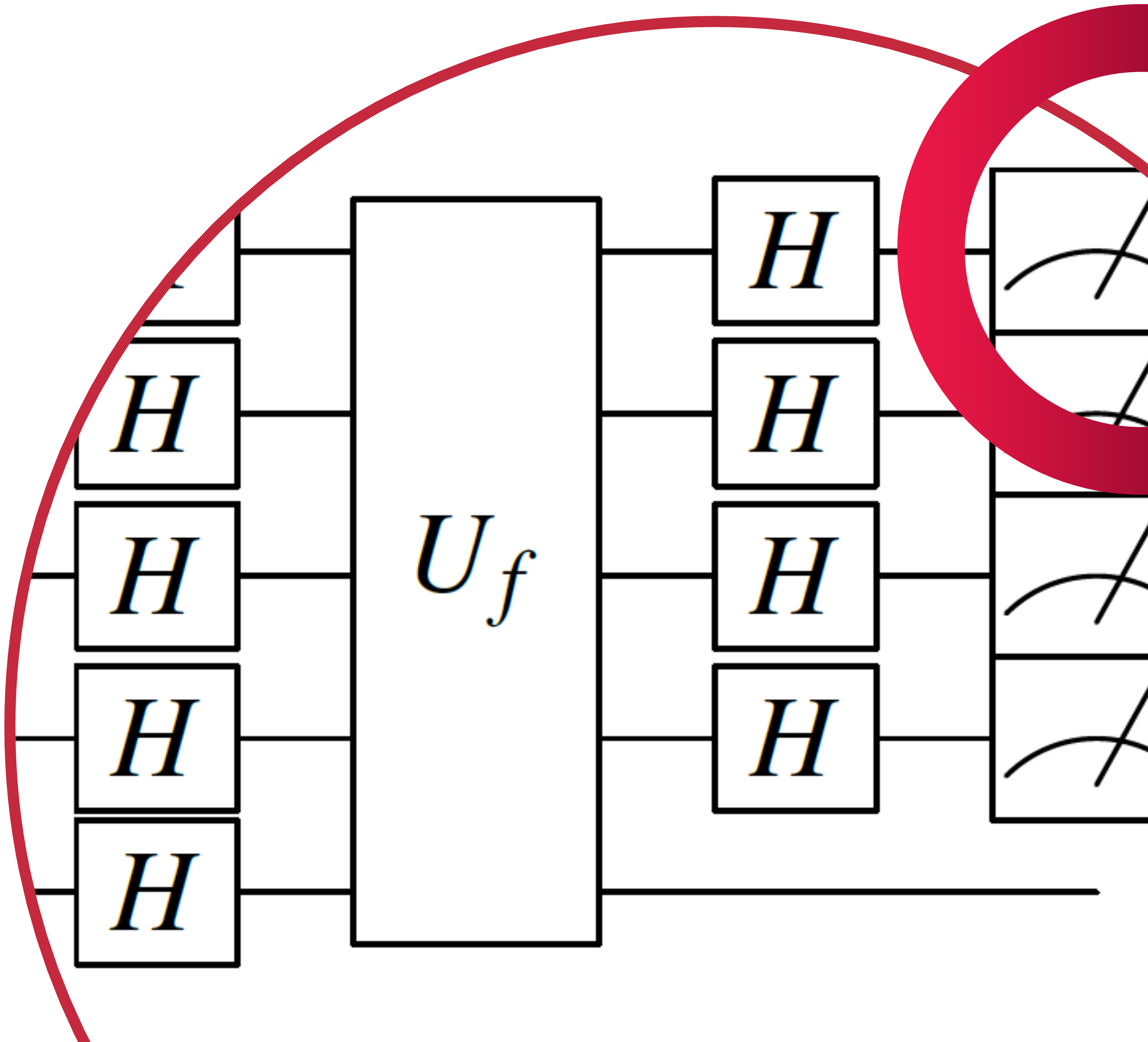
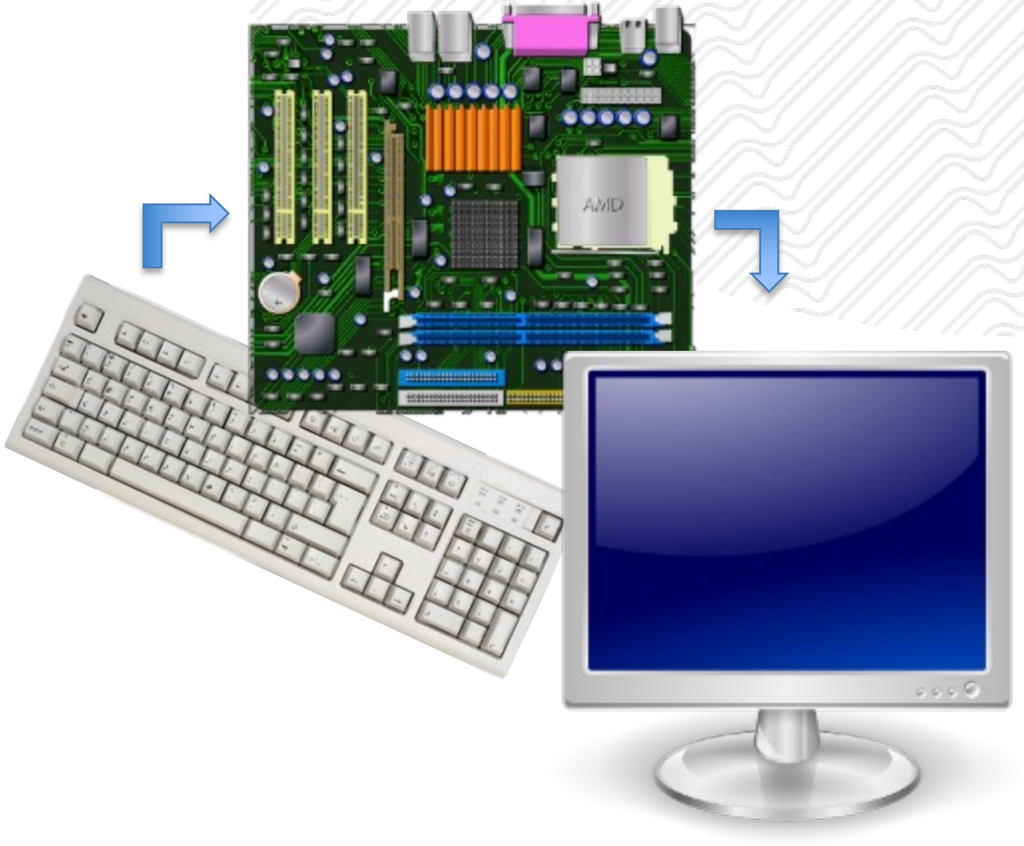
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

A Beginner's Guide to Quantum Computing

Sarah Li & John Donohue

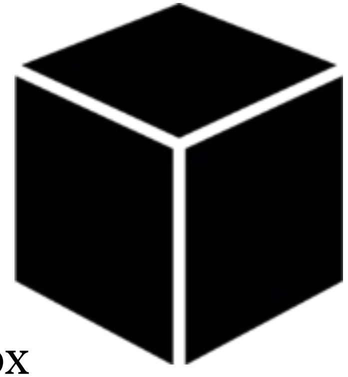


What's a Computer?



A computer is an
information processor

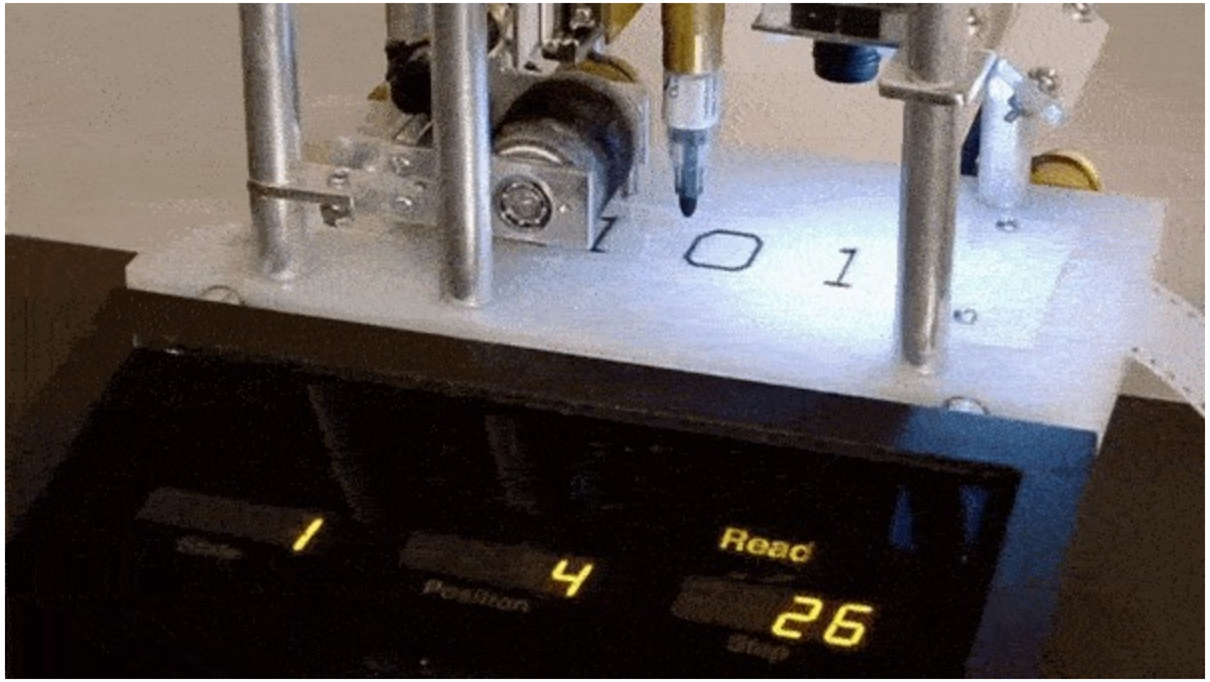
11011110
00110001
01101010
Input



Black box
Obeys certain logical rules

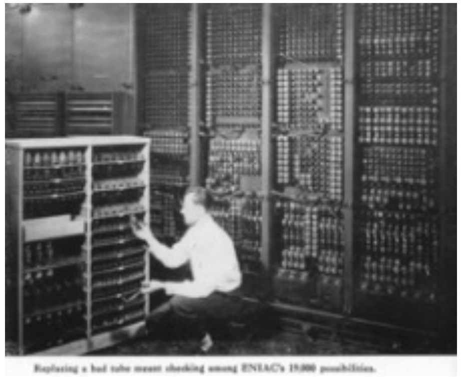
Output
10000111
00001010
00110101

What's a Computer?



Credit: Mike Davey http://aturingmachine.com/

What's a Computer?



Despite their different appearances,
all of these computers
follow the exact same rules.

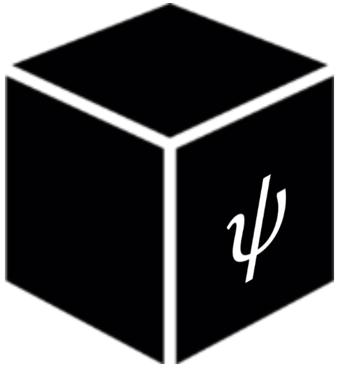
What's a *Quantum* Computer?

