0\$*, |*1\$*, |*2\$*, |*3\$*}* with  $\sum_{i=1}^n \frac{1}{i}$  notation. When  $\sum_{i=1}^n \frac{1}{i}$  system is system is system in the decimal system in the decimal system i of *n* qubits may be taken to be *{|bn*−1*bn*−<sup>2</sup> *...b*0\$*}*, where *bn*−1*, bn*−2*,...,b*<sup>0</sup> ∈ **The set** express the decimal system of the decimal system. The decimal system of the decimal system of the decimal system of the decimal system of the decimal system. The decimal system of the decimal system of the decima

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

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

is an orthonormal basis of a two-qubit system and is called the **Bell basis**. <del>√2011</del> Statemental stasts or a two quart system and is called the Bell state. Each vector is called the Bell state or the Bell vector. Note that all the Bell  $\text{states are entangled.}$ Eddin vector is called the Bell state of the Bell vector. Note that all the Bell basis and interests. States are critain grow. *\*<br>| basis of a two-qubit system and is<br>| s called the Bell state or the Bell vector.  $\frac{1}{10}$ 

EXERCISE. The Bell basis is obtained from the binary basis  $\{ |00\rangle, |01\rangle, \rangle$ |10), |11}} by a unitary transformation. Write down the unitary transformation explicitly. The state or the Bell state or the Bell state or the Bell state or the Bell state o EVEDCICE The Bell basis is obtained from the binary |10), |11}} by a unitary transformation. Write down the unitary<br>transformation explicitly  $\alpha$  *|*10\$*,*  $\alpha$  |*10\$*,  $\alpha$  |*110\$*,  $\alpha$  |*110\$* 

Among three-qubit entangled states, the following two states are ។<br>ប is called the Greenberger-Horne-Zeilinger state and is often abbreviated important for various reasons and hence deserve special names. The state tion explicitly. for various reasons and hence deserve special names. The state deserve special names. The  $\mathsf{state}$  and unitary transformation. Write down the unitary transformation. Write down the unitary transformation of  $\mathsf{true}$ 

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

is called the Greenberger-Horne-Zeilinger state and is often  $\frac{4}{3}$ abbreviated as the GHZ state. Another important three-qubit state is the W state is the W state is called the Greenberg state and is often abbreviated the Greenberg sta

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

# Quantum Computation

A quantum computation is a collection of the following three elements:

- A register or a set of registers,
- A unitary matrix U, which is tailored to execute a given quantum algorithm
- Measurements to extract information we need.

More formally, we say a quantum computation is the set  $\{H, U, \{M_m\}\}\$ , where H =  $C^{2n}$  is the Hilbert space of an n-qubit register,  $U \in U(2^n)$ represents the quantum algorithm and {M<sub>m</sub>} is the set of measurement operators. The hardware along with equipment to control the qubits is called a quantum computer.

#### Single Qubit Quantum Gates gate is easily found as *I* = *|*0!"0*|* + *|*1!"1*|* = Similarly we introduce *X* : *|*0! → *|*1!*, |*1! → *|*0!, *Y* : *|*0!→−*|*1!*, |*1! → *|*0!, and *Z* : *|*0! → *|*0!*, |*1!→−*|*1!, whose matrix representations are Similarly we introduce *X* : *|*0! → *|*1!*, |*1! → *|*0!, *Y* : *|*0!→−*|*1!*, |*1! → *|*0!, and *Z* : *|*0! → *|*0!*, |*1!→−*|*1!, whose matrix representations are

$$
I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
$$
  
\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* = *I* = *negotion* (*NOT*) frace is the trivial (identity) transform  $Z$  the phase shift and  $Y = XZ$  the quality *Y* = *|*0!"1*|* − *|*1!"0*|* = that these gates are unitary.  $\Gamma$ he transformation *I* is the trivial (identity) transformation, while *X* is the  $\overline{\phantom{a}}$  asily verified that negation (NOT), *Z* the phase shift and  $Y = XZ$  the combination of them. It  $_{\rm 120}$ is easily verified that these gates are unitary. The transformation *I* is the trivial (identity) transformation, while *X* is the

*ZA* = *LACTUBE*. I THU t <mark>ne Hamil</mark> **2** *a*  $\frac{1}{2}$  *n* and the manifestion that *Imprements* these = σ*z.* (4.4) **Exercise: Eind the Hamiltonian that implements these gates, and show** *|***1000** they are implemented. ||I|||coman that implements these gates, and show and the first state is **partlel** Let *{|*00!*, |*01!*, |*10!*, |*11!*}* be a basis for the two-qubit system. In the following,  $\frac{1}{2}$  representing the lomitanian that implements these gates and show Exercise: Find the Hamiltonian that implements these gates, and show how they are implemented.

