

# **Introduction to Quantum Information Processing**

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

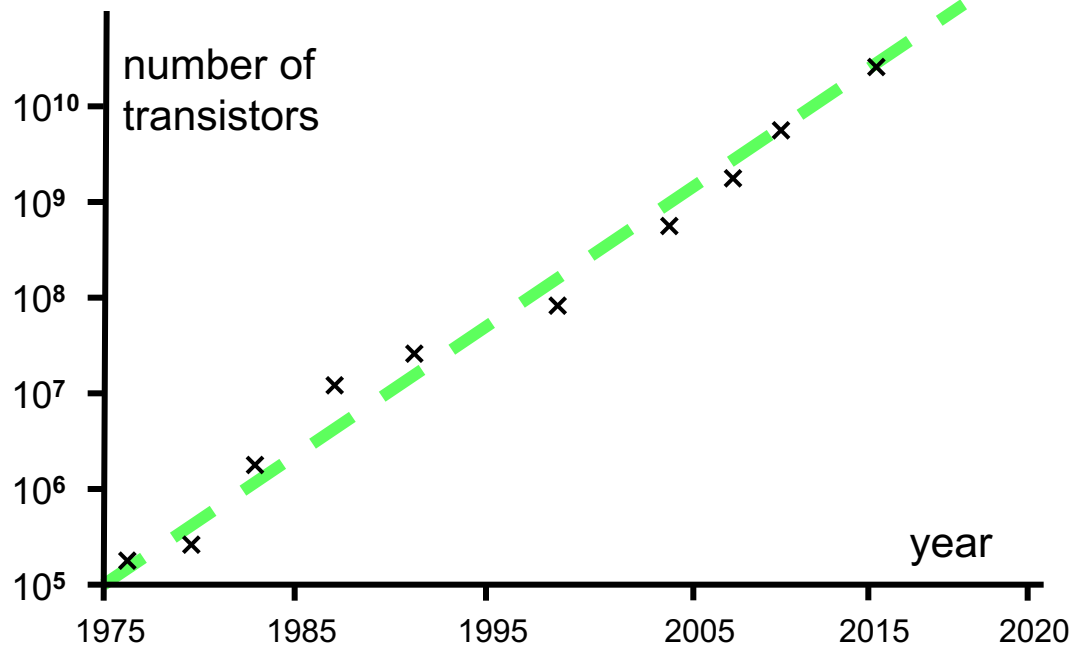
## **Lectures 1–3 (2019)**

**Richard Cleve**

DC 2117 / QNC 3129

[cleve@uwaterloo.ca](mailto:cleve@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

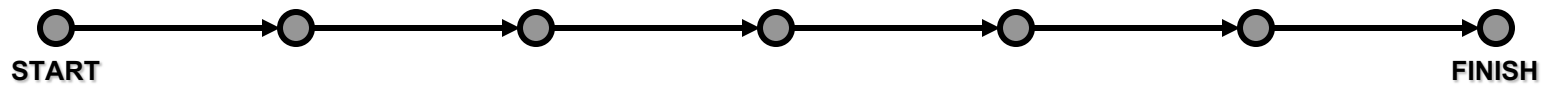
New types of behavior to make use of?

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

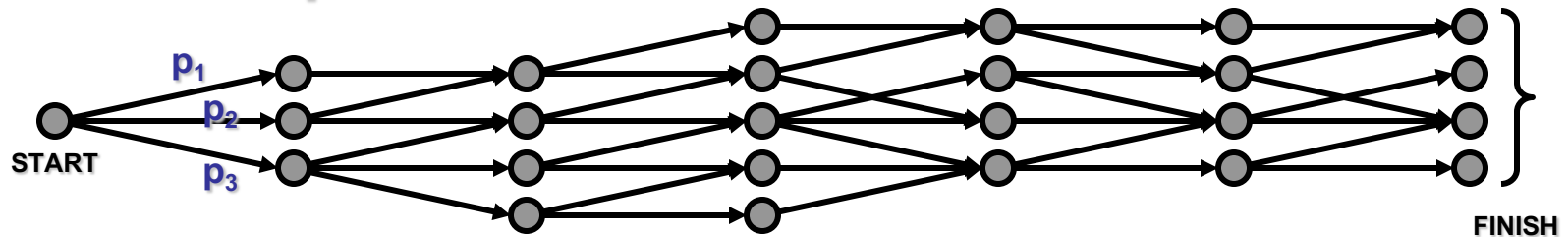
This could be used to break most of the existing public-key cryptosystems on the internet, such as RSA

# Nontechnical schematic view of quantum algorithms

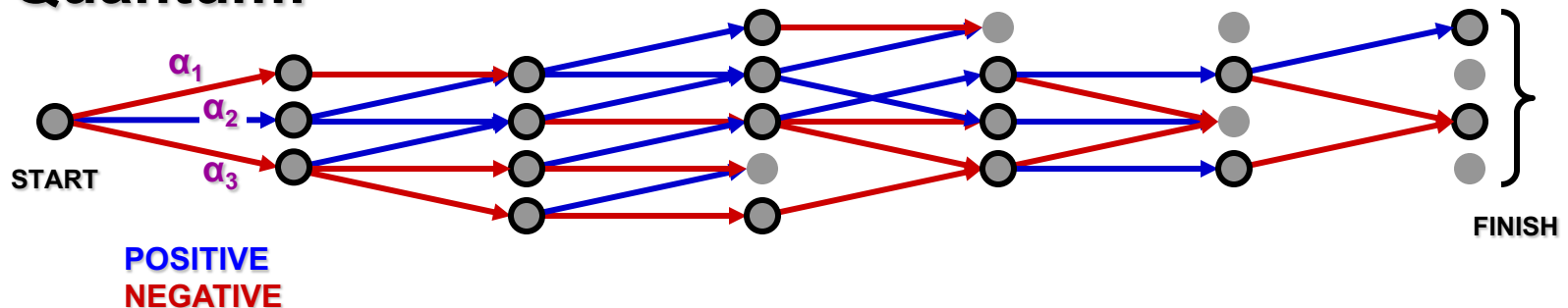
## Classical deterministic:



## Classical probabilistic:



## Quantum:



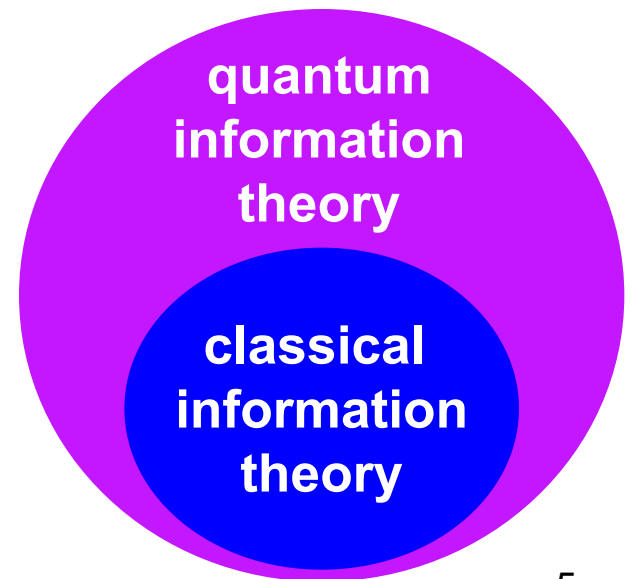
# Also with quantum information:

- 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”
- Experimental progress → quantum devices closer to reality?

## Quantum information theory:

generalization of notions in classical information theory, such as

- entropy
- compression
- error-correcting codes
- quantum 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:

- classical algorithms and complexity
- linear algebra
- probability theory

## 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, 2000). Optional fun background reading.

# Basic framework of quantum information

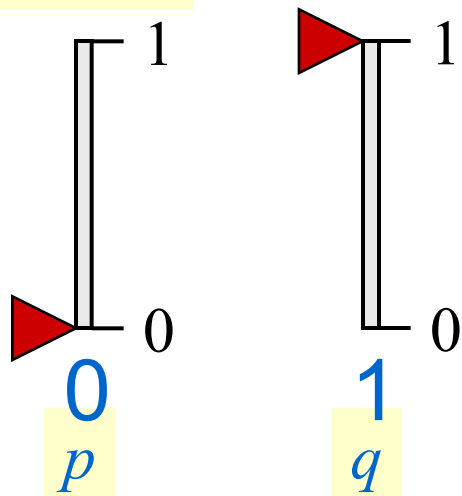


# Types of information

is quantum information digital or analog?

