Introduction to Quantum Information Processing

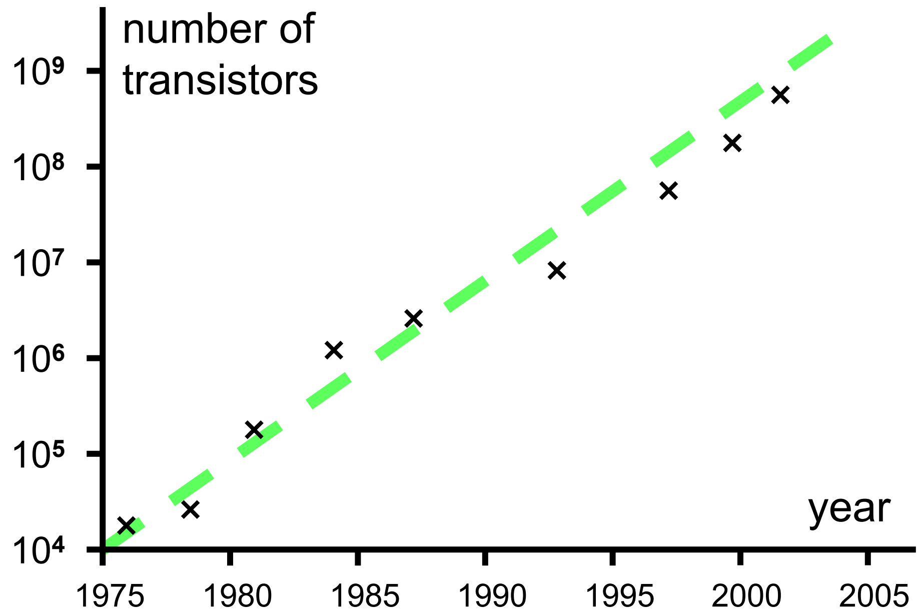
CS 467 / CS 667
Phys 667 / Phys 767
C&O 481 / C&O 681

Lecture 1 (2005)

Richard Cleve
DC 3524
cleve@cs.uwaterloo.ca

Overview

Moore's Law



Following trend … atomic scale in 15-20 years

Quantum mechanical effects occur at this scale:

- Measuring a state (e.g. position) disturbs it
- Quantum systems sometimes seem to behave as if they are in several states at once
- Different evolutions can interfere with each other

Quantum mechanical effects

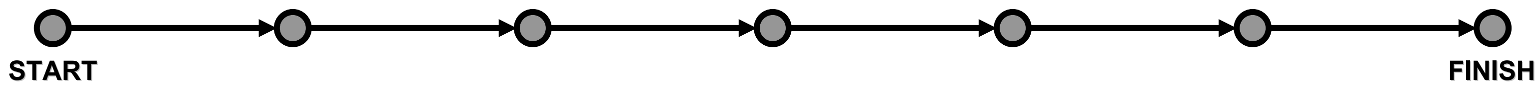
Additional nuisances to overcome?
or
New types of behavior to make use of?

[Shor, 1994]: polynomial-time algorithm for factoring integers on a ***quantum computer***

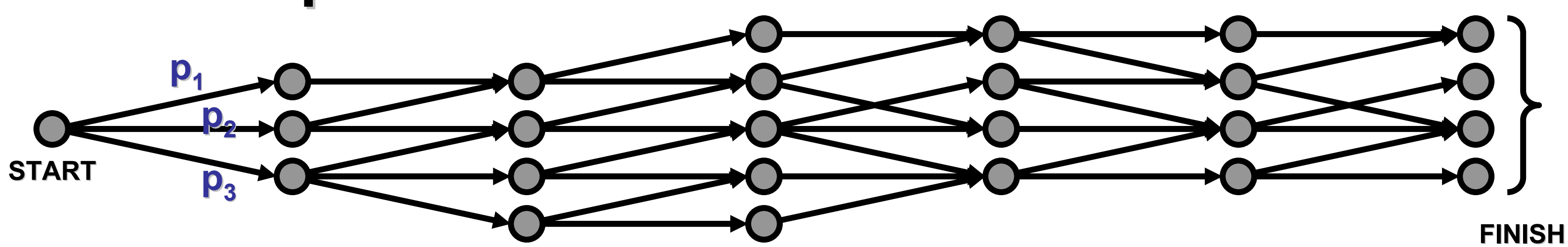
This could be used to break most of the existing public-key cryptosystems on the internet, such as RSA