Three other quantum gates will play a large part in what follows, the Hadamard gate (denoted *H*), phase gate (denoted *S*), and  $\pi/8$  gate (denoted *T*):

$$
H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}.
$$
 (4.2)

A couple of useful algebraic facts to keep in mind are that  $H = (X + Z)/\sqrt{2}$  and  $S = T^2$ . You might wonder why the T gate is called the  $\pi/8$  gate when it is  $\pi/4$  that appears in the definition. The reason is that the gate has historically often been referred to as the  $\pi/8$  gate, simply because up to an unimportant global phase T is equal to a gate which  $\frac{1}{\text{has } \text{exp}(\pm i\pi/8) \text{ appearing on its diagonals.}}$  $\mathbb{R}$  return to this picture of this picture of this picture of this picture of the intuition.  $P(\pm in)$  of appearing on its analysians.

$$
T = \exp(i\pi/8) \left[ \begin{array}{cc} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{array} \right]. \tag{4.3}
$$

Nevertheless, the nomenclature is in some respects rather unfortunate, and we often refer<br>to this rate as the  $T$  rate. to this gate as the  $T$  gate.

The Pauli matrices give rise to three useful classes of unitary matrices when they are exponentiated, the *rotation operators* about the  $\hat{x}$ ,  $\hat{y}$ , and  $\hat{z}$  axes, defined by the equations:

$$
R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}
$$
(4.4)

$$
R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}
$$
(4.5)

$$
R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2} \end{bmatrix}.
$$
 (4.6)

 $\frac{1}{2}$  unitary transformation defined by The **Hadamard gate** or the **Hadamard transformation** *H* is an important unitary transformation defined by  $\overline{\phantom{a}}$  -<sup>−</sup>*i*sin <sup>θ</sup> <sup>2</sup> cos <sup>θ</sup>

$$
U_{\rm H}: |\hspace{.05cm}0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \begin{array}{c} \text{-} \\ \text{-} \\ \text{-} \\ \text{+} \\ \text{+} \end{array} \tag{4.9}
$$
\n
$$
|\hspace{.06cm}1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).
$$

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-Walsh 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  $|00...0\rangle$ : exp(*iAx*) = cos(*x*)*I* + *i*sin(*x*)*A.* (4.7)  $\text{F1}$  the state  $[00...0]$ .

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

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 *Wn*. Note that  $\mathcal{L}_{\text{H}}$ . (Bloch sphere interpretation of rotations) of  $\mathcal{L}_{\text{H}}$ 

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

## Exercises  $v_{\rm c}$ mysterious looking factor of two in the definition of the rotation matrices.

**Exercise 4.7:** Show that  $XYX = -Y$  and use this to prove that  $XR_y(\theta)X = R_y(-\theta).$ 

Exercise 4.8: An arbitrary single qubit unitary operator can be written in the form

$$
U = \exp(i\alpha)R_{\hat{n}}(\theta) \tag{4.9}
$$

for some real numbers  $\alpha$  and  $\theta$ , and a real three-dimensional unit vector  $\hat{n}$ .

- 1. Prove this fact.
- The shows that the control bit and the target bit and the target bit in a CNOT gate bit 2. Find values for  $\alpha$ ,  $\theta$ , and  $\hat{n}$  giving the Hadamard gate *H*.
	- 3. Find values for  $\alpha$ ,  $\theta$ , and  $\hat{n}$  giving the phase gate

$$
S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.
$$
 (4.10)

### Exercise 4.13: (Circuit identities) It is useful to be able to simplify circuits by inspection, using well-known identities. Prove the following three identities:

$$
HXH = Z; \quad HYH = -Y; \quad HZH = X. \tag{4.18}
$$

Exercise 4.14: Use the previous exercise to show that  $HTH = R_x(\pi/4)$ , up to a where  $\frac{1}{\sqrt{2}}$  denotes the first qubit, while  $\frac{1}{\sqrt{2}}$  denotes the second. What are the second. What are the second  $g$ lobal phase. global phase. 6

#### Two qubit gates: CNOT Gate The transformation *I* is the trivial (identity) transformation, while *X* is the  $\mathcal{L}_\text{max}$  and the gate flips the gate flips the gate flips the gate flips the seco-putation. The gate flips the sec- $M\cap$  qubit  $\sigma$ ates $\cdot$  ( $M(1)$ ) is easily qubit (the control qubit) is  $\sigma$ *|*1!, while leaving the second bit unchanged when the first qubit state is *|*0!. qubit gates: CNOT Gate EXERCISE 4.2 Let (*a|*0! + *b|*1!) ⊗ *|*0! be an input state to a CNOT gate. *|*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,  $T_{\text{MLO}}$  qubit gator: CNIAT G *|*1!, while leaving the second bit unchanged when the first qubit state is *|*0!.