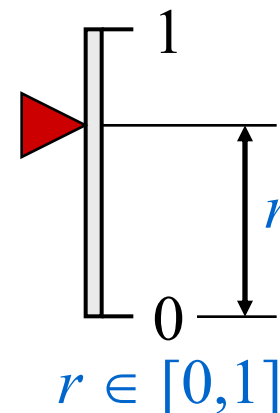
probabilistic

digital:



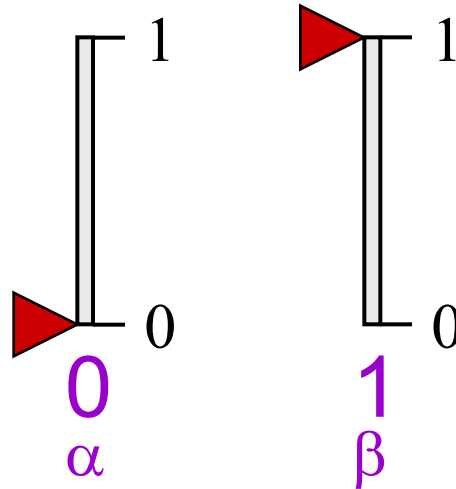
- Probabilities  $p, q \geq 0$ ,  $p + q = 1$
- *Cannot* explicitly extract  $p$  and  $q$  (only statistical inference)
- In any concrete setting, explicit state is 0 or 1
- Issue of precision (imperfect ok)

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  $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
- *Cannot* explicitly extract  $\alpha$  and  $\beta$  (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:**  $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$      $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

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

**Bracket:**  $\langle\phi|\psi\rangle$  denotes  $\langle\phi|\cdot|\psi\rangle$ , the inner product of  $|\phi\rangle$  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:** 
$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

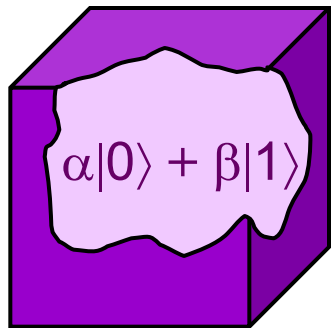
**NOT (bit flip):**  $\sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

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

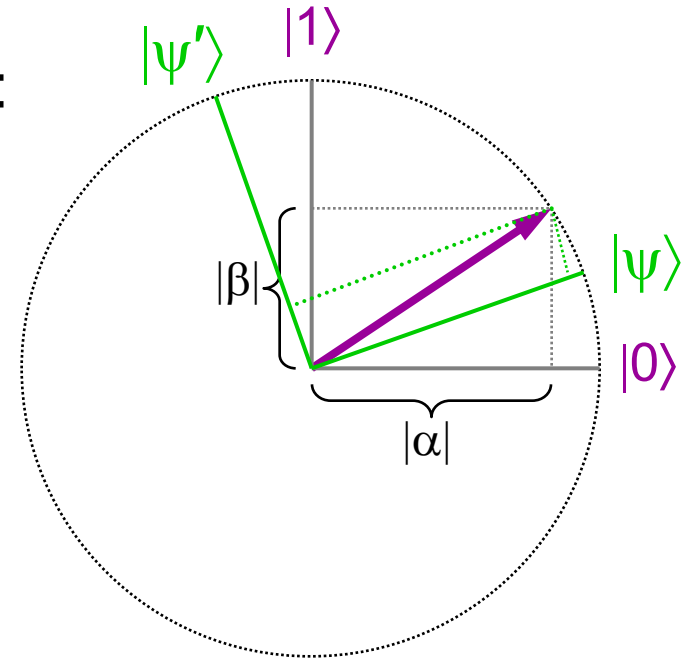
**Phase flip:**  $\sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

# Basic operations on qubits (II)

(2) Apply a “standard” measurement:



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

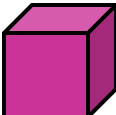


... and the quantum state collapses

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

**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:

$$\forall x, \alpha_x \in \mathcal{C}$$
$$\sum_x |\alpha_x|^2 = 1$$
$$\begin{bmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{bmatrix}$$

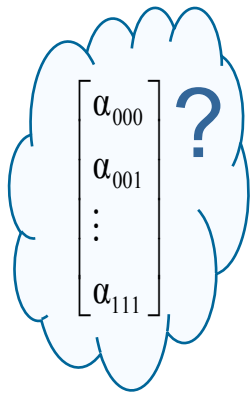
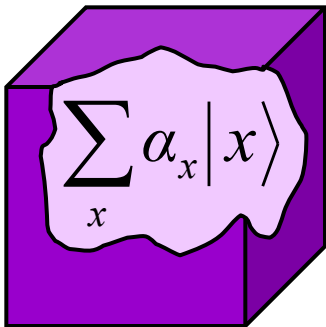
Dirac notation:  $|000\rangle, |001\rangle, |010\rangle, \dots, |111\rangle$  are basis vectors,

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

# Operations on $n$ -qubit states

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

**Measurements:**




$$\left\{ \begin{array}{ll} 000 & \text{with prob } |\alpha_{000}|^2 \\ 001 & \text{with prob } |\alpha_{001}|^2 \\ \vdots & \vdots \\ 111 & \text{with prob } |\alpha_{111}|^2 \end{array} \right.$$

... 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):

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

# Entanglement

What about the following state?


$$\underbrace{\quad} \underbrace{\quad} = \underbrace{\quad} \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

**This cannot be expressed as a product state!**

It's an example of an *entangled* state

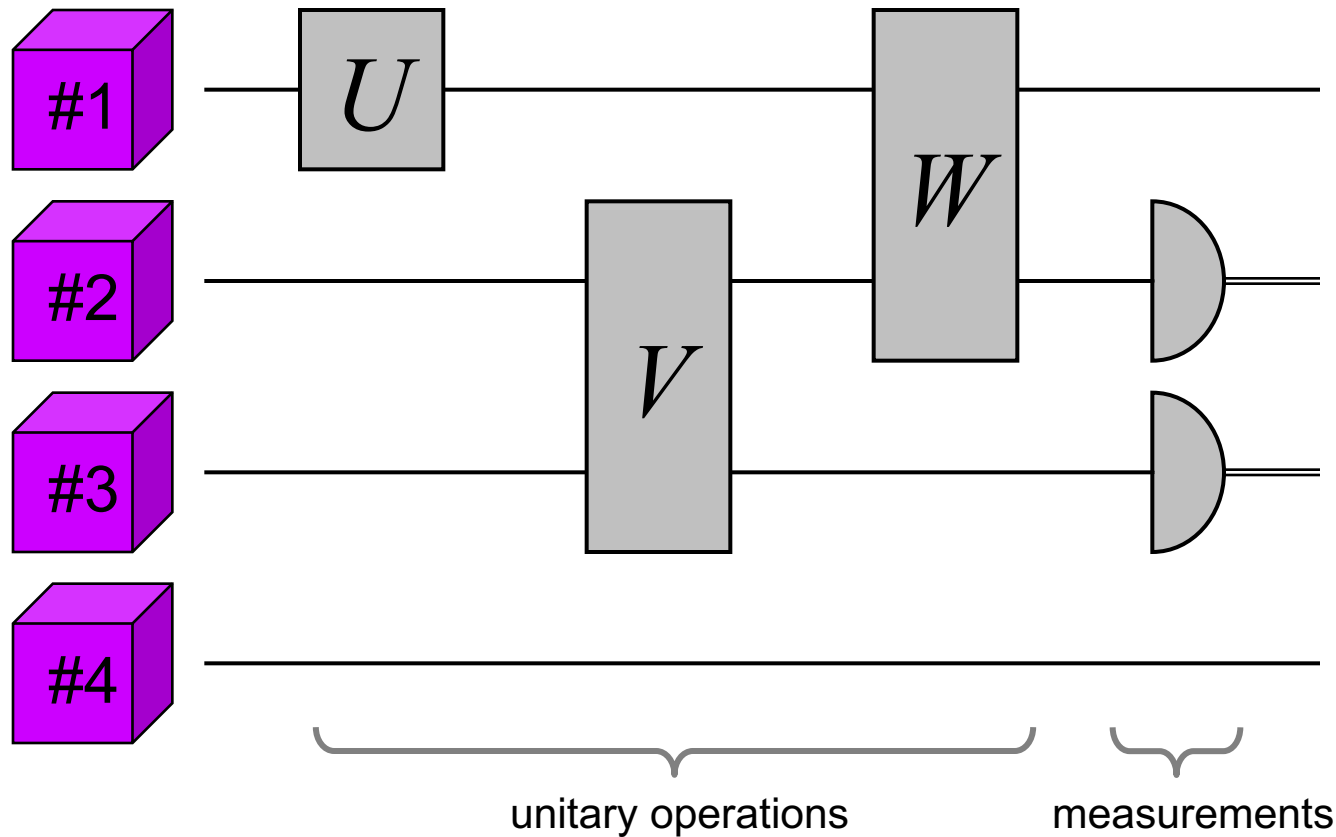
... which can exhibit interesting “nonlocal” correlations



