Introduction to Quantum Computing

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Unitary Transformations

Quantum Transformations: Linearity

- A **quantum transformation** is a mapping from the state space of a quantum system to itself.
- Nature does not allow arbitrary quantum transformations.
- It forces these transformations to respect:
  - Properties connected to quantum superposition;
  - Properties connected to quantum measurement.

Superposition and Linearity

- The transformations must be linear transformations of the vector space associated with the state space of the quantum system.
- This ensures that a state that is a superposition of other states goes to the superposition of their images.
- More precisely, for any quantum transformation U and any superposition

$$|\psi\rangle = a_1|\psi_1\rangle + \cdots + a_k|\psi_k\rangle,$$

we have

$$U(a_1|\psi_1\rangle + \cdots + a_k|\psi_k\rangle) = a_1 U|\psi_1\rangle + \cdots + a_k U|\psi_k\rangle.$$

- Unit length vectors must go to unit length vectors.
- This implies that orthogonal subspaces go to orthogonal subspaces.

Transformations and Measurement

- Measuring and then applying a transform to the outcome should give the same result as first applying the transform and then measuring in the transformed basis.
- Specifically, the probability of obtaining outcome $U|\phi\rangle$ should be the same whether:
  - We first apply U to $|\psi\rangle$ and then measure with respect to the decomposition $\oplus US_i$;
  - We first measure $|\psi\rangle$ with respect to the decomposition $\oplus S_i$ and then apply U.
- These properties hold if U preserves the inner product.
- For any $|\psi\rangle$ and $|\phi\rangle$, the inner product of their images, $U|\psi\rangle$ and $U|\phi\rangle$, must be the same as the inner product between $|\psi\rangle$ and $|\phi\rangle$,

$$\langle\phi|U^\dagger U|\psi\rangle = \langle\phi|\psi\rangle.$$

Unitary Transformations

- A straightforward mathematical argument shows that the last condition holds for all $|\psi\rangle$ and $|\phi\rangle$ only if $U^\dagger U = I$.
- In other words, the quantum transformation U must be a **unitary linear transformation**, i.e., its adjoint $U^\dagger$ must be equal to its inverse,

$$U^\dagger = U^{-1}.$$

- Furthermore, this condition is sufficient.
- The set of allowed transformations of a quantum system corresponds exactly to the set of unitary operators on the complex vector space associated with the state space of the quantum system.
- Since unitary operators preserve the inner product, they map orthonormal bases to orthonormal bases.
- In fact, conversely, any linear transformation that maps an orthonormal basis to an orthonormal basis is unitary.

Properties of Unitary Transformations

- Geometrically, all quantum state transformations are rotations of the complex vector space associated with the quantum state space.
- The i-th column of the matrix is the image $U|i\rangle$ of the i-th basis vector.
- So for a unitary transformation given in matrix form, U is unitary if and only if the set of columns of its matrix representation are orthonormal.
- Since $U^\dagger$ is unitary if and only if U is, it follows that U is unitary if and only if its rows are orthonormal.
- The product $U_1 U_2$ of two unitary transformations is again unitary.
- If U_1 and U_2 are unitary transformations of X_1 and X_2, the tensor product $U_1 \otimes U_2$ is a unitary transformation of $X_1 \otimes X_2$.
- Linear combinations of unitary operators are not in general unitary.

Transformations versus Measurement

- An obvious consequence of the unitary condition is that every quantum state transformation is reversible.
- In the standard circuit model of quantum computation:
  - All computation is carried out by quantum transformations;
  - Measurement is used only at the end to read out the results.
- Recall that measurement can effect changes in quantum states.
- So an alternative means to achieve computation is via the dynamics of measurement, rather than using quantum state transformations.
- In an alternate, but equally powerful, model of quantum computation, all computation takes place by measurement.

Transformations versus Measurements (Cont'd)

- The phrases **quantum transformation** or **quantum operator** refer to unitary operators acting on the state space, not measurement operators.
- Measurements are modeled by operators.
- However, the behavior of measurement is not modeled by the direct action of the measurement's Hermitian operator on the state space.
- It is rather modeled by the indirect, probabilistic procedure described by the measurement postulate.
- One of the least satisfactory aspects of quantum theory is that there are two distinct classes of manipulations of quantum states:
  - Quantum transformations;
  - Measurement.

The No-Cloning Principle

- A consequence of the unitary condition is that unknown quantum states cannot be copied or cloned.
- Linearity of unitary transformations alone implies this result.
- Suppose U is a unitary transformation that clones,

$$U(|a\rangle|0\rangle) = |a\rangle|a\rangle, \quad \text{for all quantum states } |a\rangle.$$

- Let $|a\rangle$ and $|b\rangle$ be two orthogonal quantum states.
- That U clones means

$$U(|a\rangle|0\rangle) = |a\rangle|a\rangle \quad \text{and} \quad U(|b\rangle|0\rangle) = |b\rangle|b\rangle.$$

- Consider $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$.
- By linearity,

$$U(|c\rangle|0\rangle) = \frac{1}{\sqrt{2}}(U(|a\rangle|0\rangle) + U(|b\rangle|0\rangle)) = \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |b\rangle|b\rangle).$$

The No-Cloning Principle (Cont'd)

- But, since U is a cloning transformation,

$$U(|c\rangle|0\rangle) = |c\rangle|c\rangle = \frac{1}{2}(|a\rangle|a\rangle + |a\rangle|b\rangle + |b\rangle|a\rangle + |b\rangle|b\rangle).$$

- This is not equal to $\frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |b\rangle|b\rangle)$.
- Thus, there is no unitary operation that can reliably clone all quantum states.
- The No-Cloning Theorem tells us that it is impossible to clone a specific unknown quantum state reliably.
- It does not preclude the construction of a known quantum state from a known quantum state.

The No-Cloning Principle (Cont'd)

- It is possible to perform an operation that appears to be copying the state in one basis but does not do so in others.
- For example, consider a given unknown state

$$a|0\rangle + b|1\rangle.$$

- It is possible to obtain n particles in an entangled state

$$a|00\ldots0\rangle + b|11\ldots1\rangle.$$

- But it is not possible to create the n particle state

$$(a|0\rangle + b|1\rangle) \otimes \cdots \otimes (a|0\rangle + b|1\rangle).$$

Subsection 2

Some Simple Quantum Gates

Quantum Gates and Quantum Circuits

- As in classical computation, in quantum computation arbitrarily complex computations can be achieved by composing simple elements.
- The term **quantum gate** refers to any quantum state transformation that acts on only a small number of qubits.
- A **quantum gate array** or **quantum circuit** is a sequence of quantum gates.

Practical Issues

- In the quantum information processing, gates are mathematical abstractions useful for describing quantum algorithms.
- Quantum gates do not necessarily correspond to physical objects, as they do in the classical case.
- So the gate terminology and its accompanying graphical notation must not be taken too literally.
- For solid state or optical implementations, there may be actual physical gates.
- In NMR and ion trap implementations the qubits are stationary particles, and the gates are operations on these particles using magnetic fields or laser pulses.
- For such implementations, gates operate on a physical register of qubits.

Sufficiency Issues

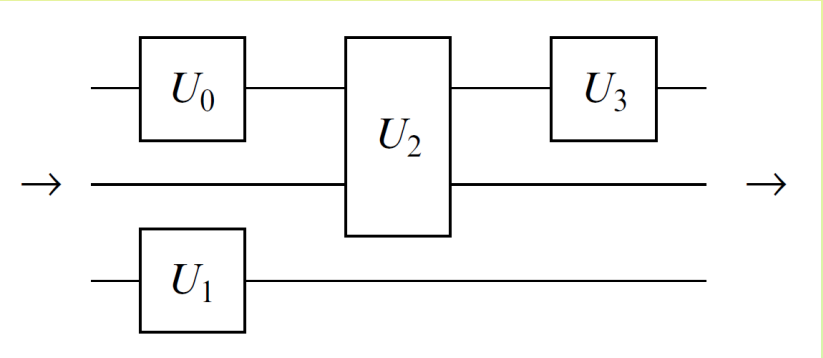
- Ideally, from a practical point of view, we would write all our computations in terms of gates that are easy to implement physically and are robust.
- However, we do not yet know which ones these are.
- Furthermore, we would like to realize physically a quantum computer capable of performing arbitrary quantum transformations.
- For this, it would be convenient to have only finitely many gates that could generate all unitary transformations.
- Unfortunately, such a set is impossible.
  - There are uncountably many quantum transformations.
  - On the other hand, a finite set of generators can only generate countably many elements.

Approximation

- We will see that it is possible for finite sets of gates to generate arbitrarily close approximations to all unitary transformations.
- A number of such finite sets are known.
- It is unclear which will be most practical for physical implementation.
- For analyzing quantum algorithms, it is useful to have a standard set of gates with which to analyze the efficiency of quantum algorithms.
- The set we use includes:
  - All one-qubit gates;
  - A two-qubit gate that will be described later.

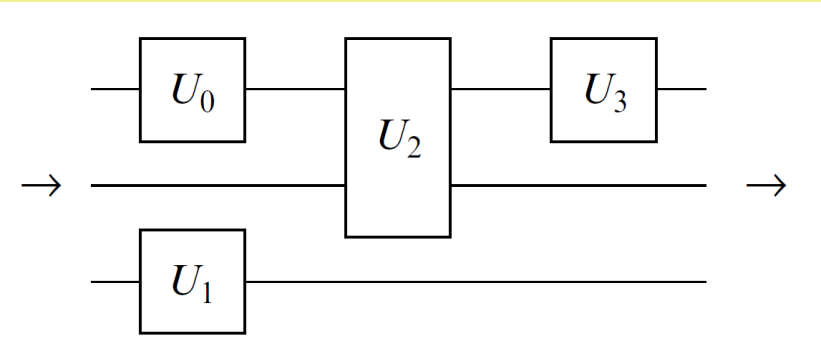
Graphical Notation

- Simple transformations are graphically represented by appropriately labeled boxes which are connected to form more complex circuits.