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  $|0\rangle$ . It has two expressions of the action of the contract of the contract of the contract of the first qubit (t The CNOT (controlled-NOT) gate is a two-qu

Let *{|*00!*, |*01!*, |*10!*, |*11!*}* be a basis for the two-qubit system. In the following,  $U_{\text{CNOT}}$  :  $|00\rangle \mapsto |00\rangle$ ,  $|01\rangle \mapsto |01\rangle$ ,  $|10\rangle \mapsto |11\rangle$ ,  $|11\rangle \mapsto |10\rangle$ . **b**  $|01\rangle$ ,  $|01\rangle$   $|10\rangle$ ,  $|11\rangle$   $|11\rangle$ ,  $|10\rangle$  $U_{\text{CNOT}}~: |00\rangle \mapsto |00\rangle,~|01\rangle \mapsto |01\rangle,~|10\rangle \mapsto |11\rangle,~|11\rangle \mapsto |10\rangle.$  $U_{\rm CNC}$  $U\text{CNOT}$  :  $|00\rangle \mapsto |00\rangle$ ,  $|01\rangle \mapsto |01\rangle$ ,  $|10\rangle \mapsto |1\rangle$ 





Let  $\{|i\rangle\}$  be the basis vectors, where  $i \in \{0,1\}$ . The action of CNOT on that is,  $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1$  and  $1 \oplus$  $\begin{array}{c} 1000, 1000 \end{array}$  $\overline{a}$   $\overline{b}$  $1 = 0.$ Let  $\{|i\rangle\}$  be the basis vectors, where  $i \in \{0,1\}$ . The action of CNOT on Let  $\{|i\rangle\}$  be the basis vectors, where  $i \in \{0, 1\}$ . The action of CNOT on<br>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  $1 \oplus 1 = 0$ .  $\cos i \in (0, 1]$ . The estion of CNOT on basis vectors, where  $i \in \{0, 1\}$ . The action of CNOT on having a matrix form  $\mathbf{I}$  at  $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$  be the best state

*U*CNOT = *|*00!"00*|* + *|*01!"01*|* + *|*11!"10*|* + *|*10!"11*|* EXERCISE 4.1 Show that the *U*CNOT cannot be written as a tensor prod-= *|*0!"0*|* ⊗ *I* + *|*1!"1*|* ⊗ *X,* (4.5) The second expression of the RHS in Eq. (4.5) shows that the action of  $\mu$ CNO Williams that the action of *UCNOT* The following identity holds when the control  $\alpha$ <sup>1</sup> is in  $\alpha$ <sup>1</sup> in  $\alpha$ <sup>1</sup> is unitary and, moreover, more over, more over, more over, more over, more over, m

$$
\begin{array}{rcl}\n\text{CNOT} & = & |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \\
& = & \frac{1}{2}(I + Z) \otimes I + \frac{1}{2}(I - Z) \otimes X \\
& = & \frac{1}{2}I \otimes (I + X) + \frac{1}{2}Z \otimes (I - X)\n\end{array}
$$

### on the target qubit is *I* when the control qubit is in the state *|*0!, while it is σ*<sup>x</sup>* Control-U Gate idempotent, i.e., *U*<sup>2</sup> CNOT = *I*.

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 EXERCISE 4.1 Show that the *U*CNOT cannot be written as a tensor prod-

The SWAP gate acts on a tensor product state as EXERCISE 4.2 Let (*a|*0! + *b|*1!) ⊗ *|*0! be an input state to a CNOT gate.

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

The explict form of  $U_{\text{SWAP}}$  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 is the output  $\sim$  the time flows from the time flows from the right. The right to the right to the right. equess to say, it works as a line<br>



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. 68 *QUANTUM COMPUTING*

#### Exercise the input state *|i*!*|j*! is written as *|i*!*|i* ⊕ *j*!, where *i* ⊕ *j* is an addition mod 2, 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

**EXERCISE 4.1** Show that the  $U_{\text{CNOT}}$  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  $\frac{1}{8}$ circuit on a tensor product state  $|\psi_1\rangle \otimes |\psi_2\rangle$ .

Given the outcome of Exercise 4.3(c) and the mathematical expression of the CNOT gate, one can write

$$
\begin{array}{rcl}\n\text{SWAP} & = & \text{CNOT} \overline{\text{CNOT}} \text{CNOT} \\
& = & \frac{1}{2}(I \otimes I + Z \otimes Z) + \frac{1}{2}X \otimes X(I \otimes I - Z \otimes Z)\n\end{array}
$$

This expression (using the relation Y = XZ) can be rewritten as:

$$
SWAP = \frac{1}{2}(I \otimes I + X \otimes X - Y \otimes Y + Z \otimes Z)
$$

elati √2 (*|*0! + *|*1!) ⊗ Given the relation between the gates X, Y, Z and the Pauli matrices, we have also:

SWAP = 
$$
\frac{1}{2}(I \otimes I + \bar{\sigma} \otimes \bar{\sigma}) = \frac{1}{2}(I \otimes I + \sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z)
$$

*|x*!*.* (4.11)

## Exercise EXERCISE 4.4 Show that *W<sup>n</sup>* is unitary.

<sup>√</sup>2*<sup>n</sup>*

EXERCISE 4.5 Show that the two circuits below are equivalent:



transformation, or  $\mathcal{M}$  as a straightformation, and denoted as  $\mathcal{M}$  as a straightformation, and denote

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  $|11\rangle$ ?

#### 3 qubit gate: CCNOT (Toffoli) Gate (3) Find the matrix representation of the circuit (c). Find the action of the circuit on a tensor product state *|*ψ1! ⊗ *|*ψ2!. *Quantum Gates, Quantum Circuit and Quantum Computation* 71  $\sigma$  explicit generic con

 $T$ he **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 oned-Con 1 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.  $\frac{1}{2}$ 

# $\mathcal{A} = \mathcal{A} \cup \mathcal{A}$  walshed the contribution of the contribution  $\mathcal{A} = \mathcal{A} \cup \mathcal{A}$ 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  $|1\rangle$ bits when and only when the first (top) qubit is in the state  $|1\rangle$ (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 en simple circuit for the Toget made up of *ing in and π/8 g* built from just this gate set. Figure 4.9 illustrates a simple circuit for the Toffoli gate  $N\delta T^1$



Because of the great usefulness of the Toffoli gate it is interesting to see how it can be

Figure 4.9. Implementation of the Toffoli gate using Hadamard, phase, controlle $\frac{1}{N}$  and  $\pi/8$  gates.

Exercise 4.24: Verify that Figure 4.9 implements the Toffoli gate. Exercise 4.24: Verify that Figure 4.9 implements the Toffoli gate.

Exercise 4.25: (Fredkin gate construction) Recall that the Fredkin Exercise 4.25: (Fredkin gate construction) Recall that the Fredkin (controlled-swap) gate performs the transform (controlled-swap) gate performs the transform



- (1) Give a quantum circuit which uses three Toffoli gates to construct the Fredkin gate (*Hint*: think of the swap gate construction – you can control each gate, one at a time).
- (2) Show that the first and last Toffoli gates can be replaced by CNOT gates.
- (3) Now replace the middle Toffoli gate with the circuit in Figure 4.8 to obtain a Fredkin gate construction using only six two-qubit gates.
- (4) Can you come up with an even simpler construction, with only five two-qubit gates?



### Exercise van Fredekin gate construction using only six two-qubit gates.  $\mathbf{S}$  Now replace the middle Toffoli gate with the circuit in  $\mathbf{S}$  to obtain  $(4)$  Can you come up with an even simpler construction, with only five  $\mathcal{L}$

Exercise 4.26: Show that the circuit:



up to relative phases than it is to do the Toffoli directly.

 $\text{CNOT}$ EXOT: USING  $\mathcal{C}$  and Toffolia gates, construction construct a quantum circuit to  $\mathcal{C}$  and  $\mathcal{C}$  to  $\mathcal{C}$  and  $\mathcal{C}$  are constructed as  $\mathcal{C}$  and  $\mathcal{C}$  are constructed as  $\mathcal{C}$  and  $\mathcal{C}$  are cons

Exercise 4.27: Using just CNOTs and Toffoli gates, construct a quantum circuit to perform the transformation

$\left[ \begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right] \ .$				

This kind of partial cyclic permutation operation will be useful later, in Chapter 7. How may we implement *C<sup>n</sup>*(*U*) gates using our existing repertoire of gates, where *U*  $\sum_{i=1}^n a_i$  unitary single circuit for achieving containing  $\sum_{i=1}^n a_i$ 



produce the product *c*<sup>1</sup> *· c*<sup>2</sup> *...cn*. To do this, the first gate in the circuit s *c*<sup>1</sup> and  $\overline{a}$   $\overline{a}$   $\overline{b}$   $\overline{c}$   $\overline{$ 

# 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.

In general: Observe that the OR gate is implemented with the *X* and the CCNOT gates and, more over, the *X* gate is obtained from the CCNOT gate by put the CCNOT gate by put the CCNOT gate by put

- 1. Take a classical gate. If irreversible, consider its reversible variant. If you a gradual gate. *We calculately condition to 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. EXERCISE 4.9 Show that the NAND gate can be obtained from the CC-3. Extend it by linearity to the whole space.

