

Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 1 (2017)

Jon Yard

QNC 3126

jyard@uwaterloo.ca

TAs

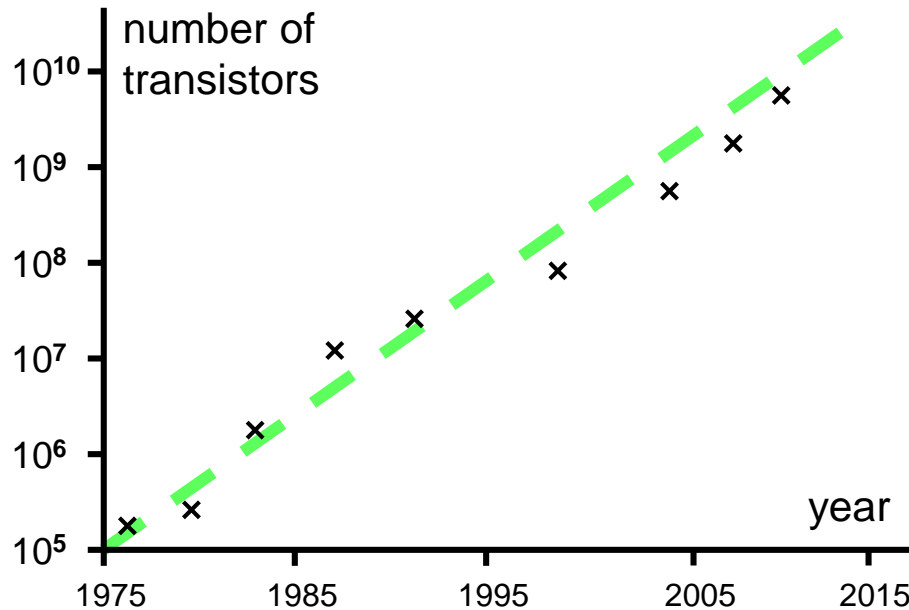
Nitica Sakharwade

nsakharwade@perimeterinstitute.ca

Chunhao Wang

chunhao.wang@uwaterloo.ca

Moore's Law



Following trend ... will reach atomic scale

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

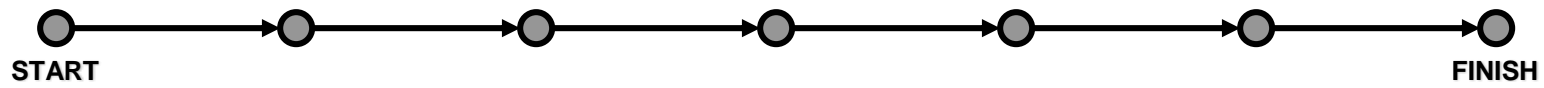
New types of behavior to make use of?

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

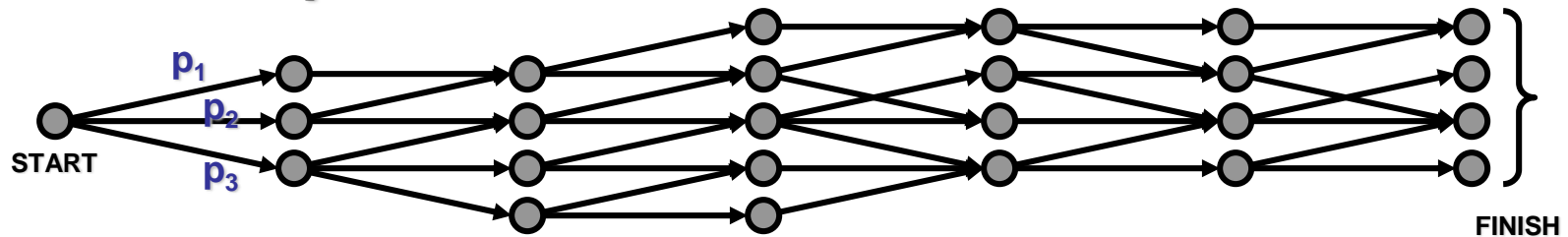
This could be used to break most of the existing public-key cryptosystems on the internet, such as RSA

