Quantum Computation- Quantum Circuits

- *The theory of computation has traditionally been studied almost entirely in the abstract, as a topic in pure mathematics. This is to miss the point of it. Computers are physical objects, and computations are physical processes. What computers can or cannot compute is determined by the laws of physics alone, and not by pure mathematics.*
- – David Deutsch

- *Like mathematics, computer science will be somewhat different from the other sciences, in that it deals with artificial laws that can be proved, instead of natural laws that are never known with certainty.*
- – Donald Knuth

- *The opposite of a profound truth may well be another profound truth.*
- – Niels Bohr

Quantum Computation- Quantum Circuits

- First, we explain in detail the fundamental model of quantum computation, the quantum circuit model.
- Second, we demonstrate that there exists a small set of gates which are universal, that is, any quantum computation whatsoever can be expressed in terms of those gates.

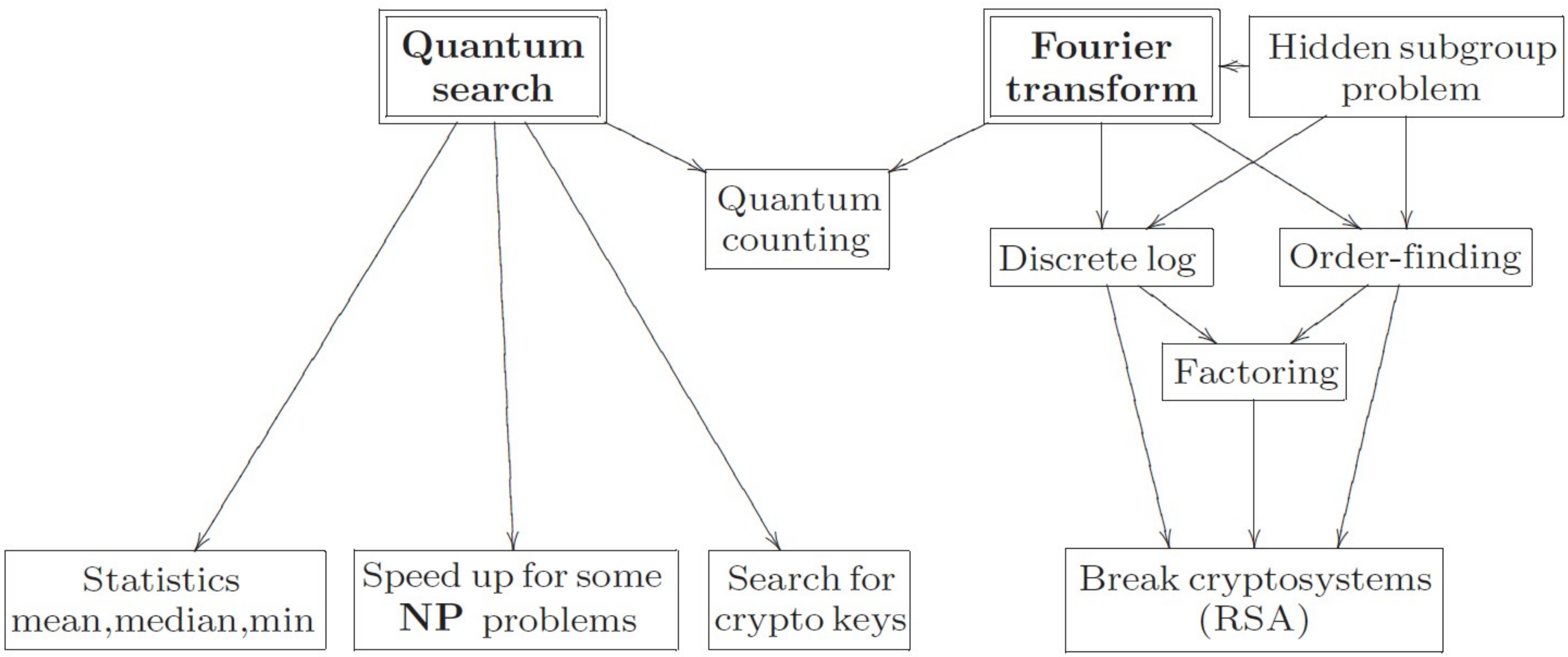
Quantum Computation- Quantum Circuits- Quantum algorithms

- Practically speaking, many interesting problems are impossible to solve on a classical computer, not because they are in principle insoluble, but because of the astronomical resources required to solve realistic cases of the problem.
- The spectacular promise of quantum computers is to enable new algorithms which render feasible problems requiring exorbitant resources for their solution on a classical computer.