# Structure among subsystems

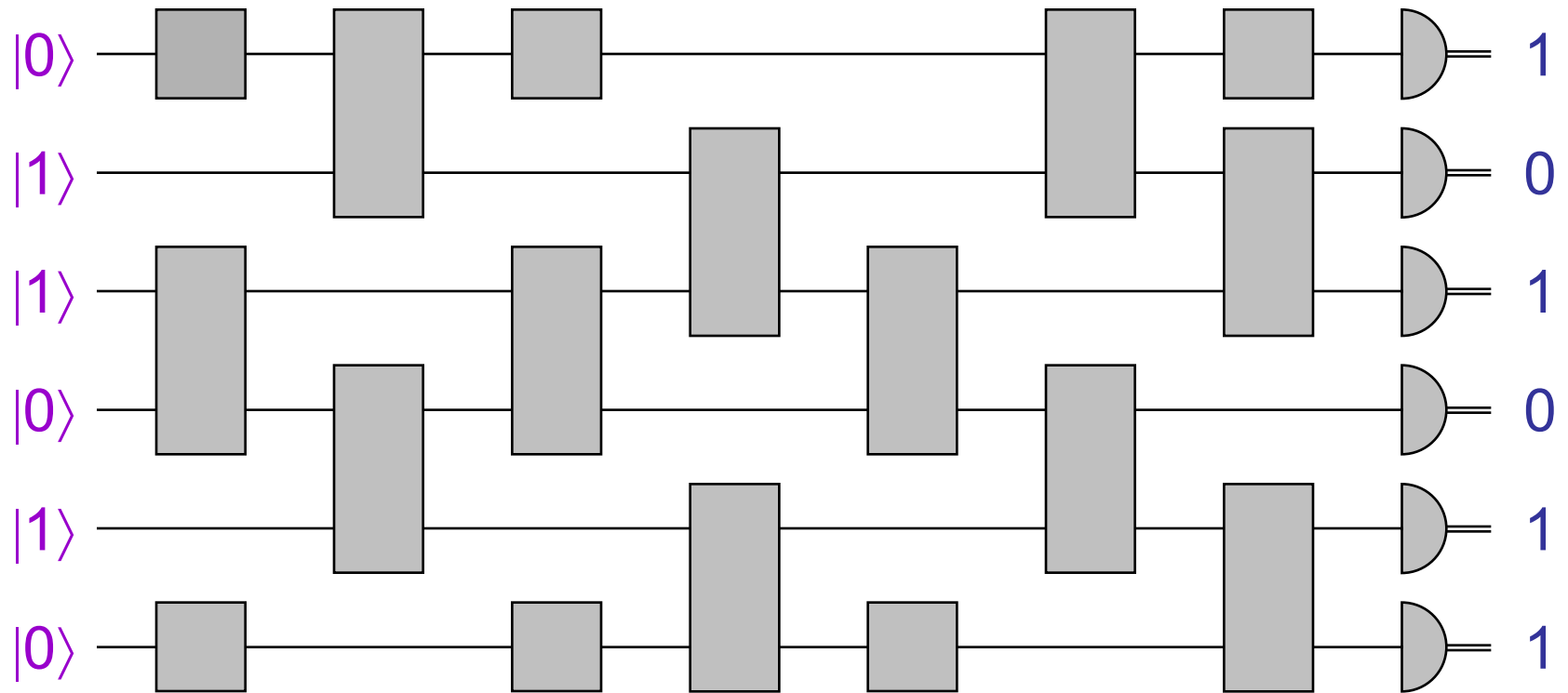
qubits:

time  $\longrightarrow$



# Quantum computations

Quantum circuits:



“Feasible” if circuit-size scales polynomially

# **Introduction to Quantum Information Processing**

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

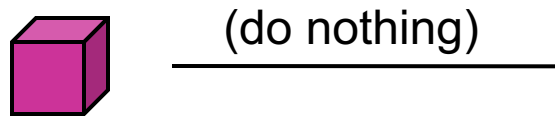
## **Lecture 2 (2019)**

**Richard Cleve**

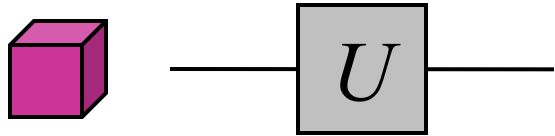
DC 2117 / QNC 3129

[cleve@uwaterloo.ca](mailto:cleve@uwaterloo.ca)

# 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:

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

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

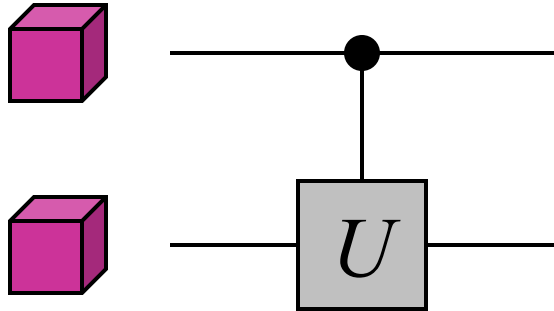
$$|1\rangle|0\rangle \rightarrow |1\rangle U|0\rangle$$

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

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- $U =$

Maps basis states as:

$$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$$

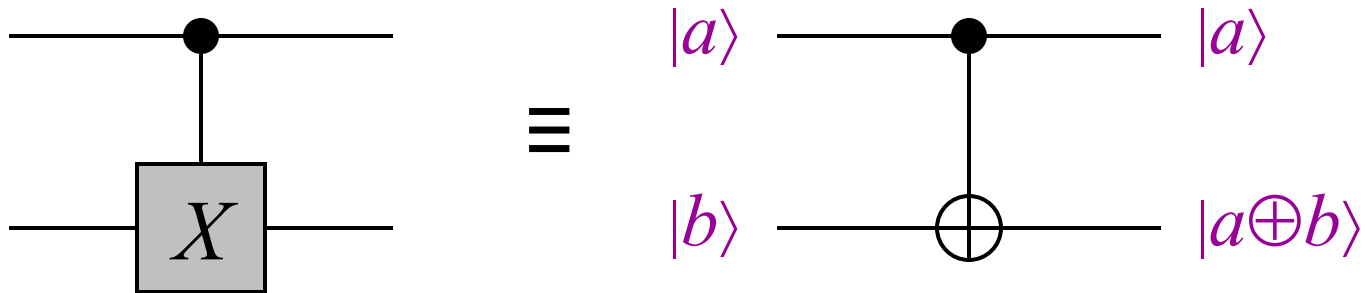
$$|0\rangle|1\rangle \rightarrow |0\rangle|1\rangle$$

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

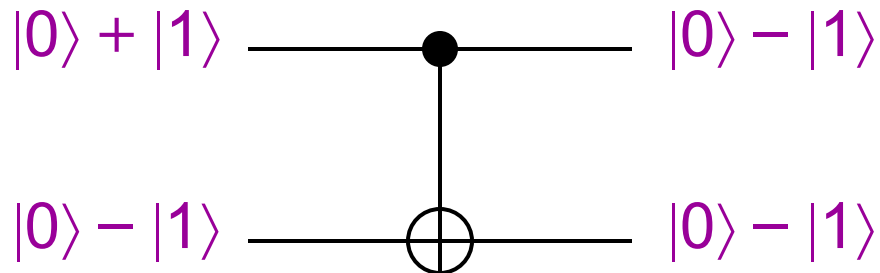
$$|1\rangle|1\rangle \rightarrow |1\rangle U|1\rangle$$

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

# Controlled-NOT (CNOT)



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





# “Famous” single-qubit gates

## Pauli

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

## Hadamard

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

## Phase

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

These generate the **Clifford group** (related to the symmetry group of the cube or octahedron)

A notable non-Clifford gate ( $T$  gate, a.k.a.  $\pi/8$  gate)

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/8} \end{pmatrix}$$

# Superdense coding

# How much classical information in $n$ qubits?

$2^n - 1$  complex numbers apparently needed to describe an arbitrary  $n$ -qubit pure quantum state:

$$\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \dots + \alpha_{111}|111\rangle$$

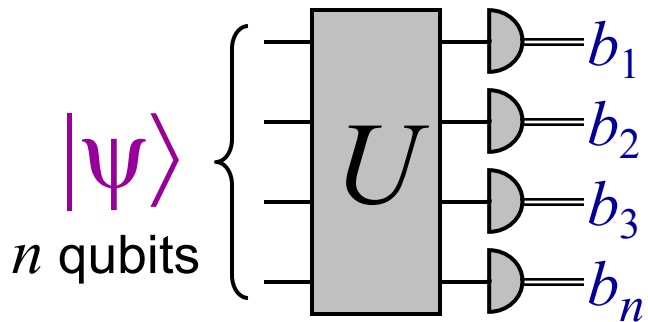
Does this mean that an exponential amount of classical information is somehow “stored” in  $n$  qubits?

