Quantum Computing

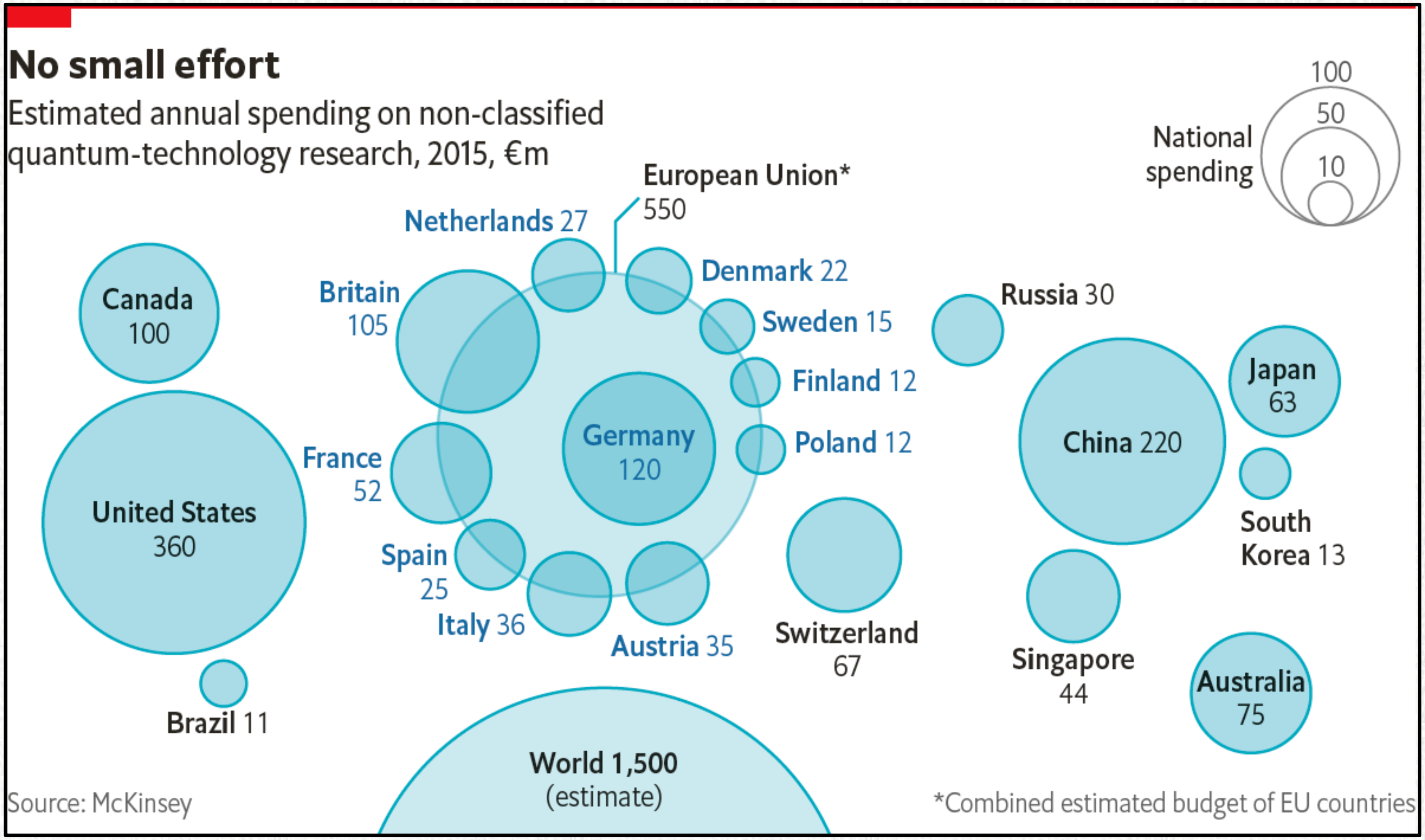
Bill Silver
Computer Science Department
Bowdoin College

Physics of Computation Conference Endicott House MIT May 6-8, 1981

1 Freeman Dyson
2 Gregory Chaitin
3 James Crutchfield
4 Norman Packard
5 Panos Ligomenides
6 Jerome Rothstein
7 Carl Hewitt
8 Norman Hardy
9 Edward Fredkin
10 Tom Toffoli
11 Rolf Landauer
12 John Wheeler
13 Frederick Kantor
14 David Leinweber
15 Konrad Zuse
16 Bernard Zeigler
17 Carl Adam Petri
18 Anatol Holt
19 Roland Vollmar
20 Hans Bremerman
21 Donald Greenspan
22 Markus Buettiker
23 Otto Floberth
24 Robert Lewis
25 Robert Suaya
26 Stan Kugell
27 Bill Gosper
28 Lutz Priese
39 Madhu Gupta
30 Paul Benioff
31 Hans Moravec
32 Ian Richards
33 Marian Pour-El
34 Danny Hillis
35 Arthur Burks
36 John Cocke
37 George Michaels
38 Richard Feynman
39 Laurie Lingham
40 Thiagarajan
41 ?
42 Gerard Vichniac
43 Leonid Levin
44 Lev Levitin
45 Peter Gacs
46 Dan Greenberger

Source: https://mitendicotthouse.org/physics-computation-conference/

Worldwide R&D in 2015



Source: The Economist, *Here, There, and Everywhere*, March 2017

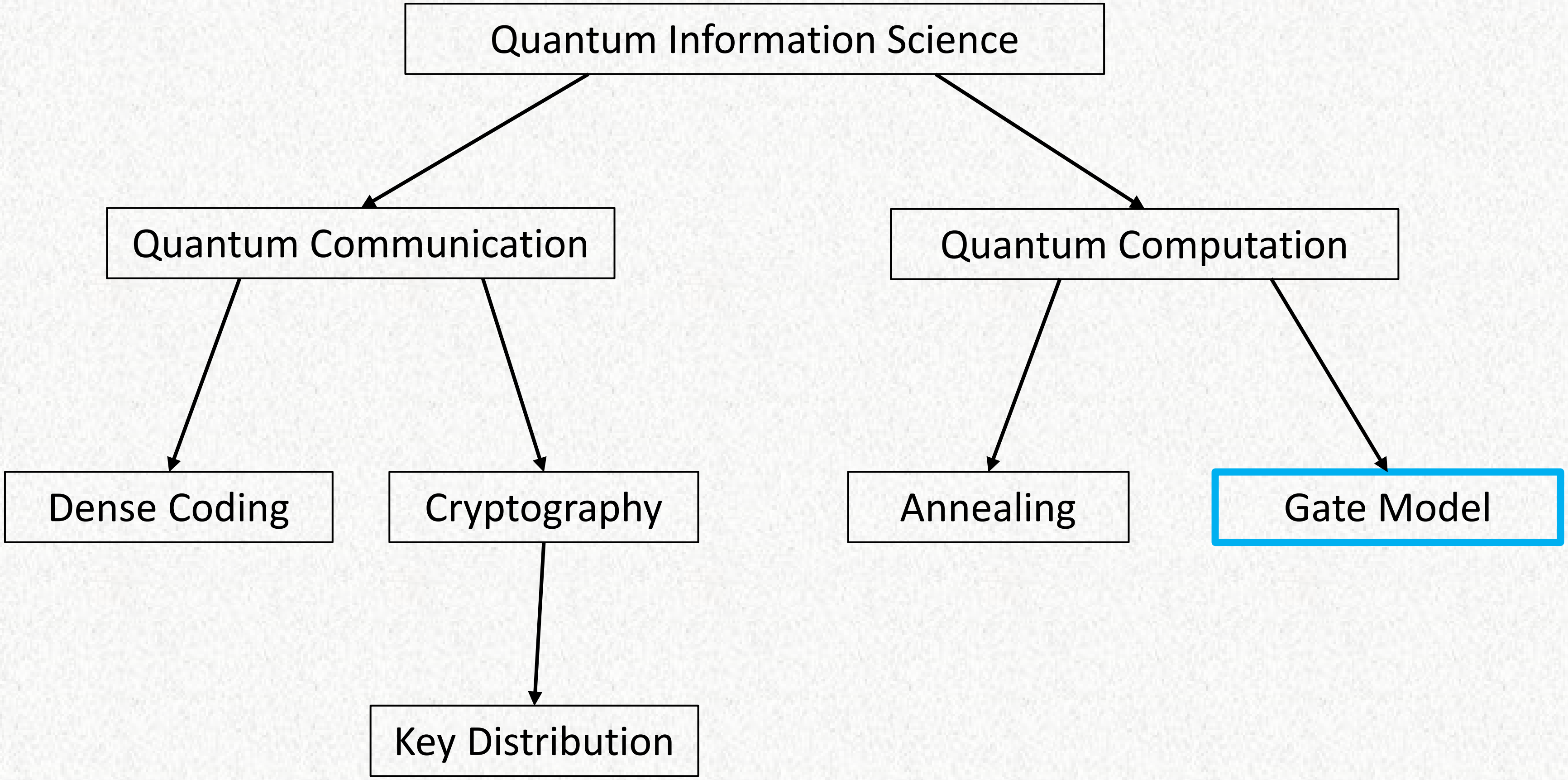
Popular Press

NEWSWEEK MAGAZINE

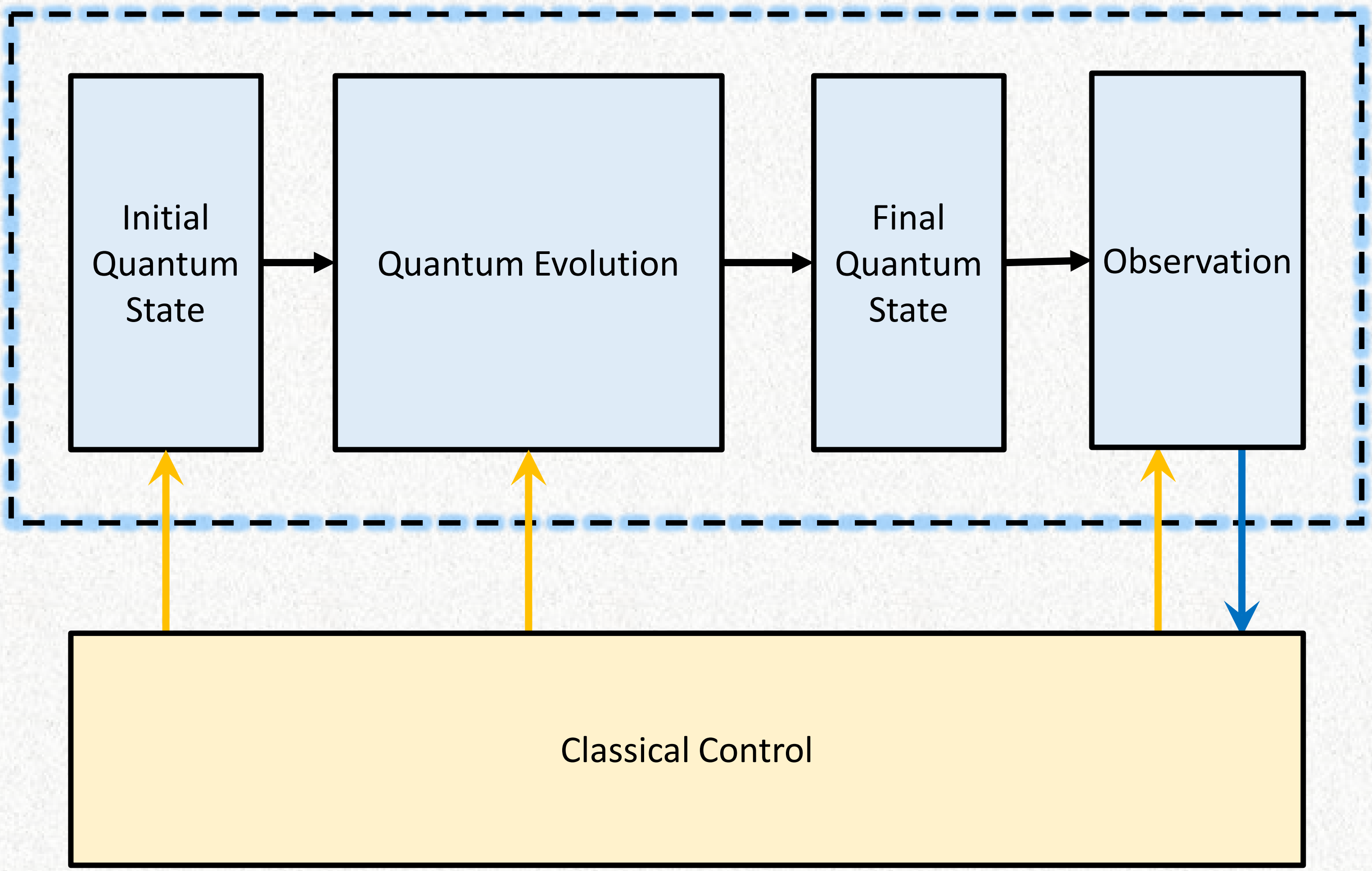
As China Leads Quantum Computing Race, U.S. Spies Plan for a World with Fewer Secrets

BY **FRED GUTERL** ON 12/14/20 AT 5:00 AM EST

Quantum Taxonomy, Abridged



A Quantum Computer



Highlights

- Machine state
  - qubit: two-state unit of information
  - state of n qubits is $N = 2^n$-dimensional complex vector
  - 2 constraints: unit length, unobservable global phase
  - $2N – 2 = 2(N – 1)$ degrees of freedom
  - superposition of N basis states
- Evolution
  - rotation and/or reflection of state vector
  - N x N matrix multiply
  - quantum parallelism
- Observation
  - squared magnitude of vector component is probability of observing the corresponding basis state

Quantum State

Qubit State

$$\binom{c_0}{c_1} = c_0 \binom{1}{0} + c_1 \binom{0}{1}$$

$$c_0 \,|0\rangle + c_1 \,|1\rangle$$

$$|c_0|^2 + |c_1|^2 = 1$$

$$\begin{pmatrix} a_0 e^{i\phi_0} \\ a_1 e^{i\phi_1} \end{pmatrix}$$

$$a_0^2 + a_1^2 = 1$$

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) e^{i\phi_0} \\ \sin\left(\frac{\theta}{2}\right) e^{i\phi_1} \end{pmatrix}$$