We've already seen that we can encode and process information in a quantum system

11011110
00110001
01101010

Input

A quantum computer is a *quantum information processor*



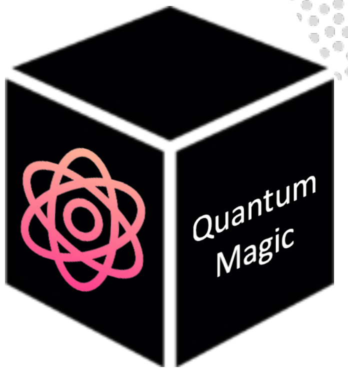
Output

10000111
00001010
00110101

Black box obeys different rules, such as unitary evolution, but can take advantage of superposition and entanglement

Classical vs. Quantum Computing

- Uses bits as input and output
- Gives one answer per run
- Can fake randomness
- Can observe the computation partway through
- Can only measure the bits in one way



- Uses bits as input and output
- Gives one answer per run
- Is fundamentally uncertain
- Observing the computation partway disturbs quantum states and ruins the process
- Can measure qubits in infinite ways

Early Quantum Computing

- Preliminaries
- Quantum circuit notation
- Oracle problems
- The Deutsch-Josza Problem
- Overview of Quantum Computing Implementations

Preliminaries

Quantum States

A state describes properties of a system

Classical

A quantum state describes properties of a quantum system

Quantum

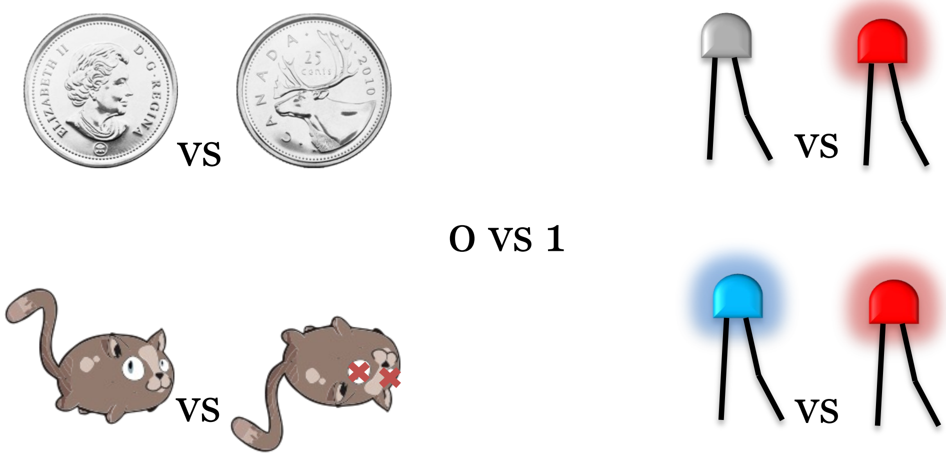
Specifics Tomorrow!

Energy State Electron Spin Circuit QED Photon Polarization

Mutually Exclusive States

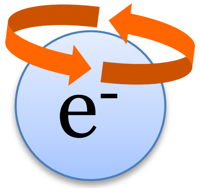
- Two states are mutually exclusive if they are:
  - Distinguishable and impossible to confuse
  - Cannot both occur at the same time

Classical

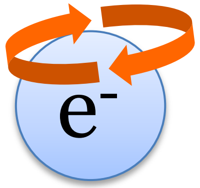


Quantum

For example, consider electron spin



Can only take one of two values (⟳ or ⟲)



Which of the following are **NOT** mutually exclusive?

A. Heads *or* Tails on a coin

B. Wearing Red Socks *or* Wearing a Blue Shirt

Can do both at the same time

C. Being in Toronto *or* Being in Montreal

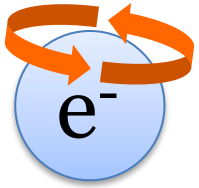
D. Having a Ball *or* Not Having a Ball

E. All of the above are mutually exclusive

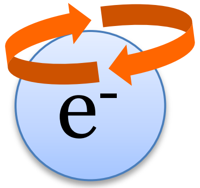
States as Vectors

1) Quantum states are described by **unit vectors** in complex, potentially **high-dimensional Hilbert spaces**.

Consider electron spin



Can only take one of two values



We'll represent them as
a pair of orthogonal unit vectors

$$v_{\circlearrowleft} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad v_{\circlearrowright} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

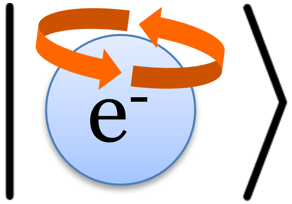
Why orthogonal?
They're impossible to confuse!
A ↻ electron has no ↺ component,
just like an x-vector has no y-component

States as Kets

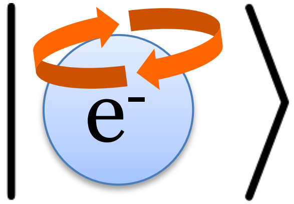
We call any two-dimensional quantum state a "qubit"

Qubit = Quantum Bit

We use a "ket" to denote a quantum state vector



$:= |0\rangle$



$:= |1\rangle$

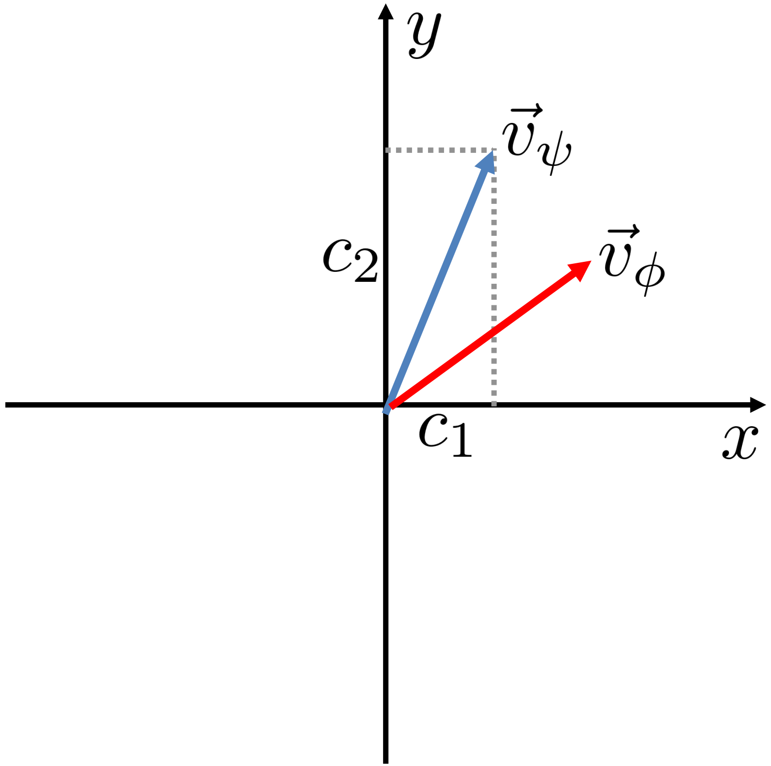
$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

We'll see this for numerous physical systems,
but the end result is always the same:
<u>Linear algebra is the rulebook for quantum mechanics</u>

States as Kets

$$|\psi\rangle = \vec{v}_\psi = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

A "ket" is a column vector



For now,
think of each component as how alike the state is to each of the mutually exclusive options.

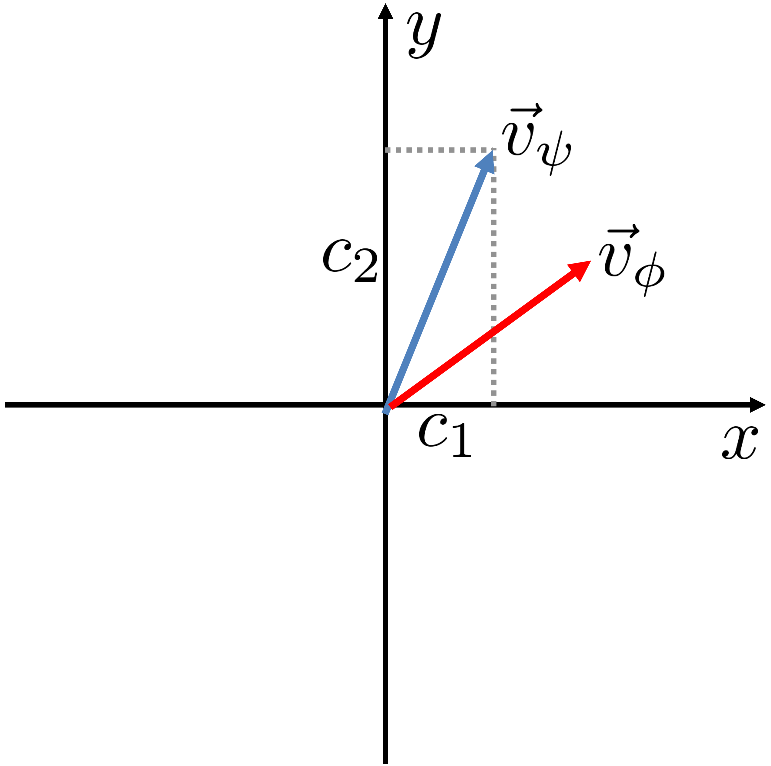
$$|\psi\rangle = \begin{bmatrix} 0.97 \\ 0.22 \end{bmatrix} \text{ is more like } |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|\psi\rangle = \begin{bmatrix} 0.26 \\ 0.96 \end{bmatrix} \text{ is more like } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Bra-Ket Notation

$$|\psi\rangle = \vec{v}_\psi = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

A "ket" is a column vector



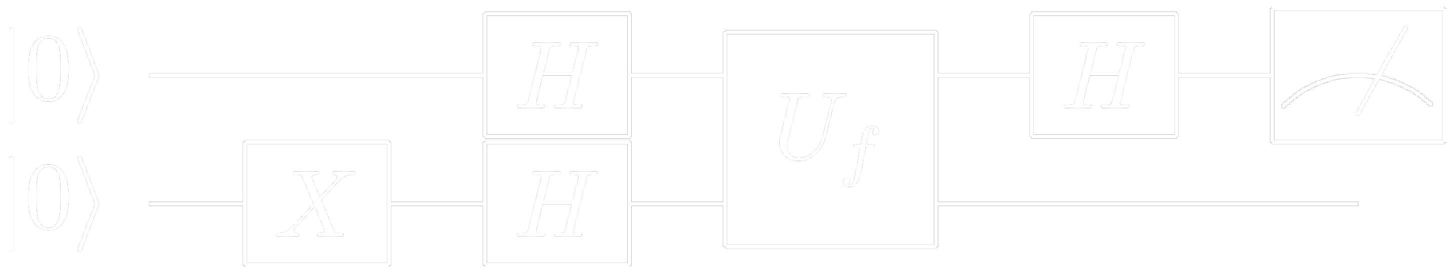
$$\langle\psi| = \vec{v}_\psi^\dagger = \begin{bmatrix} \bar{c}_1 & \bar{c}_2 \end{bmatrix}$$

A "bra" is it's conjugate transpose
(row vector)

$$\langle\phi|\psi\rangle = \vec{v}_\phi^\dagger \vec{v}_\psi = \vec{v}_\phi \cdot \vec{v}_\psi$$