Quantum algorithms

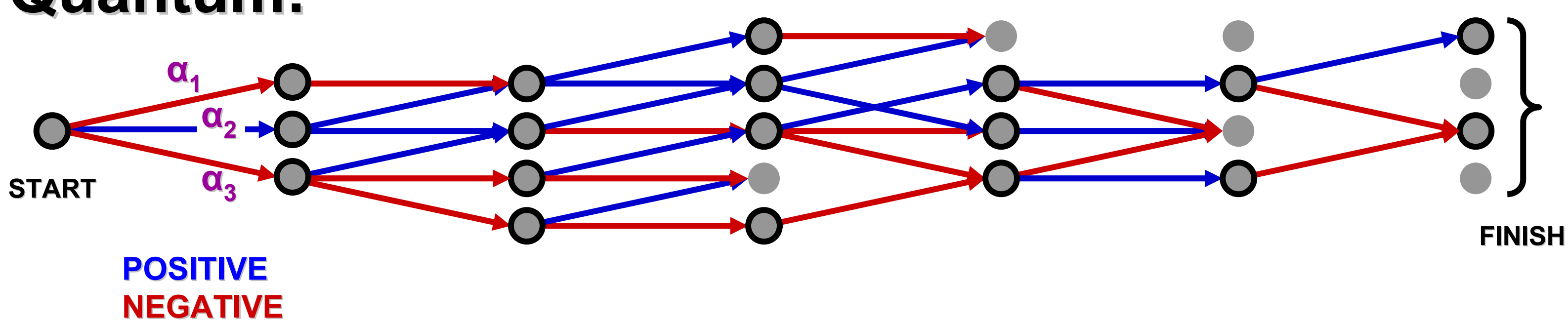
Classical deterministic:



Classical probabilistic:



Quantum:

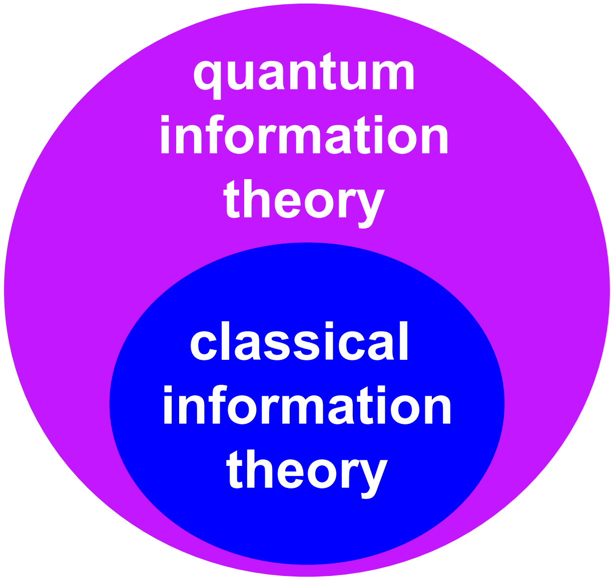


Also with quantum information:

- Fast***er*** algorithms for combinatorial search [Grover '96]
- Unbreakable codes with short keys [Bennett, Brassard '84]
- Communication savings in distributed systems [C, Buhrman '97]
- More efficient "proof systems" [Watrous '99]

… and an extensive quantum information theory arises, which generalizes classical information theory

For example: a theory of quantum error-correcting codes



This course covers the basics of quantum information processing

Topics include:

- Quantum algorithms and complexity theory
- Quantum information theory
- Quantum error-correcting codes*
- Physical implementations*
- Quantum cryptography
- Quantum nonlocality and communication complexity

* Jonathan Baugh

General course information

Background:

- classical algorithms and complexity
- linear algebra
- probability theory

Evaluation:

- 3 assignments (15% each)
- midterm exam (20%)
- written project (35%)

Recommended text:

"Quantum Computation and Quantum Information"
by Nielsen and Chuang (available at the UW Bookstore)