Quantum Computation- Quantum Circuits- Quantum algorithms

- The first class of algorithms is based upon Shor's *quantum Fourier transform*, and includes remarkable algorithms for solving the factoring and discrete logarithm problems, providing a striking exponential speedup over the best known classical algorithms.
- The second class of algorithms is based upon Grover's algorithm for performing *quantum searching*. These provide a less striking but still remarkable quadratic speedup over the best possible classical algorithms.

Quantum Computation- Quantum Circuits- Quantum algorithms



Quantum Computation- Quantum Circuits- Single qubit operations

- The development of our quantum computational toolkit begins with operations on the simplest quantum system of all – a single qubit.
- A single qubit is a vector $|\psi\rangle = a|0\rangle + b|1\rangle$ parameterized by two complex numbers satisfying $|a|^2 + |b|^2 = 1$.
- Operations on a qubit must preserve this norm, and thus are described by *2×2 unitary matrices.*
- Of these, some of the most important are the Pauli matrices; it is useful to list them again here:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Quantum Computation- Quantum Circuits- Single qubit operations

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

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

Quantum Computation- Quantum Circuits- Single qubit operations

- 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 has $\exp(\pm i\pi/8)$ appearing on its diagonals.
- $$T = \exp(i\pi/8)\begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix}$$

Quantum Computation- Quantum Circuits- Single qubit operations

- The Pauli matrices give rise to three useful classes of unitary matrices when they are exponentiated, the *rotation operators about the xˆ, yˆ, and zˆ axes, defined by the equations:*

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

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

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

Quantum Computation- Quantum Circuits- Single qubit operations

- **Exercise: Let x be a real number and A a matrix such that $A^2 = I$. Show that $\exp(iAx) = \cos(x)I + i \sin(x)$**

- **Exercise: Show that, up to a global phase, the π/8 gate satisfies $T = R_z(\pi/4)$.**

- **Exercise: Express the Hadamard gate H as a product of R_x and R_z rotations and $e^{i\varphi}$ for some φ.**

Quantum Computation- Quantum Circuits- Single qubit operations

- If $\hat{n} = (n_x, n_y, n_z)$ is a real unit vector in three dimensions then we generalize the previous definitions by defining a rotation by θ about the $\hat{n}$ axis by the equation

$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\, \hat{n} \cdot \vec{\sigma}/2) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) (n_x X + n_y Y + n_z Z),$$

- where σ denotes the three component vector (X,Y,Z) of Pauli matrices. This is a vector whose elements are Pauli matrices.

Quantum Computation- Quantum Circuits- Single qubit operations

- Exercise: Show that $XYX = -Y$ and use this to prove that $XR_y(\theta)X = R_y(-\theta)$.
- Exercise: An arbitrary single qubit unitary operator can be written in the form

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

- for some real numbers *α and ϑ, and a real three-dimensional unit vector n ˆ.*
  - 1. Prove this fact.
  - 2. Find values for α, θ, and nˆ giving the Hadamard gate H.
  - 3. Find values for α, θ, and nˆ giving the phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Quantum Computation- Quantum Circuits- Single qubit operations

- An arbitrary unitary operator on a single qubit can be written in many ways as a combination of rotations, together with global phase shifts on the qubit. The following theorem provides a means of expressing an arbitrary single qubit rotation that will be particularly useful in later applications to controlled operations.
- Theorem: (Z-Y decomposition for a single qubit) Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that
- $$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Quantum Computation- Quantum Circuits- Single qubit operations

- **Corollary: Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A,B,C on a single qubit such that ABC = I and U = $e^{i\alpha}$AXBXC, where α is some overall phase factor.**

- **Proof is available in the book**

- Exercise: Give *A, B, C, and α for the Hadamard gate.*

Quantum Computation- Quantum Circuits- Single qubit operations

- Exercise: (Circuit identities) It is useful to be able to simplify circuits by inspection, using well-known identities. Prove the following three identities:
- $HXH = Z$; $HYH = -Y$; $HZH = X$.
- Exercise: Use the previous exercise to show that $HTH = R_x(\pi/4)$, *up to a* global phase.

Quantum Computation- Quantum Circuits- Single qubit operations

- Symbols for the common single qubit gates are shown in this figure. Recall the basic properties of quantum circuits: time proceeds from left to right; wires represent qubits, and a ‘/’ may be used to indicate a bundle of qubits.