- Each horizontal line corresponds to a qubit.
- The transformations on the left are performed first.
- The processing proceeds from left to right.

Graphical Notation (Cont'd)



- The boxes U_0, U_1 and U_3 correspond to single-qubit transformations.
- The one labeled U_2 corresponds to a two-qubit transformation.
- We talk about applying an operator U to qubit i of an n-qubit quantum system.
- This means that we apply the operator

$$I \otimes \cdots \otimes I \otimes U \otimes I \otimes \cdots \otimes I$$

to the entire system, where I is the single-qubit identity operator, applied to each of the other qubits of the system.

Pauli Transformations

- The **Pauli transformations** are the most commonly used single-qubit transformations.
- The identity transformation I.

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

- The negation X (the classical NOT operation on $|0\rangle$ and $|1\rangle$, viewed as classical bits).

$$X: \quad |1\rangle\langle 0| + |0\rangle\langle 1| \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Pauli Transformations (Cont'd)

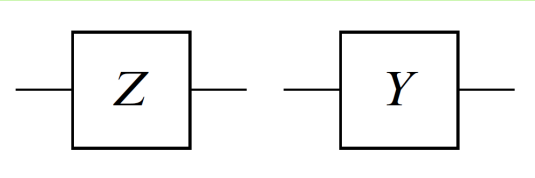
- The change Z of the relative phase of a superposition in the standard basis.

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

- A combination $Y = ZX$ of negation and phase change.

$$Y: \quad -|1\rangle\langle 0| + |0\rangle\langle 1| \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

- In graphical notation, these gates are represented by boxes labeled appropriately.



Notation

- There is variation in the literature as to which transformations are the Pauli transformations, and the notation used.
- The main discrepancy is whether $-i(|0\rangle\langle 1| - |1\rangle\langle 0|)$ is considered the Pauli transformation instead of $Y = |0\rangle\langle 1| - |1\rangle\langle 0|$, as we do here.
- The operator $\boldsymbol{iY}$ is Hermitian, which is a useful property in some settings, e.g., if we wanted to use it to describe measurement.
- Also, sometimes the notation σ_x, σ_y, and σ_z is used instead.
- Throughout we use I, X, Y and Z for the Pauli operators representing single-qubit transformations.
- The notation $\sigma_x = X$, $\sigma_y = -\boldsymbol{i}Y$ and $\sigma_z = Z$ is used when the Pauli operators are used to describe quantum states.

The Hadamard Transformation

- Another important single-qubit transformation is the Hadamard transformation,

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|).$$

- Alternatively, it is specified by

$$H: \quad |0\rangle \to |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \to |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

- This produces an even superposition of $|0\rangle$ and $|1\rangle$ from either of the standard basis elements.
- Note that $HH = I$.
- In the standard basis, the matrix for the Hadamard transformation is

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Multiple- from Single-Qubit Transformations

- Multiple-qubit transformations can be constructed as tensor products of single-qubit transformations.
- These are uninteresting as multiple-qubit transformations.
- They are equivalent to performing the single-qubit transformations on each of the qubits separately in some order.
- For example,

$$U \otimes V$$

can be obtained by:

  - First applying $U \otimes I$;
  - Then applying $I \otimes V$.

Transformations and Entanglement

- More interesting are those multiple-qubit transformations that can change the entanglement between qubits of the system.
- Entanglement is not a local property.
- This means that transformations that act separately on two or more subsystems cannot affect the entanglement between those subsystems.
- Let $|\psi\rangle$ be a two-qubit state.
- Let U and V be single-qubit unitary transformations.
- Then $(U \otimes V)|\psi\rangle$ is entangled if and only if $|\psi\rangle$ is.
- We look at a class of two-qubit controlled gates that illustrates the effects transformations can have on entanglement.

The Controlled-NOT

- The controlled-NOT gate, C_{not}, acts on the standard basis for a two-qubit system, with $|0\rangle$ and $|1\rangle$ viewed as classical bits.
- It flips the second bit if the first bit is 1 and leaves it unchanged otherwise.
- The C_{not} transformation has representation

$$\begin{aligned} C_{\text{not}} &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \\ &= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|. \end{aligned}$$

- From this it is easy to read off its effect on the standard basis elements.

$$\begin{aligned} C_{\text{not}}: \quad & |00\rangle \to |00\rangle \\ & |01\rangle \to |01\rangle \\ & |10\rangle \to |11\rangle \\ & |11\rangle \to |10\rangle. \end{aligned}$$

The Controlled-NOT (Cont'd)

- The matrix representation (in the standard basis) for C_{not} is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

- Observe that C_{not} is unitary.
- Moreover, it is its own inverse.
- The C_{not} gate cannot be decomposed into a tensor product of two single-qubit transformations.

The Controlled-NOT: Effect on States

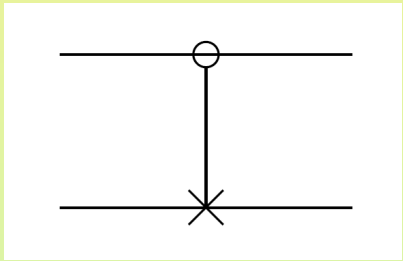
- The importance of the C_{not} gate for quantum computation stems from its ability to change the entanglement between two qubits.
- E.g., it takes the unentangled two-qubit state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$ to the entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,

$$\begin{aligned} C_{\text{not}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) &= C_{\text{not}}\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \end{aligned}$$

- We remarked that C_{not} is its own inverse.
- So it can also take an entangled state to an unentangled one.

The Controlled-NOT: Diagram

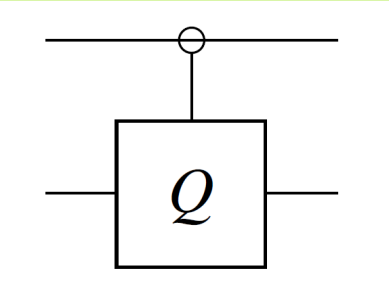
- The controlled-NOT gate is so common that it has its own graphical notation.



  - The open circle indicates the control bit;
  - The $\times$ indicates negation of the target bit;
  - The line between them indicates that the negation is conditional, depending on the value of the control bit.
- Some authors use a solid circle to indicate negative control, in which the target bit is toggled when the control bit is 0 instead of 1.

Controlled-Q

- We consider a useful class of two-qubit controlled gates, which generalizes the C_{not} gate.
- These gates perform a single-qubit transformation Q on the second qubit, when the first qubit is $|1\rangle$, and do nothing, when it is $|0\rangle$.
- They have graphical representation



Controlled-Q (Cont'd)

- We use the following shorthand for a controlled-Q transformation,

$$\bigwedge Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q.$$

- E.g., in this notation The transformation C_{not} becomes

$$\bigwedge X.$$

- In the standard computational basis, the two-qubit operator $\bigwedge Q$ is represented by the 4×4 matrix

$$\begin{pmatrix} I & 0 \\ 0 & Q \end{pmatrix}.$$

Controlled Phase Shift

- We look at the controlled phase shift

$$\bigwedge e^{\boldsymbol{i}\theta},$$

  where $e^{\boldsymbol{i}\theta}$ is shorthand for $e^{\boldsymbol{i}\theta} I$.
- In the standard basis, the controlled phase shift changes the phase of the second bit if and only if the control bit is one:

$$\bigwedge e^{\boldsymbol{i}\theta} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{\boldsymbol{i}\theta}|10\rangle\langle 10| + e^{\boldsymbol{i}\theta}|11\rangle\langle 11|.$$

Controlled Phase Shift (Cont'd)

- Its effect on the standard basis elements is as follows.

$$\begin{aligned} \wedge e^{\boldsymbol{i}\theta}: \quad & |00\rangle \to |00\rangle \\ & |01\rangle \to |01\rangle \\ & |10\rangle \to e^{\boldsymbol{i}\theta}|10\rangle \\ & |11\rangle \to e^{\boldsymbol{i}\theta}|11\rangle \end{aligned}$$

- Finally, its matrix representation is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{\boldsymbol{i}\theta} & 0 \\ 0 & 0 & 0 & e^{\boldsymbol{i}\theta} \end{pmatrix}.$$

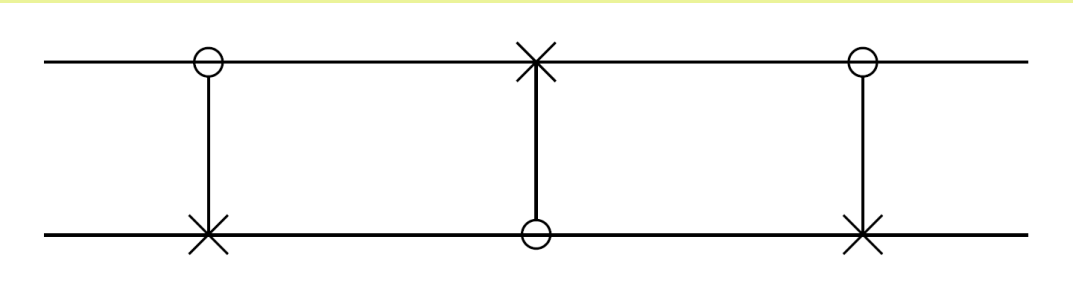
Controlled Phase Shift (Cont'd)

- The controlled phase shift makes use of a single-qubit transformation.
- This transformation was a physically meaningless global phase shift when applied to a single-qubit system.
- But, when used as part of a conditional transformation, this phase shift becomes nontrivial, since it changes the relative phase between elements of a superposition.
- E.g., it takes

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \mapsto \frac{1}{\sqrt{2}}(|00\rangle + e^{\boldsymbol{i}\theta}|11\rangle).$$

The Swap Circuit

- Graphical icons can be combined into quantum circuits.
- The following circuit, for instance, swaps the value of the two bits.