Nontechnical schematic view of quantum algorithms

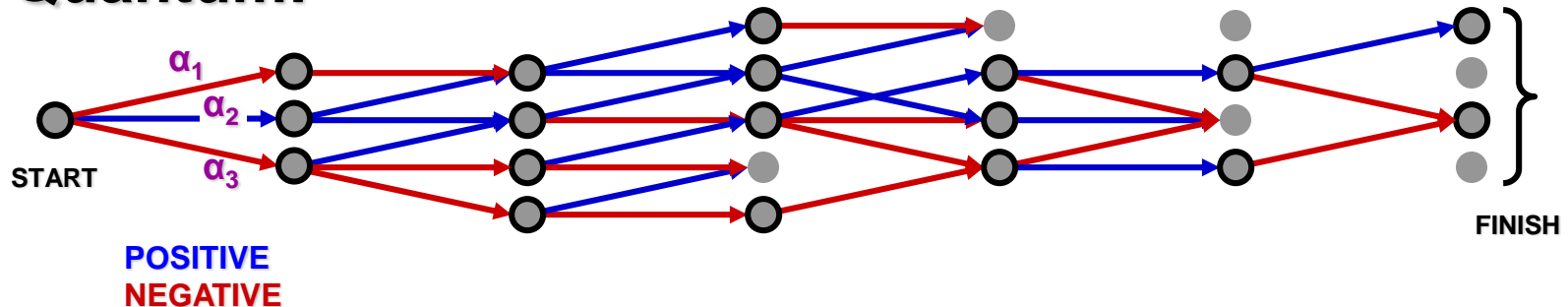
Classical deterministic:



Classical probabilistic:



Quantum:

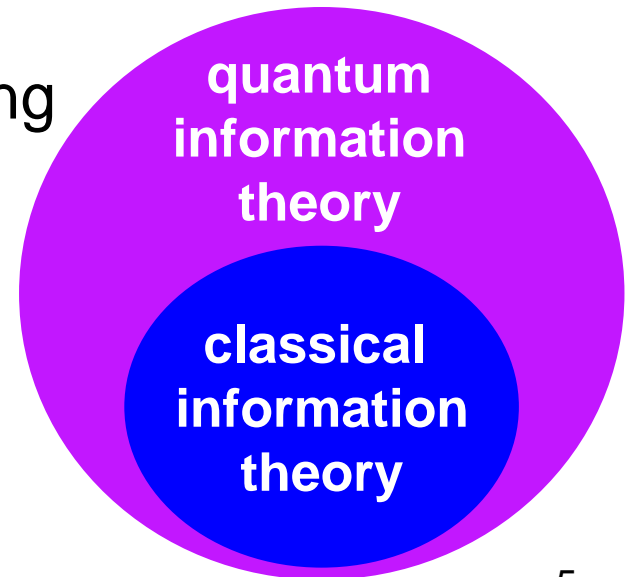


Also with quantum information:

- Faster algorithms for several combinatorial search problems and for evaluating game trees (polynomial speed-up)
- Fast algorithms for simulating quantum mechanical systems
- Communication savings in distributed systems
- Various notions of “quantum proof systems”
- Recent experimental progress → rapidly growing industry may be bringing quantum computers closer to reality

Quantum information theory:

- Framework for modeling and overcoming quantum mechanical noise
- Generalizes notions in classical information theory, such as
 - error-correcting codes
 - entropy
 - compression
 - correlation → entanglement



This course covers the basics of quantum information processing

Topics include:

- Introduction to the quantum information framework
- Quantum algorithms (including Shor's factoring algorithm and Grover's search algorithm)
- Computational complexity theory
- Density matrices and quantum operations on them
- Distance measures between quantum states
- Entropy and noiseless coding
- Error-correcting codes and fault-tolerance
- Non-locality
- Cryptography

General course information

Background:

- linear algebra
- probability theory
- classical algorithms and complexity

Evaluation:

- 5 assignments (12% each)
- project presentation (40%)

Recommended texts:

An Introduction to Quantum Computation, P. Kaye, R. Laflamme, M. Mosca (Oxford University Press, 2007). Primary reference.