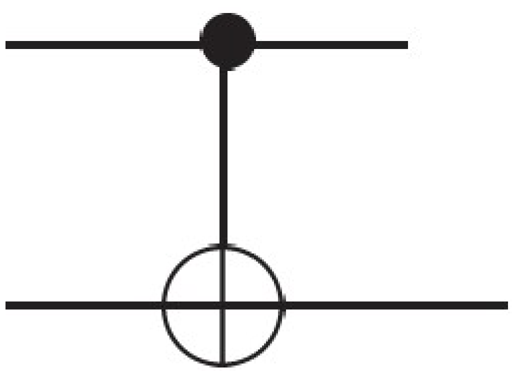
Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X	$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y	$-\boxed{Y}-$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z	$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase	$-\boxed{S}-$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Quantum Computation- Quantum Circuits- Controlled operations

- 'If A is true, then do B'. This type of controlled operation is one of the most useful in computing, both classical and quantum.
- The prototypical controlled operation is the controlled-NOT.
- CNOT is a quantum gate with two input qubits, known as the control qubit and target qubit, respectively.
- In terms of the computational basis, the action of the CNOT is given by $|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle$;

Quantum Computation- Quantum Circuits- Controlled operations

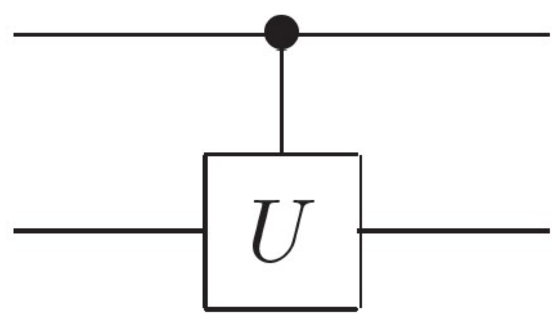
- if the control qubit is set to |1> then the target qubit is flipped, otherwise the target qubit is left alone.



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

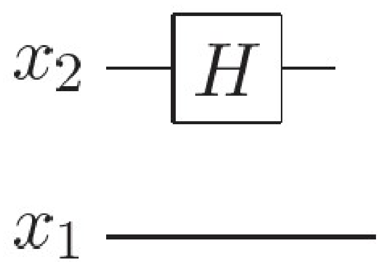
Quantum Computation- Quantum Circuits- Controlled operations

- More generally, suppose U is an arbitrary single qubit unitary operation. A controlled- U operation is a two qubit operation, again with a control and a target qubit.
- If the control qubit is set then U is applied to the target qubit, otherwise the target qubit is left alone.
- That is, $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$



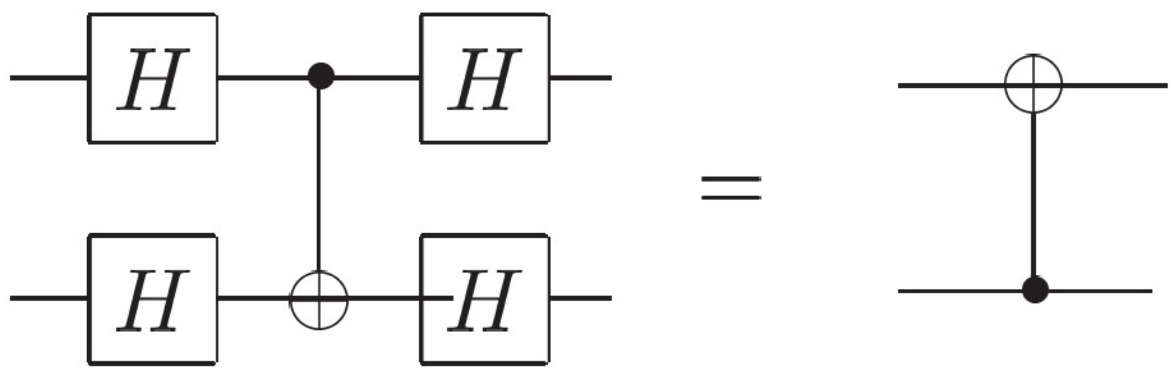
Quantum Computation- Quantum Circuits- Controlled operations

- Exercise 4.16: (Matrix representation of multi-qubit gates) What is the *4×4* unitary matrix for the circuit



- in the computational basis?

Quantum Computation- Quantum Circuits- Controlled operations

- Exercise: (CNOT basis transformations) Unlike ideal classical gates, ideal quantum gates do not have (as electrical engineers say) 'high-impedance' inputs. In fact, the role of 'control' and 'target' are arbitrary – they depend on what basis you think of a device as operating in. We have described how the CNOT behaves with respect to the computational basis, and in this description the state of the control qubit is not changed. However, if we work in a different basis then the control qubit *does* change: we will show that its phase is flipped depending on the state of the 'target' qubit! Show that
- 

Quantum Computation- Quantum Circuits- Controlled operations

- Introducing basis states $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$, use this circuit identity to show that the effect of a CNOT with the first qubit as control and the second qubit as target is as follows:

$$
\begin{aligned}
|+\rangle|+\rangle &\rightarrow |+\rangle|+\rangle \\
|-\rangle|+\rangle &\rightarrow |-\rangle|+\rangle \\
|+\rangle|-\rangle &\rightarrow |-\rangle|-\rangle \\
|-\rangle|-\rangle &\rightarrow |+\rangle|-\rangle
\end{aligned}
$$

Quantum Computation- Quantum Circuits- Controlled operations

- Thus, with respect to this new basis, the state of the target qubit is not changed, while the state of the control qubit is flipped if the target starts as $|-\rangle$, otherwise it is left alone. That is, in this basis, the target and control have essentially interchanged roles!