- In other words, this **swap circuit** takes

$$|00\rangle \mapsto |00\rangle \quad |01\rangle \mapsto |10\rangle \quad |10\rangle \mapsto |01\rangle \quad |11\rangle \mapsto |11\rangle.$$

- Additionally, for all single-qubit states $|\psi\rangle$ and $|\phi\rangle$,

$$|\psi\rangle|\phi\rangle \mapsto |\phi\rangle|\psi\rangle.$$

Caution 1: Phases in Specifications of Transformations

- We discussed the important distinction between the quantum state space (projective space) and the associated complex vector space.
- We need to keep this distinction in mind when interpreting the standard ways quantum state transformations are specified.
- A unitary transformation on the complex vector space is completely determined by its action on a basis.
- The unitary transformation is not completely determined by specifying what states the states corresponding to basis states are sent to, a subtle distinction.
- E.g., the controlled phase shift takes the four quantum states represented by $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$ to themselves.
  - $|10\rangle$ and $e^{\boldsymbol{i}\theta}|10\rangle$ represent exactly the same quantum state;
  - $|11\rangle$ and $e^{\boldsymbol{i}\theta}|11\rangle$ represent exactly the same quantum state.

Caution 1: Phases in Specifications (Cont'd)

- As we saw above, this transformation is not the identity transformation since it takes $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ to $\frac{1}{\sqrt{2}}(|00\rangle + e^{\boldsymbol{i}\theta}|10\rangle)$.
- To avoid mistakes, remember that notation such as

$$|00\rangle \rightarrow |00\rangle \quad |01\rangle \rightarrow |01\rangle \quad |10\rangle \rightarrow e^{\boldsymbol{i}\theta}|10\rangle \quad |11\rangle \rightarrow e^{\boldsymbol{i}\theta}|11\rangle$$

  is used to specify a unitary transformation on the complex vector space in terms of vectors in that vectors space.
- It is not a representation in terms of the states corresponding to these vectors.
- Specifying that the vector $|0\rangle$ goes to the vector $-|1\rangle$ is different from specifying that $|0\rangle$ goes to $|1\rangle$ because the two vectors $-|1\rangle$ and $|1\rangle$ are different vectors even if they correspond to the same state.
- The quantum transformation on the state space is easily derived from the unitary transformation on the associated complex vector space.

Caution 2: Basis Dependence of the Notion of Control

- The notion of the control bit and the target bit is a carryover from the classical gate and should not be taken too literally.
- In the standard basis, the C_{not} operator behaves exactly as the classical gate does on classical bits.
- However, one should not conclude that the control bit is never changed.
- When the input qubits are not one of the standard basis elements, the effect of the controlled gate can be somewhat counterintuitive.

Caution 2: Basis Dependence of Control (Cont'd)

- E.g., consider the C_{not} gate in the Hadamard basis $\{|+\rangle, |-\rangle\}$:

$$
\begin{aligned}
C_{\text{not}}: \quad & |++\rangle \to |++\rangle \\
& |+-\rangle \to |--\rangle \\
& |-+\rangle \to |-+\rangle \\
& |--\rangle \to |+-\rangle.
\end{aligned}
$$

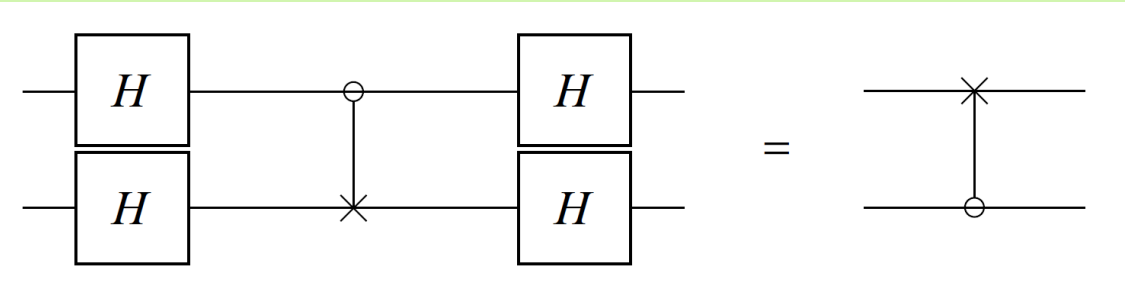
- In the Hadamard basis:
  - The state of the second qubit remains unchanged;
  - The state of the first qubit is flipped depending on the state of the second bit.
- Thus, in this basis the sense of which bit is the control bit and which the target bit has been reversed.
- The transformation has not been changed at all.
- Only the way we are thinking about it has changed.

Caution 2: Basis Dependence of Control (Cont'd)

- In most bases, we do not see a control bit or a target bit at all.
- E.g., as we have seen, the controlled-NOT transforms

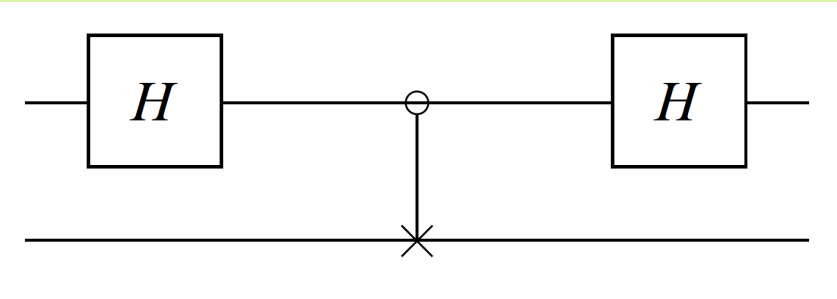
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

- In this case the controlled-NOT entangles the qubits so that it is not possible to talk about their states separately.
- A related fact, useful in constructing algorithms and in quantum error correction, is that the following two circuits are equivalent:



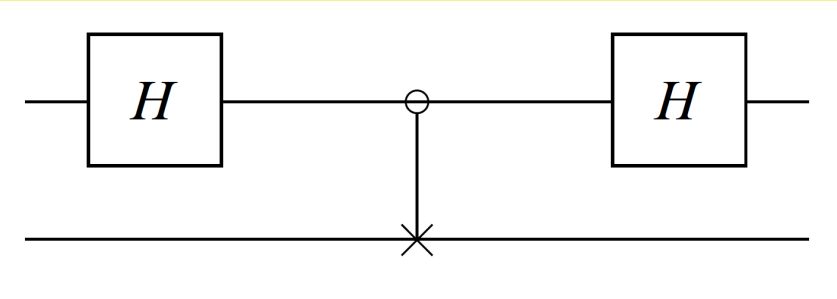
Caution 3: Reading Circuit Diagrams

- The graphical representation of quantum circuits can be misleading if one is not careful to interpret it properly.
- In particular, one cannot determine the effect the transformation has on the input qubits, even if they are all in standard basis states, by simply looking at the line in the diagram corresponding to that qubit.
- Look at the following circuit acting on input state $|0\rangle|0\rangle$.



- The Hadamard transformation is its own inverse.
- So it might at first appear that the first qubit's state would remain unchanged by the transformation.

Caution 3: Reading Circuit Diagrams (Cont'd)



- It is not the case that the first qubit's state remains unchanged.
- Recall from Caution 2 that the controlled-NOT gate does not leave the first qubit unaffected in general.
- In fact, this circuit takes

$$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle).$$

- This cannot be seen immediately from the circuit, but must be explicitly calculated.

Subsection 3

Applications of Simple Gates

Introducing Dense Coding

- Dense coding aims to encode and transmit two classical bits.
- It uses:
  - A shared EPR pair;
  - One quantum bit.
- EPR pairs can be distributed ahead of time.
- So only one qubit needs to be physically transmitted to communicate two bits of information.
- This result is surprising, since, as was explained, only one classical bit's worth of information can be extracted from a qubit.

Introducing Teleportation

- Teleportation is the opposite of dense coding.
- It uses two classical bits to transmit the state of a single qubit.
- Teleportation is surprising in two respects.
- In spite of the No-Cloning Principle of quantum mechanics, there exists a mechanism for the transmission of an unknown quantum state.
- It shows that two classical bits suffice to communicate a qubit state that can be in any one of an infinite number of possible states.

Initial Setup for Dense Coding and Teleportation

- The key to both dense coding and teleportation is the use of entangled particles.
- The initial setup is the same for both processes.
- Alice and Bob wish to communicate.
- Each is sent one of the entangled particles making up an EPR pair

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

- Suppose Alice is sent the first particle, and Bob the second:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle).$$

Initially Allowable Transformations

- Up until Alice sends Bob her particle or vice versa:
  - Alice can perform transformations only on her particle;
  - Bob can perform transformations only on his particle.
- In other words, until a particle is transmitted between them:
  - Alice can perform transformations only of the form $Q \otimes I$ on the EPR pair, where Q is a single-qubit transformation;
  - Bob can perform transformations only of the form $I \otimes Q$.
- More generally, for $K = 2^k$, let $I^{(K)}$ be the $2^k \times 2^k$ identity matrix.
- If Alice has n qubits and Bob has m qubits, then:
  - Alice can perform transformations only of the form $U \otimes I^{(M)}$, where U is an n-qubit transformation;
  - Bob can perform transformations only of the form $I^{(N)} \otimes U$.