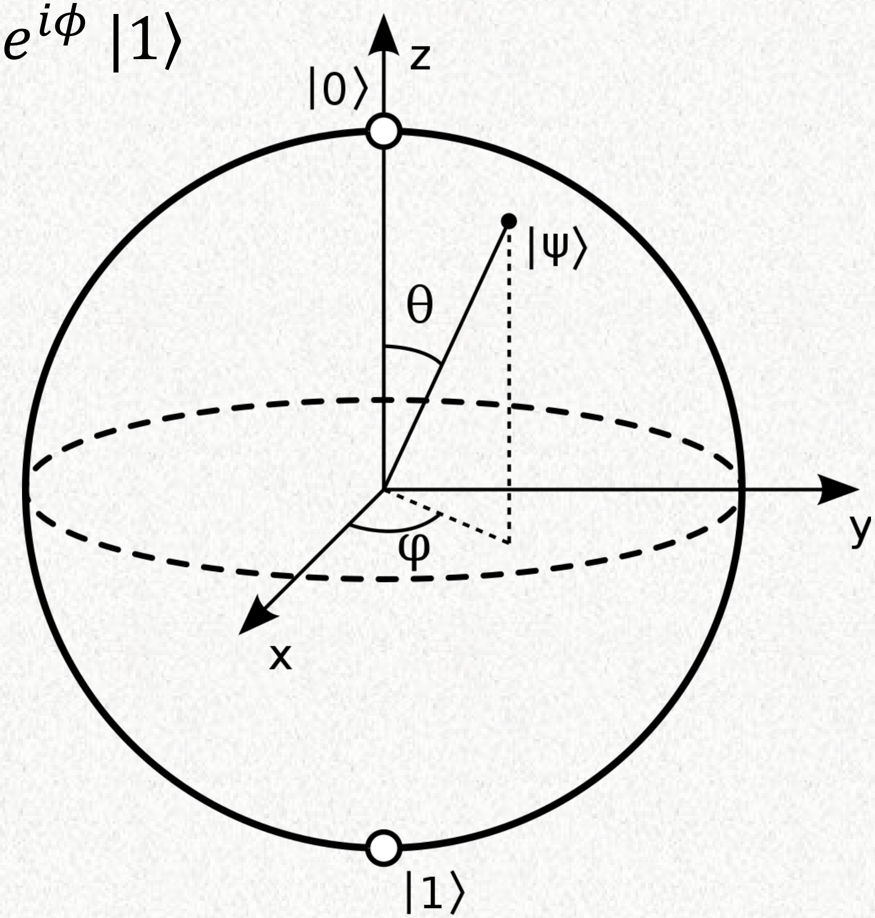
$$e^{i\phi_0} \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) e^{i(\phi_1 - \phi_0)} \end{pmatrix}$$

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) e^{i\phi} \end{pmatrix}$$

2(N – 1) = 2 degrees of freedom

Bloch Sphere

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle$$



By Smite-Meister - Own work, CC BY-SA 3.0,
https://commons.wikimedia.org/w/index.php?curid=5829358

Three-Qubit State

2^3 = 8-dimensional complex vector space

$$|\psi\rangle = \begin{pmatrix} c_{000} \\ c_{001} \\ c_{010} \\ c_{011} \\ c_{100} \\ c_{101} \\ c_{110} \\ c_{111} \end{pmatrix}$$

$$|\psi\rangle = c_{000}|000\rangle + c_{001}|001\rangle + c_{010}|010\rangle + c_{011}|011\rangle + c_{100}|100\rangle + c_{101}|101\rangle + c_{110}|110\rangle + c_{111}|111\rangle$$

2(N – 1) = 14 degrees of freedom

n-Qubit State

2^n = N-dimensional complex vector space

$$\begin{pmatrix} c_{0\ldots0} \\ c_{0\ldots1} \\ \vdots \\ c_{1\ldots1} \end{pmatrix}$$

$$c_{0\ldots0}|0\ldots0\rangle + \quad c_{0\ldots1}|0\ldots1\rangle + \cdots + c_{1\ldots1}|1\ldots1\rangle$$

2(N – 1) degrees of freedom

Two Qubits

Considered Separately

$$|\psi_\alpha\rangle = \binom{\alpha_0}{\alpha_1}$$

2 degrees of freedom

$$|\psi_\beta\rangle = \binom{\beta_0}{\beta_1}$$

2 degrees of freedom

Considered Together

$$|\psi_c\rangle = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix}$$

6 degrees of freedom

Entanglement!

Two Independent Qubits

$$|\psi_\alpha\rangle = \begin{pmatrix}\alpha_0 \\ \alpha_1\end{pmatrix} \qquad |\psi_\beta\rangle = \begin{pmatrix}\beta_0 \\ \beta_1\end{pmatrix}$$

$$|\psi_\alpha\psi_\beta\rangle = \begin{pmatrix}\alpha_0 \\ \alpha_1\end{pmatrix} \otimes \begin{pmatrix}\beta_0 \\ \beta_1\end{pmatrix} = \begin{pmatrix}\alpha_0 \begin{pmatrix}\beta_0 \\ \beta_1\end{pmatrix} \\ \alpha_1 \begin{pmatrix}\beta_0 \\ \beta_1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1\end{pmatrix}$$

tensor product

An Entangled State

$$|\psi_{Bell}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad =? \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

Quantum Evolution

Conjugate Transpose

- transpose vector or matrix
- replace every element with its complex conjugate

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)e^{i\phi} \end{pmatrix}^{\dagger} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & \sin\left(\frac{\theta}{2}\right)e^{-i\phi} \end{pmatrix}$$

$$\begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix}^{\dagger} = \begin{pmatrix} e^{-i\pi/4} & e^{i\pi/4} \\ e^{i\pi/4} & e^{-i\pi/4} \end{pmatrix}$$

$$|\psi\rangle^{\dagger} = \langle\psi|$$

Inner Product

Function of two vectors that is

- scalar-valued
- linear
- independent of basis

Defines geometry of space

- length
- angle
- distance

$$a^\dagger b \qquad \langle a|\,|b\rangle \implies \langle a|b\rangle$$

Length:

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & \sin\left(\frac{\theta}{2}\right)e^{-i\phi} \end{pmatrix} \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)e^{i\phi} \end{pmatrix}$$

$$= \cos^2\left(\frac{\theta}{2}\right) + \sin^2\left(\frac{\theta}{2}\right) = 1$$

Quantum Evolution Rules

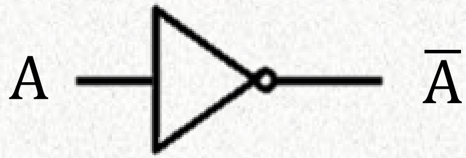
- Preserves geometry of complex vector space
- Rotation/reflection of state vector
- Unitary operator U: $UU^\dagger = U^\dagger U = I$

$$
\begin{aligned}
&\langle U\psi_1 | U\psi_2 \rangle \\
&= (U\psi_1)^\dagger \, (U\psi_2) \\
&= (\psi_1^\dagger U^\dagger) \, (U\psi_2) \\
&= \psi_1^\dagger (U^\dagger U) \psi_2 \\
&= \psi_1^\dagger \psi_2 = \langle \psi_1 | \psi_2 \rangle
\end{aligned}
$$

The Gate Model

- Rotate initial state vector to one with high probability of observing desired result
- Small steps that can be
  - understood by designer
  - implemented by hardware
- Steps are “gates”, by analogy with classical digital logic
- Universal gate set
  - achieve any rotation/reflection by composition
  - quantum machine language

Logical Not



$$\mathrm{A} = \,!\mathrm{A}$$

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

$$X\ |0\rangle = |1\rangle$$

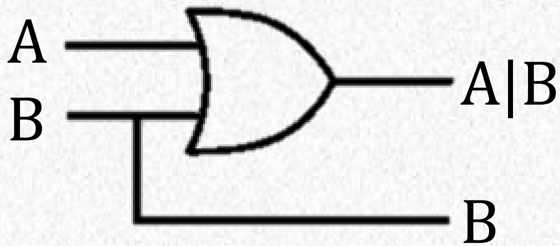
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$X\ |1\rangle = |0\rangle$$

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

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_0 \end{pmatrix}$$

Logical OR



$$F = A \mid B$$

$$\text{OR}\,|BA\rangle = |BF\rangle$$

$$\text{OR}\ |00\rangle = |00\rangle$$

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

$$\text{OR}\ |10\rangle = |11\rangle$$

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

$$\text{OR}\ |01\rangle = |01\rangle$$

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

$$\text{OR}\ |11\rangle = |11\rangle$$

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

Universal Computation?

Reversible

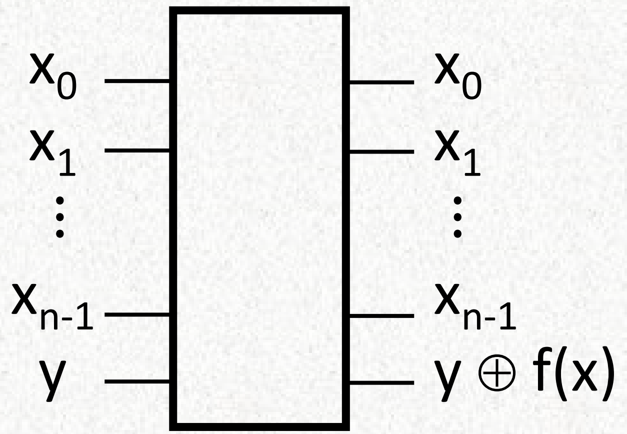
- Logical not, xor
- Two’s complement +, –
- Swap

Irreversible

- Logical and, or
- Multiplication
- Sort
- Assignment, copy

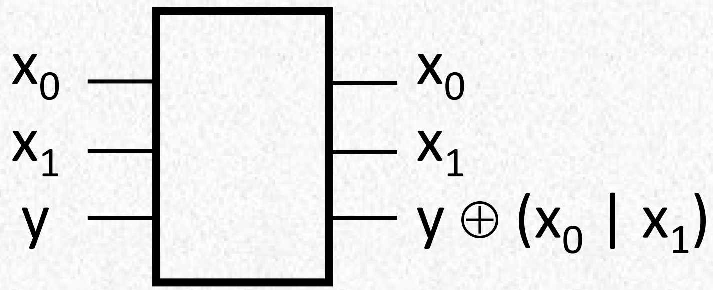
Universal Combinatorial Logic

$f(x_i)$ is any Boolean function of n Boolean variables x_i



This circuit is a unitary operation
and so can always be realized.

Unitary Logical OR



$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} c_{000} \\ c_{001} \\ c_{010} \\ c_{011} \\ c_{100} \\ c_{101} \\ c_{110} \\ c_{111} \end{pmatrix} = \begin{pmatrix} c_{000} \\ c_{101} \\ c_{110} \\ c_{111} \\ c_{100} \\ c_{001} \\ c_{010} \\ c_{011} \end{pmatrix}$$

Single-Qubit Pauli Gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad X \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

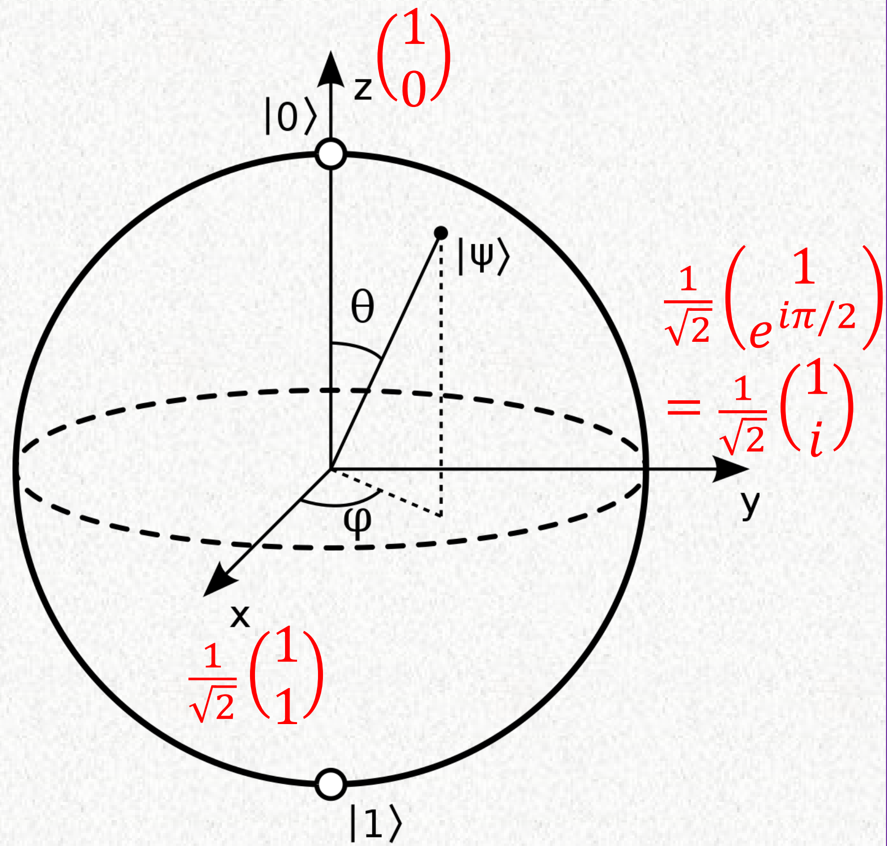
$\oplus$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Y \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}$$

Y

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad Z \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Z



rotations by π around Bloch sphere axes

Pauli Gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad X\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)e^{i\phi} \end{pmatrix} = \begin{pmatrix} \sin\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right)e^{-i\phi} \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Y\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)e^{i\phi} \end{pmatrix} = \begin{pmatrix} \sin\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right)e^{i(\pi-\phi)} \end{pmatrix}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad Z\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)e^{i\phi} \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)e^{i(\pi+\phi)} \end{pmatrix}$$