**Not in an operational sense ...**

For example, Holevo’s Theorem (from 1973) implies: one cannot convey more than  $n$  classical bits of information in  $n$  qubits

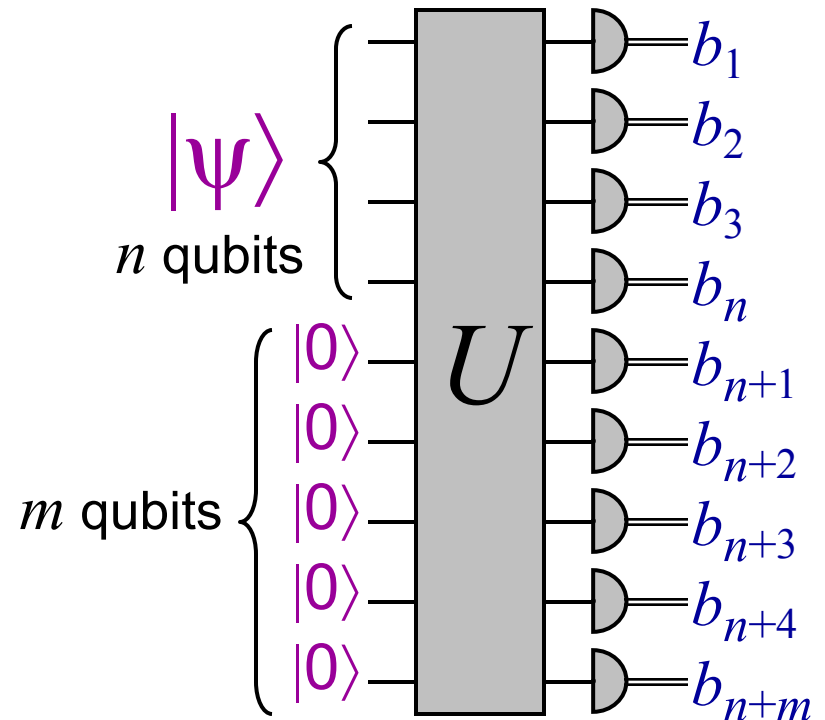
# Holevo's Theorem

Easy case:



$b_1 b_2 \dots b_n$  certainly cannot convey more than  $n$  bits!

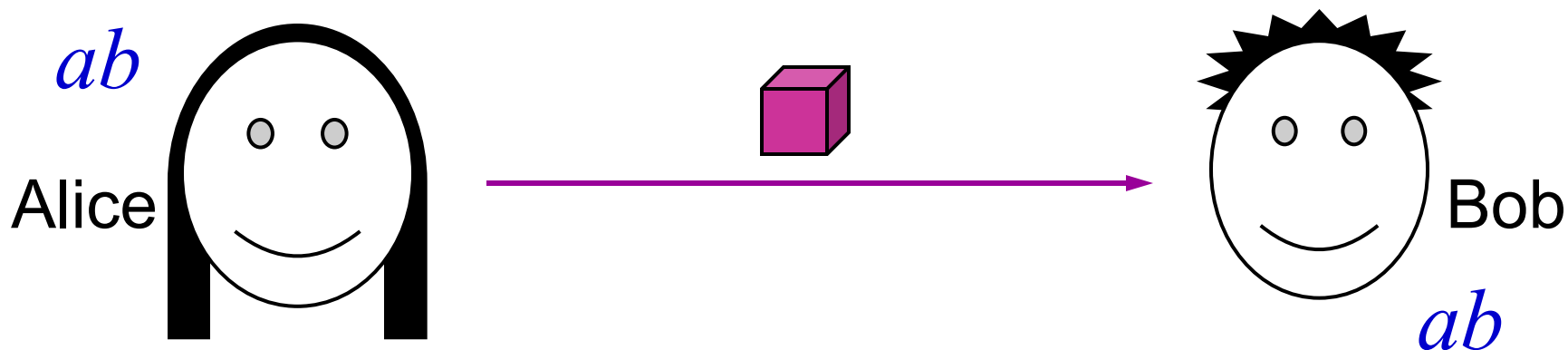
Hard case (the general case):



The difficult proof is beyond the scope of this course

# Superdense coding (prelude)

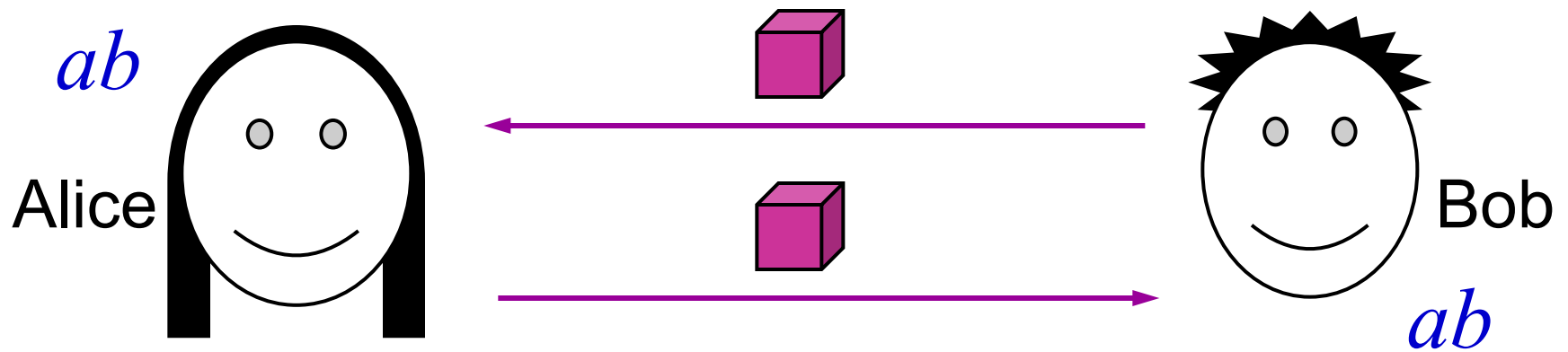
Suppose that Alice wants to convey **two** classical bits to Bob sending just **one** qubit



By Holevo's Theorem, this is **impossible**

# Superdense coding

In *superdense coding*, Bob is allowed to send a qubit to Alice first



How can this help?

# How superdense coding works

1. Bob creates the state  $|00\rangle + |11\rangle$  and sends the *first* qubit to Alice
2. Alice: if  $a = 1$  then apply  $X$  to qubit  
if  $b = 1$  then apply  $Z$  to qubit  
send the qubit back to Bob

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

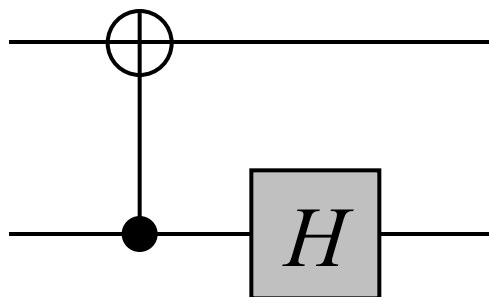
$ab$	state
00	$ 00\rangle +  11\rangle$
01	$ 00\rangle -  11\rangle$
10	$ 01\rangle +  10\rangle$
11	$ 01\rangle -  10\rangle$

} Bell basis

3. Bob measures the two qubits in the *Bell basis*

# Measurement in the Bell basis

Specifically, Bob applies



to his two qubits ...