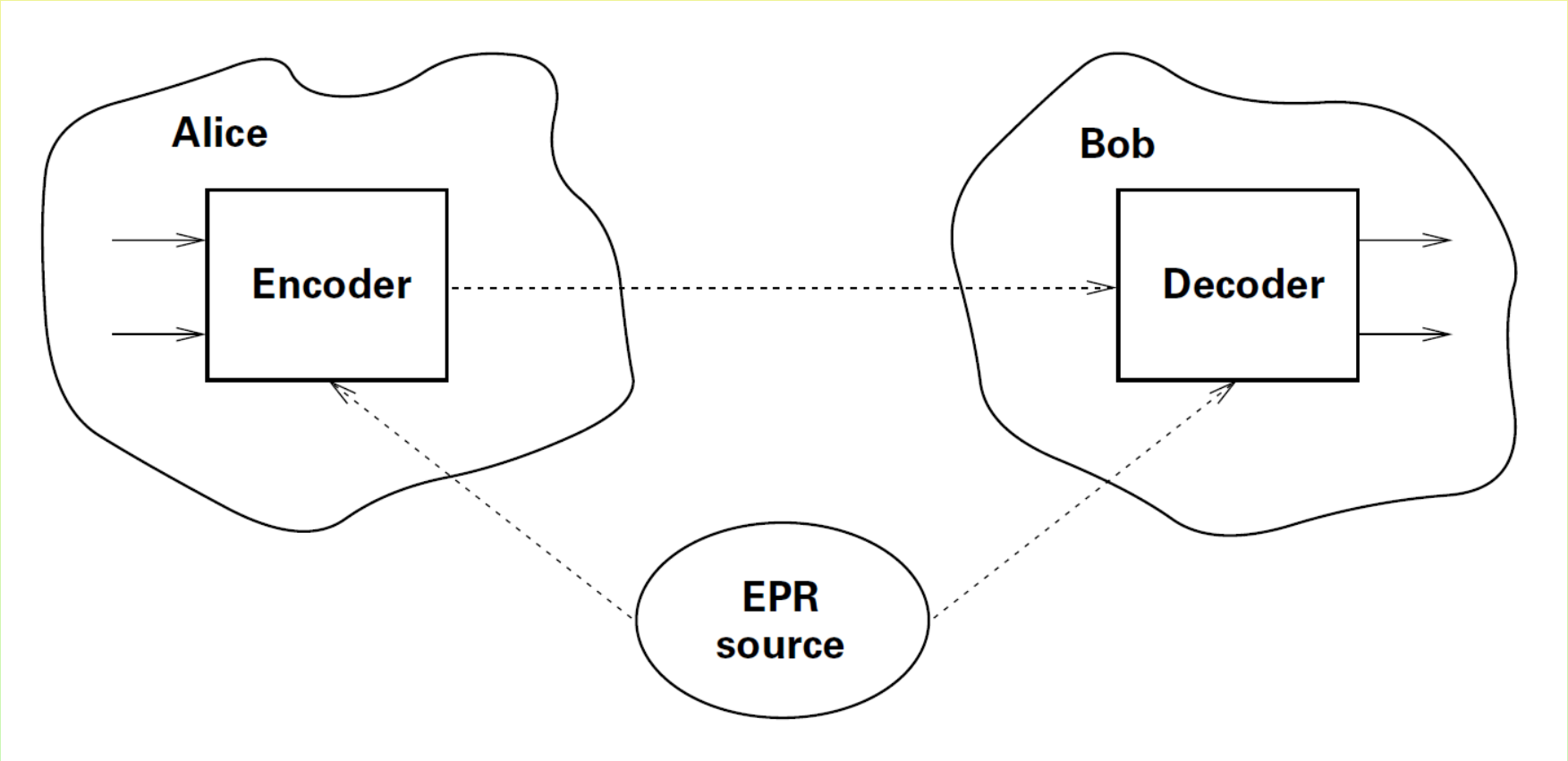
Dense Coding: Alice

- Alice wishes to transmit the state of two classical bits encoding one of the numbers 0 through 3.
- Depending on this number, Alice performs one of the Pauli transformations $\{I, X, Y, Z\}$ on her qubit of the entangled pair $|\psi_0\rangle$.
- The resulting state is shown in the following table.

Value	Transformation	New state
0	$\|\psi_0\rangle = (I \otimes I)\|\psi_0\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	$\|\psi_1\rangle = (X \otimes I)\|\psi_0\rangle$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
2	$\|\psi_2\rangle = (Z \otimes I)\|\psi_0\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
3	$\|\psi_3\rangle = (Y \otimes I)\|\psi_0\rangle$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$

- Alice then sends her qubit to Bob.

Dense Coding: Illustration



Dense Coding: Bob

- To decode the information, Bob applies:
  - A controlled-NOT to the two qubits of the entangled pair;
  - The Hadamard transformation H to the first qubit.

$$\left.\begin{array}{l} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ \frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle) \end{array}\right\} \xrightarrow{C_{\text{not}}} \left\{\begin{array}{l} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) \\ \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \\ \frac{1}{\sqrt{2}}(-|11\rangle + |01\rangle) \end{array}\right\}$$

$$= \left\{\begin{array}{l} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \otimes |1\rangle \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(-|1\rangle + |0\rangle) \otimes |1\rangle \end{array}\right\} \xrightarrow{H\otimes I} \left\{\begin{array}{l} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array}\right.$$

- Bob then measures the two qubits in the standard basis to obtain the two-bit binary encoding of the number Alice wished to send.

Quantum Teleportation

- The objective of teleportation is to transmit enough information about the quantum state of a particle, using only classical bits, so that a receiver can reconstruct the exact quantum state.
- By the No-Cloning Principle, a quantum state cannot be copied.
- So the quantum state of the original particle cannot be preserved.
- That is, the original state at the source must be destroyed in the course of creating the state at the target.
- This is the property giving *quantum teleportation* its name.

Quantum Teleportation: Alice

- Alice has a qubit whose state $|\phi\rangle = a|0\rangle + b|1\rangle$ she does not know.
- She wants to send this state to Bob through classical channels.
- As in the setup for the dense coding application, Alice and Bob each possess one qubit of an entangled pair

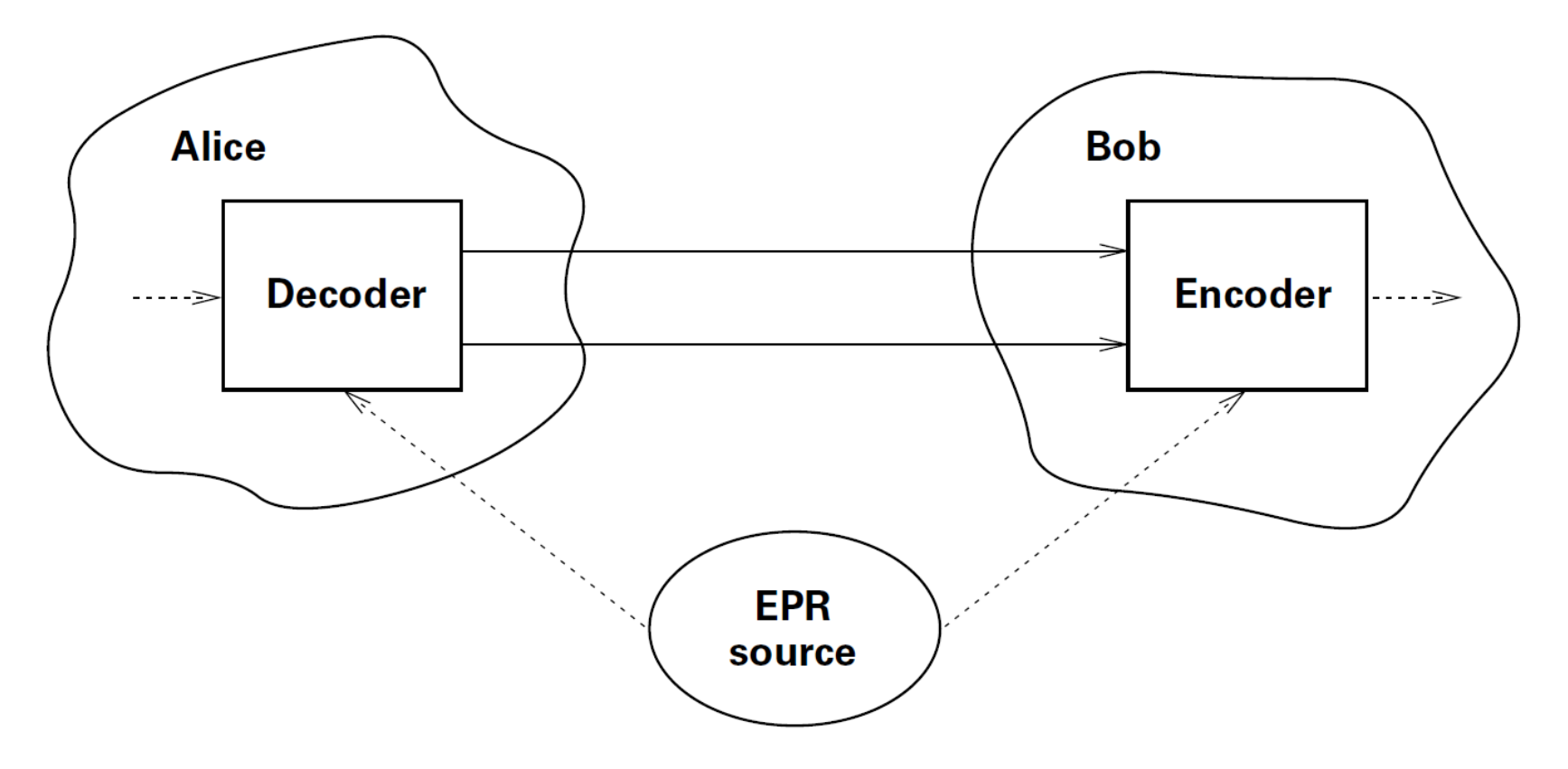
$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

- The starting state is the three-qubit quantum state

$$\begin{aligned} |\phi\rangle \otimes |\psi_0\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)) \\ &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle). \end{aligned}$$

- Alice controls the first two qubits.
- Bob controls the last qubit.