Hadamard Gate

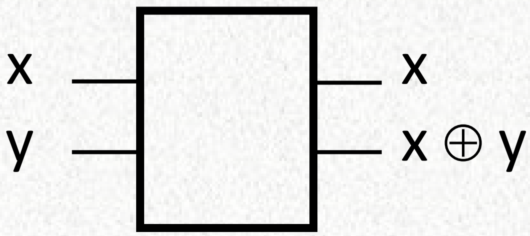
H

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

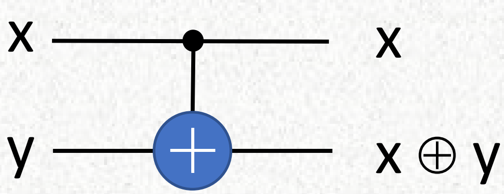
$$H\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle \qquad H|0\rangle = |+\rangle$$

$$H\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle \qquad H|1\rangle = |-\rangle$$

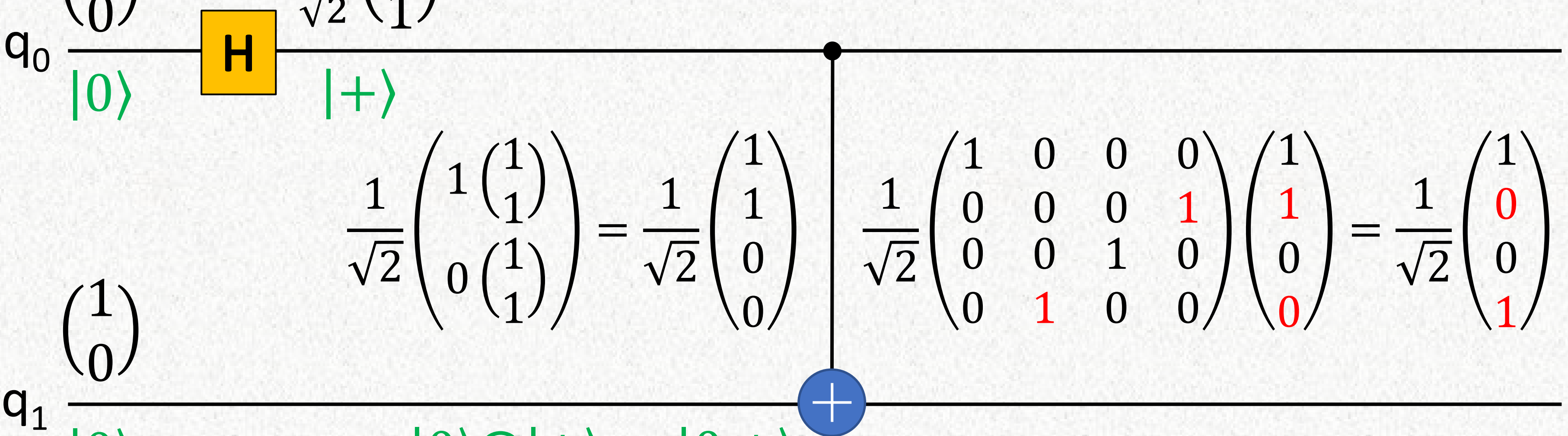
Controlled NOT



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} = \begin{pmatrix} c_{00} \\ c_{11} \\ c_{10} \\ c_{01} \end{pmatrix}$$



Bell State



$$\begin{pmatrix}1\\0\end{pmatrix} \quad \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

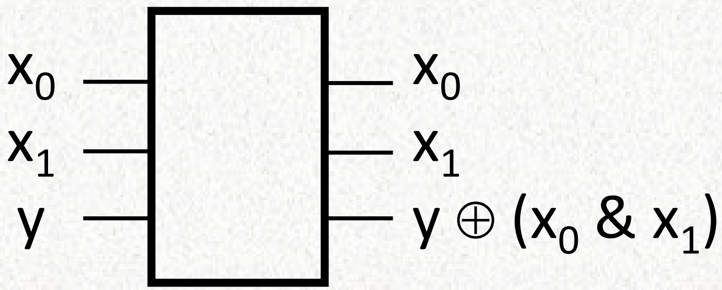
$$\begin{pmatrix}1\\0\end{pmatrix}$$

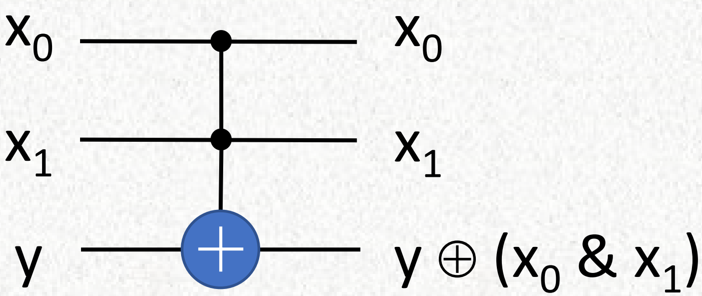
$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\begin{pmatrix}1\\1\end{pmatrix}\\0\begin{pmatrix}1\\1\end{pmatrix}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\\0\end{pmatrix}$$

$$|0\rangle\otimes|+\rangle = |0+\rangle$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}\begin{pmatrix}1\\1\\0\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$$

Toffoli Gate





$$\begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} c_{000} \\ c_{001} \\ c_{010} \\ c_{011} \\ c_{100} \\ c_{101} \\ c_{110} \\ c_{111} \end{pmatrix} = \begin{pmatrix} c_{000} \\ c_{001} \\ c_{010} \\ c_{111} \\ c_{100} \\ c_{101} \\ c_{110} \\ c_{011} \end{pmatrix}$$

Universal Gate Set

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

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

$$\sqrt{X} = \begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix}$$

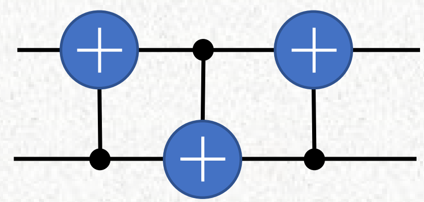
$$RZ(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

$$Y = RZ\left(\frac{\pi}{2}\right) \cdot X \cdot RZ\left(-\frac{\pi}{2}\right)$$

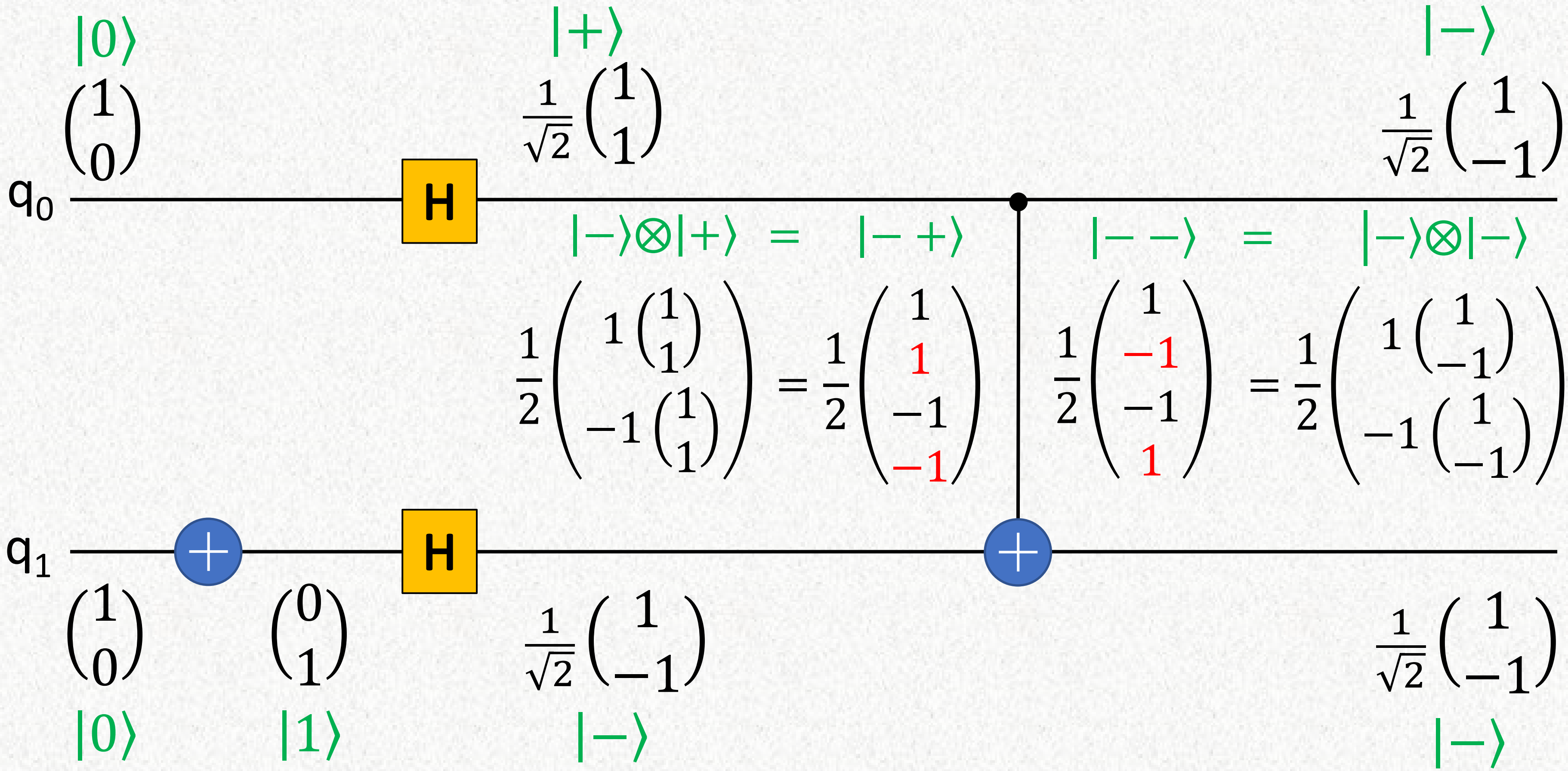
$$Z = RZ(\pi)$$

$$H = RZ\left(\frac{\pi}{2}\right) \cdot \sqrt{X} \cdot RZ\left(\frac{\pi}{2}\right)$$

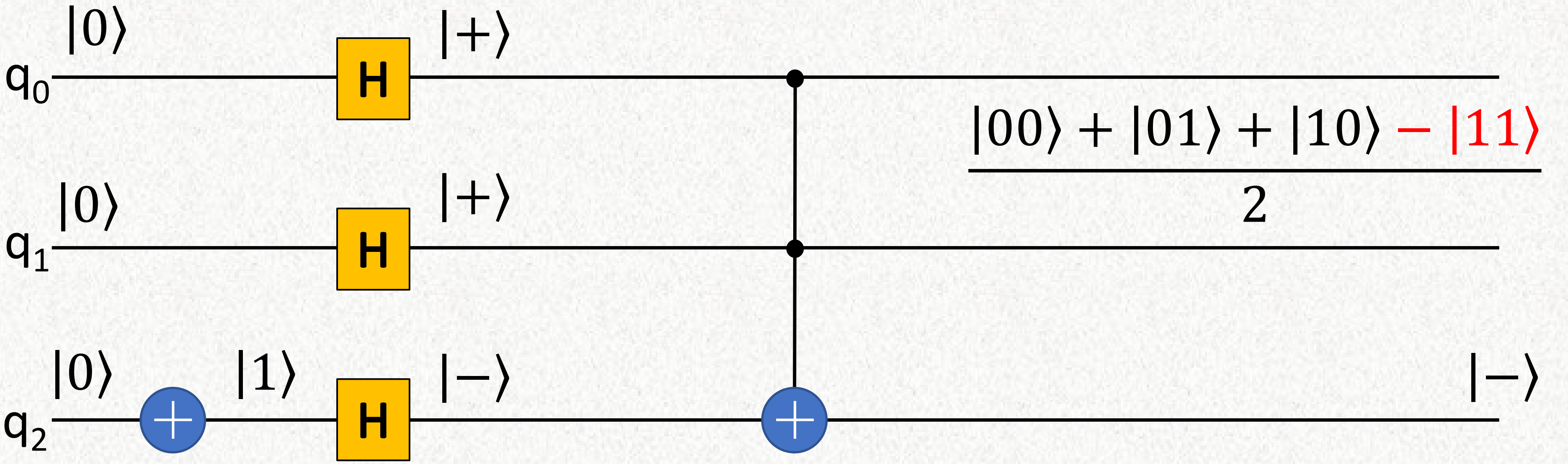
SWAP



Phase Kickback



Phase Kickback



$$|-\rangle \otimes |+\rangle \otimes |+\rangle = |-++\rangle =$$

$$(|000\rangle + |001\rangle + |010\rangle + |011\rangle$$

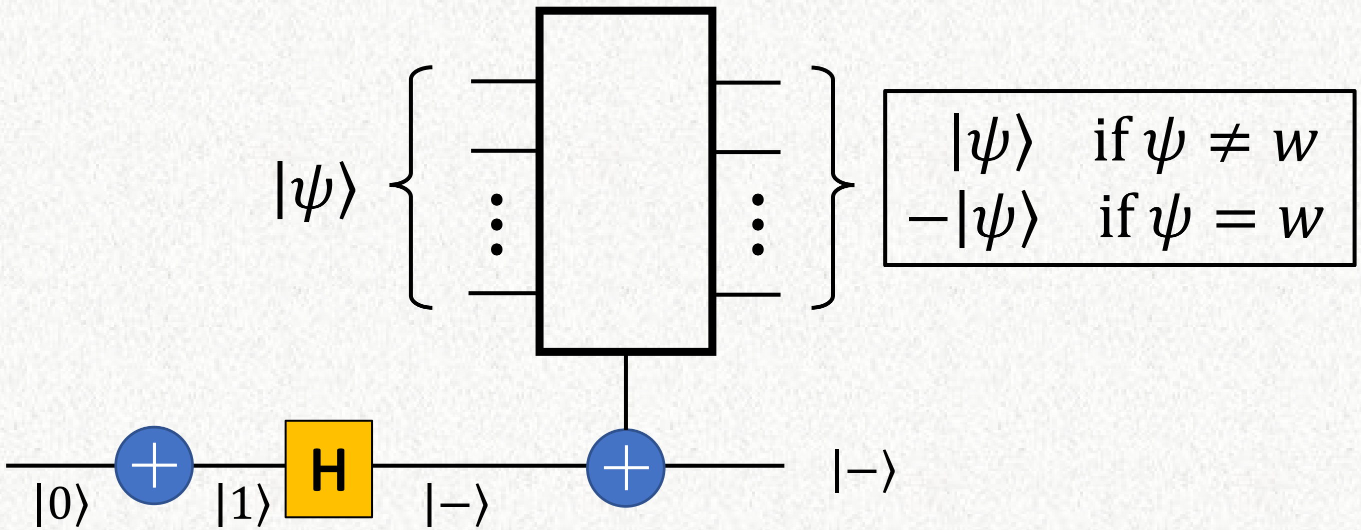
$$- |100\rangle - |101\rangle - |110\rangle - |111\rangle)/\sqrt{8}$$