Quantum Computation- Quantum Circuits- Controlled operations

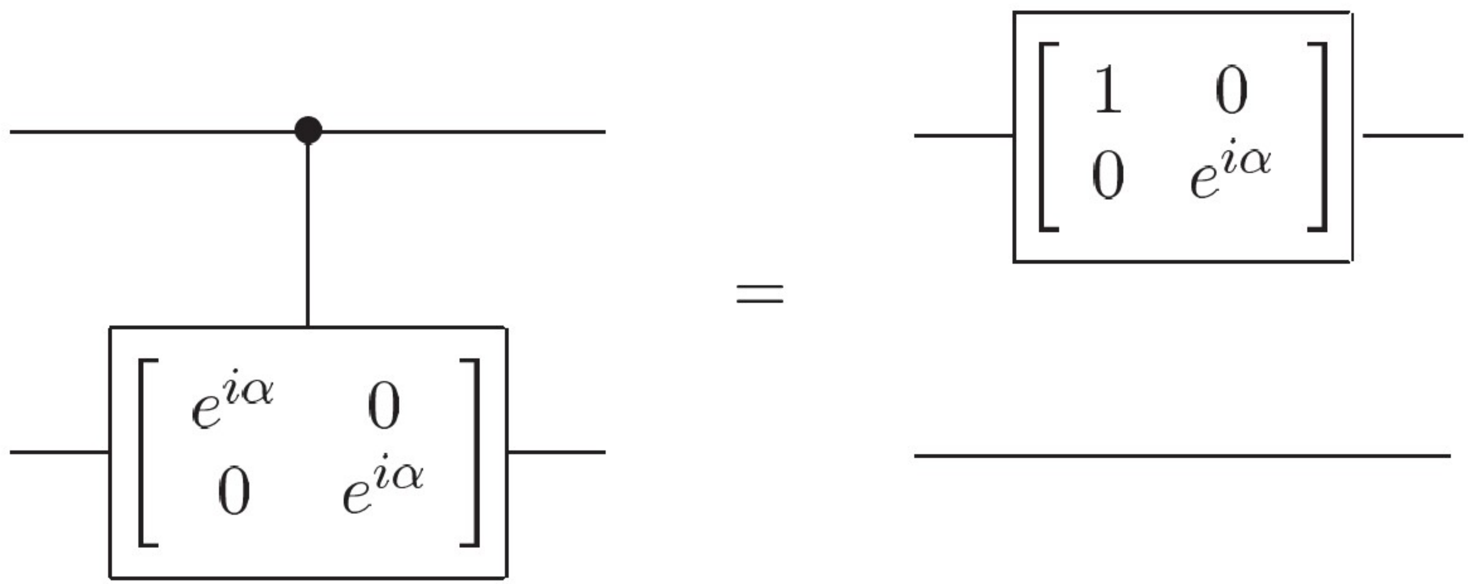
- Our immediate goal is to understand how to implement the controlled-U operation for arbitrary single qubit U, using only single qubit operations and the CNOT gate.
- Our strategy is a two-part procedure based upon the decomposition $U = e^{i\alpha}AXBXC$