Quantum Computation and Quantum Information, Michael A. Nielsen and Isaac L. Chuang (Cambridge University Press, 2000). Secondary reference.

Quantum Computation Since Democritus, Scott Aaronson (Cambridge University Press, 2012). Optional fun background reading.

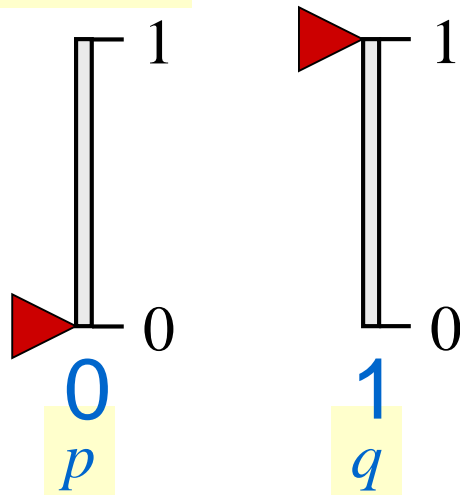
Basic framework of quantum information

Types of information

is quantum information digital or analog?

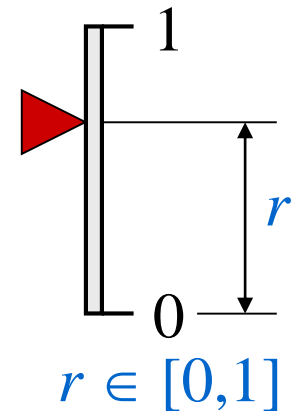
probabilistic

digital:



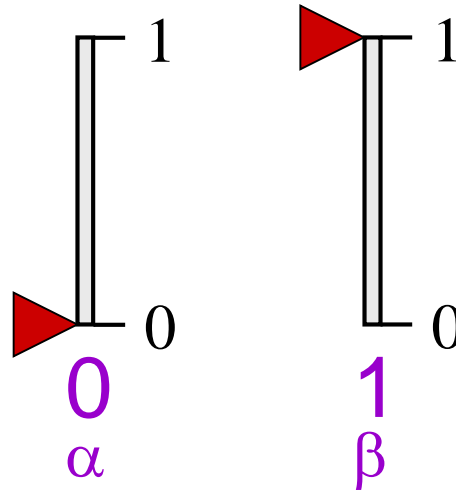
- Probabilities $p, q \geq 0, p + q = 1$
- *Cannot* explicitly extract p and q (only statistical inference)
- In any concrete setting, explicit state is 0 or 1
- Issue of precision (imperfect ok)

analog:



- 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 a vector $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$
- *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. $|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix} \in \mathbb{C}^d$

Convention: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Bra: $\langle\psi|$ always denotes a row vector that is the conjugate transpose of $|\psi\rangle$, e.g. $\langle\psi| = (\alpha_1^* \ \alpha_2^* \ \cdots \ \alpha_d^*)$

Bracket: $\langle\varphi|\psi\rangle$ denotes $\langle\varphi, \psi\rangle$, 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 (unitary means $U^\dagger U = I$)

↑
conjugate transpose

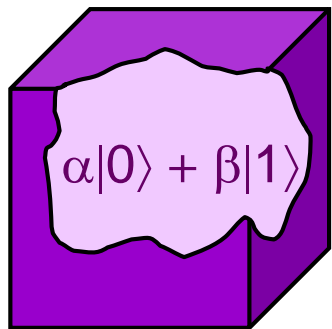
Examples:

Rotation: $\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ **NOT (bit flip):** $\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