$$(|000\rangle + |001\rangle + |010\rangle - |011\rangle$$

$$- |100\rangle - |101\rangle - |110\rangle + |111\rangle)/\sqrt{8}$$

$$|-\rangle \otimes (|00\rangle + |01\rangle + |10\rangle - |11\rangle)/2$$

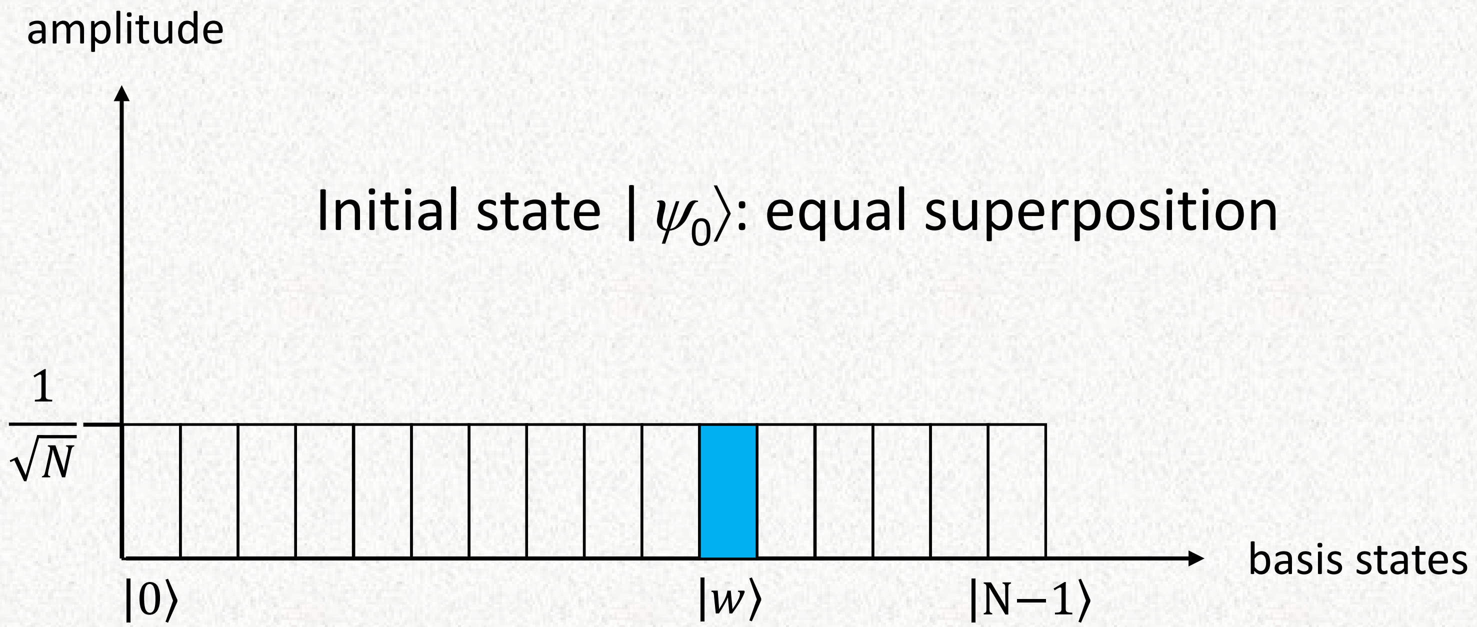
Quantum Oracle: Mark Winner



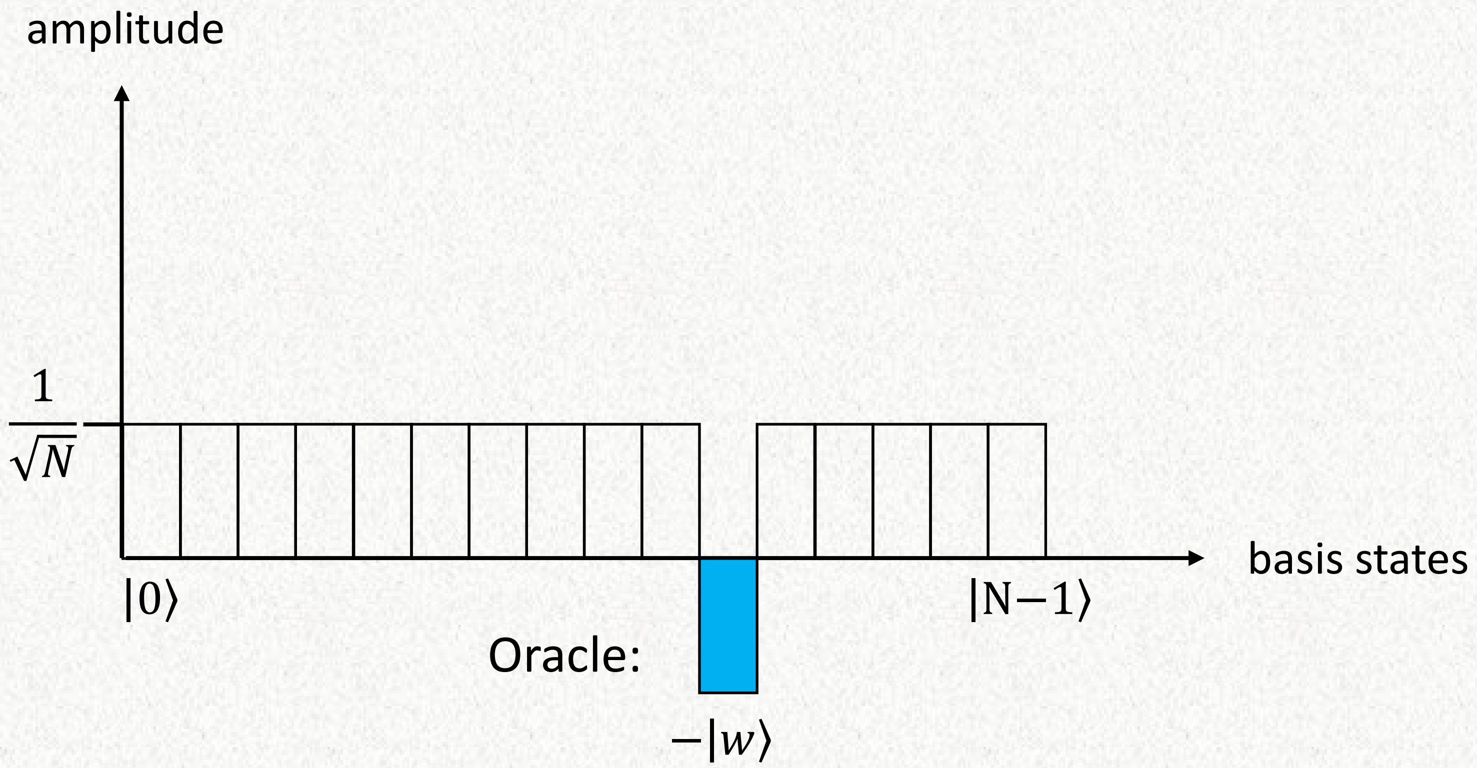
Grover's Algorithm

Search unordered list of N elements in $O\left(\sqrt{N}\right)$

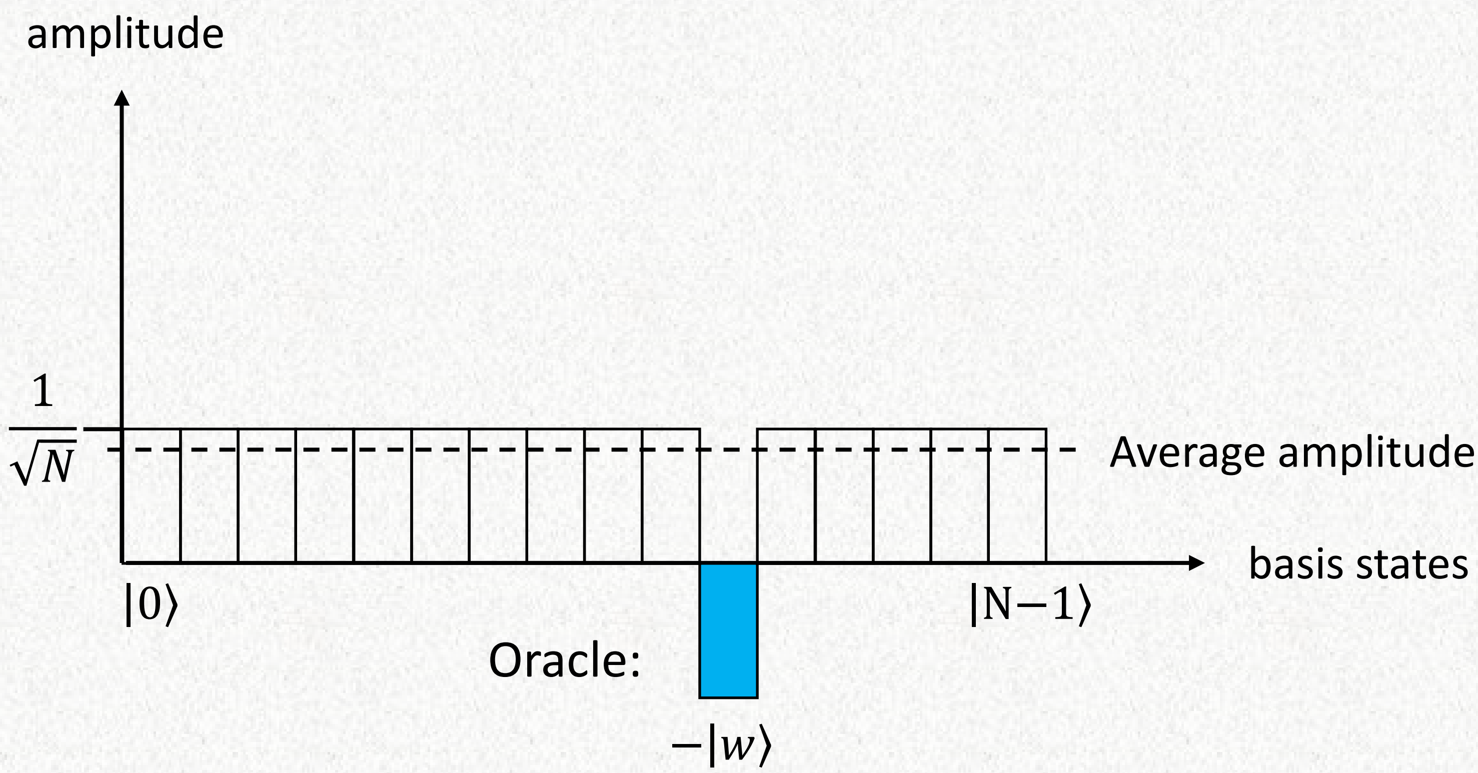
Amplitude Amplification



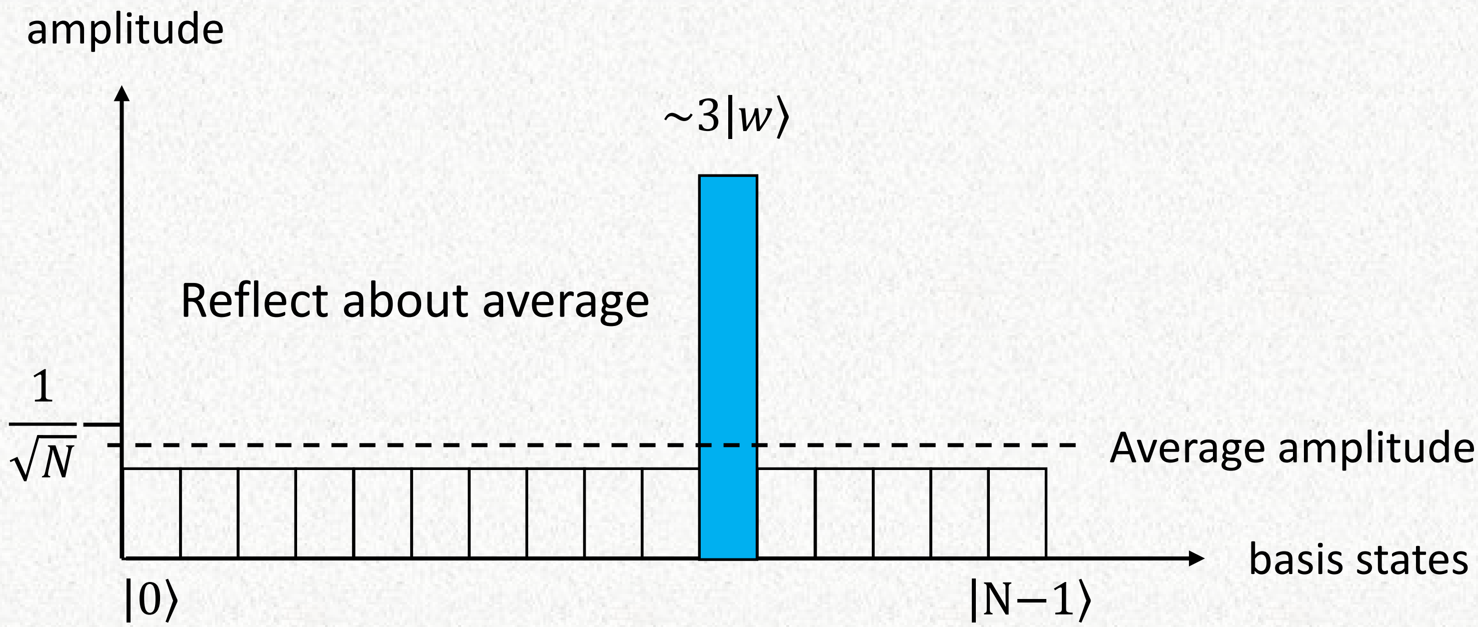
Amplitude Amplification



Amplitude Amplification



Amplitude Amplification



Amplitude Amplification is Unitary

$$A = \frac{1}{N}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

$$\begin{aligned} |\psi'\rangle &= A|\psi\rangle - (|\psi\rangle - A|\psi\rangle) \\ &= (2A - I)|\psi\rangle \end{aligned}$$

$$\begin{aligned} &(2A - I)^\dagger(2A - I) \\ &= \left(2A^\dagger - I^\dagger\right)(2A - I) \\ &= (2A - I)\,(2A - I) \\ &= 4AA - 4AI + I \\ &= 4A - 4A + I \\ &= I \end{aligned}$$