Quantum Computation- Quantum Circuits- Controlled operations

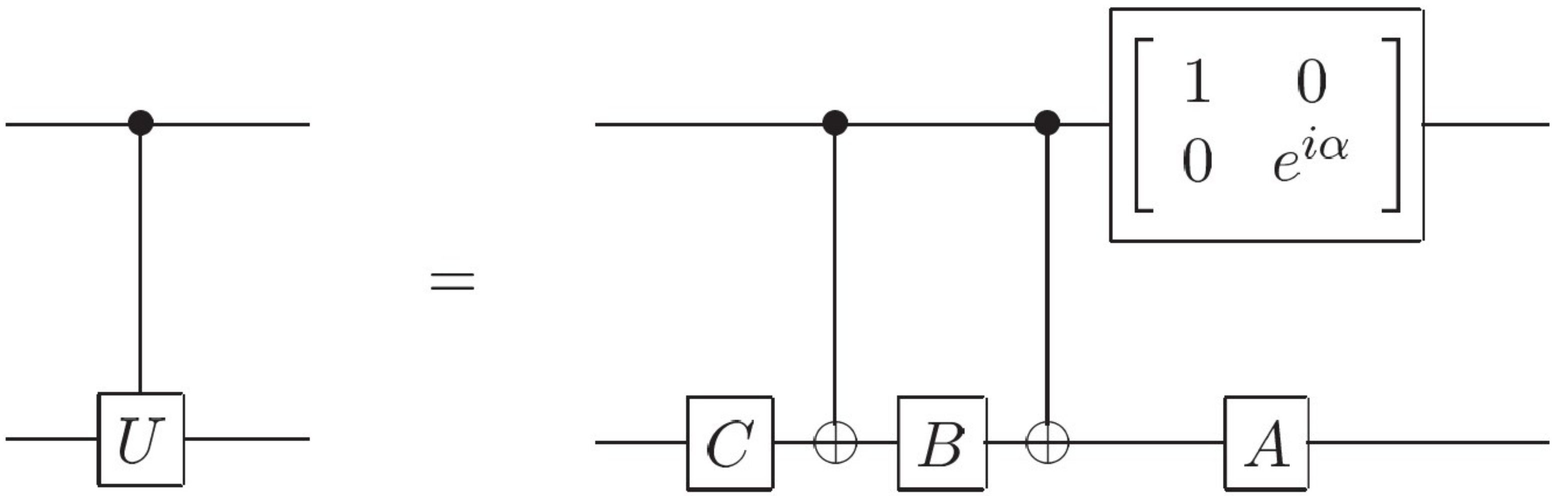
- Our first step will be to apply the phase shift exp(*iα) on the target qubit, controlled* by the control qubit. That is, if the control qubit is *|0, then the target qubit is left alone,* while if the control qubit is *|1>, a phase shift exp(iα) is applied to the target.*

Quantum Computation- Quantum Circuits- Controlled operations

$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle, \quad |10\rangle \rightarrow e^{i\alpha}|10\rangle, \quad |11\rangle \rightarrow e^{i\alpha}|11\rangle,$$



Quantum Computation- Quantum Circuits- Controlled operations



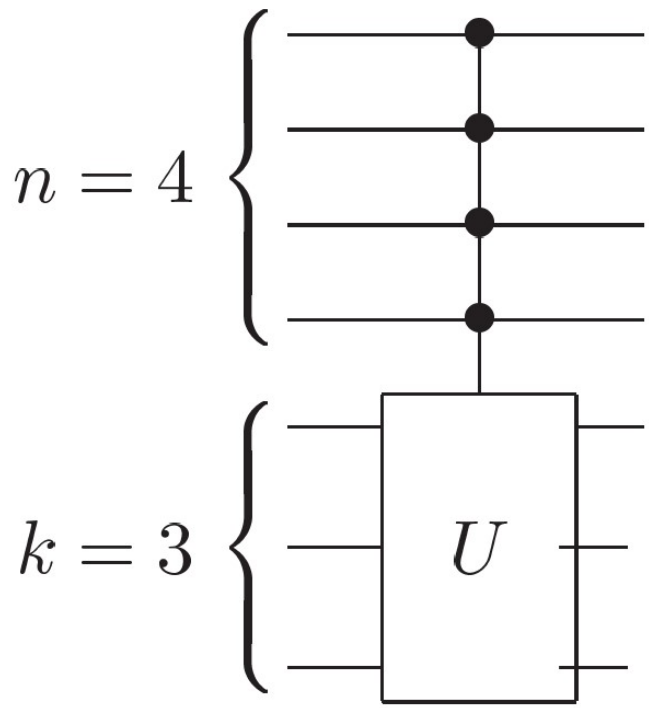
Circuit implementing the controlled-*U operation for single qubit U. α, A,B and C satisfy U = exp(iα)AXBXC, ABC = I.*

Quantum Computation- Quantum Circuits- Controlled operations

- What about conditioning on multiple qubits?
- suppose we have n + k qubits, and U is a k qubit unitary operator. Then we define the controlled operation $C^n(U)$ by the equation

$$C^n(U)|x_1 x_2 \ldots x_n\rangle|\psi\rangle = |x_1 x_2 \ldots x_n\rangle U^{x_1 x_2 \ldots x_n}|\psi\rangle$$