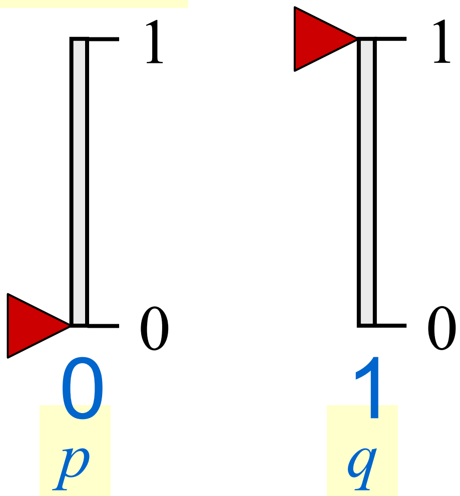
Basic framework of quantum information

Types of information

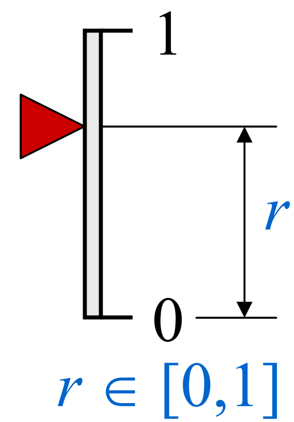
is quantum information digital or analog?

probabilistic

digital:



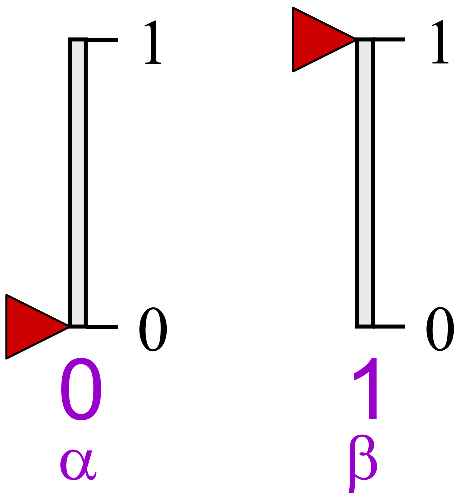
analog:



- Probabilities $p, q \geq 0, \; p + q = 1$
- *Cannot* explicitly extract p and q (only statistical inference)
- In any concrete setting, explicit state is 0 or 1
- Issue of precision (imperfect ok)

- Can explicitly extract r
- Issue of precision for setting & reading state
- Precision need not be perfect to be useful

Quantum (digital) information



- Amplitudes $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$
- Explicit state is $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
- *Cannot* explicitly extract α and β (only statistical inference)
- Issue of precision (imperfect ok)

Dirac bra/ket notation

Ket: $|\psi\rangle$ always denotes a column vector, e.g. $\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_d \end{bmatrix}$

Convention: $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Bra: $\langle\psi|$ always denotes a row vector that is the conjugate transpose of $|\psi\rangle$, e.g. $[\ \alpha^*_1 \quad \alpha^*_2 \quad \ldots \quad \alpha^*_d\ ]$

<u>**Bra**</u>**c**<u>**ket**</u>**:** $\langle\varphi|\psi\rangle$ denotes $\langle\varphi|\cdot|\psi\rangle$, the inner product of $|\varphi\rangle$ and $|\psi\rangle$

Basic operations on qubits (I)

(0) Initialize qubit to $|0\rangle$ or to $|1\rangle$

(1) Apply a unitary operation U ($U^\dagger U = I$)

Examples:

Rotation: $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$

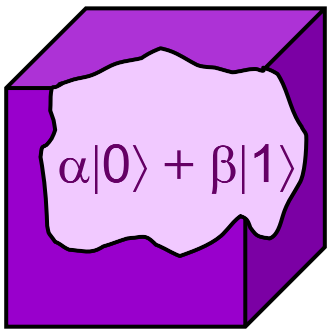
NOT (bit flip): $\sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Hadamard: $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

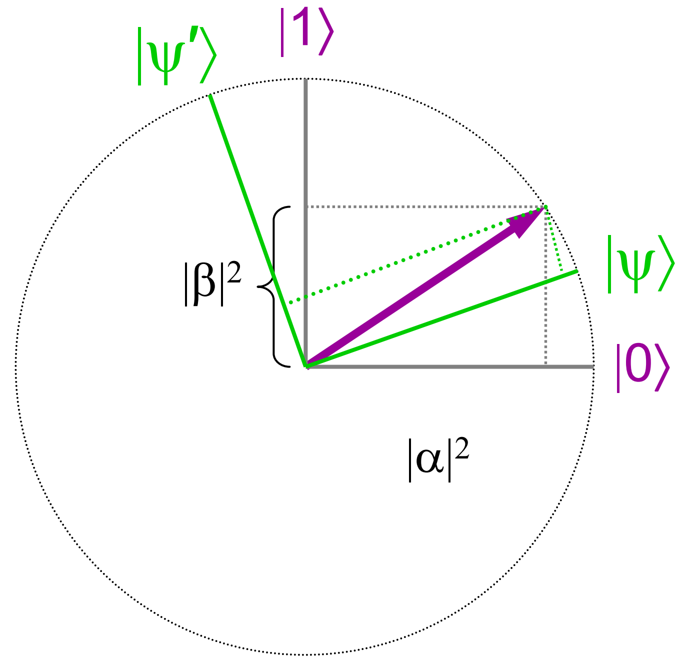
Phase flip: $\sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Basic operations on qubits (II)