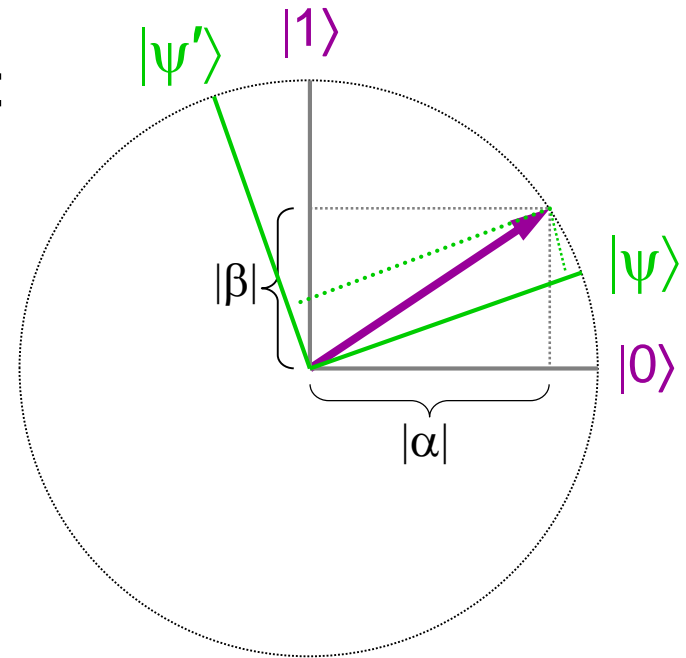
Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ **Phase flip:** $\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Basic operations on qubits (II)

(2) Apply a “standard” measurement:



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

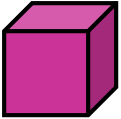


... and the quantum state collapses to $|0\rangle$ or $|1\rangle$ accordingly...

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

Question 1: can we distinguish between the two cases?

Distinguishing procedure:

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

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:

$$\forall x, p_x \geq 0$$
$$\sum_x p_x = 1$$
$$\begin{pmatrix} p_{000} \\ p_{001} \\ p_{010} \\ p_{011} \\ p_{100} \\ p_{101} \\ p_{110} \\ p_{111} \end{pmatrix}$$

Quantum states:

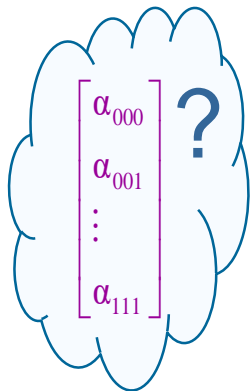
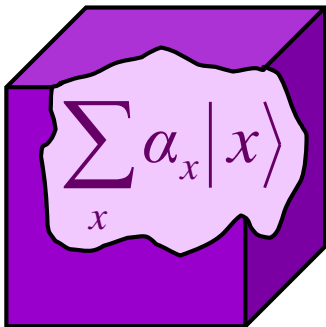
$$\forall x, \alpha_x \in \mathbb{C}$$
$$\sum_x |\alpha_x|^2 = 1 \quad |\psi\rangle =$$
$$\begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix}$$

Dirac notation: $|000\rangle, |001\rangle, |010\rangle, \dots, |111\rangle$ are basis vectors,
so $|\psi\rangle = \sum_x \alpha_x |x\rangle$.

Operations on n -qubit states

Unitary operations: $\sum_x \alpha_x |x\rangle \mapsto U \left(\sum_x \alpha_x |x\rangle \right) = \sum_x \alpha_x U|x\rangle$
($U^\dagger U = I$)

Measurements:

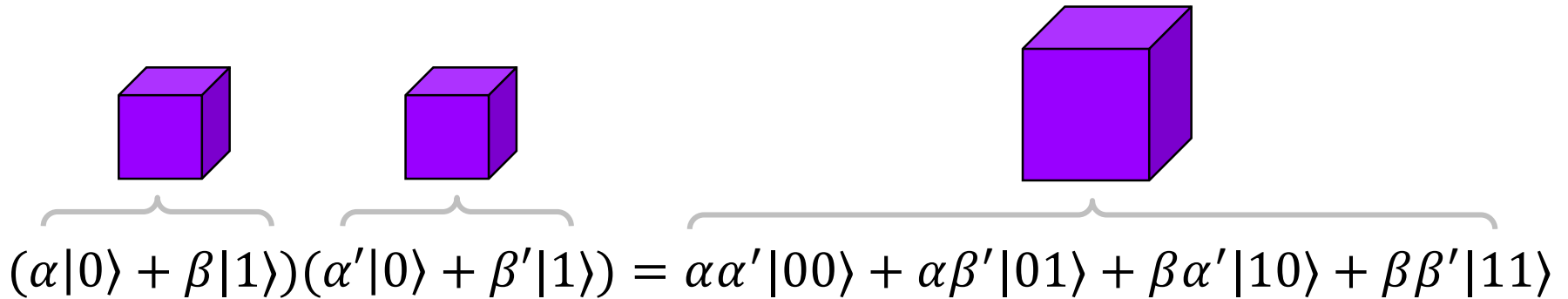


- 000 with prob $|\alpha_{000}|^2$
- 001 with prob $|\alpha_{001}|^2$
- \vdots
- 111 with prob $|\alpha_{111}|^2$

... and the quantum state collapses

(Tensor) product states

Two ways of thinking about two qubits:

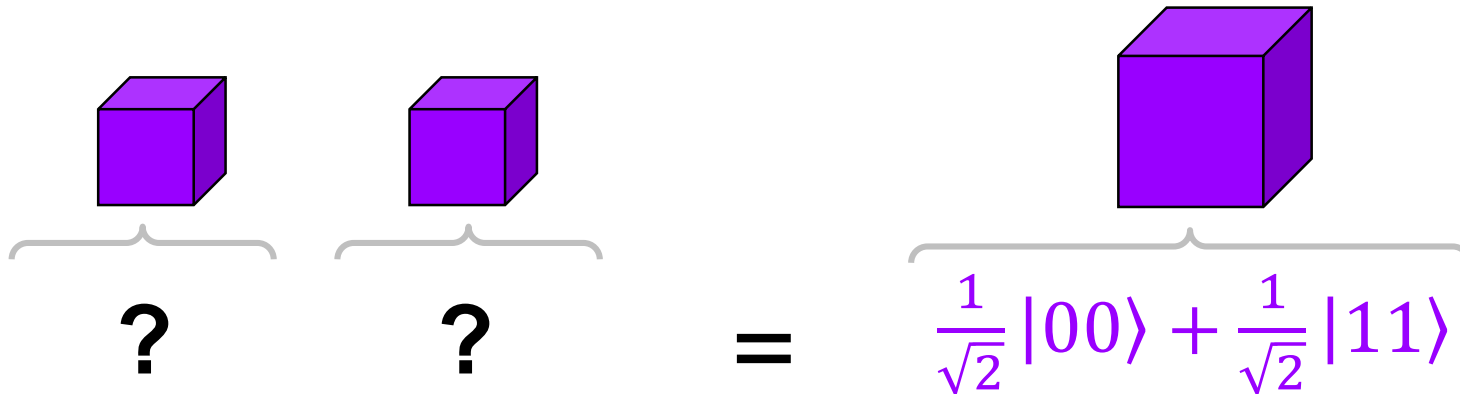

$$(\alpha|0\rangle + \beta|1\rangle)(\alpha'|0\rangle + \beta'|1\rangle) = \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle$$

This is a **product** state (tensor/Kronecker product)

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}$$

Entanglement

What about the following state?


$$\underbrace{\text{Cube}}_{?} \quad \underbrace{\text{Cube}}_{?} = \underbrace{\text{Large Cube}}_{\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle}$$

This cannot be expressed as a product state!