A bra and a ket together
provides the inner product
or overlap of the two states

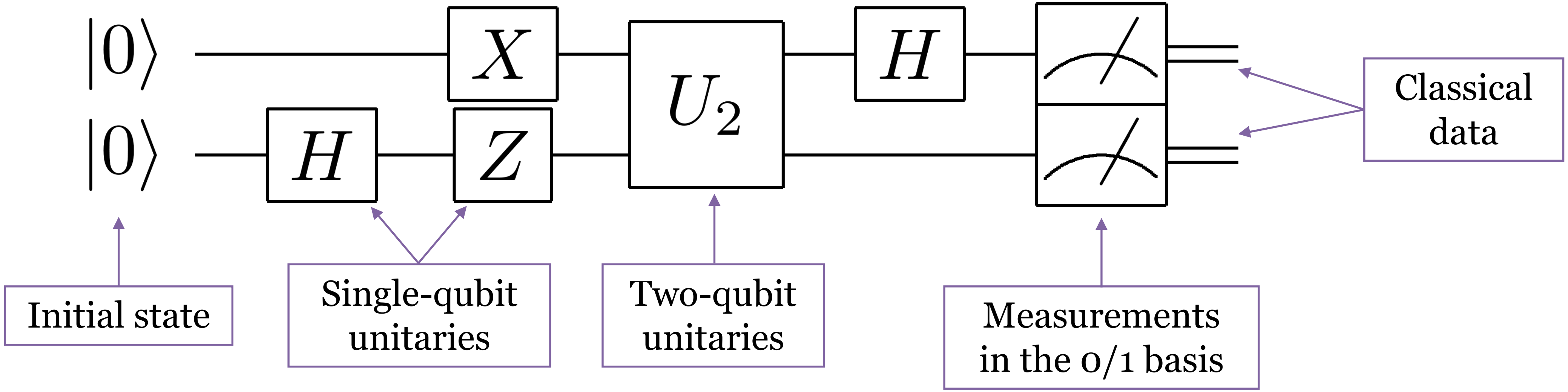
Just like the inner product
tells us how alike two vectors are,
it will tell us how alike two quantum states are



Quantum Circuits

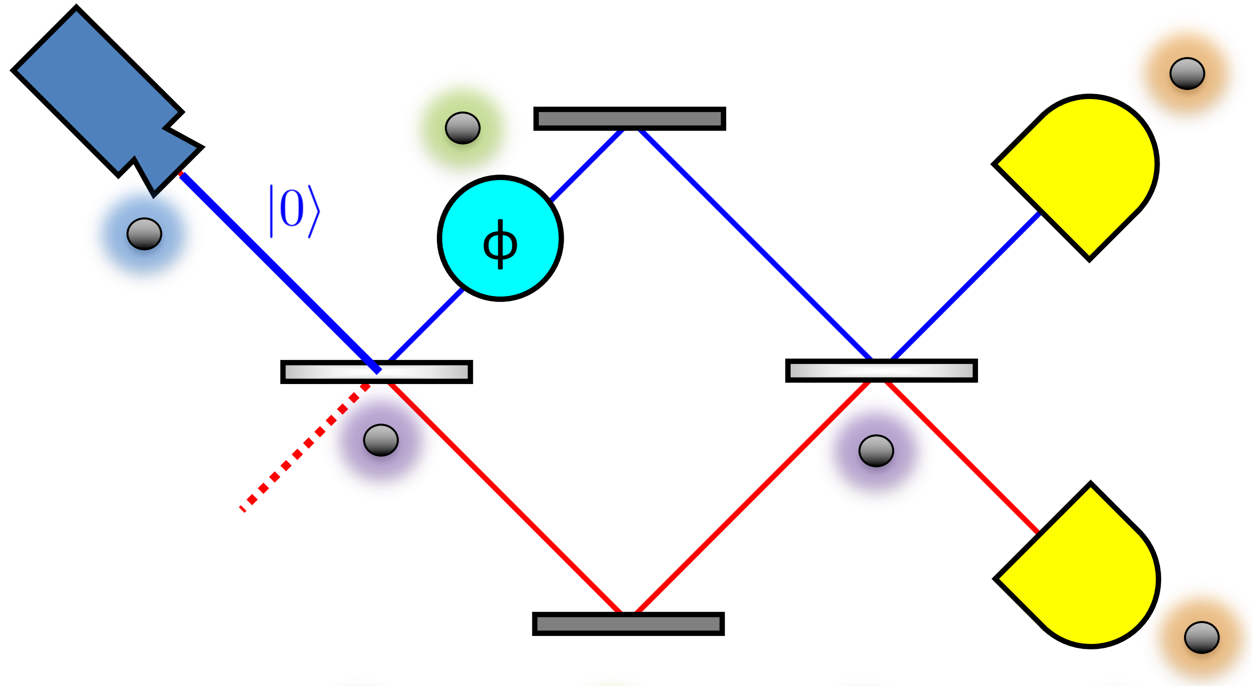
Quantum Circuit Model

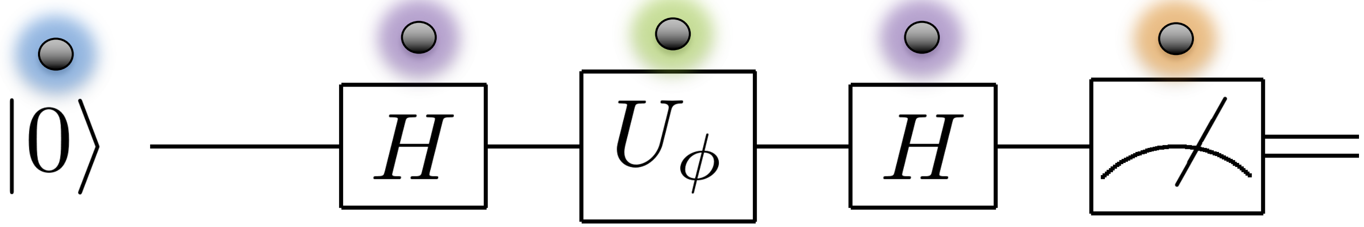
When we talk about quantum computing, we often talk about it in the *circuit representation*.



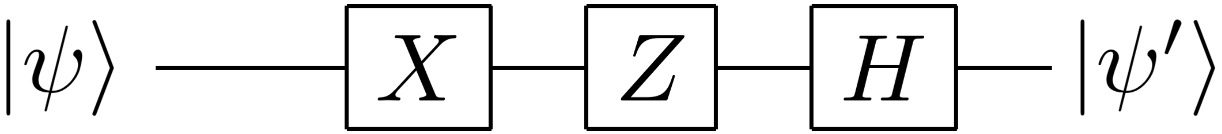
Quantum Circuit Model

Let's write the Mach-Zehnder in the circuit model…





What is $|\psi'\rangle$?



A. $ZHX|\psi\rangle$

B. $XZH|\psi\rangle$

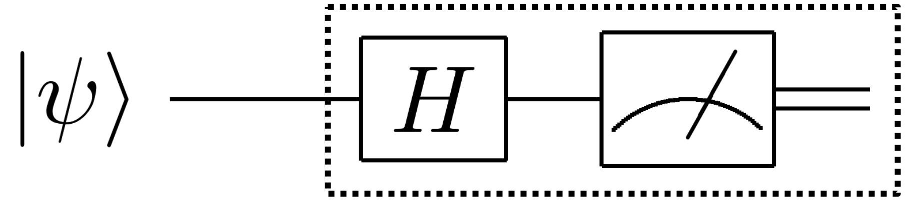
C. $HZX|\psi\rangle$

X first, then Z, then H

D. $ZXH|\psi\rangle$

E. None of the above

What does this circuit do?



A. Measure $|\psi\rangle$ in the 0/1 basis

B. Measure $|\psi\rangle$ in the +/- basis

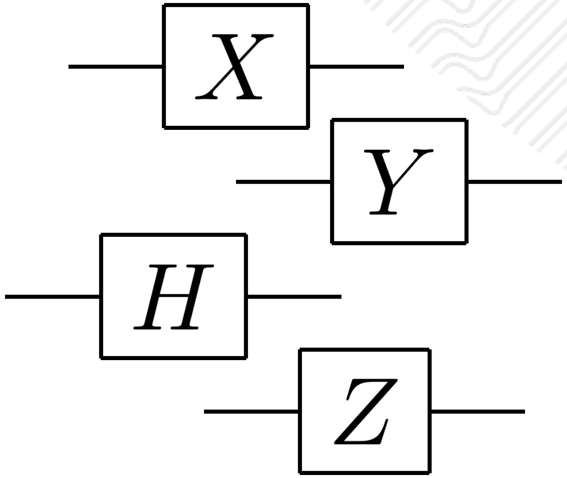
Recall : $H = |0\rangle\langle+| + |1\rangle\langle-|$

C. Transform $|0\rangle$ to $|\psi\rangle$

D. Make a copy of $|\psi\rangle$

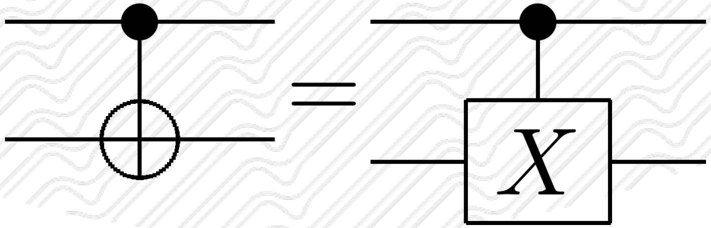
E. None of the above

Important Gates



Our familiar crew of single-qubit unitaries

The c-NOT
(Controlled-NOT)



$$U_{\text{cNOT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$U_{\text{cNOT}}|00\rangle = |00\rangle$$

$$U_{\text{cNOT}}|01\rangle = |01\rangle$$

$$U_{\text{cNOT}}|10\rangle = |11\rangle$$

$$U_{\text{cNOT}}|11\rangle = |10\rangle$$

The cNOT flips the second qubit depending on the state of the first

$$U_{\text{cNOT}} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

$$U_{\text{cNOT}} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$$

What is the following state?

$$U_{\text{cNOT}}\left(|+\rangle \otimes |0\rangle\right)$$

A. $\frac{1}{\sqrt{2}}\left(|00\rangle + |01\rangle\right)$

B. $\frac{1}{\sqrt{2}}\left(|01\rangle + |11\rangle\right)$

C. $\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$

The cNOT is an entangling gate

D. $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

Recall:
$$U_{\text{cNOT}}|00\rangle = |00\rangle$$
$$U_{\text{cNOT}}|01\rangle = |01\rangle$$
$$U_{\text{cNOT}}|10\rangle = |11\rangle$$
$$U_{\text{cNOT}}|11\rangle = |10\rangle$$

$$U_{\text{cNOT}}\left(|+\rangle \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}\left(U_{\text{cNOT}}|00\rangle + U_{\text{cNOT}}|10\rangle\right)$$

Question Break

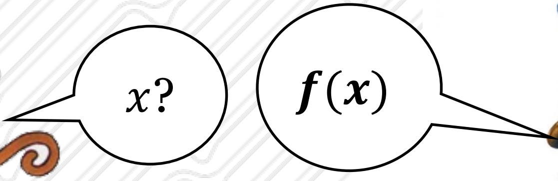
Early Quantum Computing

- Oracle problems
- The Deutsch-Josza Problem
- Overview of Quantum Computing Implementations

The Deutsch-Josza Problem

The made-up problem that started it all

Oracle Problems



<u>Phone Books</u>
Give them a name,
they give you a phone number

<u>Abstract Oracle</u>
Give an input,
get an output

But what if we want other kinds of information?
e.g. How many phone numbers have the 519 area code?
Is there an efficient way to get that out of the oracle?