Amplitude Amplification

x_k = amplitude of N-1 non-winning components after iteration *k*
y_k = amplitude of one winning component after iteration *k*

Oracle: $$|\psi_k\rangle = x_k\left(\sum_{i\neq\omega}|i\rangle\right) - y_k|w\rangle$$

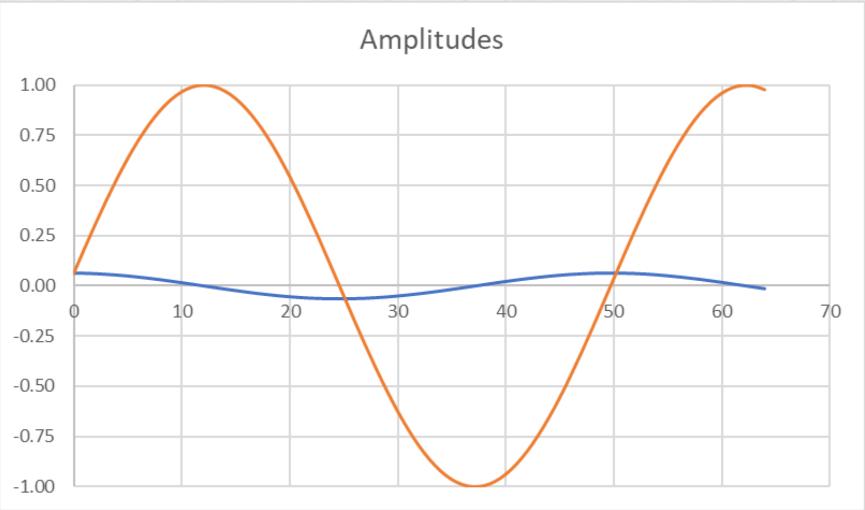
$$A = \frac{(N-1)x_k - y_k}{N}$$

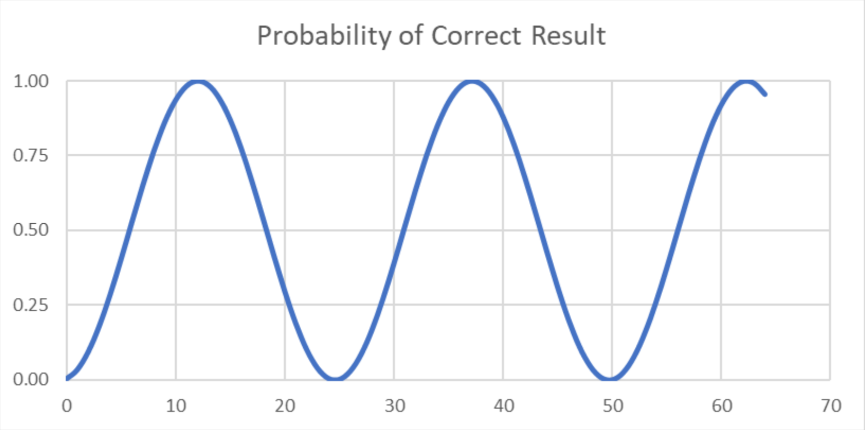
$$x_{k+1} = 2\frac{(N-1)x_k - y_k}{N} - x_k \qquad y_{k+1} = 2\frac{(N-1)x_k - y_k}{N} + y_k$$

$$x_{k+1} = x_k - \frac{2(x_k + y_k)}{N} \qquad y_{k+1} = 2x_k + y_k - \frac{2(x_k + y_k)}{N}$$

Grover: 8 Qubits, N = 256

Iteration	2(x+y)/N	x	y	P(correct)
0		0.0625	0.0625	0.0039
1	0.0010	0.0615	0.1865	0.0348
2	0.0019	0.0596	0.3076	0.0946
3	0.0029	0.0567	0.4239	0.1797
4	0.0038	0.0530	0.5336	0.2847
5	0.0046	0.0484	0.6350	0.4032
6	0.0053	0.0430	0.7264	0.5276
7	0.0060	0.0370	0.8064	0.6503
8	0.0066	0.0304	0.8739	0.7637
9	0.0071	0.0234	0.9277	0.8607
10	0.0074	0.0159	0.9670	0.9352
11	0.0077	0.0083	0.9913	0.9826
12	0.0078	0.0005	1.0000	0.9999
13	0.0078	-0.0074	0.9931	0.9862
14	0.0077	-0.0151	0.9706	0.9422
15	0.0075	-0.0225	0.9331	0.8706
16	0.0071	-0.0296	0.8809	0.7760





Grover: Number of Iterations

$$x_k = \frac{\cos(\omega k + \phi)}{\sqrt{N-1}} \qquad y_k = \sin(\omega k + \phi)$$

$$x_{k+1} = x_k - \frac{2(x_k + y_k)}{N}$$

$$= x_k \frac{N-2}{N} - y_k \frac{2}{N}$$

$$x_{k+1} = \frac{\cos(\omega(k+1) + \phi)}{\sqrt{N-1}}$$

$$= \frac{\cos(\omega k + \phi)\cos(\omega) - \sin(\omega k + \phi)\sin(\omega)}{\sqrt{N-1}}$$

$$= x_k \cos(\omega) - y_k \frac{\sin(\omega)}{\sqrt{N-1}}$$

$$\cos(\omega) = \frac{N-2}{N} \qquad \sin(\omega) = \frac{2\sqrt{N-1}}{N}$$

Grover: Number of Iterations

$$x_k = \frac{\cos(\omega k + \phi)}{\sqrt{N-1}} \qquad y_k = \sin(\omega k + \phi)$$

$$\begin{aligned} y_{k+1} &= 2x_k + y_k - \frac{2(x_k + y_k)}{N} \\ &= x_k \frac{2(N-1)}{N} + y_k \frac{N-2}{N} \end{aligned}$$

$$\begin{aligned} y_{k+1} &= \sin(\omega(k+1) + \phi) \\ &= \sin(\omega k + \phi)\cos(\omega) + \cos(\omega k + \phi)\sin(\omega) \\ &= y_k \cos(\omega) + x_k \sqrt{N-1}\sin(\omega) \end{aligned}$$

$$\cos(\omega) = \frac{N-2}{N} \qquad \sin(\omega) = \frac{2\sqrt{N-1}}{N}$$

Grover: Number of Iterations

$$\cos(\omega) = \frac{N-2}{N} \qquad \sin(\omega) = \frac{2\sqrt{N-1}}{N}$$

$$\sin\left(\frac{\omega}{2}\right) = \sqrt{\frac{1-\cos(\omega)}{2}}$$

$$= \sqrt{\frac{1-\frac{N-2}{N}}{2}}$$

$$= \frac{1}{\sqrt{N}}$$

$$\omega = 2\sin^{-1}\left(\frac{1}{\sqrt{N}}\right)$$

Grover: Number of Iterations

$$x_k = \frac{\cos(\omega k + \phi)}{\sqrt{N-1}} \qquad y_k = \sin(\omega k + \phi)$$

$$x_0 = y_0$$

$$\frac{\cos(\phi)}{\sqrt{N-1}} = \sin(\phi)$$

$$\frac{1 - \sin^2(\phi)}{N-1} = \sin^2(\phi)$$

$$\sin^2(\phi) = \frac{1}{N}$$

$$\phi = \sin^{-1}\left(\frac{1}{\sqrt{N}}\right) = \frac{\omega}{2}$$

Grover: Number of Iterations

$$y_k = \sin(\omega k + \phi)$$

$$= \sin\left(\omega k + \frac{\omega}{2}\right)$$

$$= \sin\left[\omega\left(k + \frac{1}{2}\right)\right]$$

$$\omega\left(k + \frac{1}{2}\right) \approx \frac{\pi}{2}$$

$$2\sin^{-1}\left(\frac{1}{\sqrt{N}}\right)\left(k + \frac{1}{2}\right) \approx \frac{\pi}{2}$$

$$k = \text{round}\left(\frac{\pi}{4\sin^{-1}\left(\frac{1}{\sqrt{N}}\right)} - \frac{1}{2}\right)$$

$$\left\lfloor\frac{\pi}{4\sin^{-1}\left(\frac{1}{\sqrt{N}}\right)}\right\rfloor$$

$$\approx \left\lfloor\frac{\pi}{4}\sqrt{N}\right\rfloor$$

Amplitude Amplification Circuit

$$A = \frac{1}{N}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

$$= \frac{1}{N}\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}$$

$$= |\psi_0\rangle\langle\psi_0|$$

Amplitude Amplification Circuit

$$2A - I$$

$$2|\psi_0\rangle\langle\psi_0| - I$$

$$2\left(H^{\otimes n}|0^{\otimes n}\rangle\right)\left(\langle 0^{\otimes n}|H^{\otimes n}\right) - I$$

$$H^{\otimes n}\left(2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I\right)H^{\otimes n}$$

$$H^{\otimes n}\left[2\left(X^{\otimes n}|1^{\otimes n}\rangle\right)\left(\langle 1^{\otimes n}|X^{\otimes n}\right) - I\right]H^{\otimes n}$$

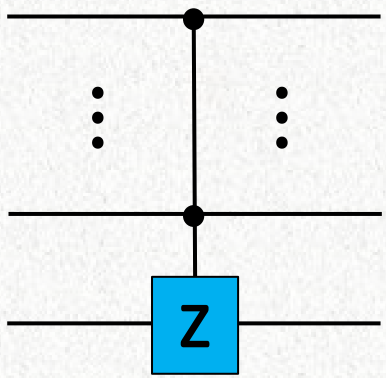
$$H^{\otimes n}X^{\otimes n}\left(2|1^{\otimes n}\rangle\langle 1^{\otimes n}| - I\right)X^{\otimes n}H^{\otimes n}$$

Amplitude Amplification Circuit

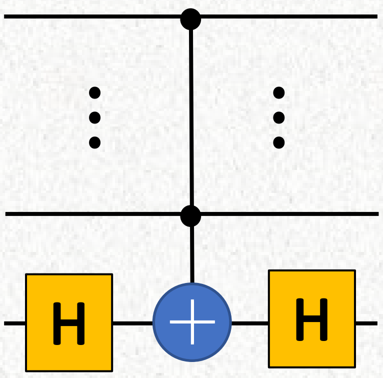
$$2\left|1^{\otimes n}\right\rangle\!\left\langle 1^{\otimes n}\right| - I$$

$$2\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = -\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{pmatrix}$$

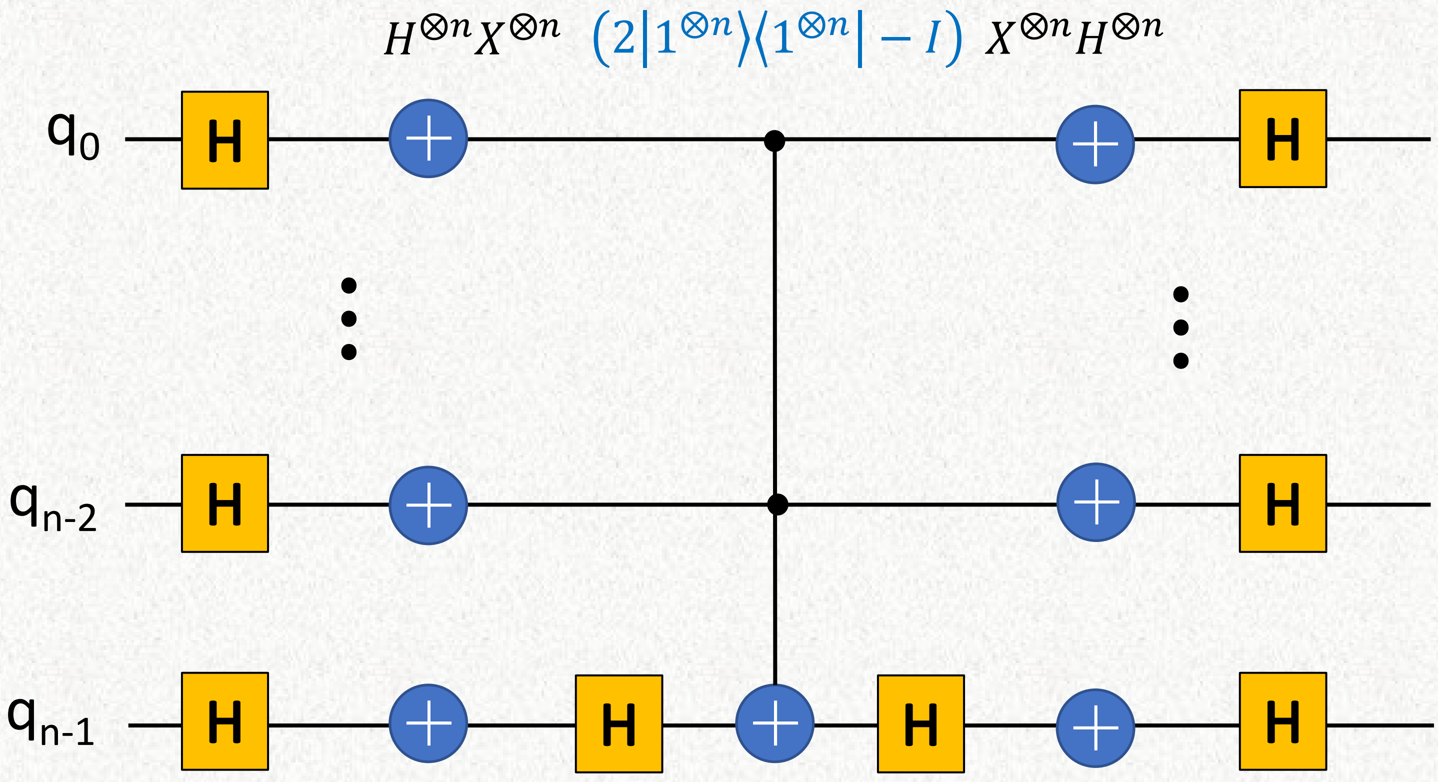
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