It's an example of an *entangled* state

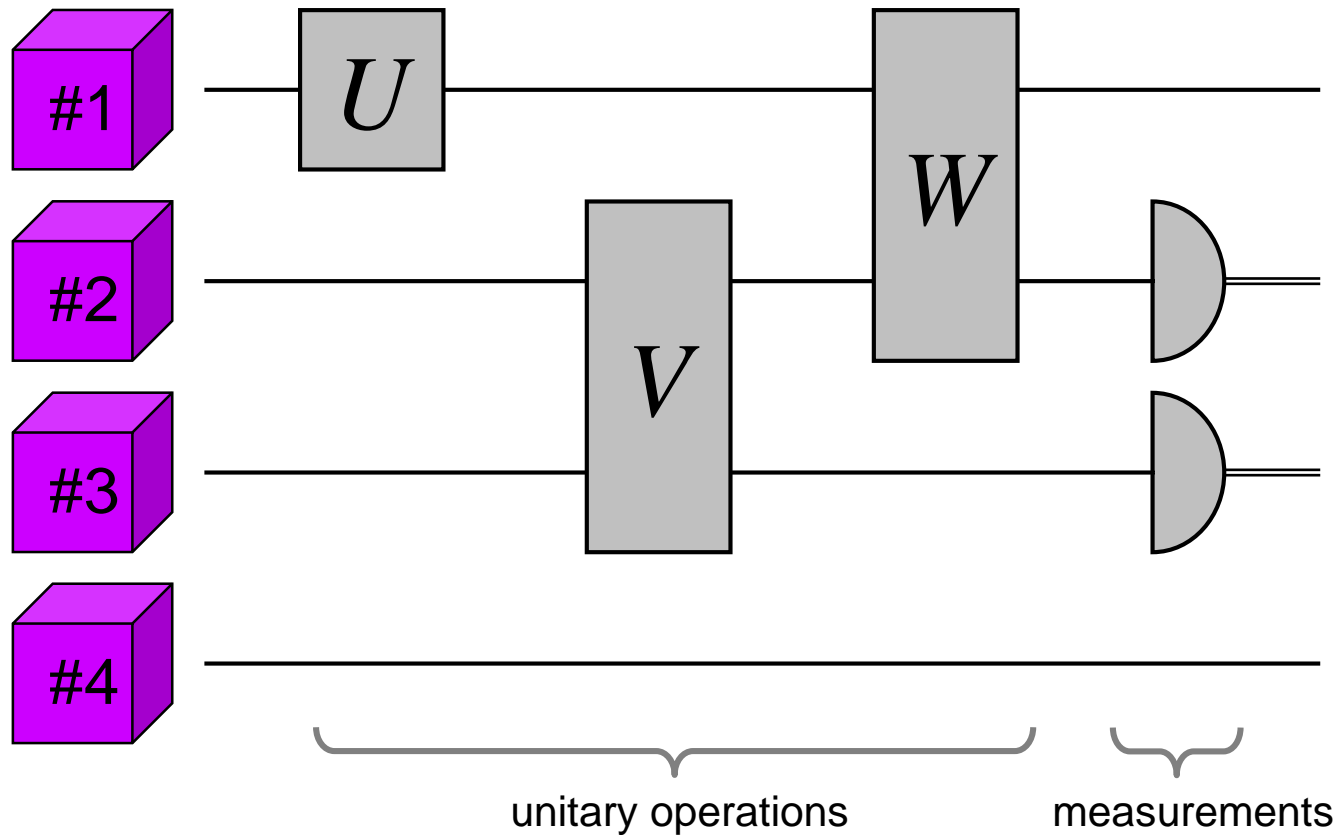
... which can exhibit interesting “nonlocal” correlations



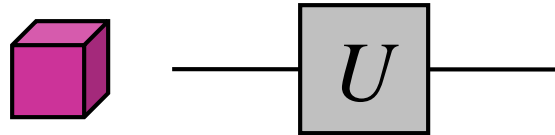
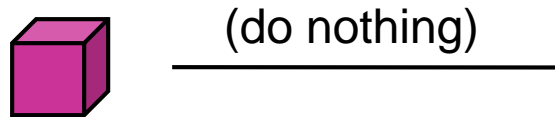
Structure among subsystems

qubits:

time \longrightarrow



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



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

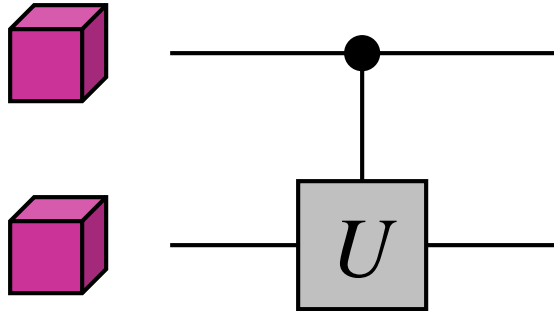
Maps basis states as

$$\begin{aligned} |0\rangle|0\rangle &\mapsto |0\rangle U|0\rangle \\ |0\rangle|1\rangle &\mapsto |0\rangle U|1\rangle \\ |1\rangle|0\rangle &\mapsto |1\rangle U|0\rangle \\ |1\rangle|1\rangle &\mapsto |1\rangle U|1\rangle \end{aligned}$$

The resulting 4x4 matrix is

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

Controlled- U gates



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

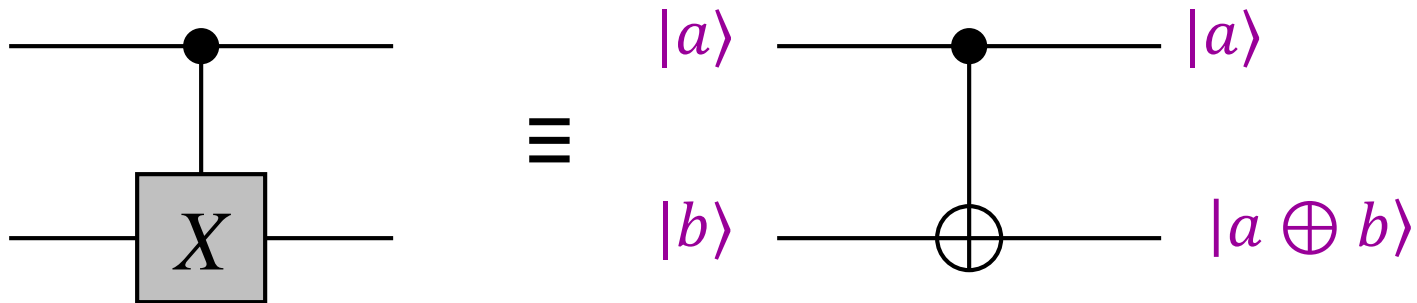
Maps basis states as

$$\begin{aligned} |0\rangle|0\rangle &\mapsto |0\rangle|0\rangle \\ |0\rangle|1\rangle &\mapsto |0\rangle|1\rangle \\ |1\rangle|0\rangle &\mapsto |1\rangle U|0\rangle \\ |1\rangle|1\rangle &\mapsto |1\rangle U|1\rangle \end{aligned}$$

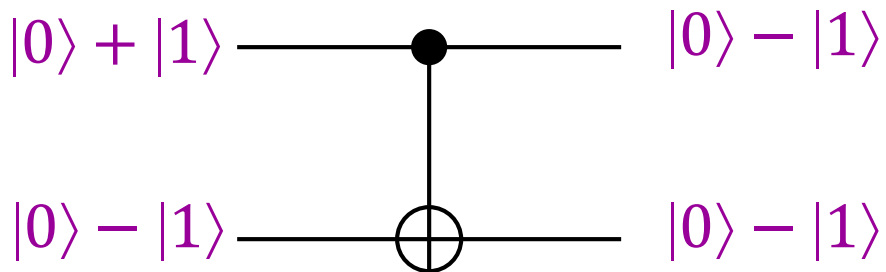
The resulting 4x4 matrix is

$$\text{Controlled-}U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}$$

Controlled-NOT (CNOT)



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



Famous single-qubit gates

All these generate the **Clifford group**, which is related to the symmetry group of a cube or octahedron. More later on this.



Pauli

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

Hadamard

$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

Phase

An important non-Clifford gate is the **T-gate** $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/8} \end{pmatrix}$