Collective property
of the possible outputs,
not one specific output

The Deutsch-Josza Problem

You are given a binary function $f(x)$

There are two possible inputs (0 or 1)

There are two possible outputs (0 or 1)

Your mission: Determine if $f(x)$ is *constant* or *balanced*

There are four possible functions:

x	$f_1(x)$
0	0
1	0

Constant

x	$f_2(x)$
0	1
1	0

Balanced

x	$f_3(x)$
0	0
1	1

Balanced

x	$f_4(x)$
0	1
1	1

Constant

The Deutsch-Josza Problem

The Deutsch-Josza Problem

What is the minimum number of queries you'd need to ask the oracle to learn if the function is constant or balanced?

A. Zero
B. One
C. Two
D. Three
E. Four

x	$f_1(x)$
0	0
1	0

Constant

x	$f_2(x)$
0	1
1	0

Balanced

x	$f_3(x)$
0	0
1	1

Balanced

x	$f_4(x)$
0	1
1	1

Constant

0?

$f(0) = 1$

Still no information on whether it is constant or balanced

After two queries, I can tell you which function it is, which is more information than we need!

Question Break

The Quantum Deutsch-Josza Solution

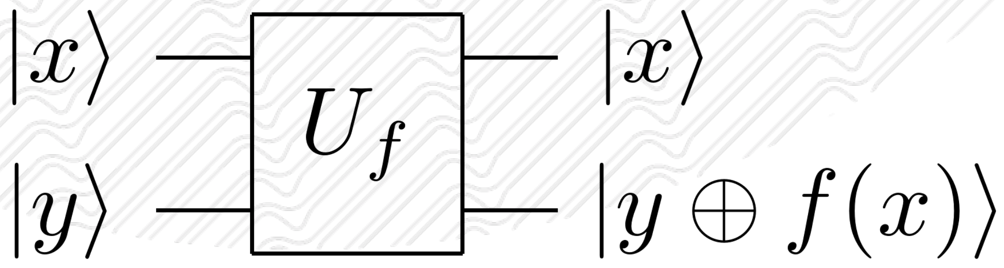
Play that one again DJ

The Quantum Oracle

Let’s say we’re able to ask for the oracle as a quantum gate:

Two-qubit
binary input

$$x = 0 \quad or \quad 1$$
$$y = 0 \quad or \quad 1$$



Control Qubit

Target Qubit

We have the two-qubit gate U_f
which has the function $f(x)$
programmed into it as:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

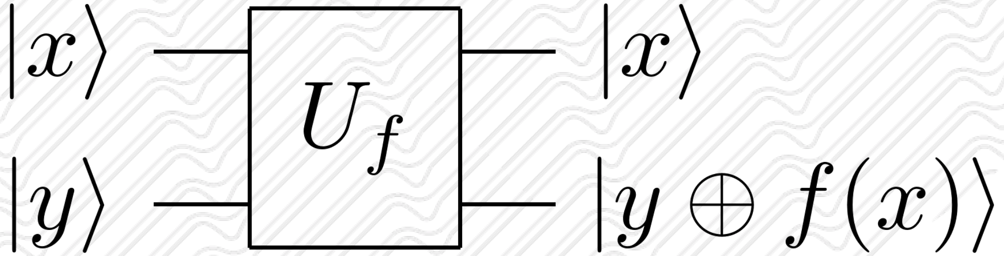
$\oplus$

Addition Mod 2
(Bitwise / XOR)

y \ $f(x)$	0	1
0	0	1
1	1	0

If $f(x) = 1$, flip y
Otherwise, do nothing

The Quantum Oracle



x	$f_2(x)$
0	1
1	0

$$U_f|0\rangle|y\rangle = |0\rangle|y \oplus f(0)\rangle = |0\rangle|!y\rangle$$

$$U_f|1\rangle|y\rangle = |1\rangle|y \oplus f(1)\rangle = |1\rangle|y\rangle$$

The control doesn't change
The target either flips or doesn't flip

The Quantum Oracle

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

What if we send in the computational basis states?

$$U_f|0\rangle|0\rangle = |0\rangle|f(0)\rangle$$

$$U_f|1\rangle|0\rangle = |1\rangle|f(1)\rangle$$

The two-query method still works just as well

What if the control is in a ***superposition*** state?

$$U_f|+\rangle|0\rangle = \frac{|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle}{\sqrt{2}}$$

Both $f(0)$ and $f(1)$ in the output state!

But when we measure, we'll get one or the other randomly

The Deutsch-Josza Solution

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

What if the target is in the $|-\rangle$ superposition state?

$$U_f|x\rangle|-\rangle = \frac{U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle}{\sqrt{2}}$$

Does nothing if $f(x) = 0$
Flips $|-\rangle$ to $-|-\rangle$ if $f(x) = 1$

$$= \frac{|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}}$$

$$= (-1)^{f(x)}|x\rangle|-\rangle$$

The Deutsch-Josza Solution

What if both the control and target are in superposition?

$$\text{Key Insight :} \quad U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$

Global Phase

Relative Phase

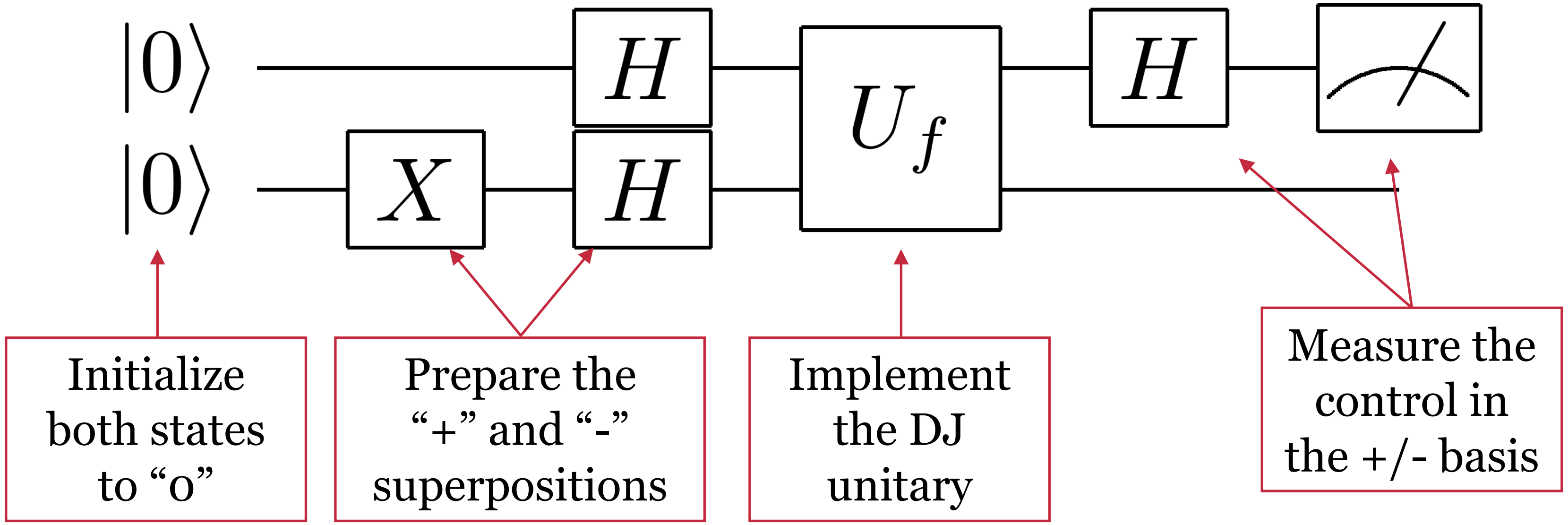
$$U_f|+\rangle|-\rangle = \frac{(-1)^{f(0)}}{\sqrt{2}}\left(|0\rangle + (-1)^{f(1)-f(0)}|1\rangle\right)|-\rangle$$

$$U_f|+\rangle|-\rangle = |+\rangle|-\rangle \text{ if } f(x) \text{ constant}$$

$$U_f|+\rangle|-\rangle = |-\rangle|-\rangle \text{ if } f(x) \text{ balanced}$$

Measuring the control qubit in the X basis tells us whether the function is constant or balanced *in one query*

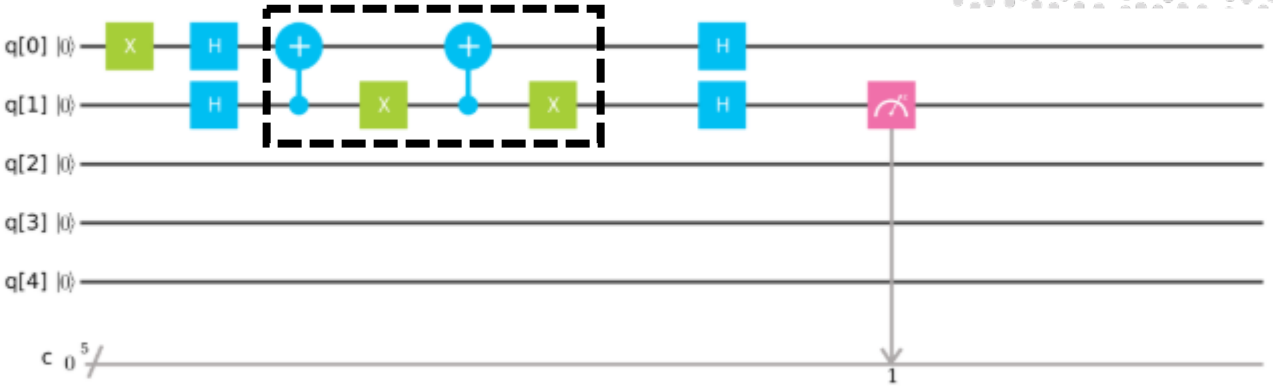
The Deutsch-Josza Circuit



Deutsch-Josza with IBM Q

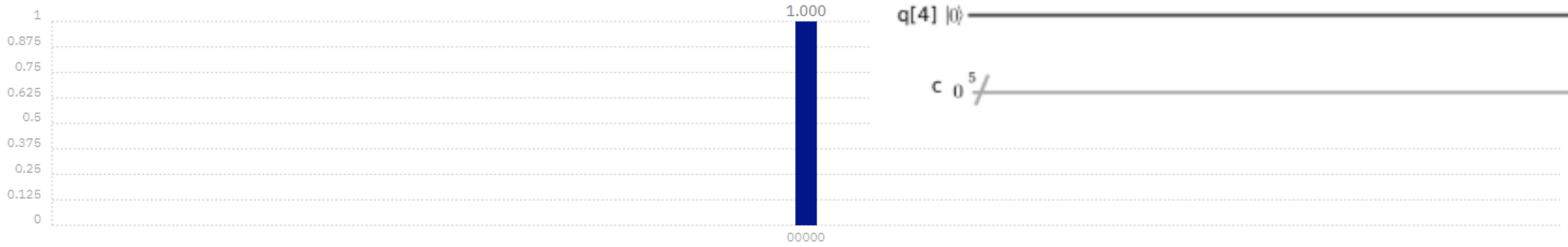
Deutsch-Jozsa algorithm in Qiskit: shorturl.at/akCHV