(3) Apply a "standard" measurement:



$$\mapsto \begin{cases} 0 \text{ with prob } |\alpha|^2 \\ 1 \text{ with prob } |\beta|^2 \end{cases}$$

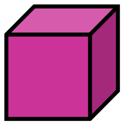


… and the quantum state collapses

(∗) There exist ***other*** quantum operations, but they can all be "simulated" by the aforementioned types

Example: measurement with respect to a different orthonormal basis $\{|\psi\rangle, |\psi'\rangle\}$

Distinguishing between two states

Let  be in state $|+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$ or $|-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$

Question 1: can we distinguish between the two cases?

Distinguishing procedure:

1. apply H
2. measure

This works because $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$

Question 2: can we distinguish between $|0\rangle$ and $|+\rangle$?

Since they're not orthogonal, they ***cannot*** be ***perfectly*** distinguished …

n-qubit systems

Probabilistic states:

$$\forall x,\ p_x \geq 0$$

$$\sum_x p_x = 1$$

$$\begin{bmatrix} p_{000} \\ p_{001} \\ p_{010} \\ p_{011} \\ p_{100} \\ p_{101} \\ p_{110} \\ p_{111} \end{bmatrix}$$

Quantum states:

$$\forall x,\ \alpha_x \in \mathbb{C}$$

$$\sum_x |\alpha_x|^2 = 1$$

$$\begin{bmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{bmatrix}$$

Dirac notation: $|000\rangle$, $|001\rangle$, $|010\rangle$, …, $|111\rangle$ are basis vectors,

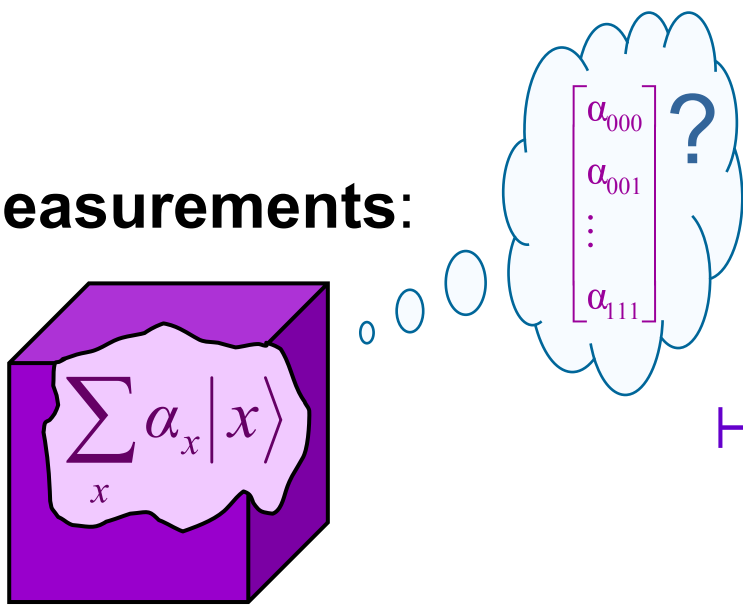
so $|\psi\rangle = \sum_x \alpha_x |x\rangle$

Operations on n-qubit states

Unitary operations: $\sum_x \alpha_x |x\rangle \quad \mapsto \quad U\left(\sum_x \alpha_x |x\rangle\right)$

$(U^\dagger U = I)$

Measurements:



$$\mapsto \begin{cases} 000 & \text{with prob } |\alpha_{000}|^2 \\ 001 & \text{with prob } |\alpha_{001}|^2 \\ \vdots & \vdots \qquad\qquad \vdots \\ 111 & \text{with prob } |\alpha_{111}|^2 \end{cases}$$