$$Z = HXH$$

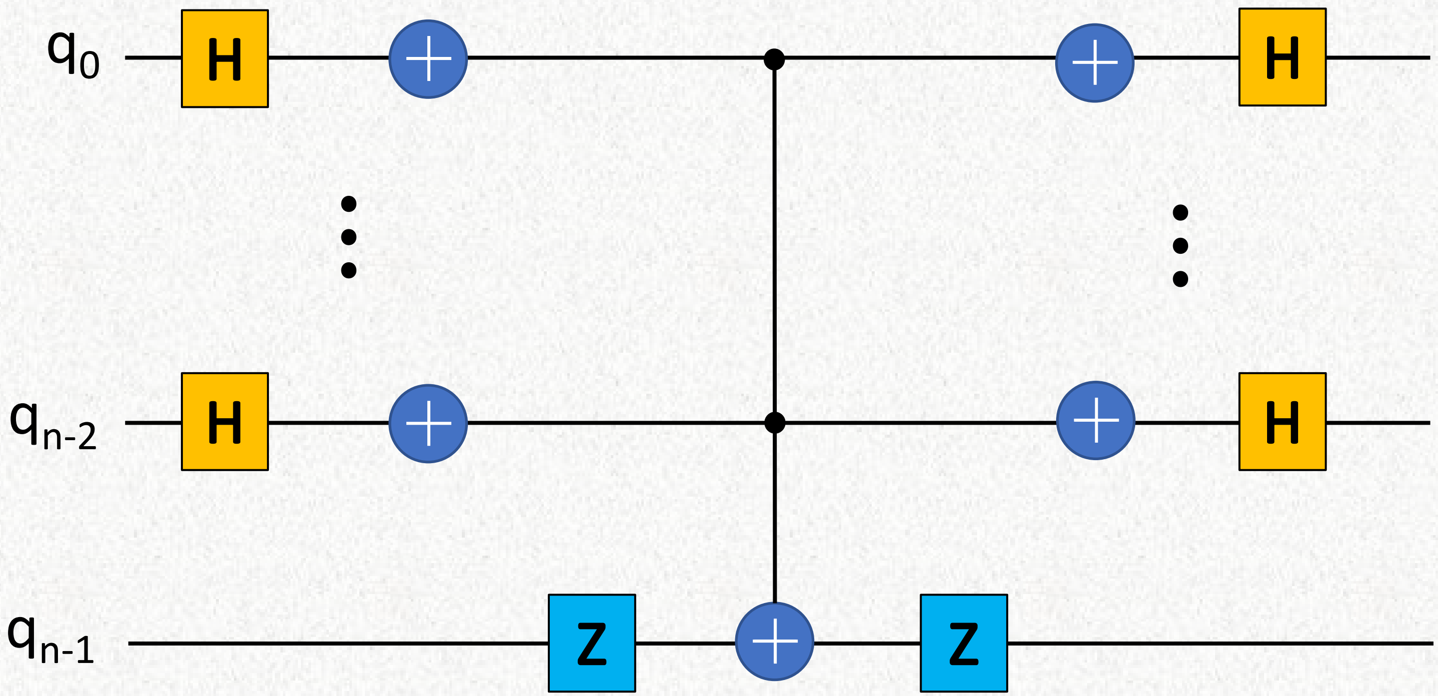


Amplitude Amplification Circuit

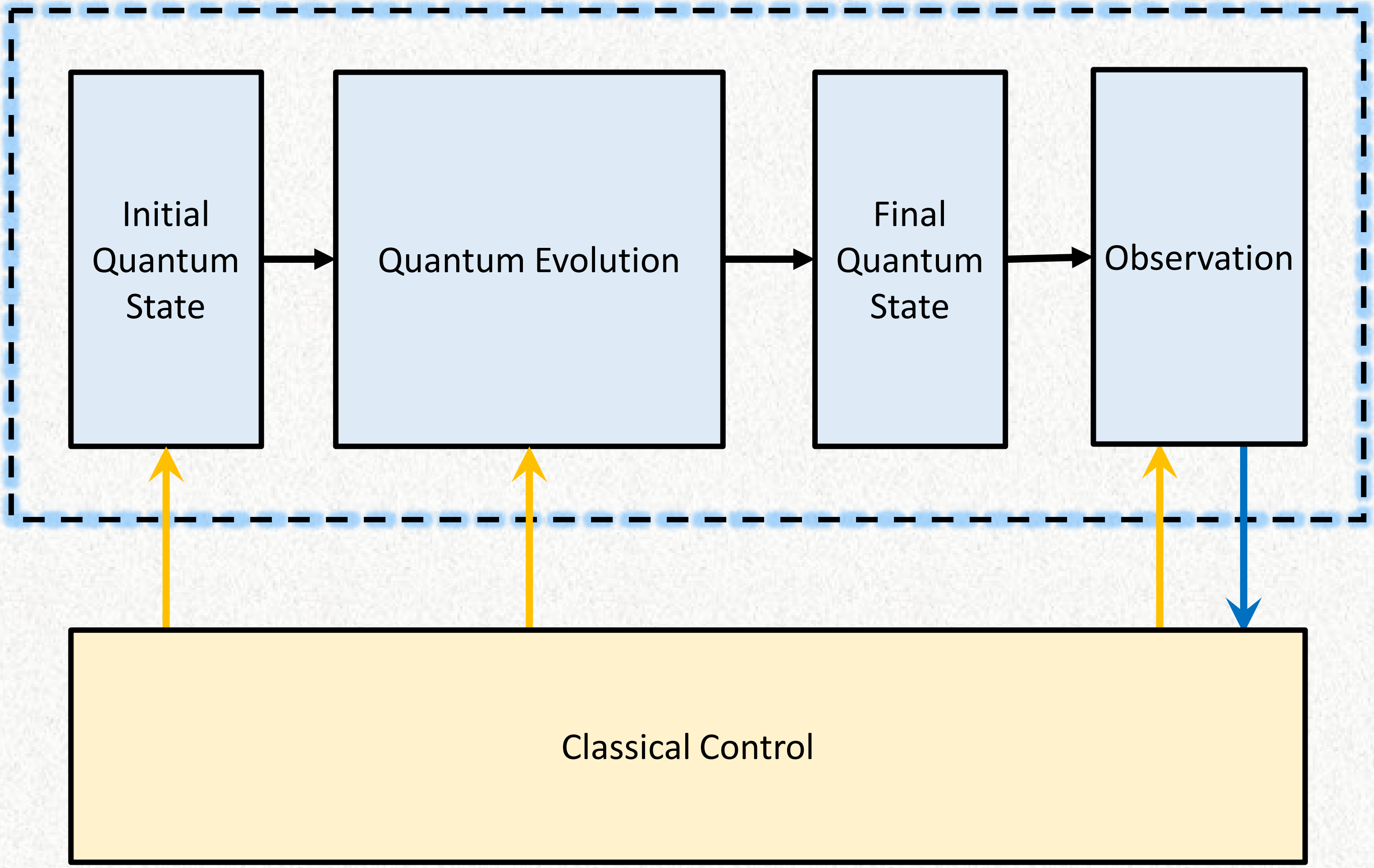


Amplitude Amplification Circuit

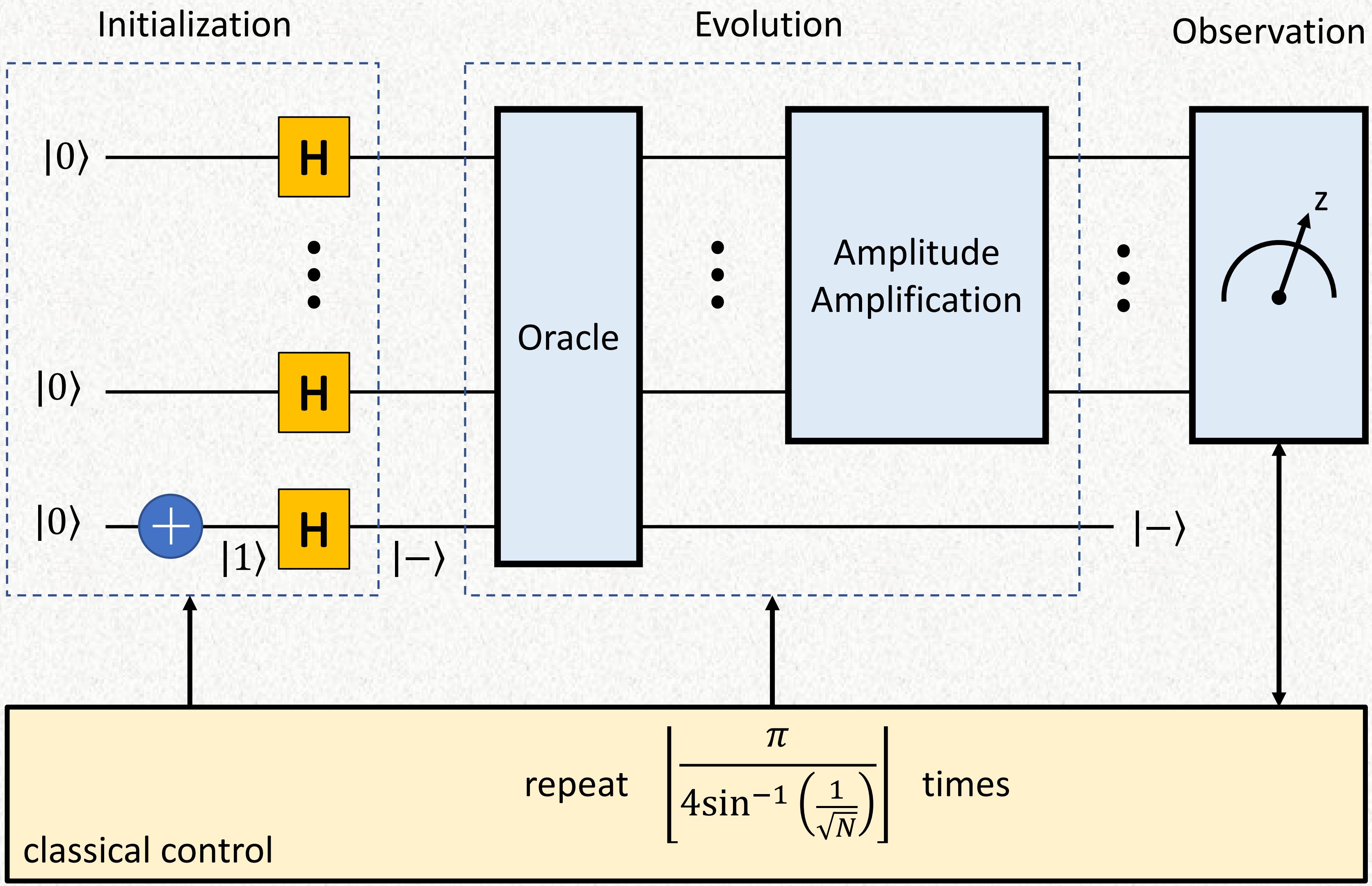
$$H^{\otimes n} X^{\otimes n} \quad \left(2|1^{\otimes n}\rangle\langle 1^{\otimes n}| - I\right) \quad X^{\otimes n} H^{\otimes n}$$



A Quantum Computer



Grover


Initialization
Evolution
Observation
$|0\rangle$
H
$|0\rangle$
H
$|0\rangle$
$|1\rangle$
H
$|-\rangle$
Oracle
Amplitude Amplification
$|-\rangle$
z
repeat $\left\lfloor \frac{\pi}{4\sin^{-1}\left(\frac{1}{\sqrt{N}}\right)} \right\rfloor$ times
classical control

Quantum Observation

Rules

- Every observable has associated Hermitian $H = H^\dagger$
- H has real eigenvalues and orthonormal eigenvectors
- Observation chooses eigenvector/eigenvalue pair
- Probability of choice $|e\rangle$,λ in state $|\psi\rangle$ is length squared of projection of $|e\rangle$ onto $|\psi\rangle$
- Measurement is λ
- $|\psi\rangle$ collapses to $|e\rangle$