DJ Oracle for $f(x) = 1$



Device: Simulator

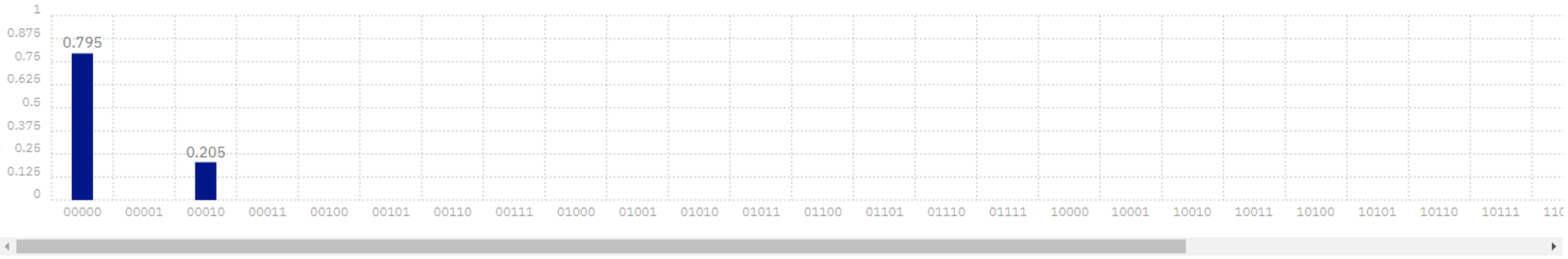
Quantum State: Computation Basis

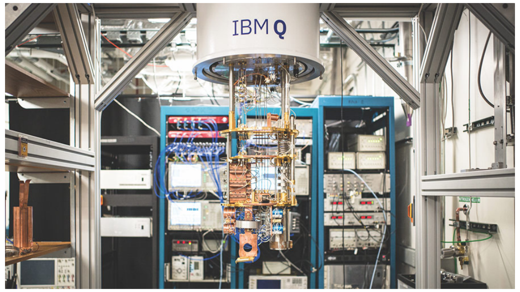


Device: ibmqx4

Quantum State: Computation Basis

Download CSV

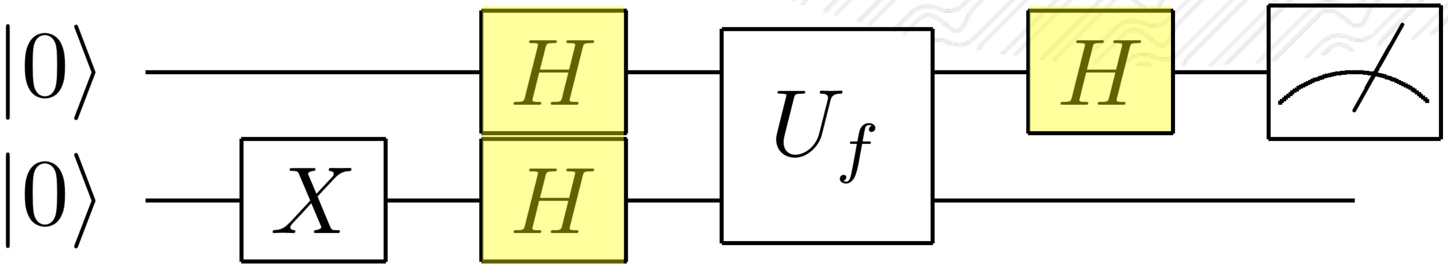




Question Break

Lessons from Deutsch-Josza

- Preparing the target in superposition wasn't enough!
  - We needed to also measure in a superposition basis



The First Rule of
Quantum Computing Club
It's not just about
"querying all possibilities
in superposition"

Lessons from Deutsch-Josza

The "target" measurement qubit wasn't actually measured

The phase was "kicked back" to the control qubit

Key to many quantum algorithms

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

$$U_f|+\rangle|-\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)|-\rangle$$

$$U_f|+\rangle|-\rangle = |+\rangle|-\rangle \text{ if } f(x) \text{ constant}$$

$$U_f|+\rangle|-\rangle = |-\rangle|-\rangle \text{ if } f(x) \text{ balanced}$$

Lessons from Deutsch-Josza

We still don’t know what $f(x)$ is exactly

x	$f_1(x)$
0	0
1	0

Constant

x	$f_2(x)$
0	1
1	0

Balanced

x	$f_3(x)$
0	0
1	1

Balanced

x	$f_4(x)$
0	1
1	1

Constant

We still need two queries to know which $f(x)$ we have,
but quantum computers allow us to extract some properties more efficiently

The Second Rule of
Quantum Computing Club
Quantum computers
don’t speed up everything

Lessons from Deutsch-Josza

It scales to many qubits

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	...
00	0	1	0	1	...
01	0	0	1	1	...
10	0	0	0	0	...
11	0	0	0	0	...

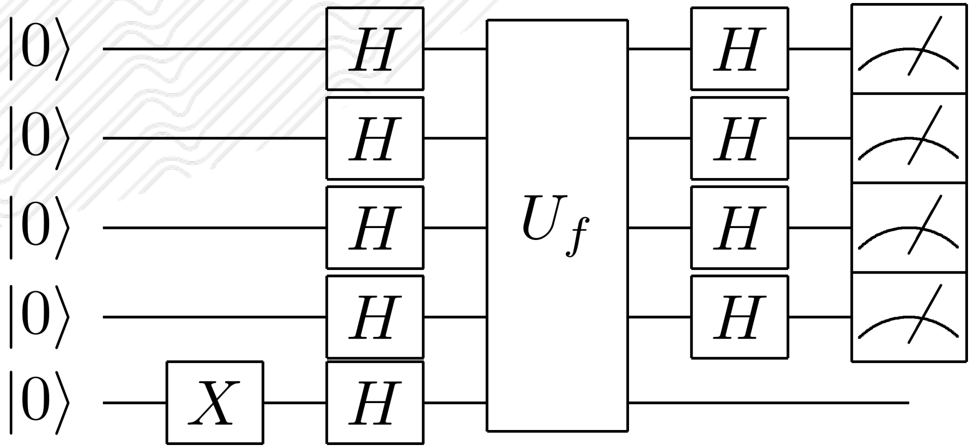
2 constant functions

$\binom{2^n}{2^{n-1}} = \frac{2^n!}{(2^{n-1}!)^2}$ balanced functions

Promise: It's either constant or balanced

We need $2^{n-1}+1$ queries to be 100% positive if $f(x)$ is constant or balanced

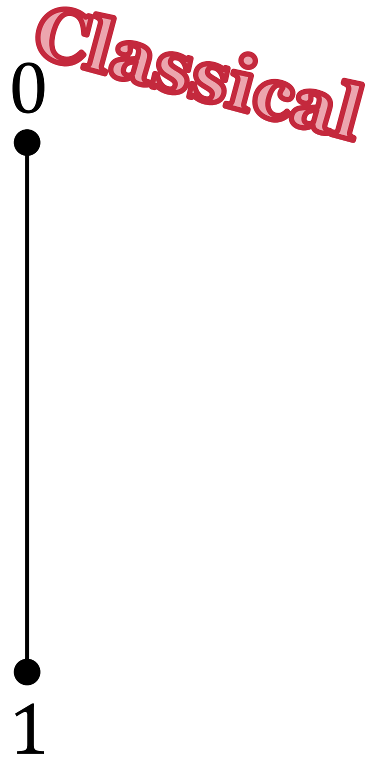
Exponential quantum speedup!



We can design a quantum circuit which tells us in **one** query if it's constant or balanced

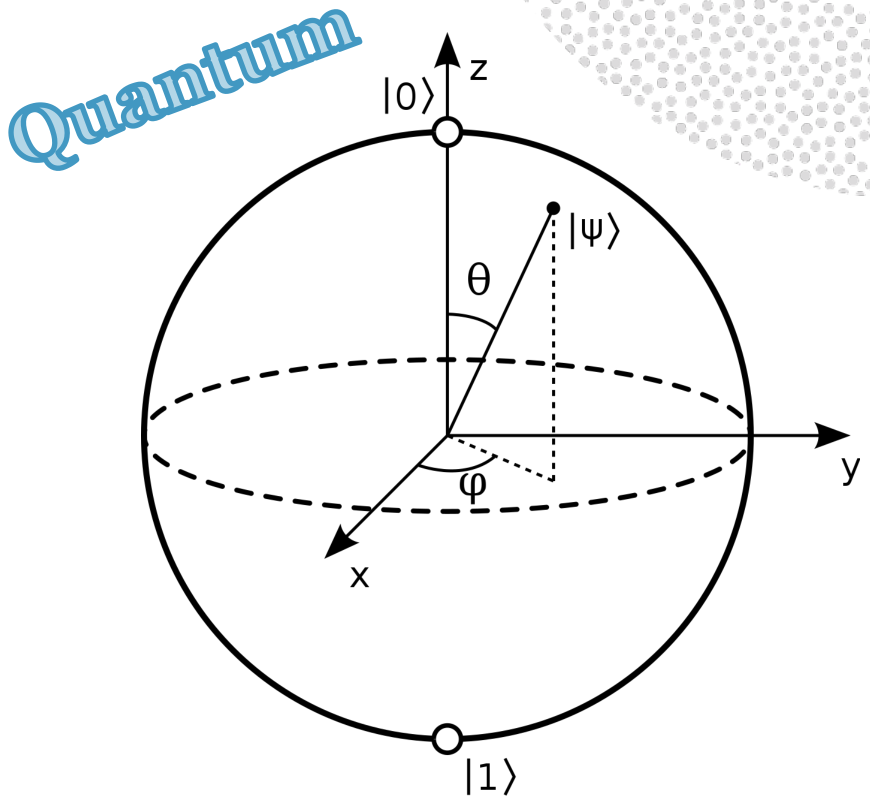
Details a bit complicated! See the notes for more

Classical vs. Quantum



$$\mathrm{VAL} = (\text{“0”})Pr(0) + (\text{“1”})Pr(1)$$

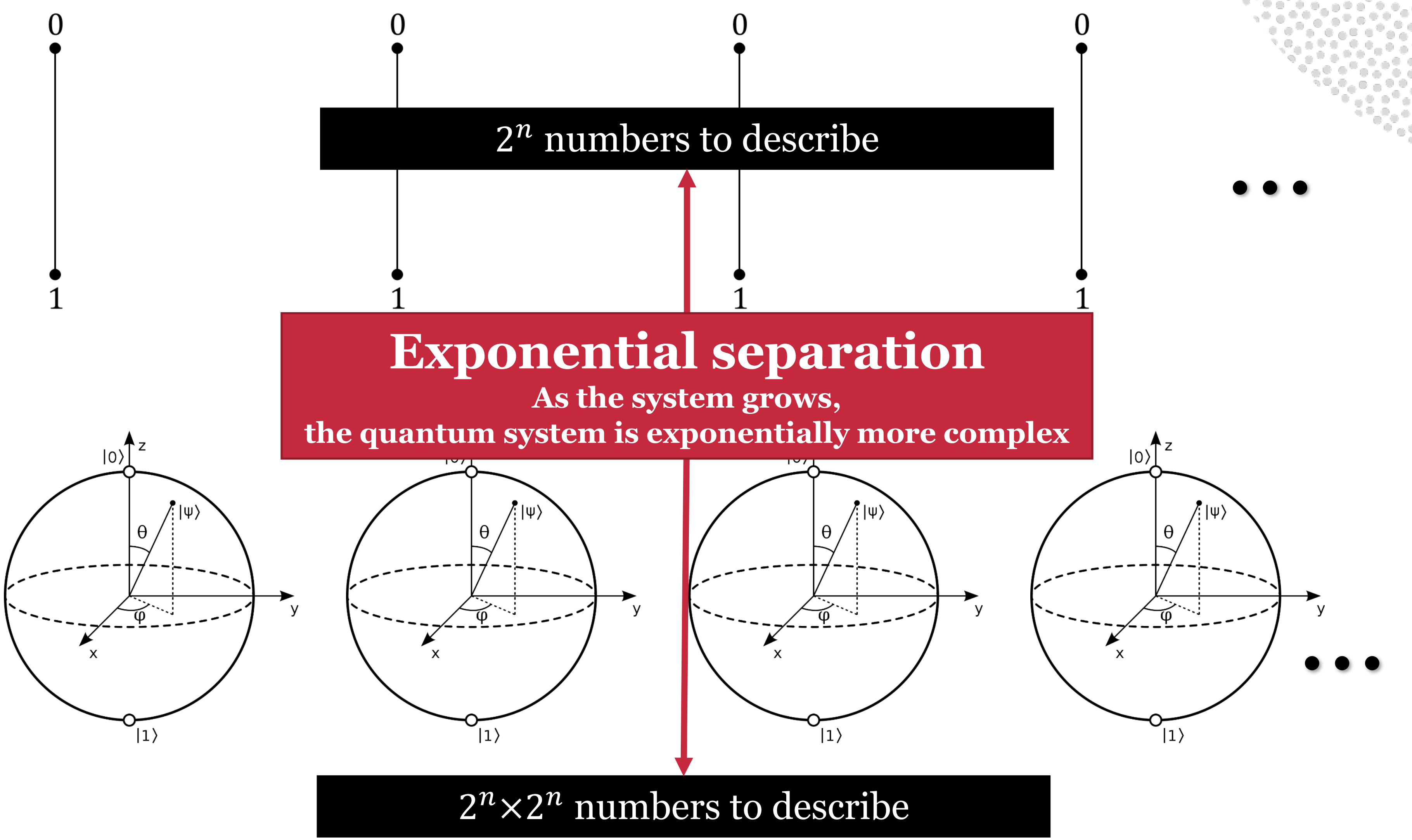
Need one measurement to know the “state”



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

Need three measurements to know the “state”

Classical vs. Quantum



But remember...