Quantum Teleportation: Illustration



Quantum Teleportation: Alice (Cont'd)

- Alice applies the decoding step used by Bob in the dense coding scenario to the combined state of the qubit $|\phi\rangle$ to be transmitted and her half of the entangled pair.
- I.e., Alice applies $C_{\text{not}} \otimes I$ followed by $H \otimes I \otimes I$ to this state,

$$
\begin{aligned}
&(H \otimes I \otimes I)(C_{\text{not}} \otimes I)(|\phi\rangle \otimes |\psi_0\rangle) \\
&= (H \otimes I \otimes I)(C_{\text{not}} \otimes I)\tfrac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle) \\
&= (H \otimes I \otimes I)\tfrac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle) \\
&= \tfrac{1}{2}(a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) \\
&\qquad\qquad + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)) \\
&= \tfrac{1}{2}(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) \\
&\qquad\qquad + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)).
\end{aligned}
$$

- Alice measures the first two qubits and obtains one of the four standard basis states $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$ with equal probability.

Quantum Teleportation: Alice (Cont'd)

- Depending on the result of her measurement, the quantum state of Bob's qubit is projected to one of:

$$a|0\rangle + b|1\rangle, \quad a|1\rangle + b|0\rangle, \quad a|0\rangle - b|1\rangle, \quad a|1\rangle - b|0\rangle.$$

- Alice sends the result of her measurement as two classical bits to Bob.
- After these transformations, crucial information about the original state $|\phi\rangle$ is contained in Bob's qubit.
- There is now nothing Alice can do on her own to reconstruct the original state of her qubit.
- In fact, the No-Cloning Principle implies that at any given time, only one of Alice or Bob can reconstruct the original quantum state.

Quantum Teleportation: Bob

- When Bob receives the two classical bits from Alice, he knows how the state of his half of the entangled pair compares to the original state of Alice's qubit.
- Bob can reconstruct the original state of Alice's qubit, $|\phi\rangle$, by applying the appropriate decoding transformation to his qubit, originally part of the entangled pair.
- The following table shows:
  - The state of Bob's qubit before the decoding has taken place;
  - The corresponding classical bits that Bob receives from Alice;
  - The decoding operator Bob should use depending on the bits received.

State	Bits Received	Decoding
$a\|0\rangle + b\|1\rangle$	00	I
$a\|1\rangle + b\|0\rangle$	01	X
$a\|0\rangle - b\|1\rangle$	10	Z
$a\|1\rangle - b\|0\rangle$	11	Y

Quantum Teleportation and Dense Coding

- After decoding, Bob's qubit will be in the quantum state,

$$a|0\rangle + b|1\rangle.$$

- This is the state in which Alice's qubit started.
- This decoding step is the encoding step of dense coding.
- The encoding step was the decoding step of dense coding.
- So teleportation and dense coding are, in some sense, inverses of each other.

Subsection 4

Realizing Unitary Transformations as Quantum Circuits

Shifts, Rotations and Phase Rotations

- We show that all single-qubit transformations can be written as a combination of three types of transformations.
  - Phase shifts $K(\delta) = e^{\boldsymbol{i}\delta} I$;
  - Rotations $R(\beta) = \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix}$;
  - Phase rotations $T(\alpha) = \begin{pmatrix} e^{\boldsymbol{i}\alpha} & 0 \\ 0 & e^{-\boldsymbol{i}\alpha} \end{pmatrix}$.
- Note that the following properties hold.
  - $K(\delta_1 + \delta_2) = K(\delta_1)K(\delta_2)$;
  - $R(\beta_1 + \beta_2) = R(\beta_1)R(\beta_2)$;
  - $T(\alpha_1 + \alpha_2) = T(\alpha_1)T(\alpha_2)$.
- In addition, the operator K commutes with K, T and R.

Comments

- Rather than write $K(\delta)$, we frequently just write the scalar factor $e^{\boldsymbol{i}\delta}$.
- As a transformation on a single-qubit system, $K(\delta)$ performs a global phase change, which is equivalent to the identity.
- However, we include it here because it will be used later as part of multiple-qubit conditional transformations in which this factor becomes a relative phase shift that is physically relevant.
- The transformations $R(\alpha)$ and $T(\alpha)$ are rotations by 2α about the y- and z-axis of the Bloch sphere respectively.

Decomposition of Single-Qubit Transformations

- We show that any single-qubit unitary transformation Q can be decomposed into a sequence of transformations of the form

$$Q = K(\delta)T(\alpha)R(\beta)T(\gamma).$$

- $K(\delta)$ is a global phase shift with no physical effect.
- So the space of all single-qubit transformations has only three real dimensions.
- Consider the transformation

$$Q = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}.$$

- Since Q is unitary, we have

$$QQ^\dagger = Q^\dagger Q = I.$$

Decomposition of Single-Qubit Transformations (Cont'd)

- These give

$$|u_{00}|^2 + |u_{01}|^2 = 1, \quad u_{00}\overline{u}_{10} + u_{01}\overline{u}_{11} = 0, \quad |u_{11}|^2 + |u_{10}|^2 = 1,$$
$$|u_{00}|^2 + |u_{10}|^2 = 1, \quad u_{00}\overline{u}_{01} + u_{10}\overline{u}_{11} = 0, \quad |u_{11}|^2 + |u_{01}|^2 = 1.$$

- We get $|u_{00}| = |u_{11}|$ and $|u_{01}| = |u_{10}|$.
- So we may set

$$|u_{00}| = |u_{11}| = \cos\beta \quad \text{and} \quad |u_{01}| = |u_{10}| = \sin\beta,$$

  for some angle β.
- Now, we can write Q as

$$Q = \begin{pmatrix} e^{\boldsymbol{i}\theta_{00}}\cos(\beta) & e^{\boldsymbol{i}\theta_{01}}\sin(\beta) \\ -e^{\boldsymbol{i}\theta_{10}}\sin(\beta) & e^{\boldsymbol{i}\theta_{11}}\cos(\beta) \end{pmatrix}.$$

Decomposition of Single-Qubit Transformations (Cont'd)

- Furthermore, the phases are not independent.
- $u_{10}\overline{u}_{00} + u_{11}\overline{u}_{01} = 0$ implies that $\theta_{10} - \theta_{00} = \theta_{11} - \theta_{01}$.
- We have

$$K(\delta)T(\alpha)R(\beta)T(\gamma) = \begin{pmatrix} e^{\boldsymbol{i}(\delta+\alpha+\gamma)}\cos\beta & e^{\boldsymbol{i}(\delta+\alpha-\gamma)}\sin\beta \\ -e^{\boldsymbol{i}(\delta-\alpha+\gamma)}\sin\beta & e^{\boldsymbol{i}(\delta-\alpha-\gamma)}\cos\beta \end{pmatrix}.$$

- So we can find δ, α, γ for a given Q by solving the system

$$\left\{ \begin{array}{rcl} \delta + \alpha + \gamma & = & \theta_{00} \\ \delta + \alpha - \gamma & = & \theta_{01} \\ \delta - \alpha + \gamma & = & \theta_{10} \end{array} \right\}$$

- Since $\theta_{11} = \theta_{10} - \theta_{00} + \theta_{01}$, the solution also satisfies $\delta - \alpha - \gamma = \theta_{11}$.

Singly Controlled Single-Qubit Transformations

- Consider an arbitrary single-qubit unitary transformation

$$Q = K(\delta)T(\alpha)R(\beta)T(\gamma).$$

- The controlled gate $\bigwedge Q$ can be implemented by:
  - First constructing
$$\bigwedge K(\delta);$$
  - Then implementing
$$\bigwedge Q',$$

  for $Q' = T(\alpha)R(\beta)T(\gamma)$.
- Then we have
$$\bigwedge Q = (\bigwedge K(\delta))(\bigwedge Q').$$
- We show how to implement these two transformations in terms of basic gates.