The gate thus obtained is the quantum generalization of the classical gate.<br>

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.

## Exercise to approximate to approximate the goal of  $\overline{C}$ esting families of unitary transformations that *can* be performed efficiently.

Exercise 4.36: Construct a quantum circuit to add two two-bit numbers *x* and *y* modulo 4. That is, the circuit should perform the transformation  $|x, y\rangle \rightarrow |x, x+y \mod 4\rangle.$ 

What the circuit should do is the following



We see that:

$$
x_0 \to x_0
$$
  
\n
$$
x_1 \to x_1
$$
  
\n
$$
y_0 \to x_0 \oplus y_0
$$
  
\n
$$
y_0 \to x_0 \oplus y_0
$$

 $y_0 \rightarrow x_0 \bigoplus y_0$  and  $y_0$  a This is implemented by a CNOT gate  $\mathcal{D}(x, y)$  we  $\mathcal{D}(x, y)$  is implemented by a CCNOT gate  $y_1 \rightarrow x_1 \bigoplus y_1 \bigoplus (x_0 y_0)$   $y_1 \bigoplus (x_0 y_0)$  is implemented by a CCNOT gate the rest by a CNOT gate



The circuit then is

# Universal Quantum Gates

Like in the classical case, there exist a universal set of quantum gates. We will now show that 82 *QUANTUM COMPUTING*

- Single qubit gates  $\mathcal{L} \left( \mathcal{L} \right)$
- CNOT gate  $\sum_{i=1}^n$  classical logic gate can be constructed by using any construction by using a bounded by using a set of  $\sum_{i=1}^n$

are universal for quantum computation. ale differential for qualitum computation. Since the  $\alpha$ 

## Two-level unitary matrix **IN THE FOLLOWING**

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

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

# *Proof of lemma: d = 3 U*<sub>2</sub> *U*<sub>2</sub> *...u*<sub>1</sub> *...*

*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<br>unitary.) We prove the above decomposition by constructing  $U_k$  evolvisitly unitary.) We prove the above decomposition by constructing  $U_k$  explicitly.

(i) Let (i) Let (i) Let

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

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

$$
U_1U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix},
$$

where *a*! *,...,j*! are some complex numbers, whose details are not necessary. where  $a', \ldots, j'$  are some complex numbers, whose details are not necessary. Observe that, <u>with this choice of  $U_1$ , the first component of the second row</u> (ii) Letter and the control of the <br>(iii) Letter and the control of the vanishes. Observe that, with this choice of *U*1, the first component of the second row vanishes.

 $\left| \frac{1}{2} \right|$ (ii) Let

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

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

$$
U_2U_1U = \begin{pmatrix} 1 \ d'' & g'' \\ 0 \ e'' & h'' \\ 0 \ f'' & j'' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 \ e'' & h'' \\ 0 \ f'' & j'' \end{pmatrix},
$$

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.

(iii) Finally let

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

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

Suppose *U* is a unitary matrix acting on C*<sup>d</sup>* with a general dimension *d*.

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 10 0 *...* 0 where the equality  $d$  is unitary,  $d$  follows from the fact that  $d$  is unitary,  $d$  is unita 0 *f*!! *j*!! = 0 *e*!! *h*!! 0 *f*!! *j*!! *,*

### Proof of lemma: any d 0 *h*!!∗ *j*!!∗ *.*

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

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

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

17

П

Exercise

**EXERCISE 4.12** Let  $U$  be a general  $4 \times 4$  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. Esercizio 4.37 del Nielsen Chuang

#### Universality theorem unitary matrix is decomposed into a product of at most 2*<sup>n</sup>*(2*<sup>n</sup>* <sup>−</sup> 1)*/*2 = <sup>2</sup>*<sup>n</sup>*−<sup>1</sup>(2*<sup>n</sup>* <sup>−</sup> 1) two-level unitary matrices. Now we are in a position to state qubit on which *<sup>U</sup>*˜ acts. In the example above, we have *<sup>|</sup>g*3" <sup>=</sup> *<sup>|</sup>*11011" ⊗ *<sup>|</sup>*1" and *<sup>|</sup>t*" <sup>=</sup> *<sup>|</sup>g*4" <sup>=</sup> *<sup>|</sup>*11011"⊗*|*0". Now the operator *<sup>U</sup>*˜ may be introduced so that  $\ldots$  on a two-dimensional subspace of the total Hilbert space of the total Hilbert space, in which the total Hilbert s ality the 0 ∗∗∗ U ∣≀ *.* I Iniversality theorem the sequence satisfies the boundary conditions *g*<sup>1</sup> = *s* and *g<sup>m</sup>* = *t*. Suppose *s* = 100101 and *t* = 110110, for example. An example of a Gray