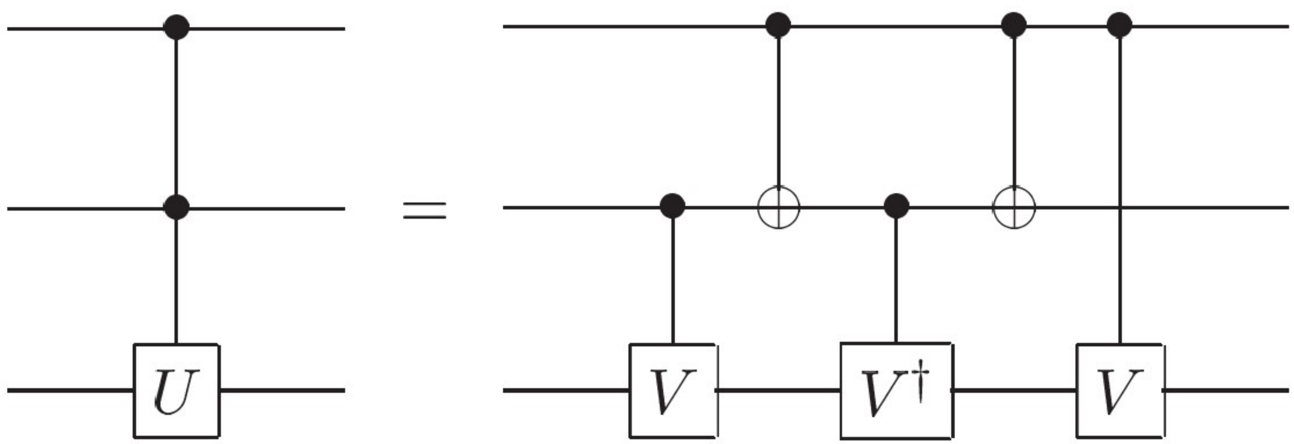
Quantum Computation- Quantum Circuits- Controlled operations



Sample circuit representation for the $C^n(U)$ operation, where U is a unitary operator on k qubits, for n = 4 and k = 3.

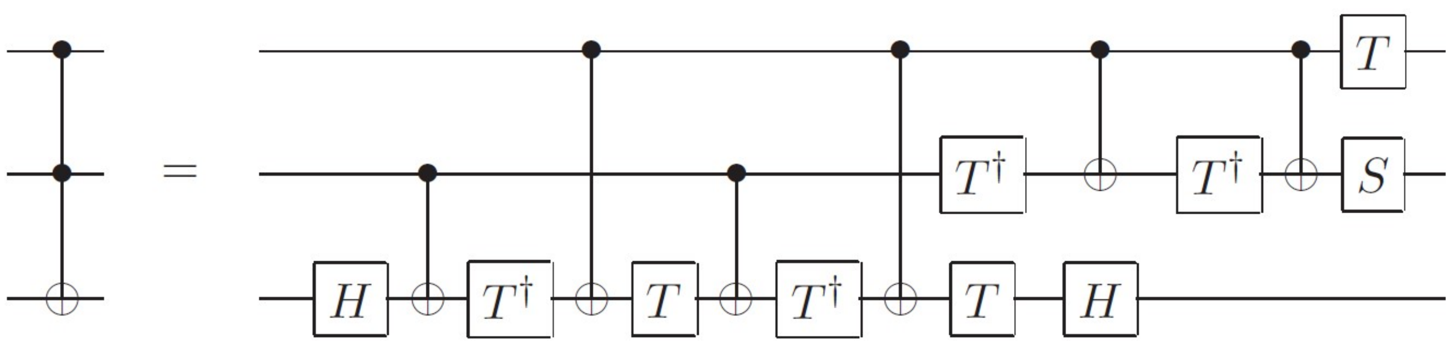
Quantum Computation- Quantum Circuits- Controlled operations

- Suppose *U is a single qubit unitary operator, and V is a unitary operator chosen so* that *$V^2 = U$. Then the operation $C^2(U)$ may be implemented using the following circuit*



Circuit for the *C2(U) gate. V is any unitary operator satisfying $V^2 = U$. The special case $V \equiv (1 - i)(I + iX)/2$ corresponds to the Toffoli gate.*

Quantum Computation- Quantum Circuits- Controlled operations

- The familiar Toffoli gate is an especially important special case of the $C^2(U)$ operation, the case $C^2(X)$.
- Ultimately we will show that any unitary operation can be composed to an arbitrarily good approximation from just the Hadamard, phase, controlled-NOT and *π/8 gates.*
- Because of the great usefulness of the Toffoli gate it is interesting to see how it can be
- built from just this gate set.
- 