Implementation of Conditional Phase Shift

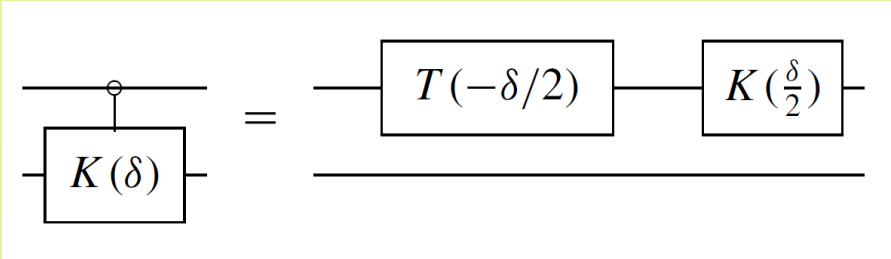
- The conditional phase shift can be implemented by primitive single-qubit operations.

$$
\begin{aligned}
\wedge K(\delta) &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes K(\delta) \\
&= |0\rangle\langle 0| \otimes I + e^{\boldsymbol{i}\delta}|1\rangle\langle 1| \otimes I \\
&= (|0\rangle\langle 0| + e^{\boldsymbol{i}\delta}|1\rangle\langle 1|) \otimes I \\
&= \begin{pmatrix} 1 & 0 \\ 0 & e^{\boldsymbol{i}\delta} \end{pmatrix} \otimes I \\
&= e^{\boldsymbol{i}\frac{\delta}{2}} \begin{pmatrix} e^{-\boldsymbol{i}\frac{\delta}{2}} & 0 \\ 0 & e^{\boldsymbol{i}\frac{\delta}{2}} \end{pmatrix} \otimes I \\
&= \left(K\left(\tfrac{\delta}{2}\right) T\left(-\tfrac{\delta}{2}\right)\right) \otimes I.
\end{aligned}
$$

Implementation of Conditional Phase Shift (Cont'd)

- We showed

$$\bigwedge K(\delta) = \left(K\left(\frac{\delta}{2}\right) T\left(-\frac{\delta}{2}\right)\right) \otimes I.$$



- It may appear surprising that the conditional phase shift $K(\delta)$ can be realized by a circuit acting on the first qubit only, with no transformations acting directly on the second qubit.
- The reason that transformations on the first qubit suffice is that a phase shift affects the whole quantum state, not just a single qubit.
- In particular, $|x\rangle \otimes a|y\rangle = a|x\rangle \otimes |y\rangle$.

Implementation of $\bigwedge Q'$

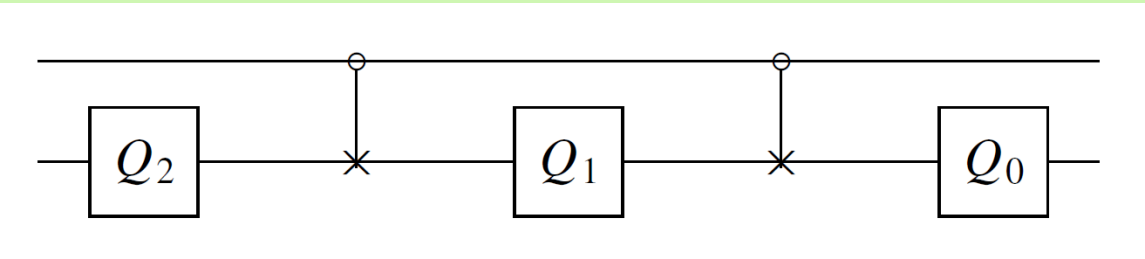
- For $Q' = T(\alpha)R(\beta)T(\gamma)$, define the following transformations:

$$\begin{aligned} Q_0 &= T(\alpha)R(\tfrac{\beta}{2}), \\ Q_1 &= R(-\tfrac{\beta}{2})T(\tfrac{-\gamma-\alpha}{2}), \\ Q_2 &= T(\tfrac{\gamma-\alpha}{2}). \end{aligned}$$

- The claim is that $\bigwedge Q'$ can be defined as

$$\bigwedge Q' = (I \otimes Q_0)C_{\text{not}}(I \otimes Q_1)C_{\text{not}}(I \otimes Q_2).$$

- Graphically, we have



Implementation of $\bigwedge Q'$ (Cont'd)

- This circuit transforms $|0\rangle \otimes |x\rangle$ as follows.

$$
\begin{aligned}
&(I \otimes Q_0)\, C_{\text{not}}\, (I \otimes Q_1)\, C_{\text{not}}\, (I \otimes Q_2)(|0\rangle \otimes |x\rangle) \\
&= (I \otimes Q_0)\, C_{\text{not}}\, (I \otimes Q_1)\, C_{\text{not}}\, (|0\rangle \otimes Q_2|x\rangle) \\
&= (I \otimes Q_0)\, C_{\text{not}}\, (I \otimes Q_1)(|0\rangle \otimes Q_2|x\rangle) \\
&= (I \otimes Q_0)\, C_{\text{not}}\, (|0\rangle \otimes Q_1 Q_2|x\rangle) \\
&= (I \otimes Q_0)(|0\rangle \otimes Q_1 Q_2|x\rangle) \\
&= |0\rangle \otimes Q_0 Q_1 Q_2|x\rangle.
\end{aligned}
$$

Implementation of $\bigwedge Q'$ (Cont'd)

- Similarly, it transforms $|1\rangle \otimes |x\rangle$ as follows.

$$
\begin{aligned}
&(I \otimes Q_0)C_{\text{not}}(I \otimes Q_1)C_{\text{not}}(I \otimes Q_2)(|1\rangle \otimes |x\rangle) \\
&= (I \otimes Q_0)C_{\text{not}}(I \otimes Q_1)C_{\text{not}}(|1\rangle \otimes Q_2|x\rangle) \\
&= (I \otimes Q_0)C_{\text{not}}(I \otimes Q_1)(|1\rangle \otimes XQ_2|x\rangle) \\
&= (I \otimes Q_0)C_{\text{not}}(|1\rangle \otimes Q_1XQ_2|x\rangle) \\
&= (I \otimes Q_0)(|1\rangle \otimes XQ_1XQ_2|x\rangle) \\
&= |1\rangle \otimes Q_0XQ_1XQ_2|x\rangle.
\end{aligned}
$$

Implementation of $\bigwedge Q'$ (Cont'd)

- Finally, note the following

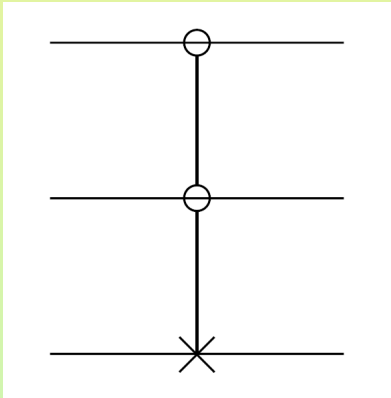
$$\begin{aligned}
Q_0 Q_1 Q_2 &= T(\alpha) R(\tfrac{\beta}{2}) R(-\tfrac{\beta}{2}) T(\tfrac{-\gamma-\alpha}{2}) T(\tfrac{\gamma-\alpha}{2}) \\
&= T(\alpha) R(\tfrac{\beta}{2} - \tfrac{\beta}{2}) T(\tfrac{-\gamma-\alpha}{2} + \tfrac{\gamma-\alpha}{2}) \\
&= T(\alpha) I T(-\alpha) \\
&= I; \\
Q_0 X Q_1 X Q_2 &= T(\alpha) R(\tfrac{\beta}{2}) X R(-\tfrac{\beta}{2}) T(\tfrac{-\gamma-\alpha}{2}) X T(\tfrac{\gamma-\alpha}{2}) \\
&= T(\alpha) R(\tfrac{\beta}{2}) (X R(-\tfrac{\beta}{2}) X) (X T(\tfrac{-\gamma-\alpha}{2}) X) T(\tfrac{\gamma-\alpha}{2}) \\
&= T(\alpha) R(\tfrac{\beta}{2}) R(\tfrac{\beta}{2}) T(\tfrac{\gamma+\alpha}{2}) T(\tfrac{\gamma-\alpha}{2}) \\
&= T(\alpha) R(\beta) T(\gamma) \\
&= Q'.
\end{aligned}$$

- In this way, we can realize a version of an arbitrary single qubit transformation controlled by a single qubit.

Multiply Controlled Single-Qubit Transformations

- The graphical notation for controlled operations generalizes to more than one control bits.
- Let $\bigwedge_k Q$ be the $(k+1)$-qubit transformation that applies Q to qubit 0 when qubits 1 through k are all 1.

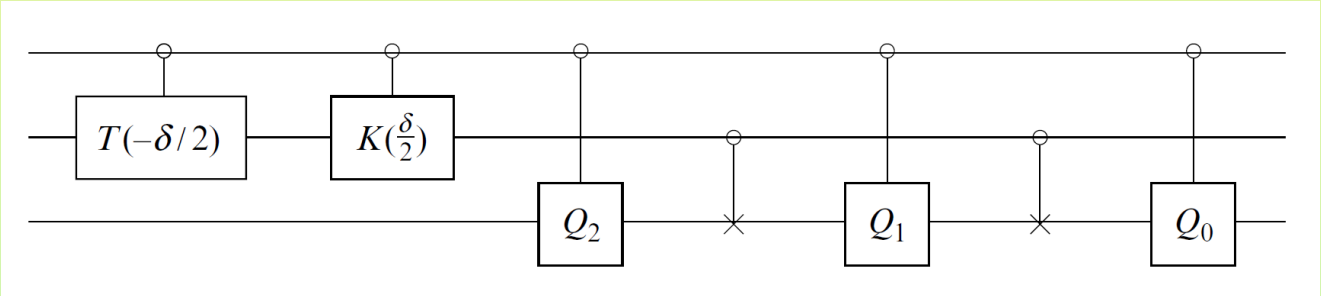
  Example: The **controlled-controlled-NOT gate**, or **Toffoli gate** $\bigwedge_2 X$, negates the last bit of three if and only if the first two are both 1.