**THEOREM 4.2** (Barenco *et al.*) The set of single qubit gates and  $CNOT$  as to universed. Nomely any unitary at a setima on an a subit CNOT gate are universal. Namely, any unitary gate acting on an *n*-qubit  $\frac{1}{\sqrt{2}}$  register can be implemented with single qubit gates and CNOT gates. so that *|g<sup>m</sup>*−<sup>1</sup>" → *|g<sup>m</sup>*−<sup>2</sup>" → *...* → *|g*1" = *|s*". Each of these steps can be  $et\ al.)$  The set of single qubit gates and ÷ 11 1 1 **i 4.2** (Barenco *et al.*) ÷ Let us consider a unitary matrix acting on an *n*-qubit system. Then this quality is the term of the ter



Step 1. The two-level unitary matrix U can be reduced to a 2x2 unitary restrix  $\mathbf{u}$  and  $\mathbf{u}$ . matrix.

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

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

$$
\blacktriangleright
$$

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

\n $U = \begin{pmatrix}\n a & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 1 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 1 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 1 & 0 & 0 & 0 \\  0 & 0 & 0 & 1 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 1 & 0 & 0 \\  0 & 0 & 0 & 0 & 1 & 0 & 0 \\  0 & 0 & 0 & 0 & 1 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 1 & 0 \\  0 & 0 & 0 & 0 & 0 & 1 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 1 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 & 0 & 0 & 0 & 0 \\  0 & 0 & 0 &$
--

 $\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$  our case s = 000 and t = 111; an example of  $(a\ 0\ 0\ 0\ 0\ 0\ c)$  Define the Gray code connecting s and t. It is  $\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$  a sequence of binary numbers such that adjacent numbers differ only by one bit. In  $\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$  Gray code is

 $b_3 = 1$  $g_4 = 1$ *q*<sup>1</sup> *q*<sup>2</sup> *q*<sup>3</sup>  $g_1 = 0 \ 0 \ 0$  $g_2 = 1 \ 0 \ 0$  $g_3 = 1 \; 1 \; 0$  $g_4 = 1 \; 1 \; 1$  $g_1 = 0 \quad 0 \quad 0$ <br>  $g_2 = 0 \quad 0 \quad 0$  $\begin{aligned} \n0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \frac{d}{f} \n\end{aligned}$ 

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

> with the target bits  $\alpha$ <sup>3</sup> and  $\alpha$ <sup>2</sup> and  $\alpha$ <sup>2</sup>.) After this control bits *q*<sup>2</sup>. 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  $\frac{1}{2}$  the sequer  $g$ <sub>110</sub> sequent

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

Then  $\mathsf{g}_{\mathsf{m}\text{-}1}$  and  $\mathsf{g}_{\mathsf{m}}$  differ only in one bit, which is identified with the single qubit on which U acts. After having applied the U gate, we bring things back. In our example: it acts on a two-dimensional subspace of the total Hilbert space of the total Hilbert space, in which the total Hilbert space, in which the total Hilbert space, in which the total Hilbert space, in wh Then *g<sup>m</sup>*−<sup>1</sup> and *g<sup>m</sup>* differ only in one bit, which is identified with the single Then  $g_{m-1}$  and  $g_m$  differ only in one bit, which is identified with the single *s* and *t* differ at most in *n* bits. where preparations, we consider the implementations, we consider the implementation of  $\mathcal{U}$ . The strate-the strate-the strategy of  $\mathcal{U}$  and  $\mathcal{U}$  and  $\mathcal{U}$  and  $\mathcal{U}$  and  $\mathcal{U}$  and  $\mathcal{U}$  and  $\mathcal{U}$ 

$$
|s\rangle = |000\rangle \longrightarrow |100\rangle \longrightarrow |110\rangle = |11\rangle \otimes |0\rangle
$$
  
\n
$$
|t\rangle
$$
  
\nDO the Gary code  
\nAct with the 2x2 gate  $\tilde{U}$   
\nUNDO the Gary code

#### Universality theorem: d = 3 example it acts on a two-dimensional subspace of the total Hilbert space, in which the so that *|g<sup>m</sup>*−<sup>1</sup>" → *|g<sup>m</sup>*−<sup>2</sup>" → *...* → *|g*1" = *|s*". Each of these steps can be is also unitary. An example of a Gray code connecting 000 and 111 is where the adjacent numbers, *g<sup>k</sup>* and *gk*+1, differ in exactly one bit. Moreover, Gray code connecting *s* and *t* is a sequence of binary numbers *{g*1*,...,gm}* the sequence satisfies the boundary conditions *g*<sup>1</sup> = *s* and *g<sup>m</sup>* = *t*. Suppose *s* = 100101 and *t* = 110110, for example. An example of a Gray