Quantum Computation- Quantum Circuits- Controlled operations

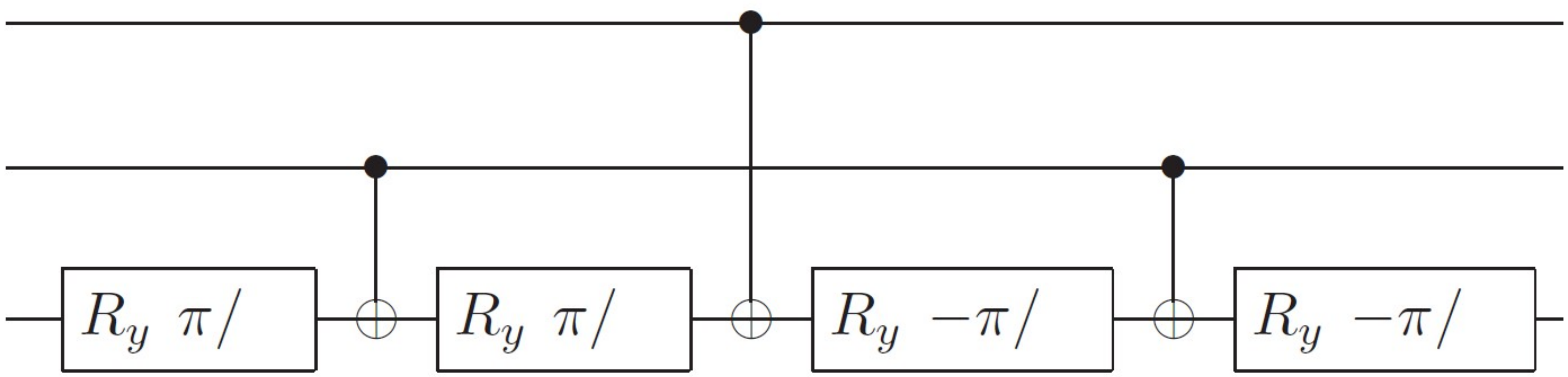
- Exercise: (Fredkin gate construction) the Fredkin (controlled-swap) gate performs the transform

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- 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).

Quantum Computation- Quantum Circuits- Controlled operations

- Exercise: Show that the circuit:



- differs from a Toffoli gate only by relative phases. That is, the circuit takes |c1, c2, t> to $e^{i\theta(c1,c2,t)}$|c1, c2, t $\oplus$ c1 · c2>, where $e^{i\theta(c1,c2,t)}$ is some relative phase factor. Such gates can sometimes be useful in experimental implementations, where it may be much easier to implement a gate that is the same as the Toffoli up to relative phases than it is to do the Toffoli directly.

Quantum Computation- Quantum Circuits- Controlled operations

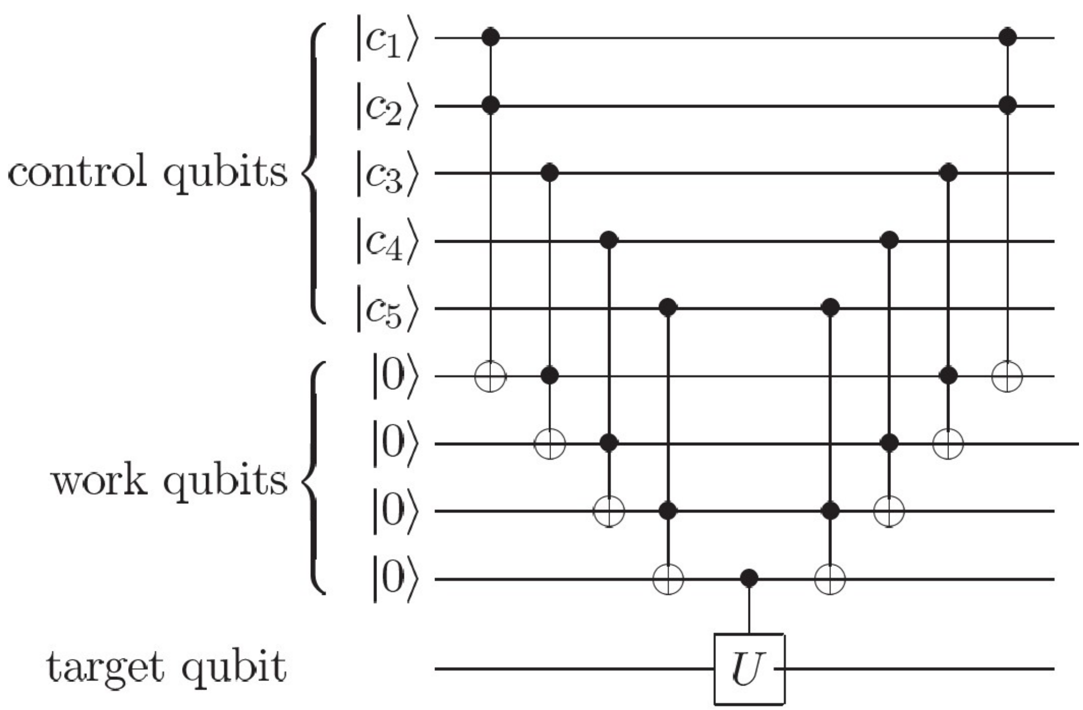
- Exercise: Using just CNOTs and Toffoli gates, construct a quantum circuit to perform the transformation