- The subscript 2 in the notation $\bigwedge_2 X$ indicates that there are two control bits.
- We write the C_{not} gate as both $\bigwedge X$ and $\bigwedge_1 X$.

Implementations

- The previous construction can be iterated to obtain arbitrary single-qubit transformations controlled by k qubits.
- To implement $\bigwedge_2 Q$, a three-qubit gate, applying Q controlled by two qubits, we replace each of Q_0, Q_1 and Q_2 in the previous construction with a single-qubit controlled version.



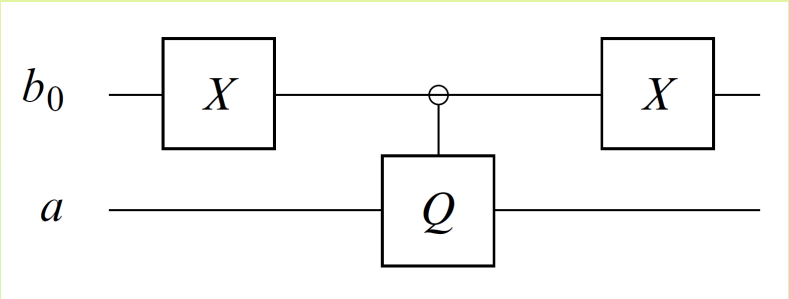
- This circuit can be expanded, as in the previous section, into single-qubit and controlled-NOT gates, for a total of:
  - Twenty five single-qubit gates;
  - Twelve controlled-NOT gates.

Implementations (Cont'd)

- Repeating this process leads to circuits for controlled versions of single-qubit transformations with k control bits, $\bigwedge_k Q$.
- The circuits obtained in this way have:
  - 5^k single-qubit transformations;
  - $\frac{1}{2}(5^k - 1)$ controlled-NOT gates.
- We will see later that significantly more efficient implementations of $\bigwedge_k Q$ are known.

Control Patterns

- All of the controlled gates seen so far are executed when the control bits are 1.
- To implement a singly controlled gate that is executed when the control bit is 0, the control bit can be negated.



- More generally, consider any length k bit-string s.
- By temporarily negating the appropriate control qubits, we may realize a controlled gate that applies Q to qubit 0 exactly when the other k qubits are in the pattern s.

Control Patterns (Cont'd)

- More precisely, let $|s\rangle$ be the k-qubit standard basis vector labeled with bit-string s.
- This construction implements the $(k+1)$-qubit controlled gate that:
  - Applies the single-qubit transformation Q to qubit 0 when qubits 1 though k are in the basis state $|s\rangle$;
  - Does nothing when qubits 1 though k are in a different basis state.
- Such constructions can be further generalized to $(k+1)$-qubit controlled gates that:
  - Apply the single-qubit transformation Q to qubit i when the other qubits are in a specific basis state;
  - Do nothing when the other qubits are in a different basis state.
- This transformation applies Q to the two-dimensional subspace spanned by the two basis vectors $|x_k \ldots x_i \ldots x_0\rangle$ and $|x_k \ldots \widehat{x_i} \ldots x_0\rangle$, where $\widehat{x_i} = x_i \oplus 1$, that differ only in bit i, and it leaves the orthogonal subspace invariant.

Notation

- The upcoming slides use such control gates to exhibit an explicit implementation of an arbitrary unitary transformation.
- The construction uses two different transformations related to a pair consisting of a k-bit string s and a single-qubit transformation Q.
  - The first applies Q to the i-th qubit with the standard ordering of the basis $\{|0\rangle, |1\rangle\}$, when the other k qubits are in state $|s\rangle$;
  - The second applies XQX to the i-th qubit, when the other qubits are in state $|s\rangle$.
- We use the notation $\bigwedge_x^i Q$, where x is a $(k+1)$-bit bit-string such that $x_k \dots x_{i+1} x_{i-1} \dots x_0 = s_{k-1} \dots s_0$, to represent both of these transformations depending on the value of x_i.
  - When x_i is 0, the single-qubit transformation Q is applied.
  - When x_i is 1, the transformation XQX is applied.

Properties

- When i is specified, the notation $\widehat{x}$ means that the i-th bit of a bit-string x has been flipped,

$$\widehat{x} = x \oplus 2^i.$$

- For any single-qubit transformation Q, if $\widehat{Q} = XQX$,

$$\bigwedge_{\widehat{x}}^{i} Q = \bigwedge_{x}^{i} \widehat{Q}.$$

- Geometrically, $\bigwedge_x^i Q$ is a rotation in the two-dimensional complex subspace spanned by standard basis vectors $|x\rangle$ and $|\widehat{x}\rangle$.

Example

- On a two-qubit system $|b_1 b_0\rangle$, the notation $\bigwedge_x^i Q$ affords, e.g., the description of the following transformations.
  - $\bigwedge_{10}^0 X$ is the standard C_{not}, with b_1 being the control bit and b_0 being the target.
  - $\bigwedge_{11}^0 X$ also represents the C_{not} transformation, since for X, we have $X = XXX$.
  - $\bigwedge_{00}^0 X$ is a controlled-NOT transformation except that now X is performed only when b_1 has value 0.
  - $\bigwedge_{01}^1 X$ describes the standard C_{not} but with b_0 as the control bit and b_1 as the target.

Preview: General Unitary Transformations

- This section presents a systematic way to implement an arbitrary unitary transformation on the 2^n-dimensional vector space associated with the state space of an n-qubit system.
- The intuitive idea behind the construction is that:
  - Any unitary transformation is simply a rotation of the 2^n-dimensional complex vector space underlying the n-qubit quantum state space;
  - Any rotation can be obtained by a sequence of rotations in two-dimensional subspaces.

Ordering Using a Gray Code

- Let $N = 2^n$.
- We write all matrices in the standard basis, but with a nonstandard ordering

$$\{|x_0\rangle, \ldots, |x_{N-1}\rangle\},$$

  so that successive basis elements differ by only one bit.
- Such a sequence of binary numbers is called a **Gray code**.
- Any Gray code will do.
- For $0 \leq i \leq N-2$, we let:
  - j_i be the bit on which $|x_i\rangle$ and $|x_{i+1}\rangle$ differ;
  - B_i be the shared pattern of all the other bits in $|x_i\rangle$ and $|x_{i+1}\rangle$.
- We show how to realize an arbitrary unitary operator U as a sequence of multiply controlled single-qubit operators $\bigwedge_{x_i}^{j_i} Q$ that perform a series of rotations, each in a two-dimensional subspace spanned by successive basis elements.

Goal for Expressing Transformations

- Consider transformations U_m, $0 \leq m \leq N-2$, of the form

$$U_m = \begin{pmatrix} I^{(m)} & 0 \\ 0 & V_{N-m} \end{pmatrix},$$

where:
  - $I^{(m)}$ is the $m \times m$ identity matrix;
  - V_{N-m} is an $(N-m) \times (N-m)$-unitary matrix.
- We show that, given any $(N \times N)$-matrix U_{m-1}, $0 < m \leq N-2$, of this form, we can write

$$U_{m-1} = C_m U_m,$$

where:
  - C_m is the product of multiply controlled single-qubit operators;
  - U_m has a larger identity component $I^{(m)}$ than U_{m-1}.
- Then, taking $V_N = U$, the unitary operator U can be written as

$$U = U_0 = C_1 \ldots C_{N-2} U_{N-2}.$$

Goal for Expressing Transformations (Cont'd)

- The transformation U_{N-2} has the form

$$U_{N-2} = \begin{pmatrix} I^{(N-2)} & 0 \\ 0 & V_2 \end{pmatrix}.$$

- This is simply the operation $\bigwedge_x^j V_2$, where:
  - $x = x_{N-2}$;
  - $j = j_{N-2}$ is the bit in which the basis vectors $|x_{N-2}\rangle$ and $|x_{N-1}\rangle$ differ.
- So it suffices to show how to implement the C_m using multiply controlled single-qubit operators.
- Then we will have succeeded in showing that any unitary operator can be expressed in terms of such operators.
- It would then follow that any unitary operator can be implemented using only C_{not}, $K(\delta)$, $R(\beta)$ and $T(\alpha)$.

Expressing Transformations

- The basis vector $|x_m\rangle$ is the first basis vector on which U_{m-1} acts nontrivially.
- Write
$$|v_m\rangle = U_{m-1}|x_m\rangle = a_m|x_m\rangle + \cdots + a_{N-1}|x_{N-1}\rangle.$$
- We may assume a_{N-1} is a positive real, possibly by multiplying U_{m-1} by a global phase.
- It suffices to find a unitary transformation W_m, composed only of multiply controlled single-qubit transformations, that:
  - Takes $|v_m\rangle$ to $|x_m\rangle$;
  - Does not affect any of the first m elements of the basis.
- Then $W_m U_{m-1}$ would have the desired form.
- We would then take $U_m = W_m U_{m-1}$ and $C_m = W_m^{-1}$.