… and the quantum state collapses

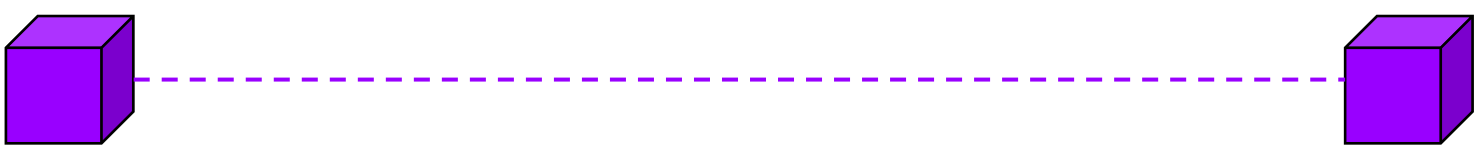
Entanglement

Product state (tensor/Kronecker product):

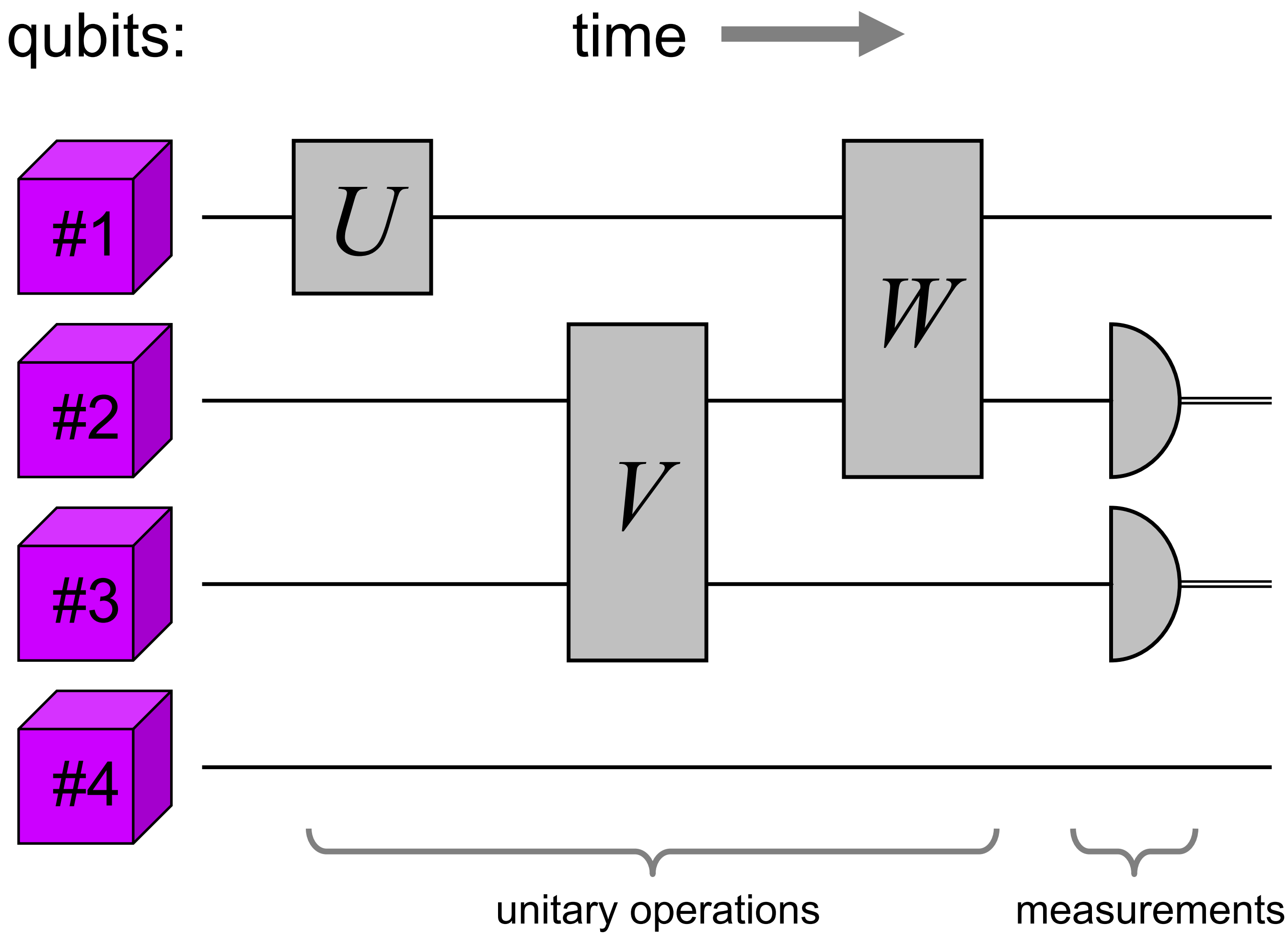
$$\left(\alpha|0\rangle+\beta|1\rangle\right)\left(\alpha'|0\rangle+\beta'|1\rangle\right)=\alpha\alpha'|00\rangle+\alpha\beta'|01\rangle+\beta\alpha'|10\rangle+\beta\beta'|11\rangle$$

Example of an ***entangled*** state: $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$

… can exhibit interesting "nonlocal" correlations:

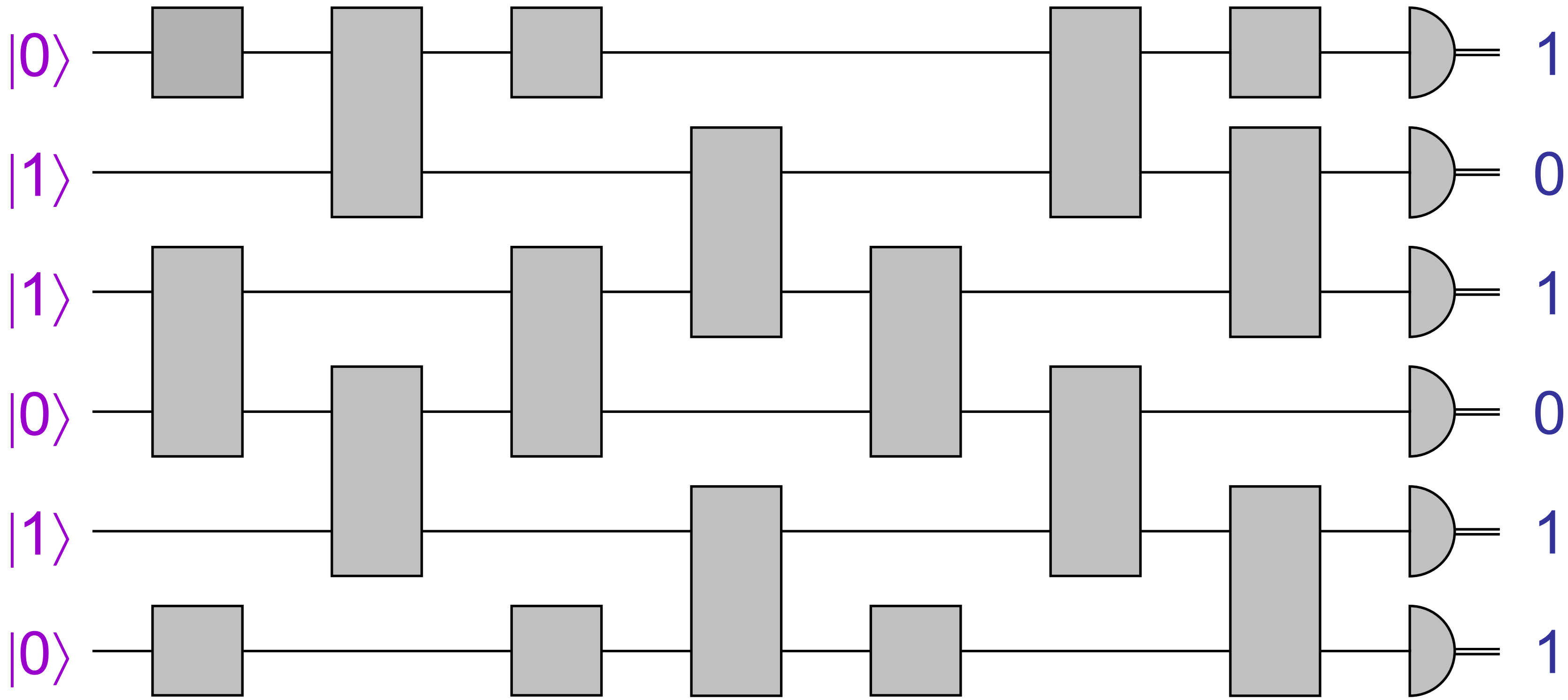


Structure among subsystems



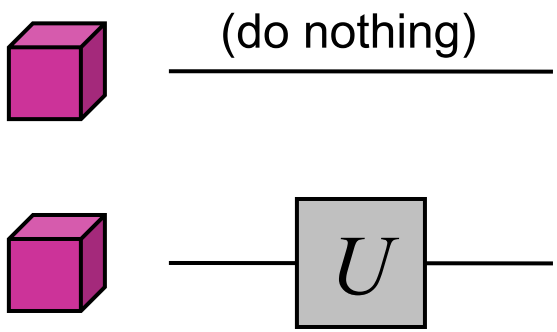
Quantum computations

Quantum circuits:



“Feasible” if circuit-size scales polynomially

Example of a one-qubit gate applied to a two-qubit system



$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

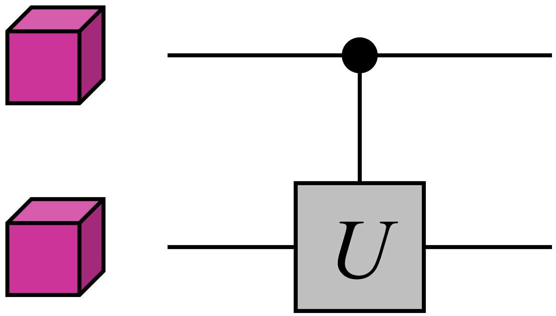
Maps basis states as:

$$|0\rangle|0\rangle \rightarrow |0\rangle U|0\rangle$$
$$|0\rangle|1\rangle \rightarrow |0\rangle U|1\rangle$$
$$|1\rangle|0\rangle \rightarrow |1\rangle U|0\rangle$$
$$|1\rangle|1\rangle \rightarrow |1\rangle U|1\rangle$$

The resulting 4x4 matrix is

$$I \otimes U = \begin{bmatrix} u_{00} & u_{01} & 0 & 0 \\ u_{10} & u_{11} & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

Controlled-U gates



$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

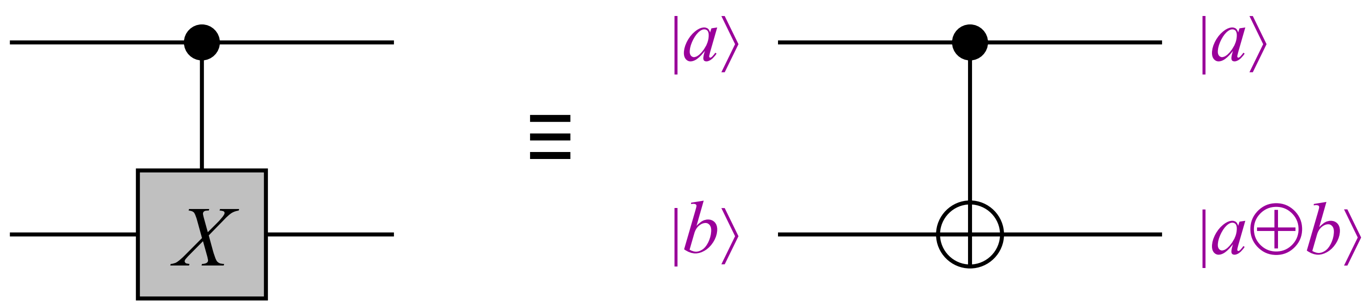
Resulting 4x4 matrix is controlled-U =

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

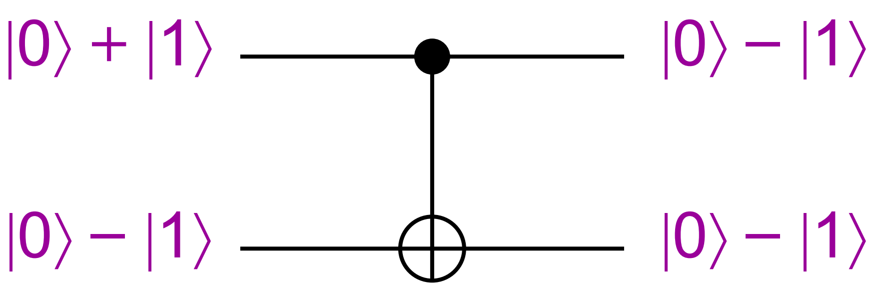
Maps basis states as:

$$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \rightarrow |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \rightarrow |1\rangle U|0\rangle$$
$$|1\rangle|1\rangle \rightarrow |1\rangle U|1\rangle$$

Controlled-NOT (CNOT)



Note: “control” qubit may change on some input states



THE END