and then measures them, yielding  $ab$

input	output
$ 00\rangle +  11\rangle$	$ 00\rangle$
$ 01\rangle +  10\rangle$	$ 01\rangle$
$ 00\rangle -  11\rangle$	$ 10\rangle$
$ 01\rangle -  10\rangle$	$- 11\rangle$

**This concludes superdense coding**



# Teleportation

# Recap

- **$n$ -qubit quantum state:**  $2^n$ -dimensional unit vector
- **Unitary op:**  $2^n \times 2^n$  linear operation  $U$  such that  $U^\dagger U = I$  (where  $U^\dagger$  denotes the conjugate transpose of  $U$ )

$U|0000\rangle =$  the 1<sup>st</sup> column of  $U$

$U|0001\rangle =$  the 2<sup>nd</sup> column of  $U$

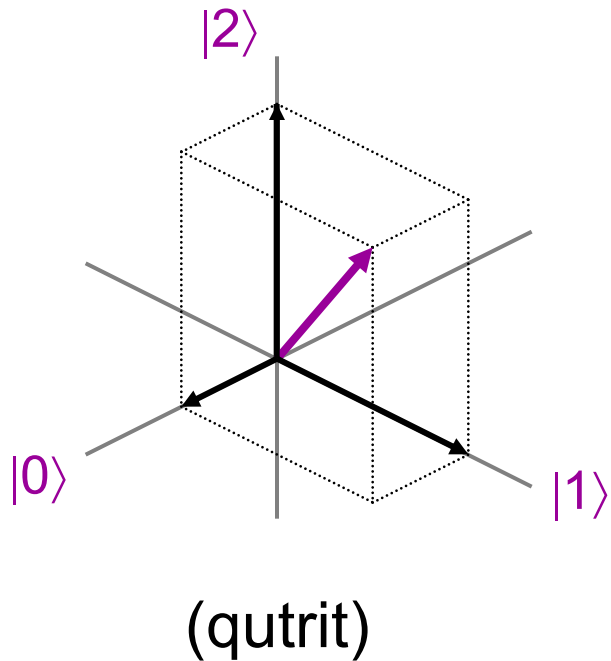
$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$

$U|1111\rangle =$  the  $(2^n)$ <sup>th</sup> column of  $U$

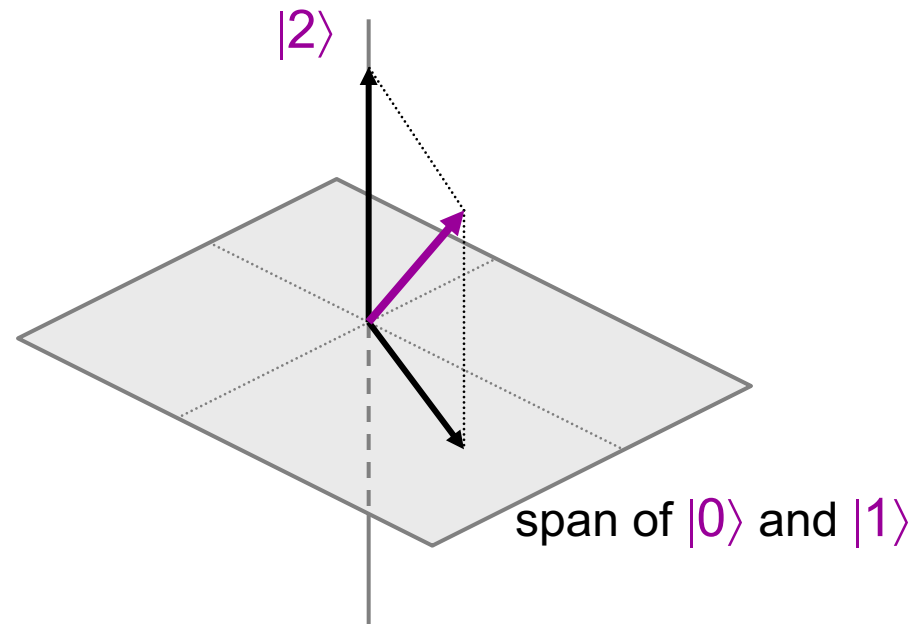
} the columns of  $U$   
are orthonormal

# Incomplete measurements (I)

Measurements up until now are with respect to orthogonal one-dimensional subspaces:



The orthogonal subspaces can have other dimensions:




# Incomplete measurements (II)

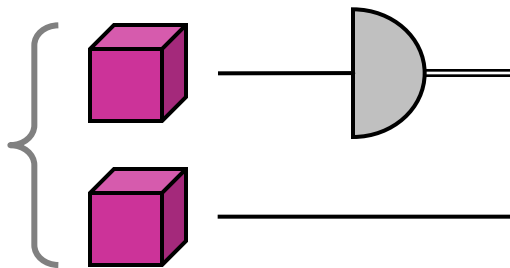
Such a measurement on  $\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle$

results in  $\left\{ \begin{array}{ll} \alpha_0 |0\rangle + \alpha_1 |1\rangle & \text{with prob } |\alpha_0|^2 + |\alpha_1|^2 \\ |2\rangle & \text{with prob } |\alpha_2|^2 \end{array} \right.$

(renormalized)



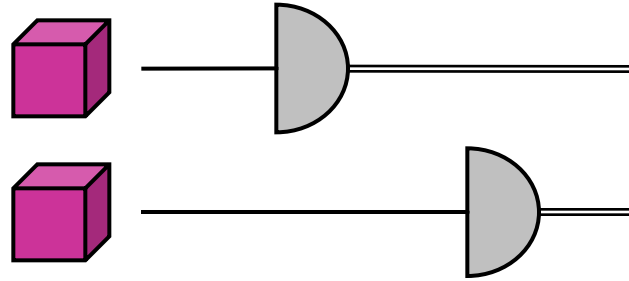
# Measuring the first qubit of a two-qubit system

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


**Defined** as the incomplete measurement with respect to the two dimensional subspaces:

- span of  $|00\rangle$  &  $|01\rangle$  (all states with first qubit 0), and
- span of  $|10\rangle$  &  $|11\rangle$  (all states with first qubit 1)


Result is 
$$\begin{cases} 0, & \alpha_{00}|00\rangle + \alpha_{01}|01\rangle & \text{with prob } |\alpha_{00}|^2 + |\alpha_{01}|^2 \\ 1, & \alpha_{10}|10\rangle + \alpha_{11}|11\rangle & \text{with prob } |\alpha_{10}|^2 + |\alpha_{11}|^2 \end{cases}$$

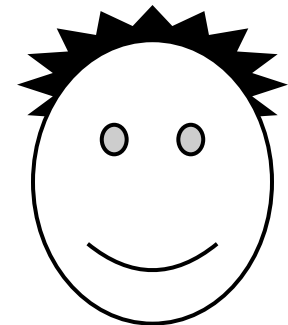
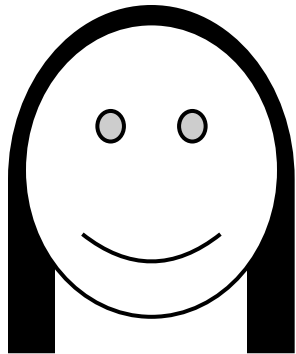


**Easy exercise:** show that measuring the first qubit and *then* measuring the second qubit gives the same result as measuring both qubits at once

# Teleportation (prelude)

Suppose Alice wishes to convey a qubit to Bob by sending just classical bits

  $\alpha|0\rangle + \beta|1\rangle$



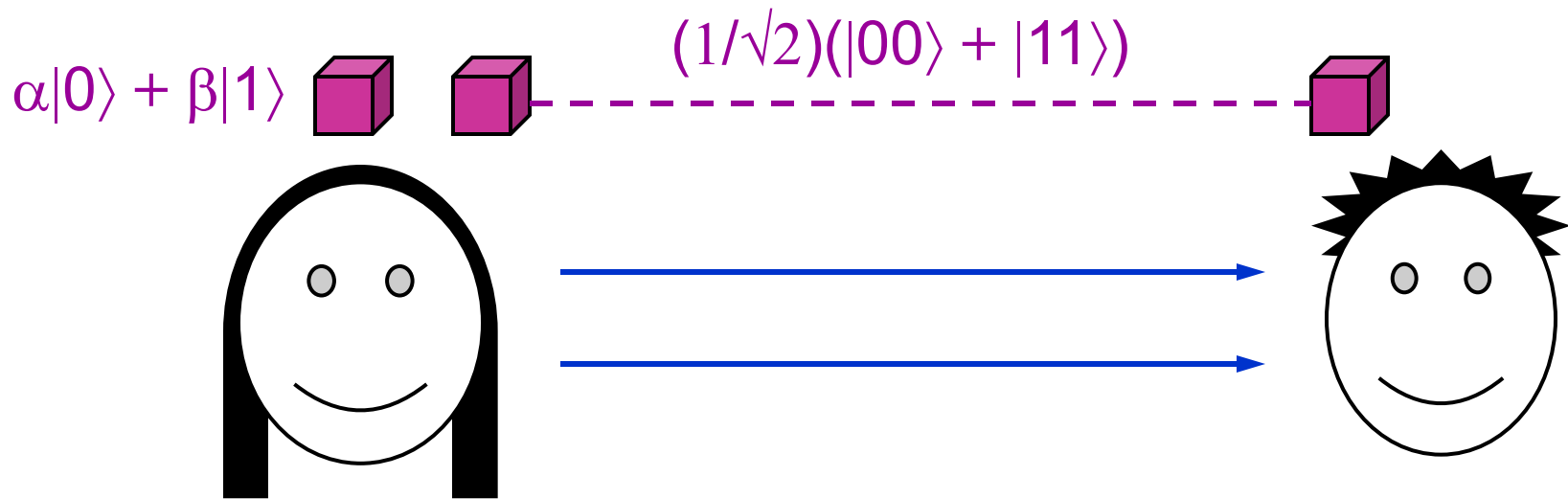
  $\alpha|0\rangle + \beta|1\rangle$

If Alice *knows*  $\alpha$  and  $\beta$ , she can send approximations of them—but this still requires infinitely many bits for perfect precision

Moreover, if Alice does *not* know  $\alpha$  or  $\beta$ , she can at best acquire *one bit* about them by a measurement

# Teleportation scenario

In teleportation, Alice and Bob also start with a Bell state



and Alice can send two classical bits to Bob

Note that the initial state of the three qubit system is:

$$(1/\sqrt{2})(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$$
$$= (1/\sqrt{2})(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$



# How teleportation works



**Initial state:**  $(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$  (omitting the  $1/\sqrt{2}$  factor)

$$= \alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle$$

$$= \frac{1}{2}(|00\rangle + |11\rangle)(\alpha|0\rangle + \beta|1\rangle)$$

$$+ \frac{1}{2}(|01\rangle + |10\rangle)(\alpha|1\rangle + \beta|0\rangle)$$

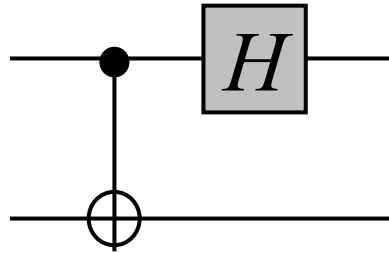
$$+ \frac{1}{2}(|00\rangle - |11\rangle)(\alpha|0\rangle - \beta|1\rangle)$$

$$+ \frac{1}{2}(|01\rangle - |10\rangle)(\alpha|1\rangle - \beta|0\rangle)$$

**Protocol:** Alice measures her two qubits *in the Bell basis* and sends the result to Bob (who then “corrects” his state)<sub>41</sub>

# What Alice does specifically

Alice applies



to her two qubits, yielding:

$$\left\{ \begin{array}{l} \frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) \\ + \frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ + \frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle) \\ + \frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle) \end{array} \right. \begin{array}{c} \text{AND} \\ \text{AND} \end{array} \left\{ \begin{array}{l} (00, \alpha|0\rangle + \beta|1\rangle) \text{ with prob. } \frac{1}{4} \\ (01, \alpha|1\rangle + \beta|0\rangle) \text{ with prob. } \frac{1}{4} \\ (10, \alpha|0\rangle - \beta|1\rangle) \text{ with prob. } \frac{1}{4} \\ (11, \alpha|1\rangle - \beta|0\rangle) \text{ with prob. } \frac{1}{4} \end{array} \right.$$

Then Alice sends her two classical bits to Bob, who then adjusts his qubit to be  $\alpha|0\rangle + \beta|1\rangle$  whatever case occurs

# Bob's adjustment procedure

Bob receives two classical bits  $a$ ,  $b$  from Alice, and:

if  $b = 1$  he applies  $X$  to qubit

if  $a = 1$  he applies  $Z$  to qubit

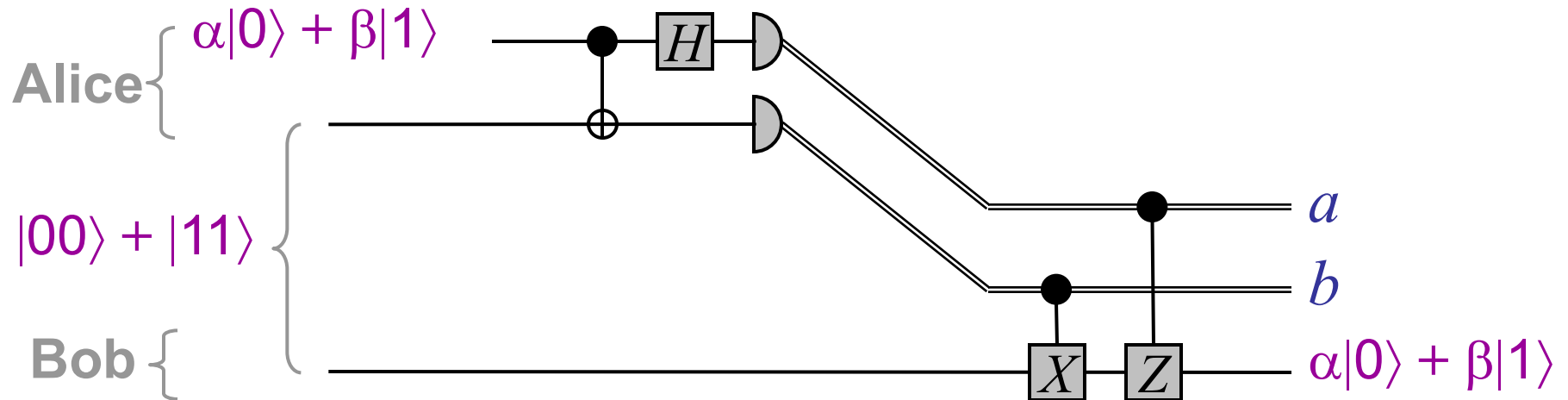
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

yielding:

$$\left\{ \begin{array}{l} 00, \quad \alpha|0\rangle + \beta|1\rangle \\ 01, \quad X(\alpha|1\rangle + \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle \\ 10, \quad Z(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle \\ 11, \quad ZX(\alpha|1\rangle - \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle \end{array} \right.$$

Note that Bob acquires the correct state in each case

# Summary of teleportation



**Quantum circuit exercise:** try to work through the details of the analysis of this teleportation protocol

# **Introduction to Quantum Information Processing**

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

## **Lecture 3 (2019)**

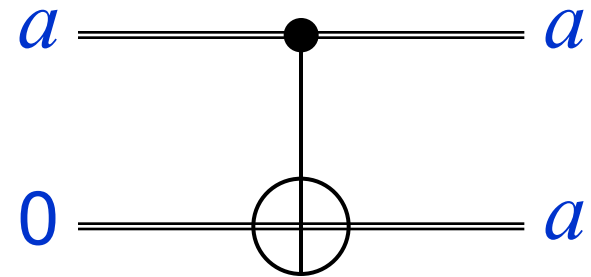
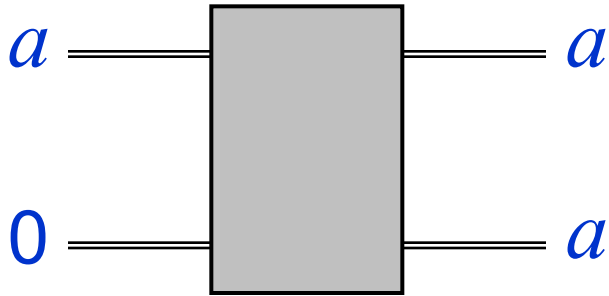
**Richard Cleve**

DC 2117 / QNC 3129

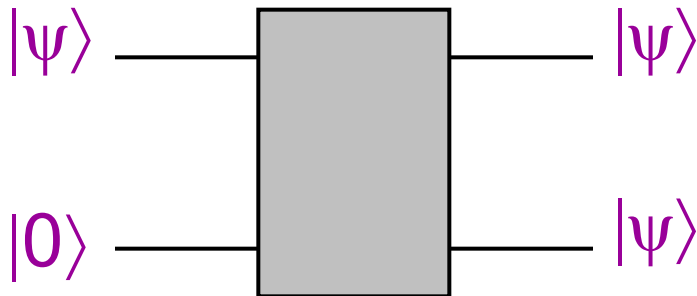
[cleve@uwaterloo.ca](mailto:cleve@uwaterloo.ca)

# No-cloning theorem

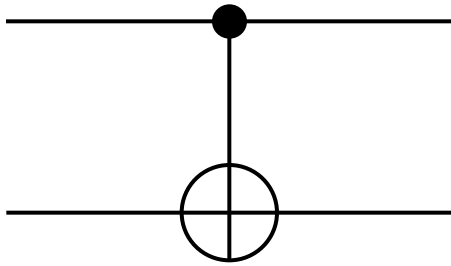
# ***Classical* information can be copied**



**What about quantum information?**



## Candidate:



works fine for  $|\psi\rangle = |0\rangle$  and  $|\psi\rangle = |1\rangle$

... but it fails for  $|\psi\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$  ...