Z Measurement Basis

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

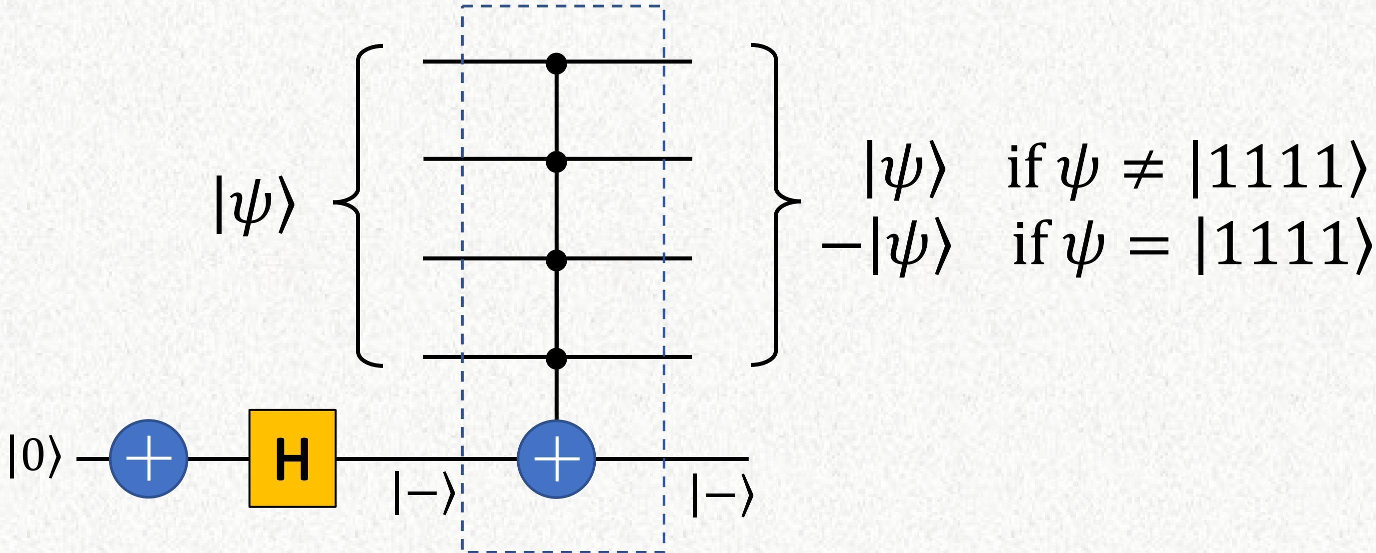
eigenvalue	eigenvector
1	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
-1	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Measurement & Collapse of Entangled State

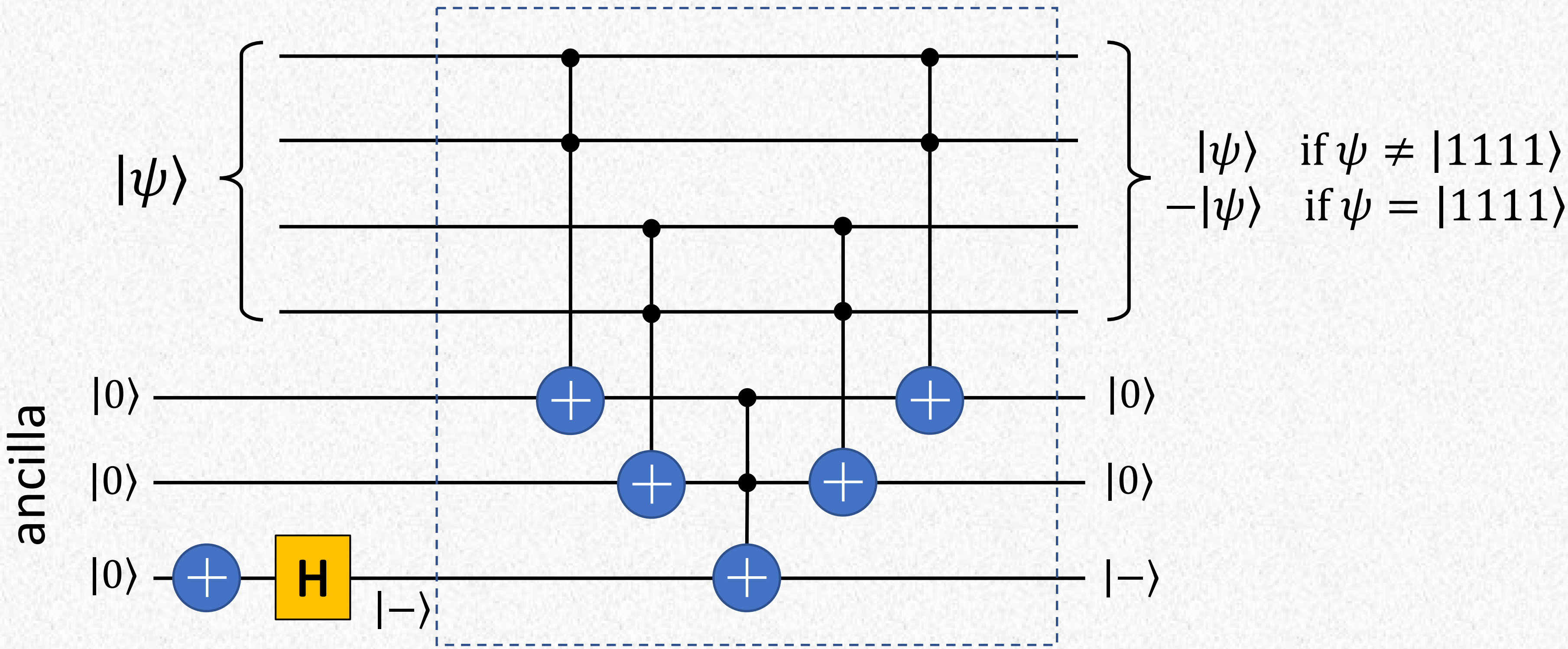
basis	initial amplitude	Measure qubit 0	
		P(0) = 2/3	P(1) = 1/3
$\lvert 000\rangle$	0	0	0
$\lvert 001\rangle$	$1/\sqrt{3}$	0	1
$\lvert 010\rangle$	$1/\sqrt{3}$	$1/\sqrt{2}$	0
$\lvert 011\rangle$	0	0	0
$\lvert 100\rangle$	$1/\sqrt{3}$	$1/\sqrt{2}$	0
$\lvert 101\rangle$	0	0	0
$\lvert 110\rangle$	0	0	0
$\lvert 111\rangle$	0	0	0

Testing Grover

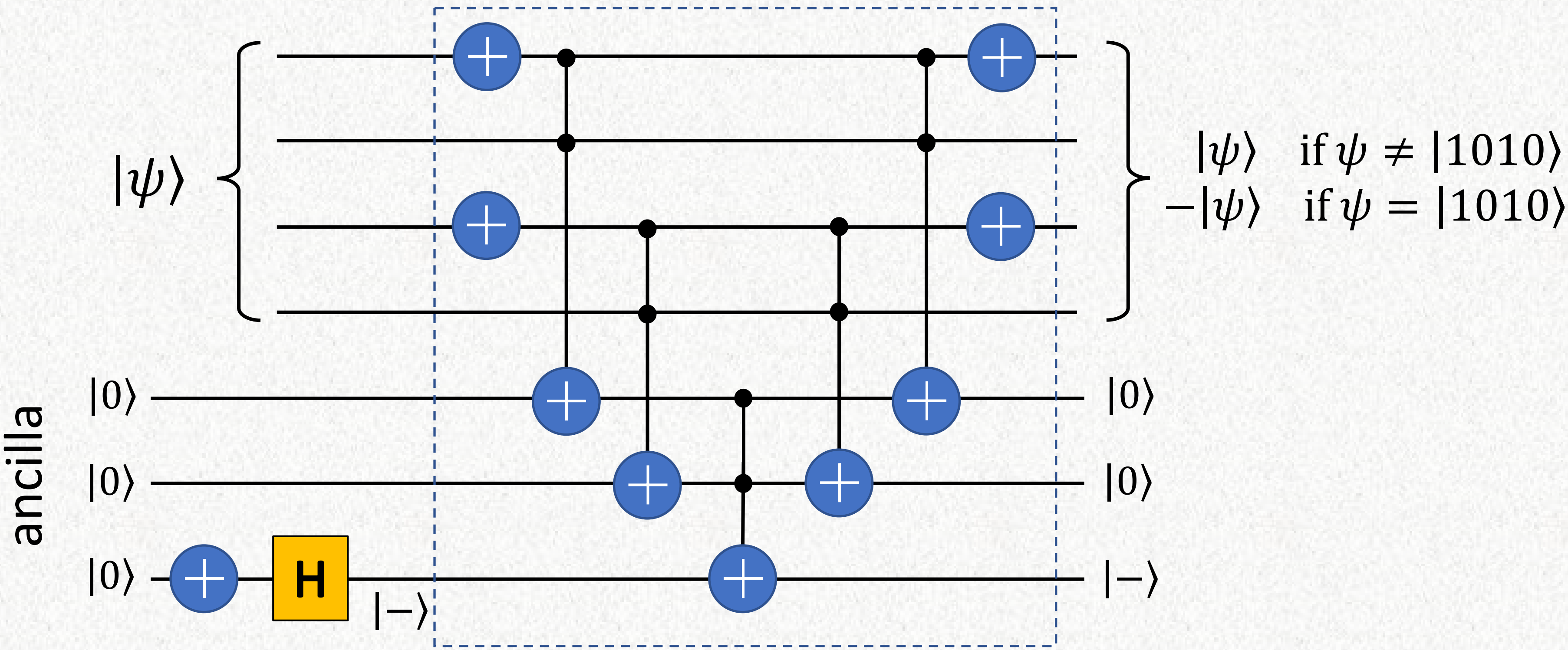
4-Qubit Test Oracle



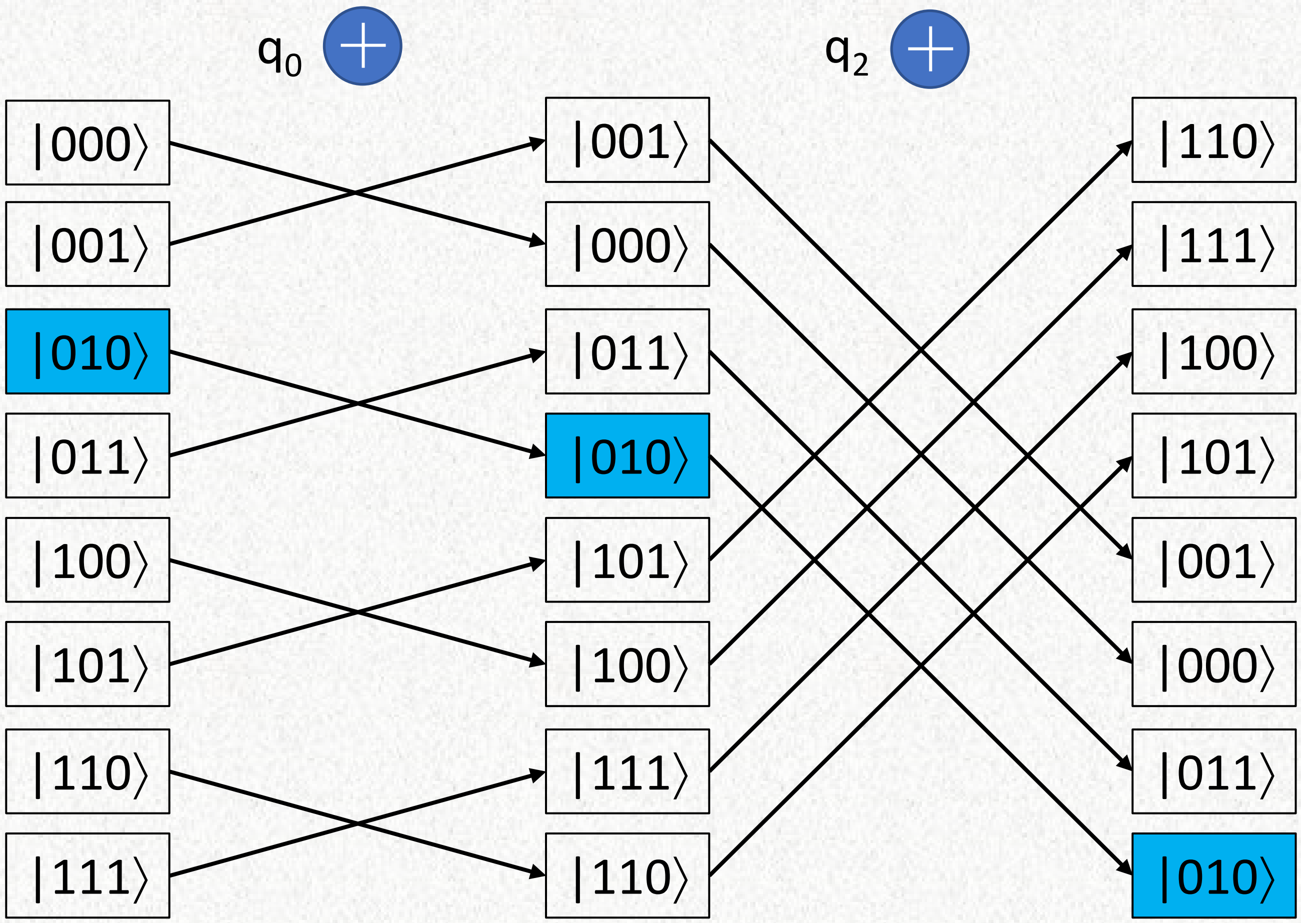
4-Qubit Test Oracle



4-Qubit Test Oracle



Select $|010\rangle$



Visual Studio Demo

- Python code
  - Multi-X
  - Oracle
  - Grover
  - scaffolding
- Circuit display
- Simulation various N
- Simulation with noise model

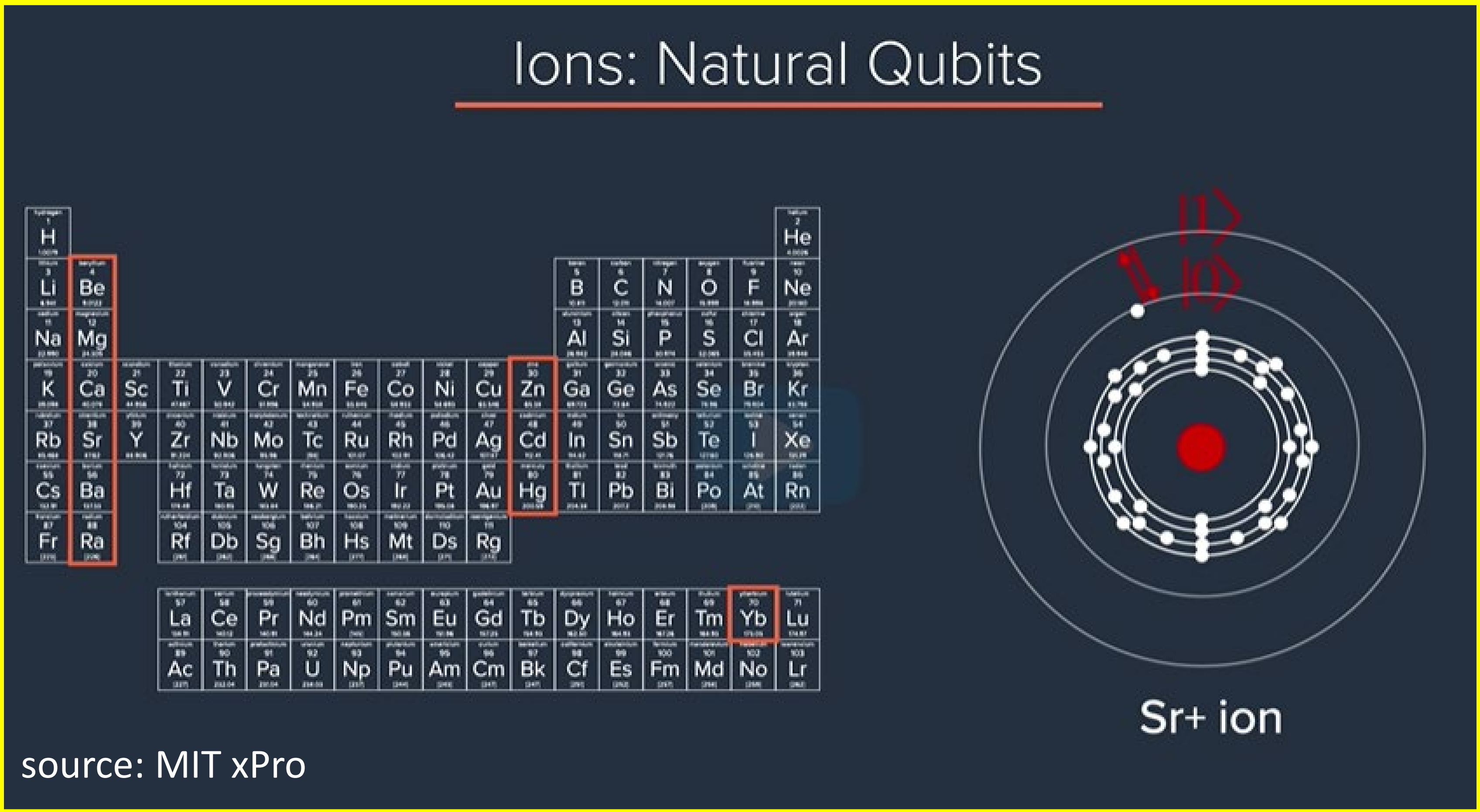
Grover Results

Grover Parameters				Probability of Correct Result			
Qubits	Winner	N	Iters	Theory	Sim	Sim w/noise	Real Hardware
2	00	4	1	1.000	1.000	0.854[1]	0.884[1]
3	101	8	2	0.945	0.943	0.376[1]	0.200[1]
4	0101	16	3	0.961	0.961	0.056[2]	
6	101010	64	6	0.997	0.998	0.016[2]	
8	01010101	256	12	1.000	1.000		

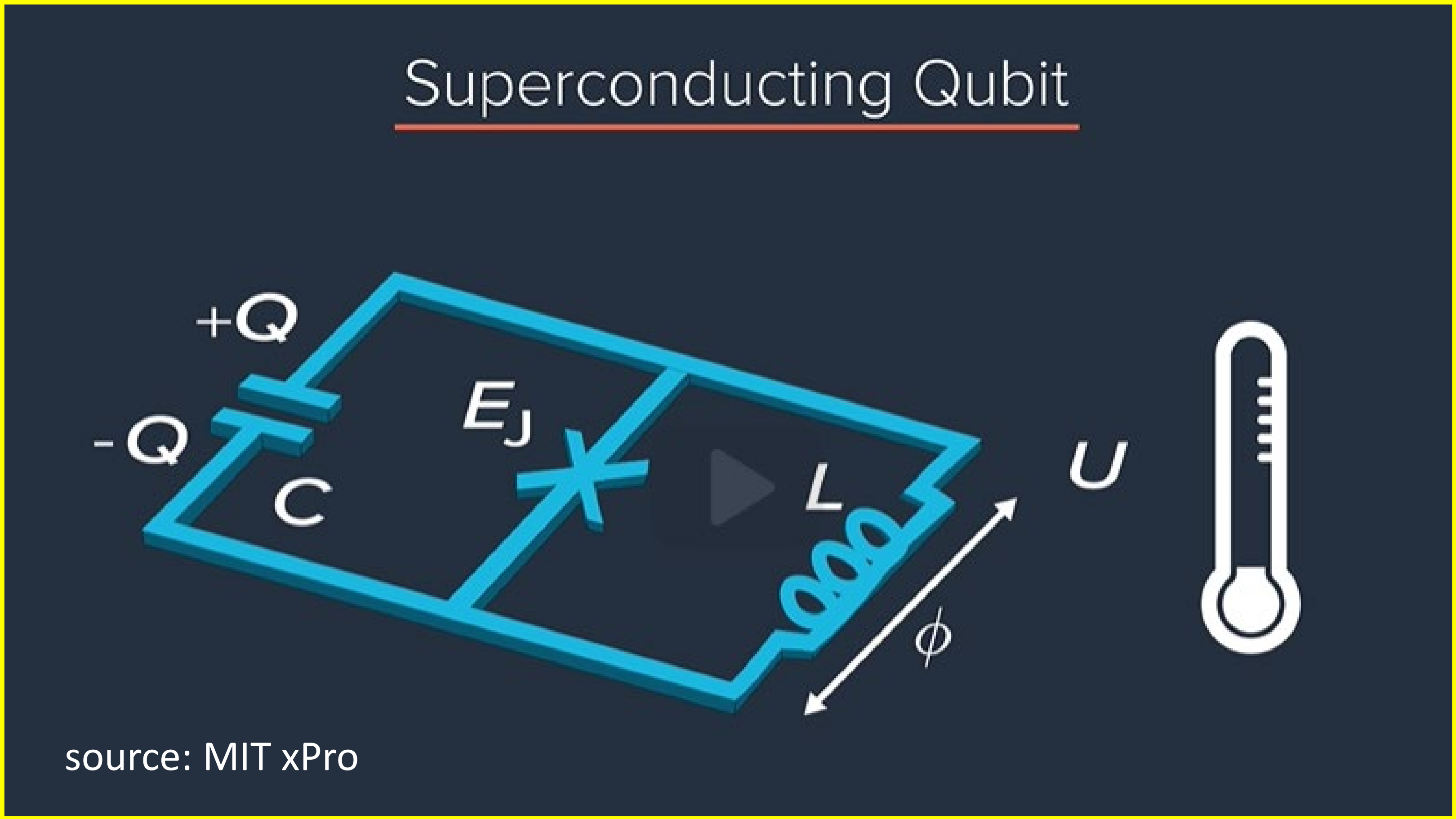
[1]Santiago QV32
[2]Melbourne QV16

Real Hardware

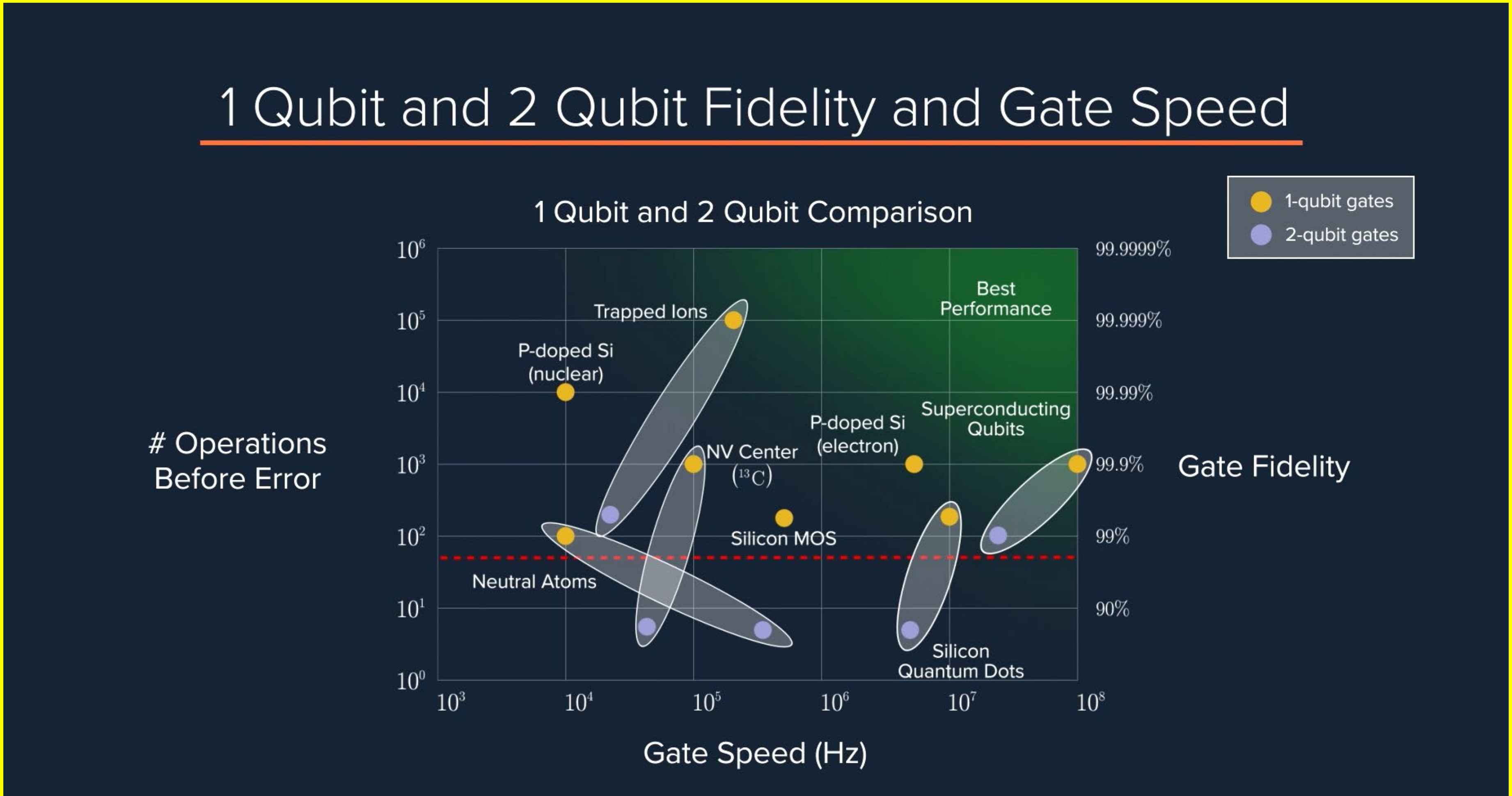
Trapped Ion Qubits



Superconducting Qubits



Qubit Comparisons



source: MIT xPro

IBM Quantum Computer

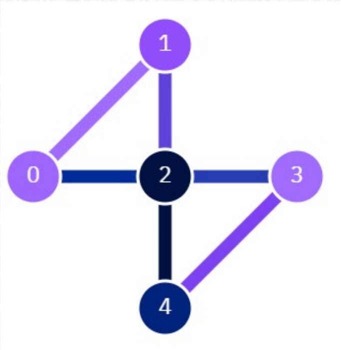
IBM Quantum Experience Demo

- Circuit composer
  - Bell state
  - QASM
- Grover job result
  - histogram
  - circuits: original, transpiled
  - QASM
- ibmq_santiago & ibmq_manhattan
  - basis gates
  - topology
  - graph view

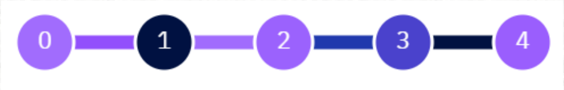
IBMQ Machine Summary

machine	qubits	QV	Gate time (μs)	T1 (μs)	T2 (μs)	CX error %
Yorktown	5	8	0.462	48	37	1.89
Santiago	5	32	0.471	115	86	0.67
Montreal	27	128	0.424	104	82	1.40

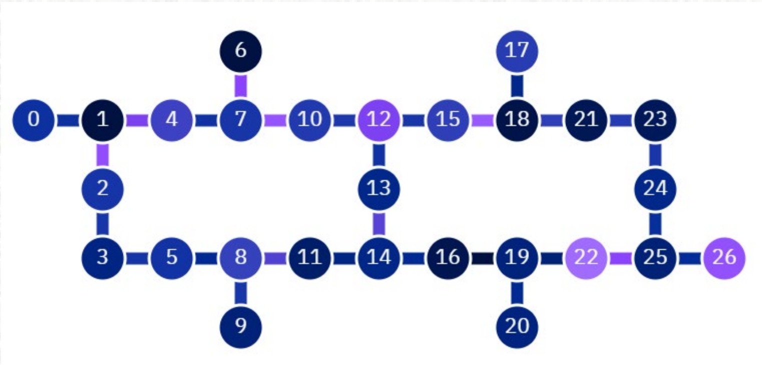
Yorktown



Santiago



Montreal



Quantum Threshold Theorem

- “A quantum computer with a physical error rate below a certain threshold can, through application of quantum error correction schemes, suppress the logical error rate to arbitrarily low levels.”[1]
- Make a reliable logical qubit from a flock of unreliable physical qubits
- Current estimates: >1000 physical qubits needed to make one reliable logical qubit

[1] https://en.wikipedia.org/wiki/Quantum_threshold_theorem