The Second Rule of
Quantum Computing Club

Quantum computers
don’t speed up everything

Quantum computers do not provide exponential enhancement for every problem

Factoring → Exponential

Search → Quadratic

Many others → Nothing

Many many others → Unknown

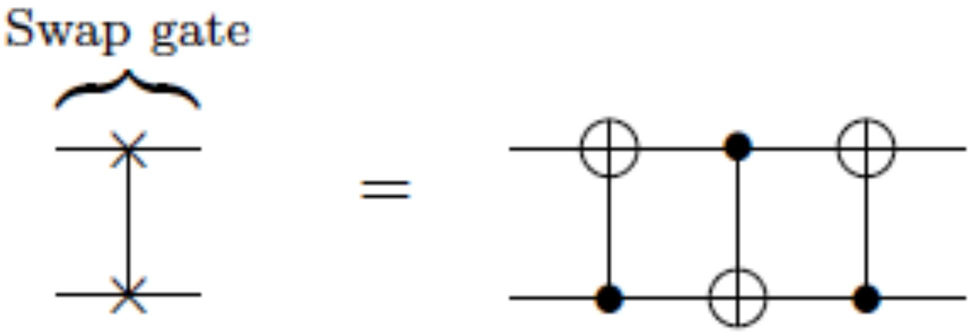
What's it useful for?

But with some quantum pieces

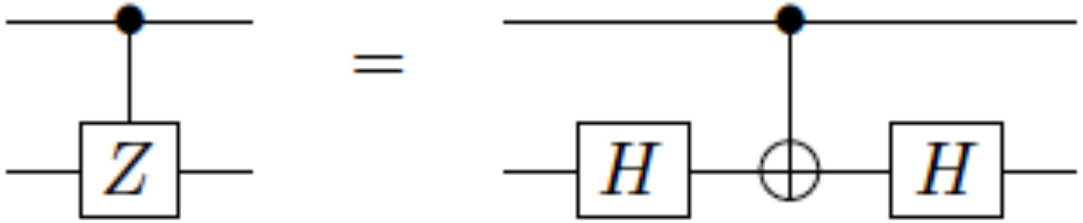
Question Break

Check out other quantum algorithms
https://quantumalgorithmzoo.org/
by Stephen Jordan (Microsoft Quantum)