Expressing Transformations (Cont'd)

- To define W_m, begin by rewriting the coefficients of the last two components of $|v_m\rangle$.

$$\begin{aligned} a_{N-2}|x_{N-2}\rangle + a_{N-1}|x_{N-1}\rangle &= \sqrt{|a_{N-2}|^2+|a_{N-1}|^2}\,\frac{a_{N-2}}{\sqrt{|a_{N-2}|^2+|a_{N-1}|^2}}|x_{N-2}\rangle \\ &\quad + \sqrt{|a_{N-2}|^2+|a_{N-1}|^2}\,\frac{a_{N-1}}{\sqrt{|a_{N-2}|^2+|a_{N-1}|^2}}|x_{N-1}\rangle \\ &= \sqrt{|a_{N-2}|^2+|a_{N-1}|^2}\,\frac{|a_{N-2}|}{\sqrt{|a_{N-2}|^2+|a_{N-1}|^2}}e^{\boldsymbol{i}\phi_{N-2}}|x_{N-2}\rangle \\ &\quad + \sqrt{|a_{N-2}|^2+|a_{N-1}|^2}\,\frac{|a_{N-1}|}{\sqrt{|a_{N-2}|^2+|a_{N-1}|^2}}|x_{N-1}\rangle. \end{aligned}$$

- Now set

$$c_{N-2} = \sqrt{|a_{N-2}|^2+|a_{N-1}|^2},\ \cos(\theta_{N-2}) = \frac{|a_{N-2}|}{c_{N-2}},\ \sin(\theta_{N-2}) = \frac{|a_{N-1}|}{c_{N-2}}.$$

- Then we have

$$|v_m\rangle = a_m|x_m\rangle + \cdots + c_{N-2}\cos(\theta_{N-2})e^{\boldsymbol{i}\phi_{N-2}}|x_{N-2}\rangle + c_{N-2}\sin(\theta_{N-2})|x_{N-1}\rangle.$$

Expressing Transformations (Cont'd)

- We wrote

$$\begin{aligned} U_{m-1}|x_m\rangle &= a_m|x_m\rangle + \cdots + a_{N-3}|x_{N-3}\rangle \\ &\quad + c_{N-2}\cos(\theta_{N-2})e^{\boldsymbol{i}\phi_{N-2}}|x_{N-2}\rangle + c_{N-2}\sin(\theta_{N-2})|x_{N-1}\rangle. \end{aligned}$$

- Then we form the operator

$$\bigwedge_{x_{N-2}}^{j_{N-2}} R(\theta_{N-2}) \bigwedge_{x_{N-2}}^{j_{N-2}} K(-\phi_{N-2}).$$

- It takes $U_{m-1}|x_m\rangle$ to $a_m|x_m\rangle + \cdots + a'_{N-2}|x_{N-2}\rangle$, where $a'_{N-2} = c_{N-2}$.
  - $\bigwedge_{x_{N-2}}^{j_{N-2}} K(-\phi_{N-2})$ cancels the $e^{\boldsymbol{i}\phi_{N-2}}$ factor.
  - $\bigwedge_{x_{N-2}}^{j_{N-2}} R(\theta_{N-2})$ rotates so that all of the amplitude that was in $|x_{N-1}\rangle$ is now in $|x_{N-2}\rangle$.
  - None of the other basis vectors are affected because the controlled part of the operators ensure that only basis vectors with bits in pattern B_{N-2} are affected.

Expressing Transformations (Cont'd)

- To obtain the rest of W_m, we iterate this procedure over all pairs of coordinates $\{a_{N-3}, a'_{N-2}\}$ through $\{a_m, a'_{m+1}\}$.
- In this way, we obtain the operator

$$W_m = \bigwedge_{x_m}^{j_m} R(\theta_m) \bigwedge_{x_m}^{j_m} K(-\phi_m) \cdots \bigwedge_{x_{N-2}}^{j_{N-2}} R(\theta_{N-2}) \bigwedge_{x_{N-2}}^{j_{N-2}} K(-\phi_{N-2}),$$

where

$$a_i = |a_i| e^{\boldsymbol{i}\phi_i}, \;\; c_i = \sqrt{|a_i|^2 + |a_{i+1}|^2}, \;\; \cos(\theta_i) = \frac{|a_i|}{c_i}, \;\; \sin(\theta_i) = \frac{|a'_{i+1}|}{c_i}.$$

- It takes $|v_m\rangle$ to $a'_m|x_m\rangle$, where $a'_i = c_i$.
- The coefficient $a'_m = 1$, since the image of $|v_m\rangle$ must be a unit vector, and the final $\bigwedge_{x_m}^{j_m} K(-\phi_m)$ ensures that it is a positive real.

Comments on Efficiency

- While this procedure provides an implementation for any unitary operator U in terms of simple transformations, the number of gates needed is exponential in the number of qubits.
- For this reason, it has limited practical value in that more efficient implementations are needed for realistic computations.
- Most unitary operators do not have efficient realizations in terms of simple gates.
- The art of quantum algorithm design is in finding useful unitary operators that have efficient implementations.

Subsection 5

A Universally Approximating Set of Gates

Finite Sets of Gates

- We just showed that all unitary transformations can be realized as a sequence of single-qubit transformations and controlled-not gates.
- From a practical point of view, we would prefer to deal with a finite set of gates.
- For any finite set of gates there are unitary transformations that cannot be realized as a combination of these gates.

The Solovay-Kitaev Theorem

- There are finite sets of gates that can approximate any unitary transformation to arbitrary accuracy.
- Furthermore, for any desired level of accuracy 2^{-d}, this approximation can be done efficiently.
- The **Solovay-Kitaev Theorem** asserts that, there is a polynomial $p(d)$, such that any single-qubit unitary transformation can be approximated to within 2^{-d} by a sequence of no more than $p(d)$ gates from the finite set.
- We will not prove the Solovay-Kitaev Theorem.
- We will exhibit a finite set of gates that can be used to approximate all unitary transformations.

Four Gates

- We saw that any unitary transformation can be realized using single-qubit and C_{not} gates.
- So it suffices to find a finite set of gates that can approximate all single-qubit transformations.
- Consider the set consisting of the following four gates.
- The Hadamard gate H,

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

- The phase gate $P_{\frac{\pi}{2}}$,

$$P_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\boldsymbol{i}\pi/2} \end{pmatrix} = |0\rangle\langle 0| + \boldsymbol{i}|1\rangle\langle 1|.$$

Four Gates (Cont'd)

- The $\frac{\pi}{8}$-gate $P_{\frac{\pi}{4}}$,

$$P_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\boldsymbol{i}\frac{\pi}{4}} \end{pmatrix} = |0\rangle\langle 0| + e^{\boldsymbol{i}\frac{\pi}{4}}|1\rangle\langle 1|.$$

- The C_{not} gate

$$C_{\text{not}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|.$$

- Recall the single-qubit operator $T(\theta) = e^{\boldsymbol{i}\theta}|0\rangle\langle 0| + e^{-\boldsymbol{i}\theta}|1\rangle\langle 1|$.
- The $\frac{\pi}{8}$-gate $P_{\frac{\pi}{4}}$ got its name because, up to a global phase, it acts in the same way as the gate $T(-\frac{\pi}{8})$, $P_{\frac{\pi}{4}} = e^{\boldsymbol{i}\frac{\pi}{8}} T(-\frac{\pi}{8})$.
- Unfortunately the name stuck in spite of the confusion it causes.

Rational and Irrational Rotations

- A rotation R is a **rational rotation** if, for some integer m, $R^m = I$.
- If no such m exists, then R is an **irrational rotation**.
- It may seem surprising that a set of gates consisting only of rational rotations on the Bloch sphere can approximate all single qubit transformations.
- The proof of sufficiency proceeds by using these gates to construct an irrational rotation.
- Such a construction is possible because the group of rotations of a sphere differs from the group of rotations of a Euclidean plane.
  - In the plane, the product of two rational rotations is always rational;
  - The analogous statement is not true for rotations of the sphere.

A Sketch of the Argument

- The gate $P_{\frac{\pi}{4}}$ is a rotation by $\pi/4$ about the z-axis of the Bloch sphere.
- The transformation $S = HP_{\frac{\pi}{4}}H$ is a rotation by $\frac{\pi}{4}$ about the x-axis.
- It can be shown that $V = P_{\frac{\pi}{4}}S$ is an irrational rotation.
- Since V is irrational, any rotation W about the same axis can be approximated to within arbitrary precision 2^{-d} by some power of V.
- Recall that any single-qubit transformation may be achieved (up to global phase) by combining rotations about the y- and z-axes.

A Sketch of the Argument (Cont'd)

- For every single-qubit operation W, there exist angles α, β, γ and δ such that

$$W = K(\delta)T(\alpha)R(\beta)T(\gamma),$$

  where:
  - $T(\alpha)$ rotates by angle α about the z-axis;
  - $R(\alpha)$ rotates by angle α about the y-axis.
- The set of rotations about any two distinct axes can achieve arbitrary single-qubit transformations.
- Now HVH has a different axis from V.
- Therefore, the two transformations H and V generate all single-qubit operators.
- There exist other universally approximating finite sets, each with its own advantages and disadvantages.

Subsection 6

The Standard Circuit Model

The Circuit Model

- A **circuit model** for quantum computation describes all computations in terms of a circuit composed of:
  - Simple gates;
  - A sequence of measurements.
- The simple gates are drawn from either one of the following:
  - A universal set of simple gates;
  - A universally approximating set of quantum gates.

The Standard Circuit Model

- The **standard circuit model** for quantum computation takes as:
  - Its gate set the C_{not} gate together with all single qubit transformations;
  - Its set of measurements single-qubit measurements in the standard basis.
- So all computations in the standard model consist of:
  - A sequence of single-qubit and C_{not} gates;
  - A sequence of single-qubit measurements in the standard basis.

Comments on the Choice

- A finite set of gates would be more realistic than the infinite set of all single-qubit transformations.
- However, the infinite set is easier to work with.
- Moreover, by the results of Solovay and Kitaev, the infinite set does not yield significantly greater computational power.
- For conceptual clarity, the n qubits of the computation are often organized into registers, subsets of the n qubits.