... where it yields output  $(1/\sqrt{2})(|00\rangle + |11\rangle)$

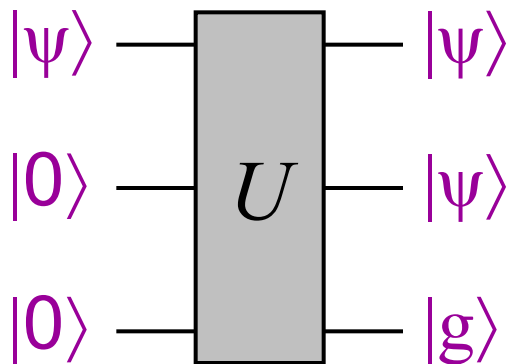
instead of  $|\psi\rangle|\psi\rangle = (1/4)(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$



# No-cloning theorem

**Theorem:** there is *no* valid quantum operation that maps an arbitrary state  $|\psi\rangle$  to  $|\psi\rangle|\psi\rangle$

**Proof:**



Let  $|\psi\rangle$  and  $|\psi'\rangle$  be two input states, yielding outputs  $|\psi\rangle|\psi\rangle|g\rangle$  and  $|\psi'\rangle|\psi'\rangle|g'\rangle$  respectively

Since  $U$  preserves inner products:

$$\langle\psi|\psi'\rangle = \langle\psi|\psi'\rangle\langle\psi|\psi'\rangle\langle g|g'\rangle \text{ so}$$

$$\langle\psi|\psi'\rangle(1 - \langle\psi|\psi'\rangle\langle g|g'\rangle) = 0 \text{ so}$$

$$|\langle\psi|\psi'\rangle| = 0 \text{ or } 1$$

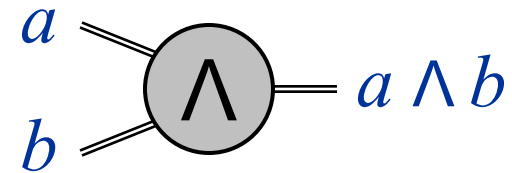
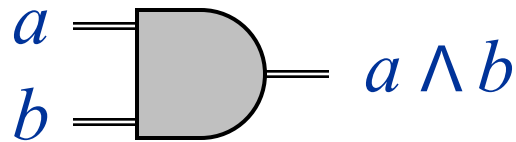
# Classical computations as circuits

# Classical (boolean logic) gates

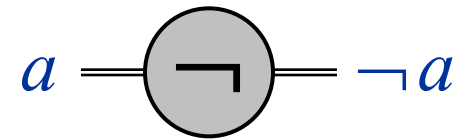
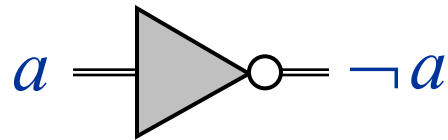
“old” notation

“new” notation

**AND** gate



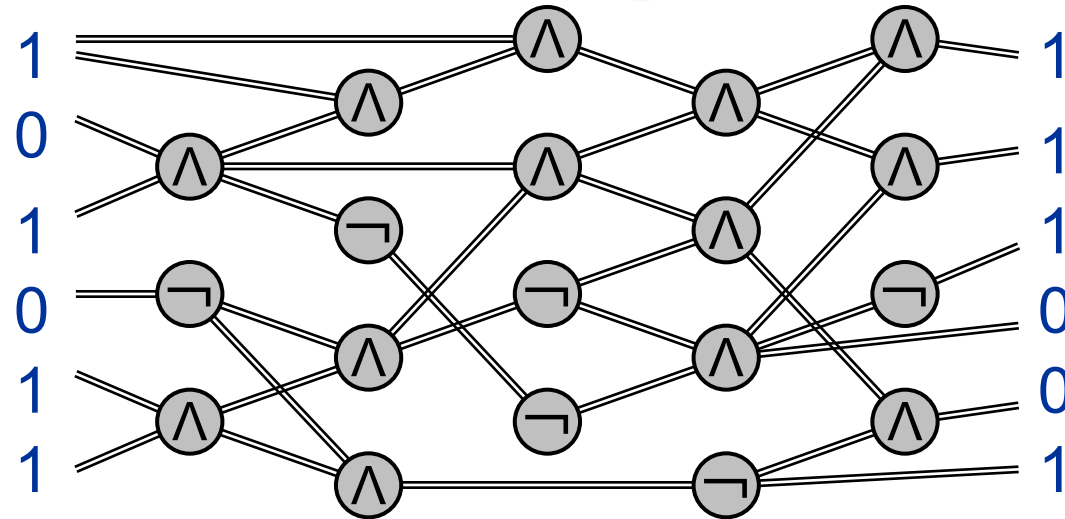
**NOT** gate



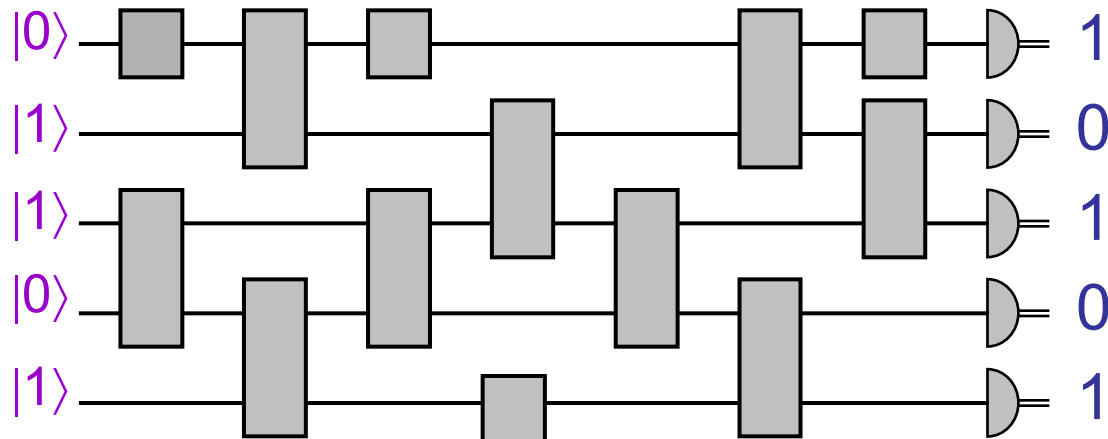
**Note:** an **OR** gate can be simulated by one **AND** gate and three **NOT** gates (since  $a \vee b = \neg(\neg a \wedge \neg b)$ )

# Models of computation

Classical circuits:



Quantum circuits:



# Multiplication problem

**Input:** two  $n$ -bit numbers (e.g. 101 and 111)

**Output:** their product (e.g. 100011)

- “Grade school” algorithm costs  $O(n^2)$  [scales up *polynomially*]
- Best currently-known **classical** algorithm costs  $O(n \log n)$
- Best currently-known **quantum** method: same

# Factoring problem

**Input:** an  $n$ -bit number (e.g. 100011)

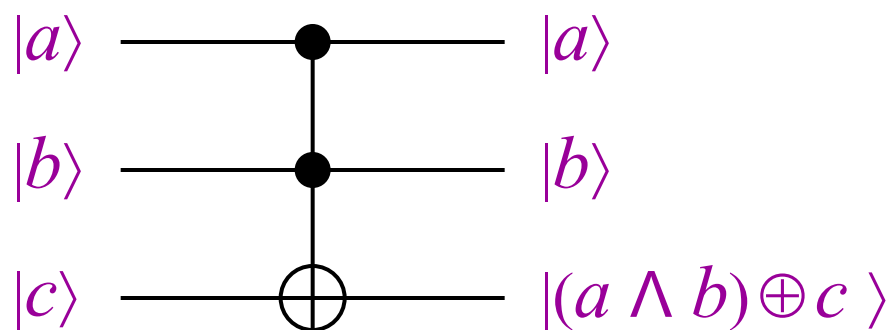
**Output:** their product (e.g. 101, 111)