Let us consider the effect on a qubit different from  $|s>$  and  $|t>$ , for  $\frac{1}{2}$  example the qubit  $\frac{101}{2}$ 



Or the qubit | 100> with the target bit *q*<sup>3</sup> and the control bits *q*<sup>1</sup> and *q*2.) After this controlled with the target bit *q*<sup>3</sup> and the control bits *q*<sup>1</sup> and *q*2.) After this controlled with the target bit *q*<sup>3</sup> and the control bits *q*<sup>1</sup> and *q*2.) After this controlled with the target bit *q*<sup>3</sup> and the control bits *q*<sup>1</sup> and *q*2.) After this controlled on the input α*|*000! + β*|*111! is



*Quantum Gates, Quantum Circuit and Quantum Computation* 87





on the input α*|*000! + β*|*111! is While on 1000> and the state of the stat *Quantum Gates, Quantum Circuit and Quantum Computation* 87 in Fig. 4.7 (a) in Fig. 4.7



*U*-gate acts only on the third qubit *a*<sup>22</sup> the gate acts only on the third qubit *bay* on the trind qubit *U*-gate acting on α*|*000! + β*|*111! yields the desired output (*a*α + *c*β)*|*000! + The gate acts only on the third qubit  $22$ 



EXERCISE 4.14 (1) Find the shortest Gray code which connects 000 with 110.  $R$ eturning to the general case, we see that inplementing the two-level unitary operation  $\mathcal{L}$ 

 $(2)$  Use this result to find a quantum circuit, such as Fig. 4.5, implementing a two-level unitary gate

 $CN$  T

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

Exercise 4.39: Find a quantum circuit using single qubit operations and CNOTs to implement the transformation

$$
\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix},
$$
\n(4.60)

It will be shown next that all the gates in the above circuit can be *I* mplemented with single-qi<br>universality of these gates. ่ไ t gates and CNOT gat<br>
– *,* (4.54) implemented with single-qubit gates and CNOT gates, which proves the

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



Controlled-*U* gate is made of at most three single-qubit gates and two CNOT **LEMMA 4.2** Let  $U \in SU(2)$ . Then there exist  $\alpha, \beta, \gamma \in \mathbb{R}$  such that  $U =$ <br> $B(\alpha)B(\beta)B(\alpha)$  where  $R_z(\alpha)R_y(\beta)R_z(\gamma)$ , 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

$$
R_z(\alpha)R_y(\beta)R_z(\gamma) = \begin{pmatrix} e^{i(\alpha+\gamma)/2}\cos(\beta/2) & e^{i(\alpha-\gamma)/2}\sin(\beta/2) \\ -e^{i(-\alpha+\gamma)/2}\sin(\beta/2) & e^{-i(\alpha+\gamma)/2}\cos(\beta/2) \end{pmatrix}.
$$
 (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  $X = \sigma_x$ .  $x \in A, B, C \in \mathcal{S}$ **L**  $\Omega$  such that

*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  $\overline{AC}$  and  $\overline{ABC} = I$ , where  $\overline{A} = \sigma_x$ .<br>
I'm a 4.2 states that  $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$  for some

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

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.

*R*<sub>*R*</sub> *R*<sup>*z*</sup>(*R*<sup>*z*</sup> *R*<sup>*z*</sup>(*R*<sup>*z*</sup>)*R*<sup>*z*</sup>(*R*<sup>*z*</sup>)*R*<sup>*z*</sup>(*R*<sup>*z*</sup>)*R*<sup>*z*</sup>(*R*<sup>*z*</sup>)*R*<sup>*z*</sup>(*R*<sup>*z*</sup>)*R*<sup>*z*</sup>(*R*<sup>*z*</sup>)*R*<sup>*z*</sup>(*R*<sup>*z*</sup>)*Az*(*R*<sup>*z*</sup>)*Az*(*R*<sup>*z*</sup>)*Az*(*R*<sup>*z*</sup>)*Az*(*R*<sup>*z*</sup>)*Az*  $\frac{1}{2}$  as  $\frac{1}{2}$ **LEMMA 4.4** Let  $U \in SU(2)$  be factorized as  $U = AXBXC$  as in the l be implemented wit *R<sup>z</sup>* ! previous Lemma. Then the controlled-*U* gate can be implemented with at  $\mathbf{t}$ 

*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  $\frac{1}{2}$  is  $\frac{1}{2}$  in  $\frac{1}{2}$  in  $\frac{1}{2}$  in  $\frac{1}{2}$ 

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

while when the control bit is 1, we have

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



ш

# $From SU(2) to (2)$ *|*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  $U = e^{i\alpha}V$ ,  $V \in SU(2)$ ,  $\alpha \in \mathbb{R}$ . So far, we have worked with  $U \in SU(2)$ . To implement a general  $U \in U(2)$ , we have worked with  $U \in U(2)$ . To  $\sup$ <br>*With*  $U \in U(2)$  we have to deal with the phase Let

LEMMA 4.5 Let LEMMA 4.5 Let

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

and

.