This kind of partial cyclic permutation operation will be useful later,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

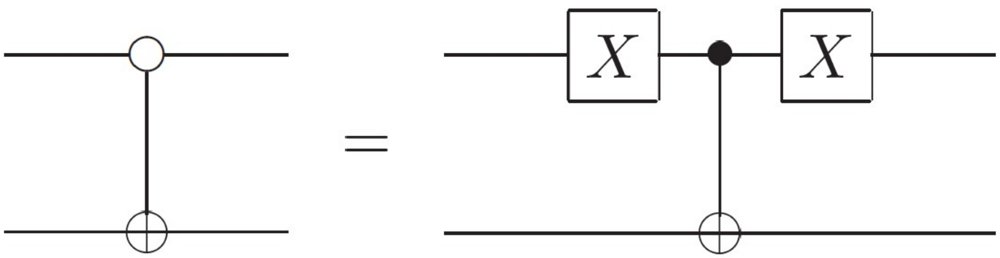
Quantum Computation- Quantum Circuits- Controlled operations

- How may we implement $C^n(U)$ gates using our existing repertoire of gates, where U is an arbitrary single qubit unitary operation?

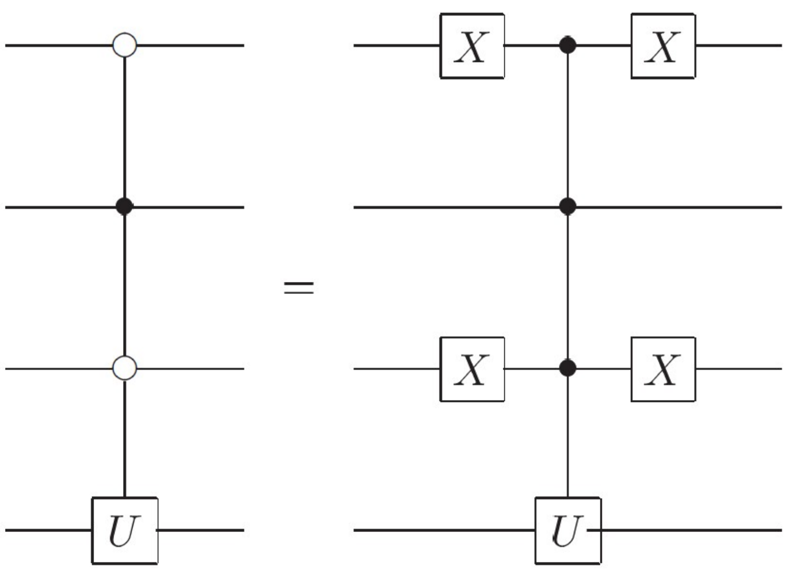


Network implementing the *Cn(U) operation, for the case n = 5.*

Quantum Computation- Quantum Circuits- Controlled operations

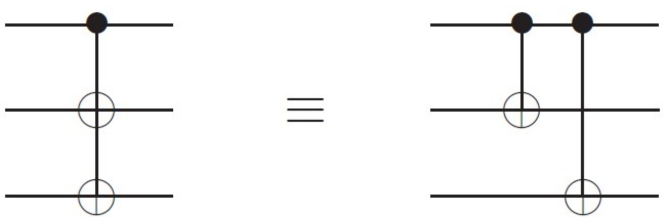


Controlled operation with a NOT gate being performed on the second qubit, conditional on the first qubit being set to zero.



Controlled-*U operation and its equivalent in terms of circuit elements we already know how to* implement. The fourth qubit has *U applied if the first and third qubits are set to zero, and the second qubit is set* to one.

Quantum Computation- Quantum Circuits- Controlled operations



Controlled- gate with multiple targets.

- Exercise: (More circuit identities) Let subscripts denote which qubit an operator acts on, and let *C be a CNOT with qubit 1 the control qubit and qubit 2* the target qubit. Prove the following identities:
-

$$
\begin{aligned}
CX_1C &= X_1X_2 \\
CY_1C &= Y_1X_2 \\
CZ_1C &= Z_1 \\
CX_2C &= X_2 \\
CY_2C &= Z_1Y_2 \\
CZ_2C &= Z_1Z_2 \\
R_{z,1}(\theta)C &= CR_{z,1}(\theta) \\
R_{x,2}(\theta)C &= CR_{x,2}(\theta).
\end{aligned}
$$

Quantum Computation- Quantum Circuits- Measurement

- **Principle of deferred measurement:**
  - **Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.**
- **Principle of implicit measurement:**
  - **Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.**