- Trial division costs  $\approx 2^{n/2}$
- Best currently-known **classical** algorithm costs  $\approx 2^{n^{1/3}}$   
[to be more precise  $2^{O(n^{1/3}\log^{2/3}n)}$  and this scaling is *not* polynomial]
- The presumed hardness of factoring is the basis of the security of many cryptosystems (e.g. RSA)
- Shors **quantum** algorithm costs  $O(n^2 \log n)$
- Implementation would break RSA — and many other public-key cryptosystems

# Simulating *classical* circuits with *quantum* circuits

# Toffoli gate

(Sometimes called a “controlled-controlled-NOT” gate)



In the computational basis, it negates the third qubit iff the first two qubits are both  $|1\rangle$

Matrix representation:

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

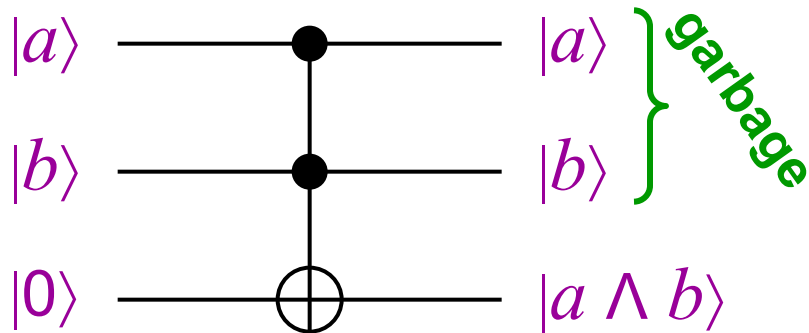


# Quantum simulation of classical

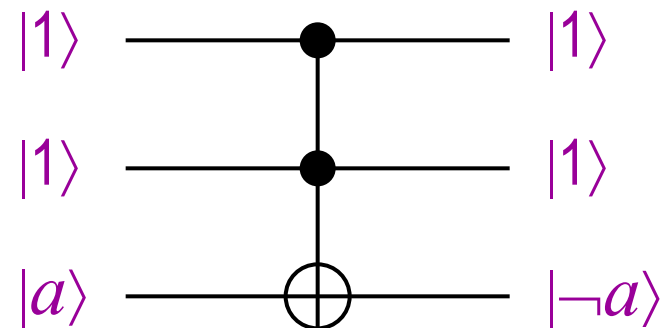
**Theorem:** a classical circuit of size  $s$  can be simulated by a quantum circuit of size  $O(s)$

**Idea:** using Toffoli gates, one can simulate:

**AND** gates



**NOT** gates

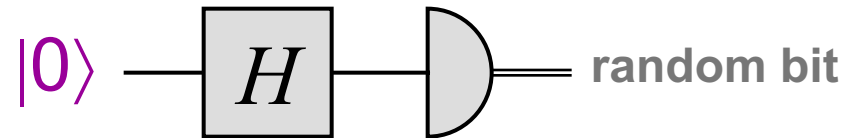


**This garbage will have to be reckoned with later on ...**

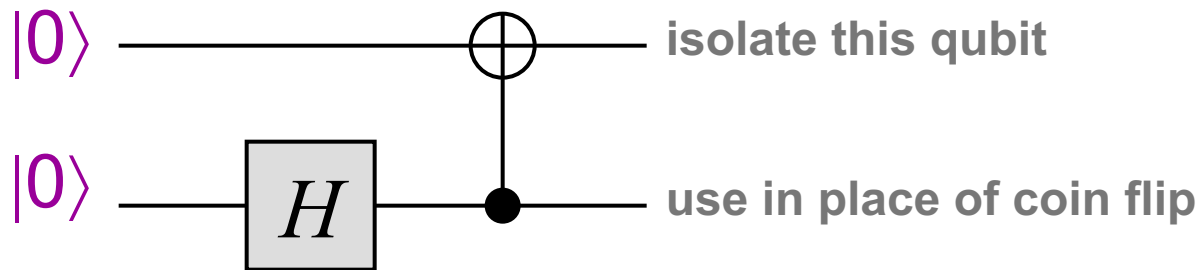
# Simulating probabilistic algorithms

Since quantum gates can simulate **AND** and **NOT**, the outstanding issue is how to simulate randomness

To simulate “coin flips”, one can use the circuit:



It can also be done without intermediate measurements:



**Exercise:** prove that this works

# Simulating *quantum* circuits with *classical* circuits

# Classical simulation of quantum

**Theorem:** a quantum circuit of size  $s$  acting on  $n$  qubits can be simulated by a classical circuit of size  $O(sn^2 2^n)$

**Idea:** to simulate an  $n$ -qubit state, use an array of size  $2^n$  containing values of all  $2^n$  amplitudes within precision  $2^{-n}$

$\alpha_{000}$
$\alpha_{001}$
$\alpha_{010}$
$\alpha_{011}$
:
$\alpha_{111}$

Can adjust this state vector whenever a unitary operation is performed at cost  $O(n^2 2^n)$

From the final amplitudes, can determine how to set each output bit

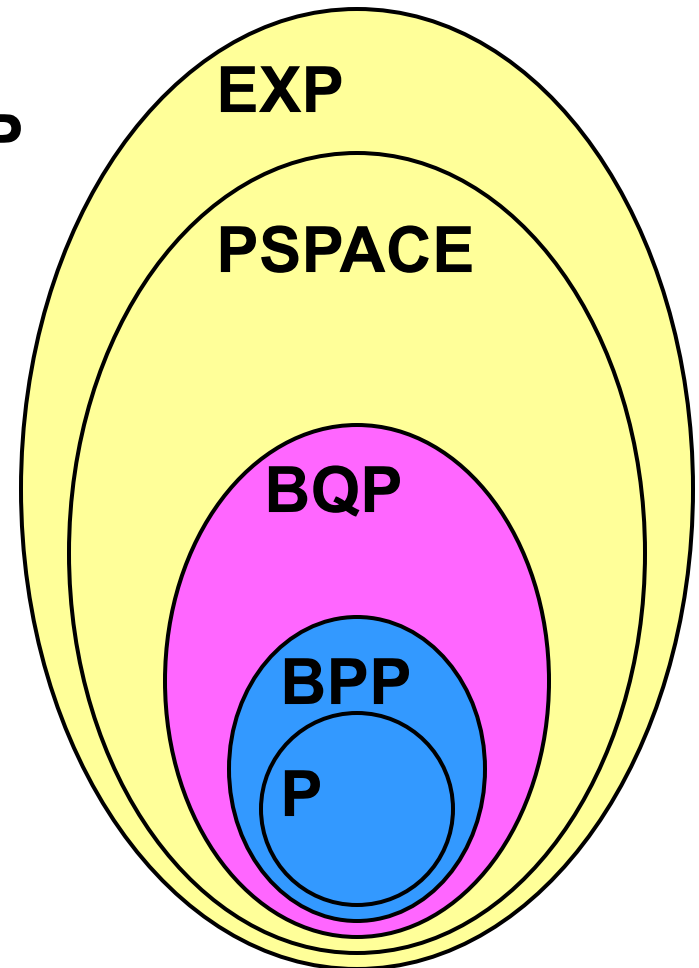
**Exercise:** show how to do the simulation using only a polynomial amount of **space** (memory)

# Some *complexity* classes

- **P (polynomial time):** the problems solved by  $O(n^c)$ -size classical circuits [technically, we restrict to decision problems and to “uniform circuit families”]
- **BPP (bounded error probabilistic polynomial time):** the problems solved by  $O(n^c)$ -size *probabilistic* circuits that err with probability  $\leq 1/4$
- **BQP (bounded error quantum polynomial time):** the problems solved by  $O(n^c)$ -size *quantum* circuits that err with probability  $\leq 1/4$
- **EXP (exponential time):** the problems solved by  $O(2^{n^c})$ -size circuits

# Summary of basic containments

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE \subseteq EXP$$



This picture will be fleshed out more later on