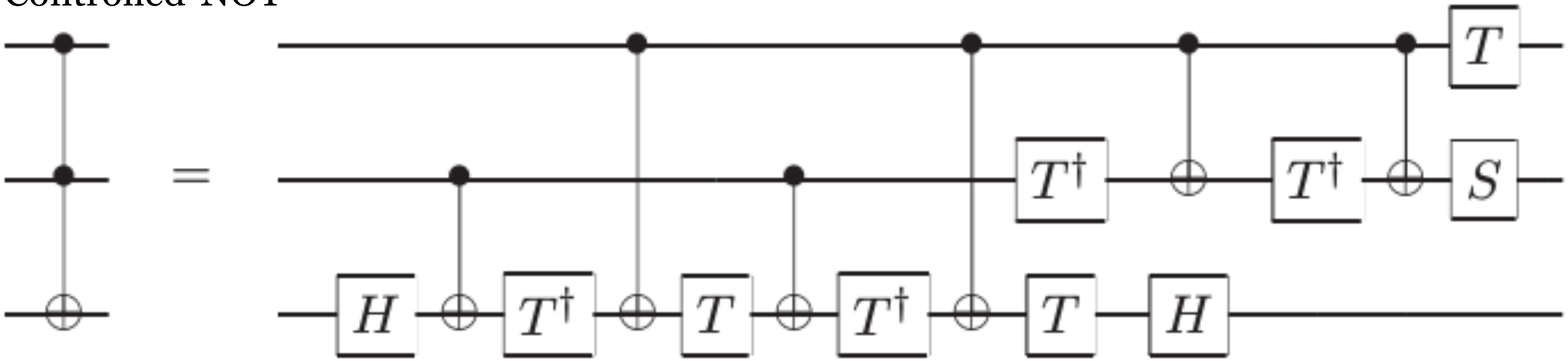
Universal Gate Sets



Controlled Phase

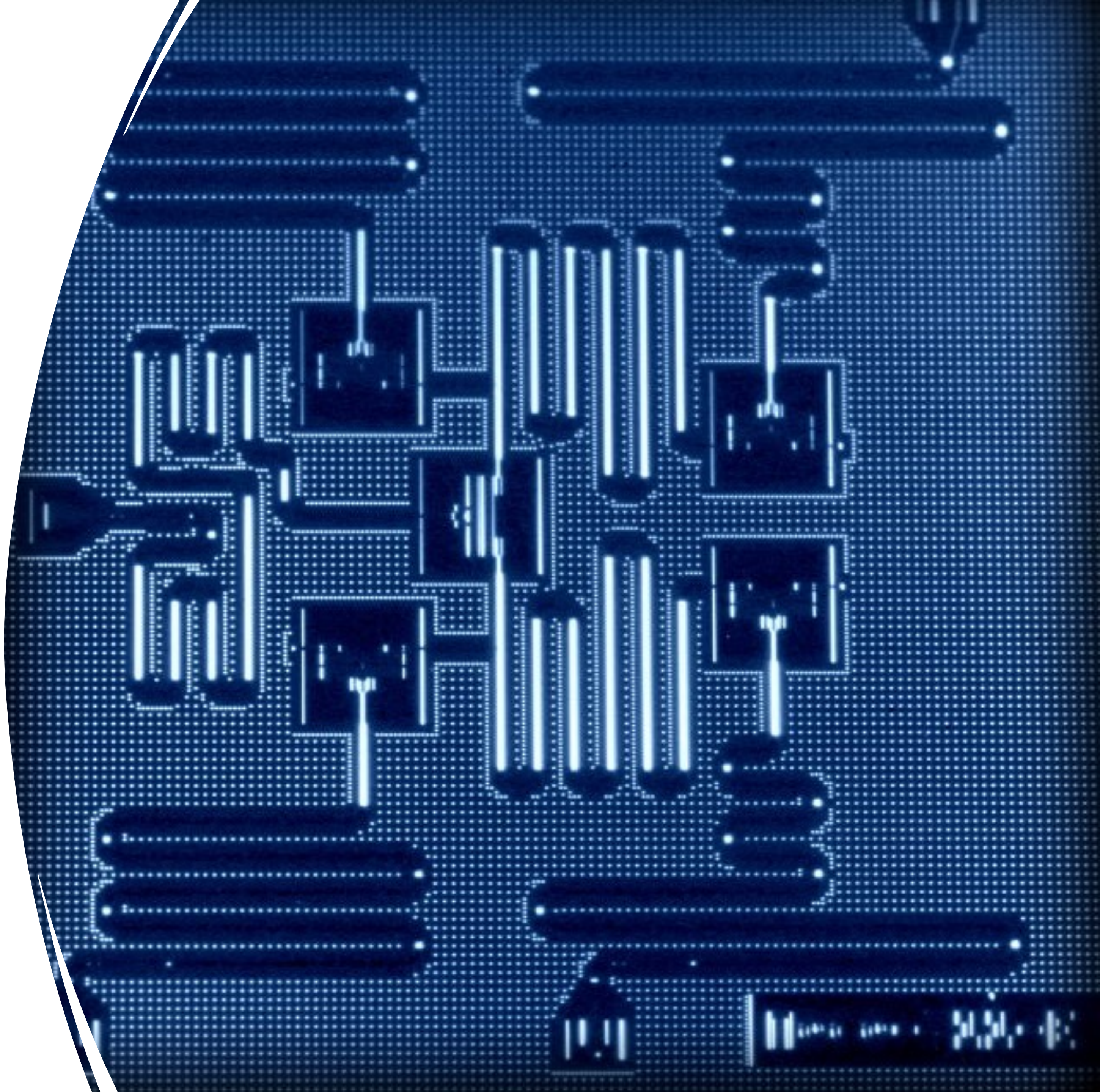


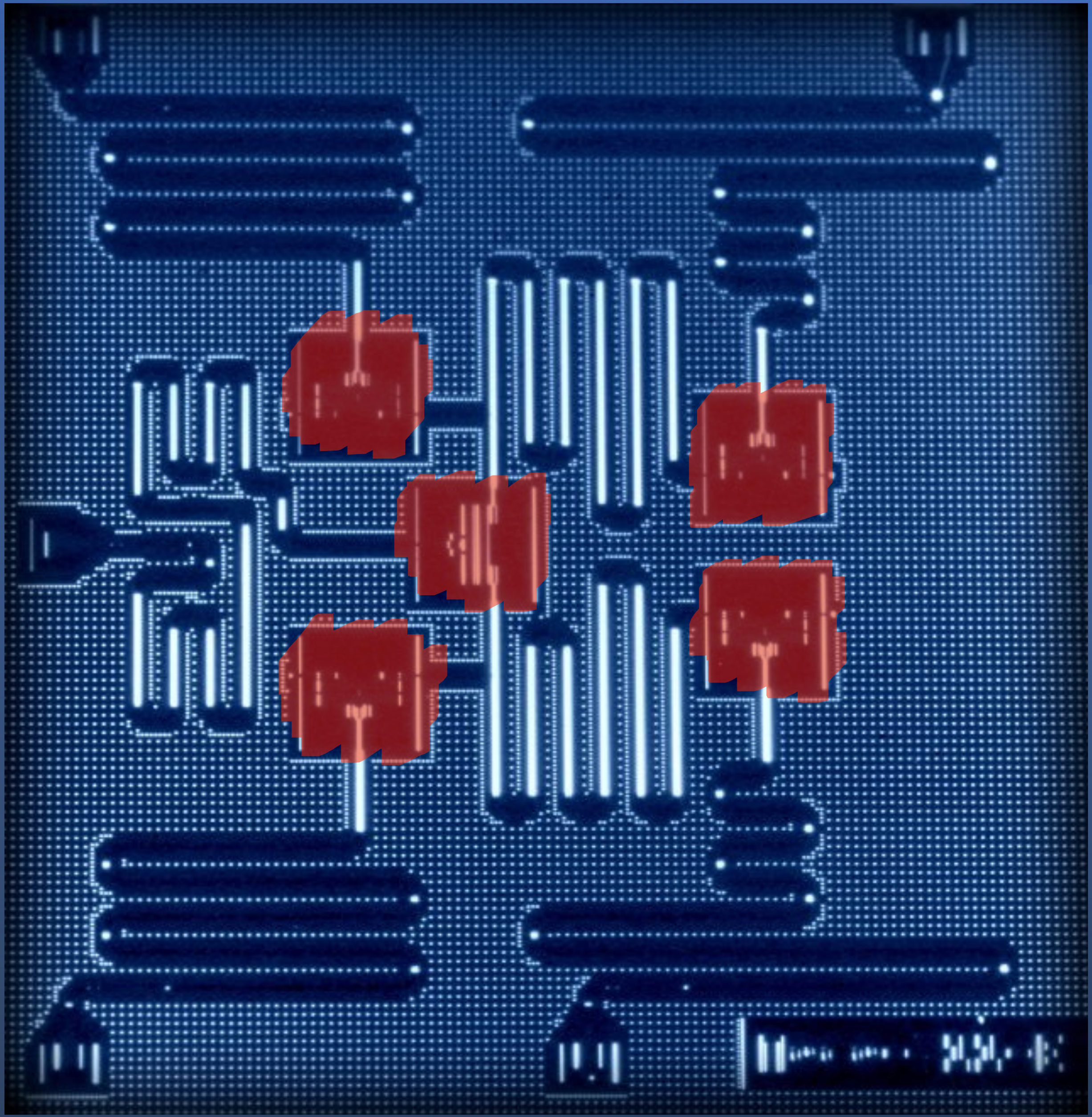
Controlled-Controlled-NOT



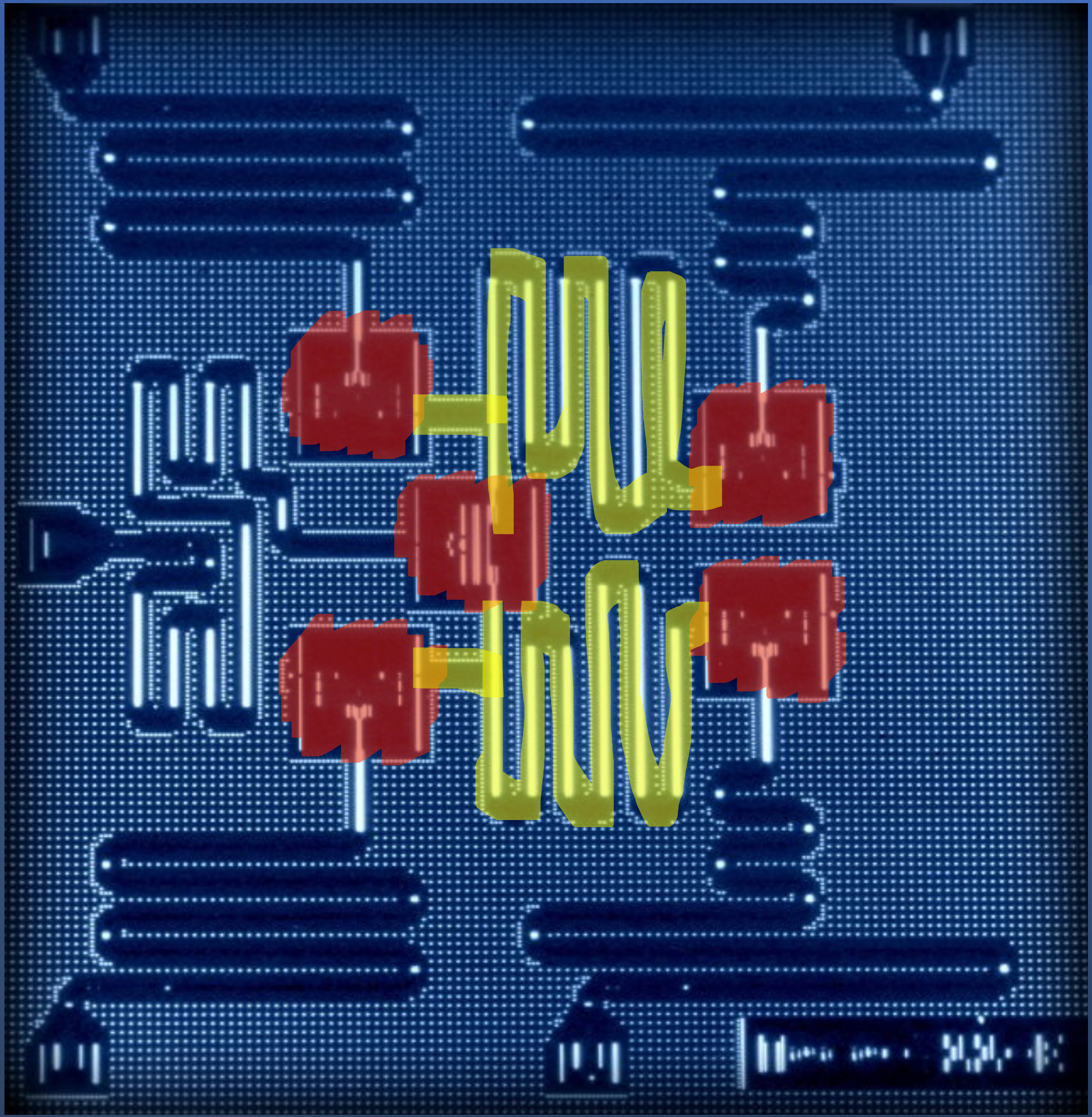
Might not be easy, but any gate can be faithfully approximated

The Chip of a Five-Qubit IBM Quantum Computer



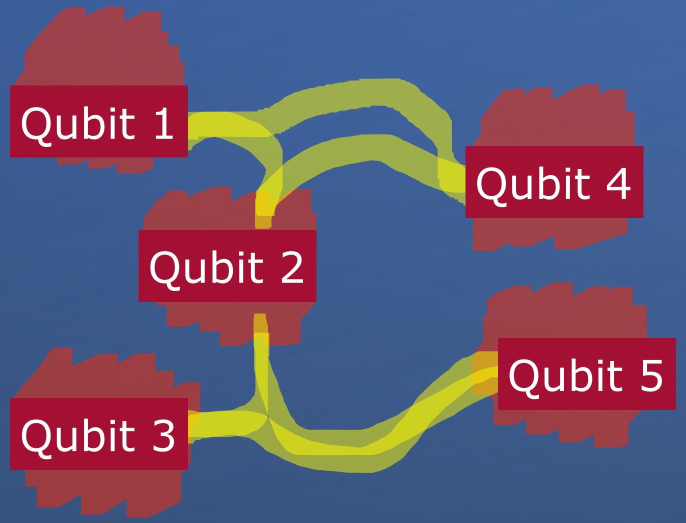


Slides courtesy of Meijer - van de Griend



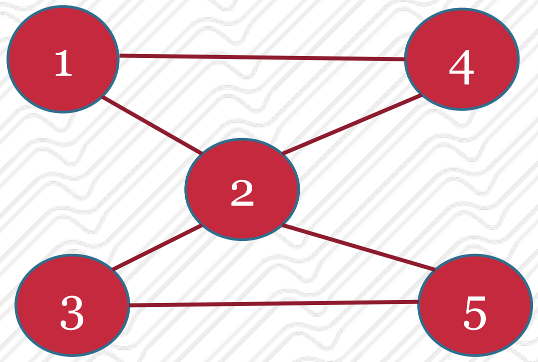
Slides courtesy of Meijer - van de Griend

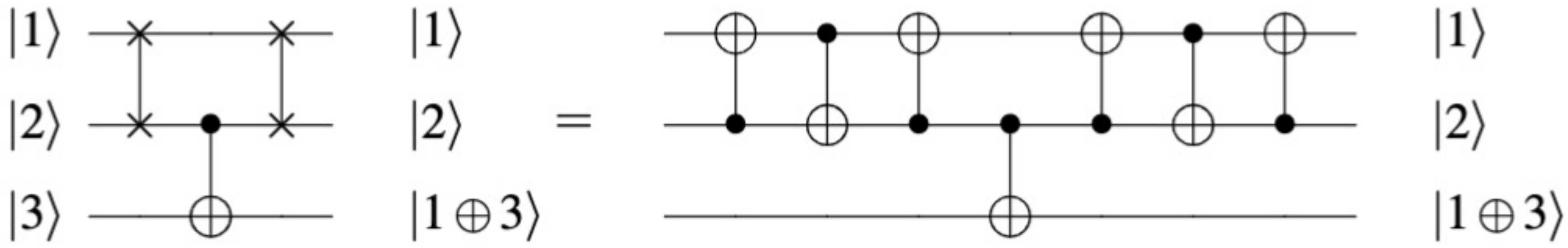
Topological Constraints



Slides courtesy of Meijer - van de Griend

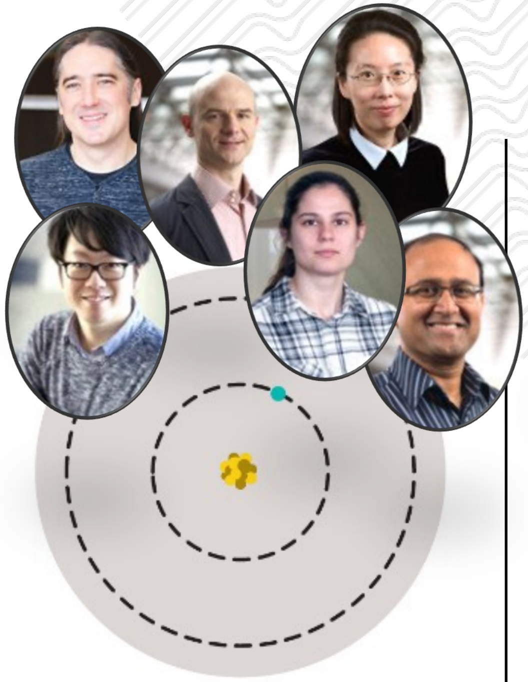
Example





Routing CNOT$(1,3)$ with SWAP gates results in 7 CNOTs.