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

gates as  $\mathbf{F}$  gate is expressed as the controlled- $\mathbf{F}$  of single qubits  $\mathbf{F}$  (4.50) Then the controlled- $\Phi(\phi)$  gate is expressed as a tensor product of single qubit gates as *U*CO CAPI CODECT AND A VEHICLE PLACED OF DIRECT QUOTE

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

 $\Phi(\phi)$ 

П

. *Proof*. The LHS is  $U$ **PC**  $U$ *H***<sub>2</sub>**  $I$ **</sub>**  $B$  $I$  $I$ 

*Proof*. The LHS is

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

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. Figure 4.9 shows the station.

*<sup>|</sup>*0!'0*<sup>|</sup>* <sup>+</sup> *<sup>e</sup><sup>i</sup>*<sup>φ</sup>*|*1!'1*<sup>|</sup>* ⊗ *I* = *U*CΦ(φ)*,* controlled- $V_2$  gate  $U_{CV_2}$ . Show that the controlled- $V_1$  gate followed by the  $\frac{2}{3}$  shows the statement of the above lemma. controlled- $V_2$  gate is the controlled- $V_2V_1$  gate  $U_{C(V_2V_1)}$  as shown in Fig. 4.10. **EXERCISE 4.15** Let us consider the controlled- $V_1$  gate  $U_{CV_1}$  and the



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  $U \in U(2)$ . Then the controlled-*U* gate  $U_{CU}$  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:

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

where

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

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



### FIGURE 4.11

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

Step 3. The CCNOT gate and its variants are implemented with CNOT gates and its variants **Controlled-** U gate is implemented with a most four single-qubit gate  $\alpha$ 



 $\mathbf{F} = \mathbf{F} \cdot \mathbf{F} \cdot \mathbf{F} \cdot \mathbf{F}$ **LEMMA 4.6** The two quantum circuits in Fig. 4.12 are equivalent, where  $U = V^2$  $U = V$  .  $U = V^2$ .

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  $|01\rangle\langle01| \otimes I$ .  $|\psi\rangle \mapsto VV^{\dagger}|\psi\rangle = |\psi\rangle$ ; 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  $|U|\psi\rangle = |U|\psi\rangle$ ; 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 *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 When the first qubit is 1 and the second is 0, the third qubit is mapped as

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

namely the controlled-controlled-*U* gate. controlled-**U** gate is implemented with a most four single-qubit gate  $\blacksquare$ 



**EXERCISE 4.17** Show that the circuit in Fig. 4.13 is a controlled- $U$  gate **EXERCISE 1.11** Show that the energy in Fig. 4.15 is a controlled  $\sigma$  gate with three control bits, where  $U = V^2$ . which direct conduct shot, where  $v = v$ .



**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.

order. The above controlled-<br><u>The above controlled-</u> U gate with  $\frac{1}{2}$  game and  $\frac{1}{2}$ The proof of the above proposition is very similar to that of Lemma 4.6 *I* otherwise. This is intuitive proposition is very similar to that of figures and Exercise 4.17 and is left as an exercise to the readers.

Theorem 4.2 has been now proved. 94 *QUANTUM COMPUTING*



order. The above controlled-*U* gate with  $(n-1)$  control bits requires  $\Theta(n^2)$ itary gates. The us write the number of the elementary gates requ 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 Decomposition of the C<sub>(</sub>*n*−1)<sup>*U*</sup> games the top denotes the top denotes the top denotes the top denotes the layer elementary gates.<sup>∗†</sup> Let us write the number of the elementary gates required

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 ire  $\Theta(n)$  elementary gates. Finally the layer V, a controlled-*V* gate  $(n-2)$  control bits, requires  $C(n-1)$  basic gates by definition. Thus we n) elementary gates. Finally the layer v, a controlled-v gate obtain a recursion relation. Thus we have a recursion relation. Thus we have  $\alpha$  $\sum_{i=1}^{n}$   $\sum_{i=1}^{n}$  $r$  function  $\Theta(n)$  elementary gates. Finally the layer V, a controlled-V gate with

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

The solution to this recursion relation is 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.

 $\blacksquare$