Pick Your Qubit



Atoms & Ions

Honeywell

AQT

IONQ

Photons

IDQ
FROM VISION TO TECHNOLOGY

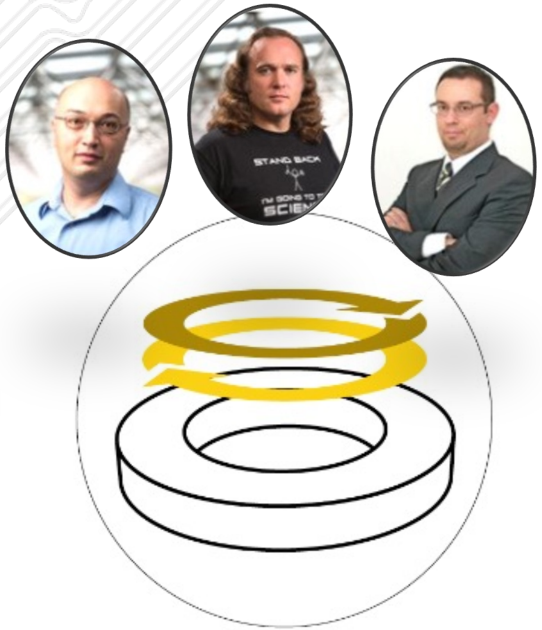
XANADU

PSIQUANTUM

Spin

intel

SILICON
QUANTUM
COMPUTING



Superconducting Circuits

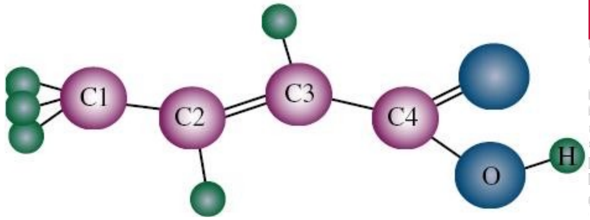
Google

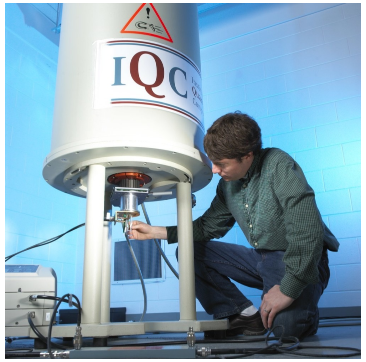
D:WAVE

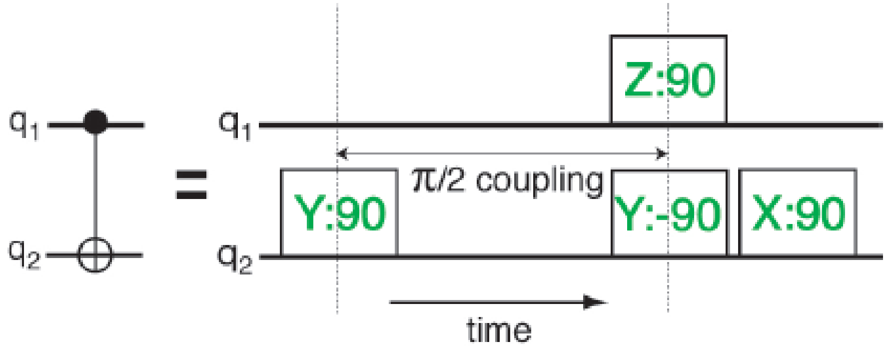
IBM Q

rigetti

Spin Systems



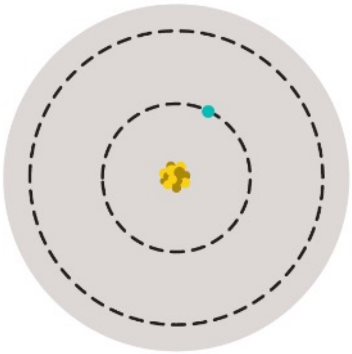


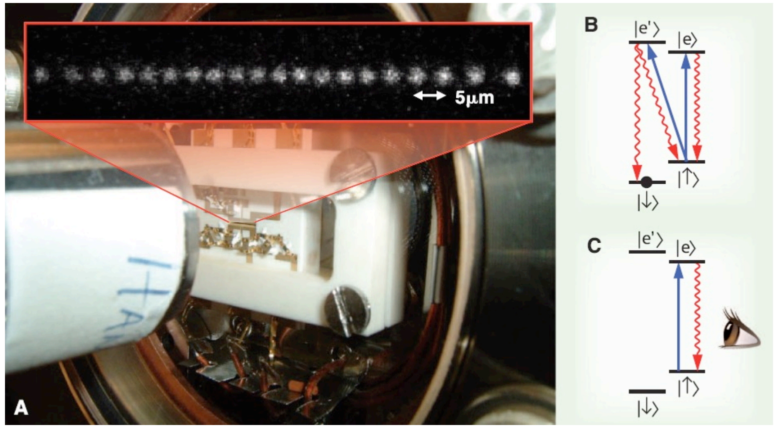


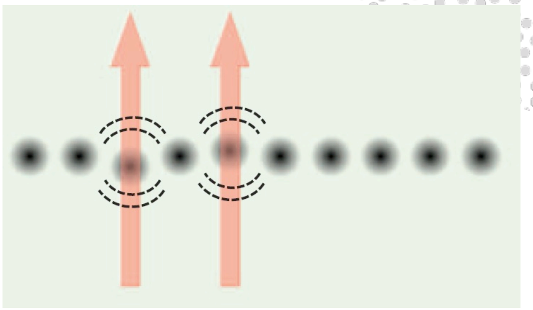
- Use nuclear or electron spins in NMR/ESR systems
- Couple through J coupling (spin-spin interaction)
- Move towards nanoscale or monolayers for true single-systems

NMR QIP Review: J. Baugh et al, Physics in Canada (2007). arXiv:0710.1447

Trapped Atoms and Ions



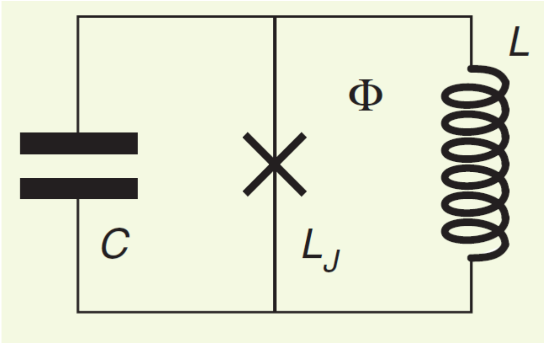


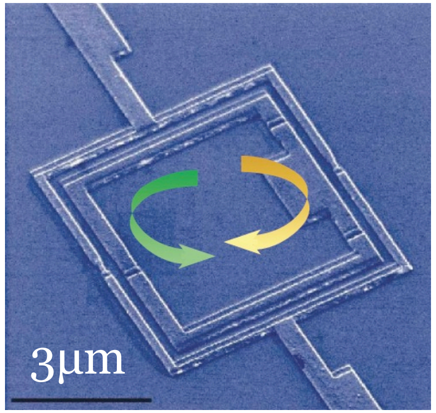


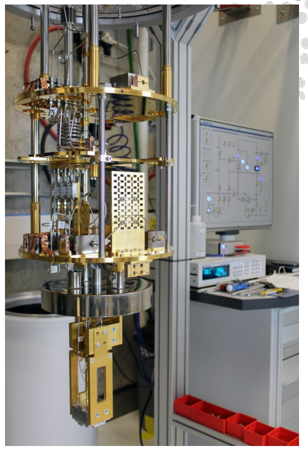
- ❖Trapped individual ions (e.g. Yb^{+}) in dynamic electric traps, or neutral atoms using optical tweezers
- ❖Use electronic energy states as qubits, fluorescence readout
- ❖Couple through collective motional modes

Review: C. Monroe and J. Kim, Science **339**, 1164 (2013).

Superconducting Circuits







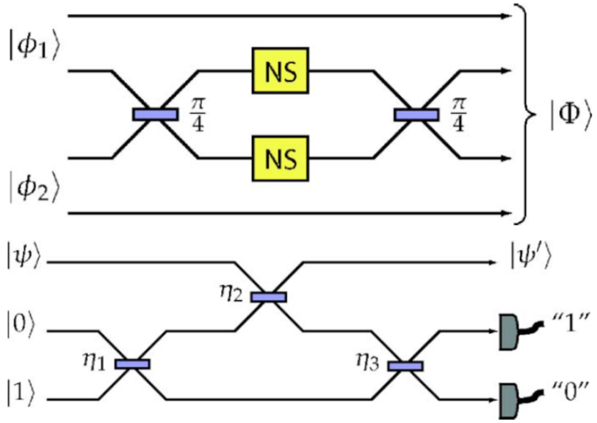
❖Flux or charge quanta in “artificial atoms” as qubits

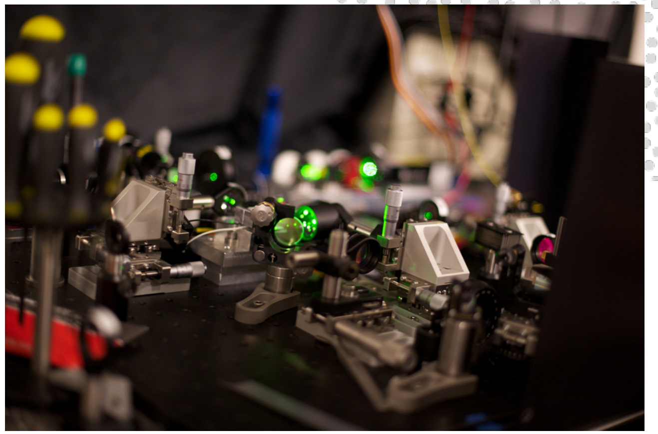
❖Write using circuit fab techniques (e.g. Al on Si)

❖Cool in dilution refrigerators, control with microwaves

Review: J. Clarke and F.K. Wilhelm, Nature **453**, 1031 (2008).
Review: M.H. Devoret and R.J. Schoelkopf, Science **339**, 1169 (2013).

Photonics





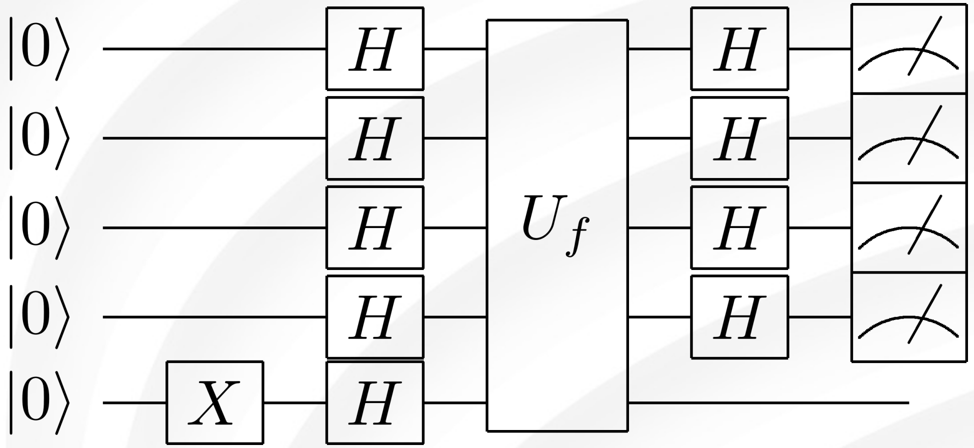
❖Generate single photons by nonlinear optics or quantum emitters

❖Directly use light's degrees of freedom (e.g. polarization)

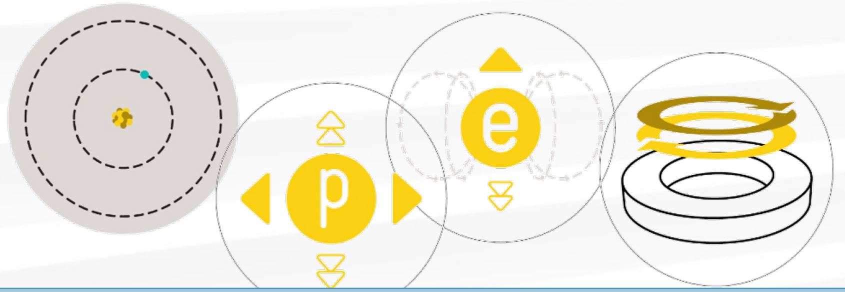
❖Couple probabilistically, or directly generate entangled cluster

Review: P. Kok et al, Rev. Mod. Phys **79**, 135 (2007).

Early Quantum Computing



Quantum algorithms can have up to exponential speedups, but only with clever design!



There are many possible physical systems, but they must satisfy certain criteria

Check out other quantum algorithms
https://quantumalgorithmzoo.org/
by Stephen Jordan (Microsoft Quantum)

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing