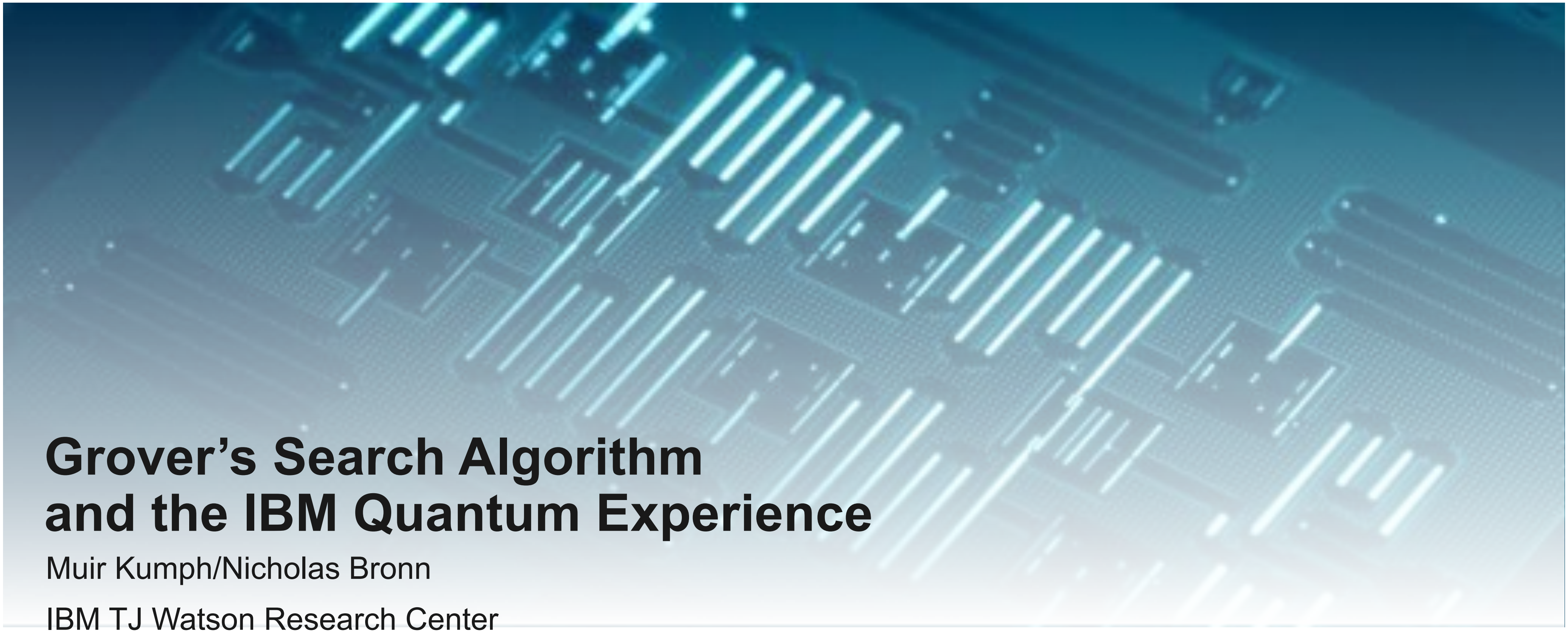


Grover's Search Algorithm and the IBM Quantum Experience

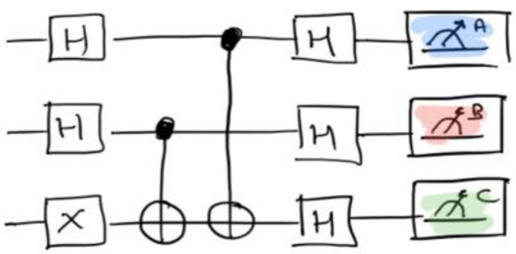
Muir Kumph/Nicholas Bronn

IBM TJ Watson Research Center

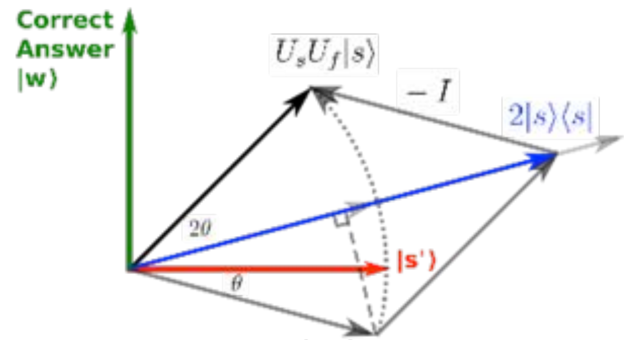
NYC Quantum Computing Meetup
February 28, 2018

Overview

Introduction



Building Quantum Circuits

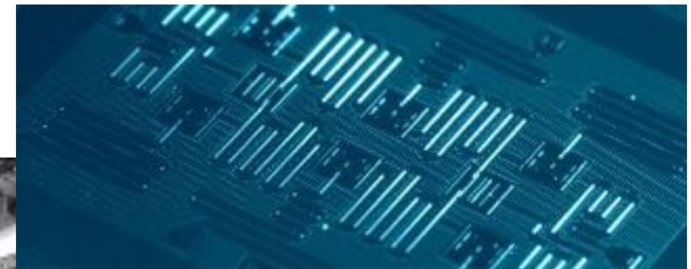


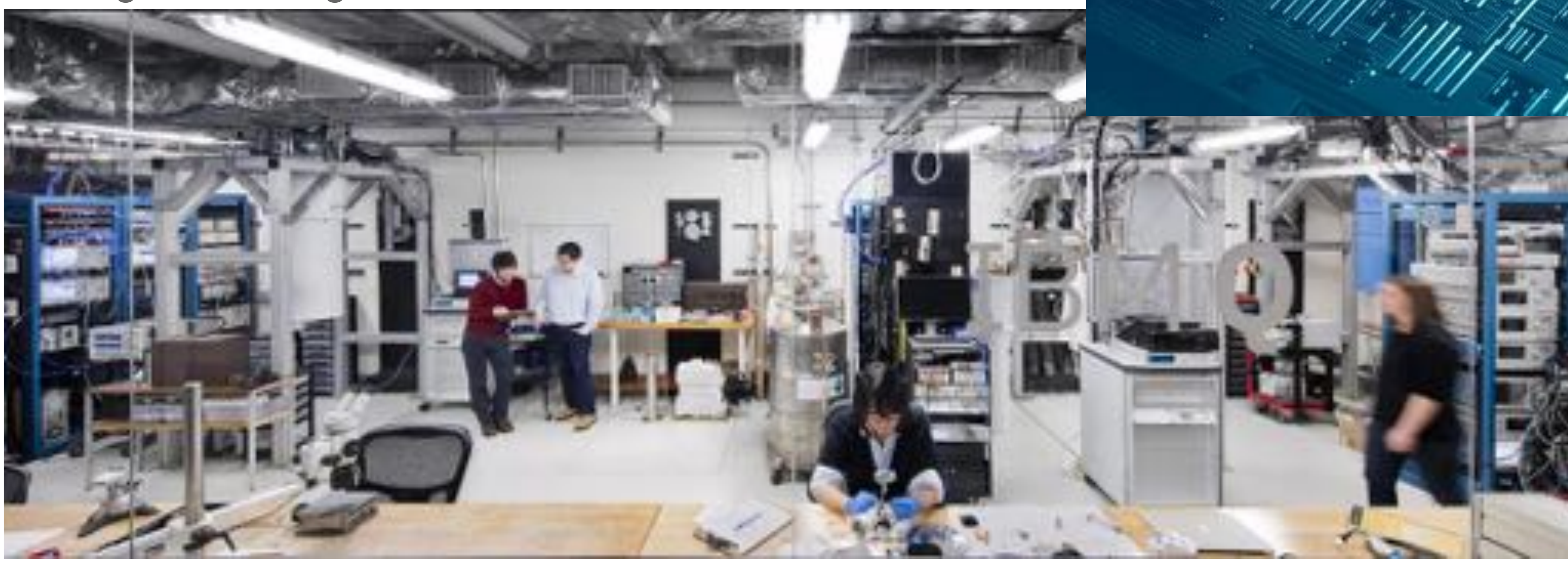
Geometric picture of Grover's algorithm

Demonstration of Grover's algorithm on IBM QE

Introduction

- Research Staff Member in the Experimental Quantum Computing Group at IBM
- Experiments involve superconducting quantum computing and
  - Integrating larger numbers of qubits
  - Fast qubit measurement and feedback
  - Among other things!





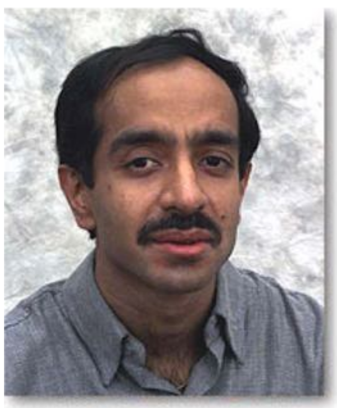
Feynman 1980

Feynman 1980

Shor 1994

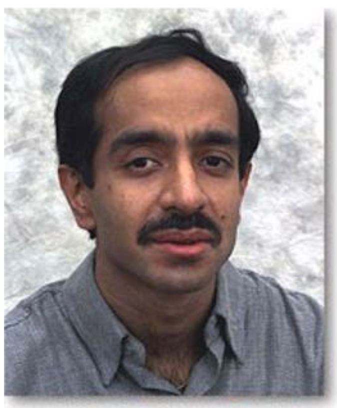

Feynman 1980


Shor 1994


Grover 1996


Feynman 1980


Shor 1994

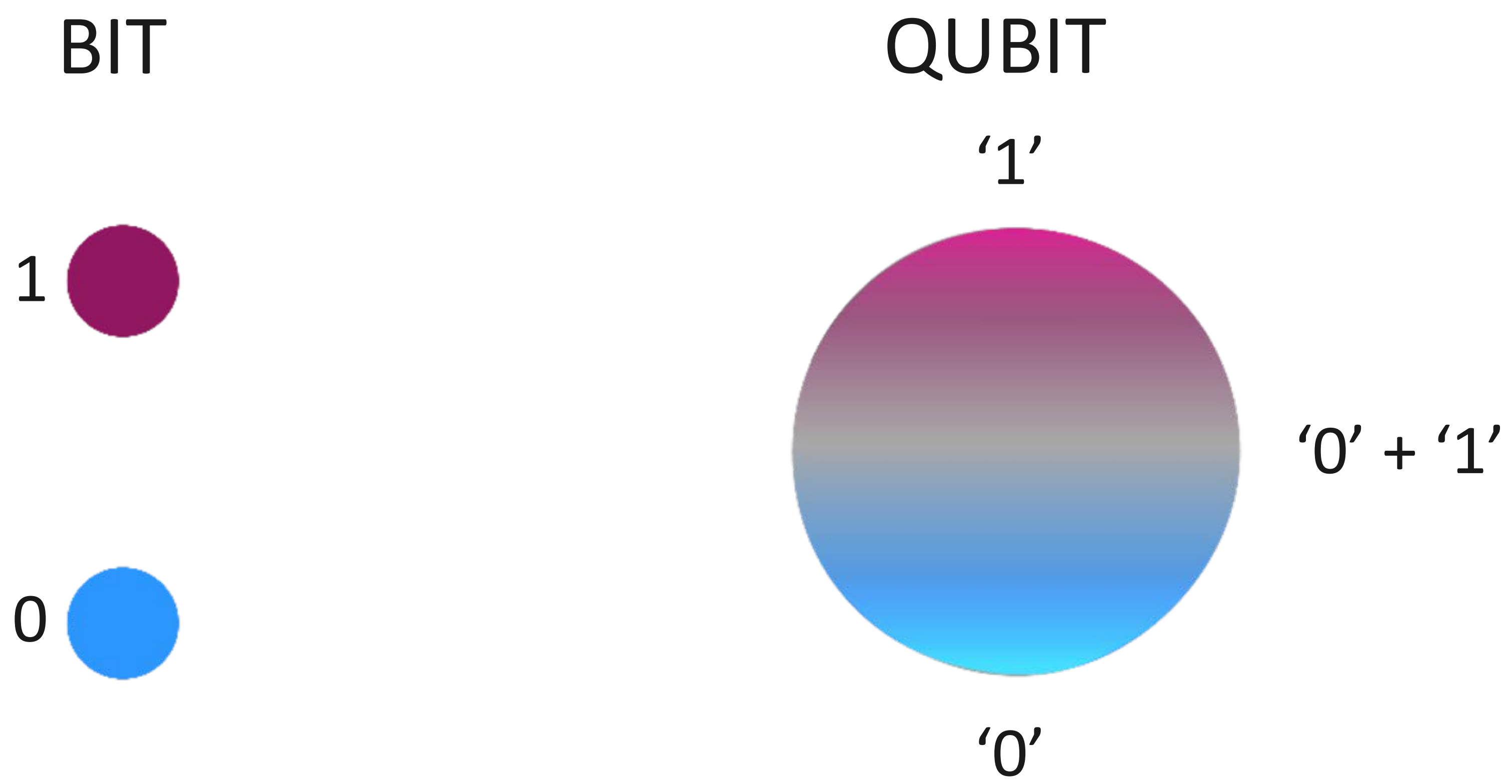

Grover 1996

2017

Grover's Search Algorithm

- One of the key algorithms for quantum computers
- Unstructured Search of N elements
  – Classical computer ~ N/2
  – Quantum computer ~ √N
- Not exponential speedup, but enough to matter for
  – Big Data applications
  – Subroutine for other quantum algorithms
- Requires two key ingredients that use *superposition* and *interference*
  – Oracle
  – Amplitude Amplification

Classical vs Quantum Bits



Qubit State and Measurement

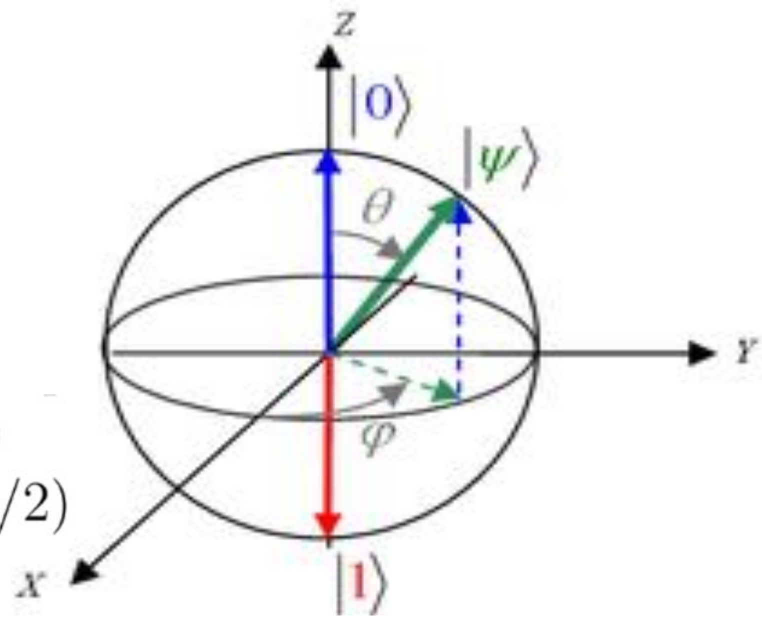
- General qubit state is a *superposition*

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

Qubit State and Measurement

- General qubit state is a *superposition*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \begin{array}{l}\alpha = \cos(\theta/2)\\ \beta = e^{i\phi}\sin(\theta/2)\end{array}$$



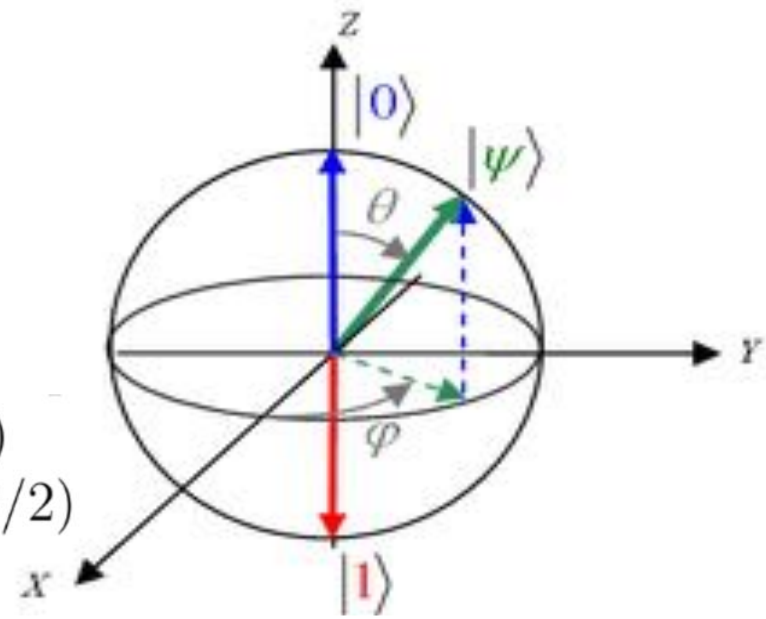
Bloch Sphere

- Amplitudes have relative phase => *interference*
- Qubit operations (using microwave pulses) rotate the state

Qubit State and Measurement

- General qubit state is a *superposition*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha = \cos(\theta/2) \quad \beta = e^{i\phi}\sin(\theta/2)$$



Bloch Sphere

- Amplitudes have relative phase => *interference*
- Qubit operations (using microwave pulses) rotate the state
- Qubit Measurement

Pre-measurement state: $\alpha|0\rangle + \beta|1\rangle$ → Possible outcomes:

- |0> with probability $|\alpha|^2$
- |1> with probability $|\beta|^2$

The Oracle and Amplitude Amplification

- **Black box** that recognizes something when it sees it

The Oracle and Amplitude Amplification

- **Black box** that recognizes something when it sees it
- Distinction between *verification* and *knowing*

  - Testing whether a key opens a door vs breaking the lock

The Oracle and Amplitude Amplification

- **Black box** that recognizes something when it sees it
- Distinction between *verification* and *knowing*

  - Testing whether a key opens a door vs breaking the lock
- Encode a list of stuff in binary and define function f s.t.
  - $f(x) = 0$ when wrong answer
  - $f(w) = 1$ when correct answer (winner!)

The Oracle and Amplitude Amplification

- **Black box** that recognizes something when it sees it
- Distinction between *verification* and *knowing*
  - Testing whether a key opens a door vs breaking the lock

- Encode a list of stuff in binary and define function f s.t.
  - $f(x) = 0$ when wrong answer
  - $f(w) = 1$ when correct answer (winner!)
- Oracle will act on superposition of all states

The Oracle and Amplitude Amplification

- **Black box** that recognizes something when it sees it
- Distinction between *verification* and *knowing*
  - Testing whether a key opens a door vs breaking the lock
- Encode a list of stuff in binary and define function f s.t.
  - $f(x) = 0$ when wrong answer
  - $f(w) = 1$ when correct answer (winner!)
- Oracle will act on superposition of all states
- Oracle is quantum operation U_f that performs

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

The Oracle and Amplitude Amplification

- **Black box** that recognizes something when it sees it
- Distinction between *verification* and *knowing*
  - Testing whether a key opens a door vs breaking the lock

- Encode a list of stuff in binary and define function f s.t.
  - $f(x) = 0$ when wrong answer
  - $f(w) = 1$ when correct answer (winner!)
- Oracle will act on superposition of all states
- Oracle is quantum operation U_f that performs

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

Index	State
1	$\|00\rangle$
2	$\|01\rangle$
3	$\|10\rangle$
4	$\|11\rangle$

The Oracle and Amplitude Amplification

- **Black box** that recognizes something when it sees it
- Distinction between *verification* and *knowing*
  - Testing whether a key opens a door vs breaking the lock

- Encode a list of stuff in binary and define function f s.t.
  - $f(x) = 0$ when wrong answer
  - $f(w) = 1$ when correct answer (winner!)
- Oracle will act on superposition of all states
- Oracle is quantum operation U_f that performs

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

Index	State	Oracle
1	$\|00\rangle$	$\|00\rangle$
2	$\|01\rangle$	$\|01\rangle$
3	$\|10\rangle$	$-\|10\rangle$
4	$\|11\rangle$	$\|11\rangle$

The Oracle and Amplitude Amplification

- **Black box** that recognizes something when it sees it
- Distinction between *verification* and *knowing*
  
  - Testing whether a key opens a door vs breaking the lock
- Encode a list of stuff in binary and define function f s.t.
  - $f(x) = 0$ when wrong answer
  - $f(w) = 1$ when correct answer (winner!)
- Oracle will act on superposition of all states
- Oracle is quantum operation U_f that performs

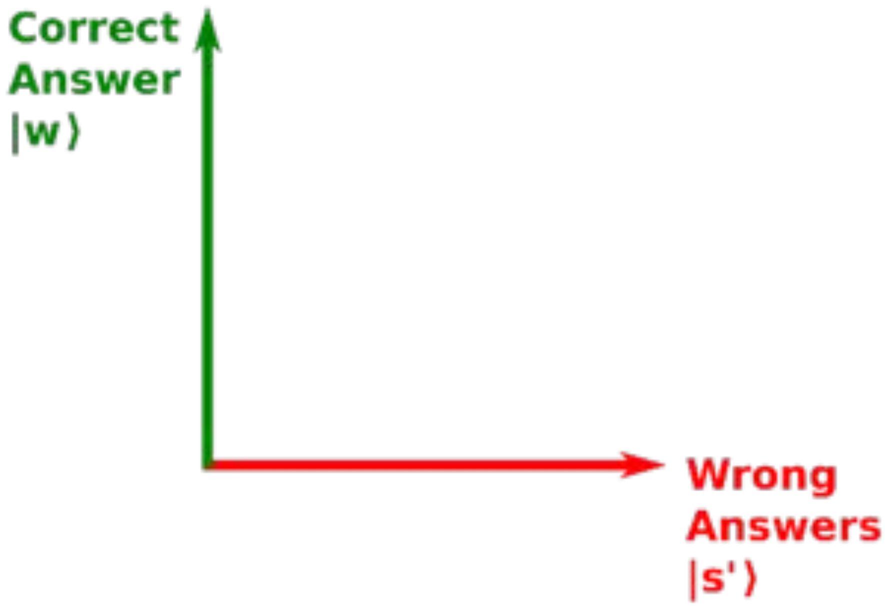
$$|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$$

- **Amplitude Amplification**
  - Use interference to increase likelihood of measuring correct index

Index	State	Oracle
1	$\|00\rangle$	$\|00\rangle$
2	$\|01\rangle$	$\|01\rangle$
3	$\|10\rangle$	$-\|10\rangle$
4	$\|11\rangle$	$\|11\rangle$

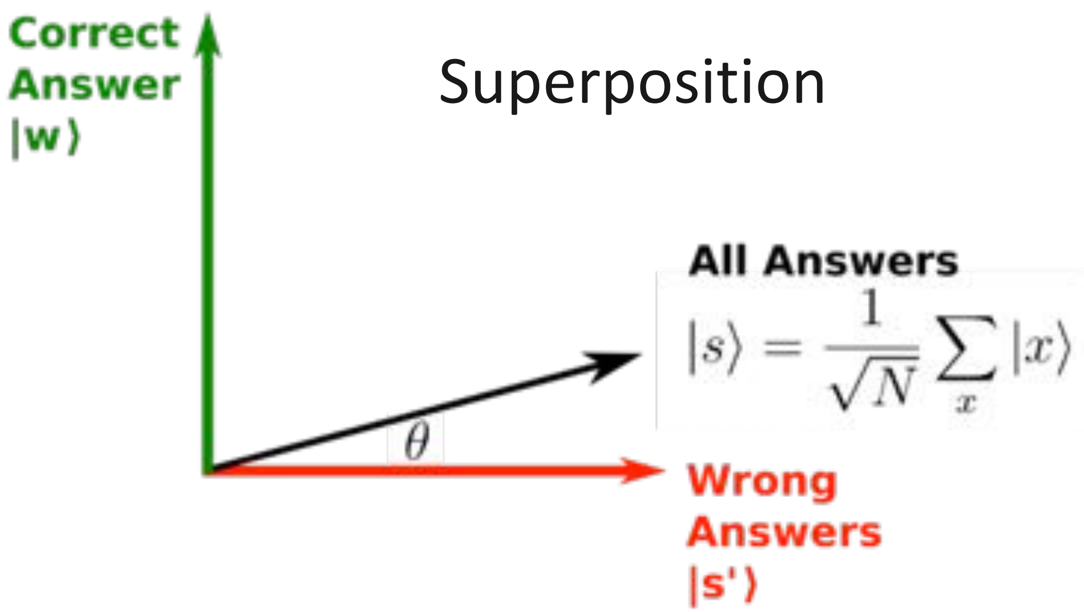
Geometry of Grover's Search Algorithm

We have $N = 2^n$ items
indexed by n qubits

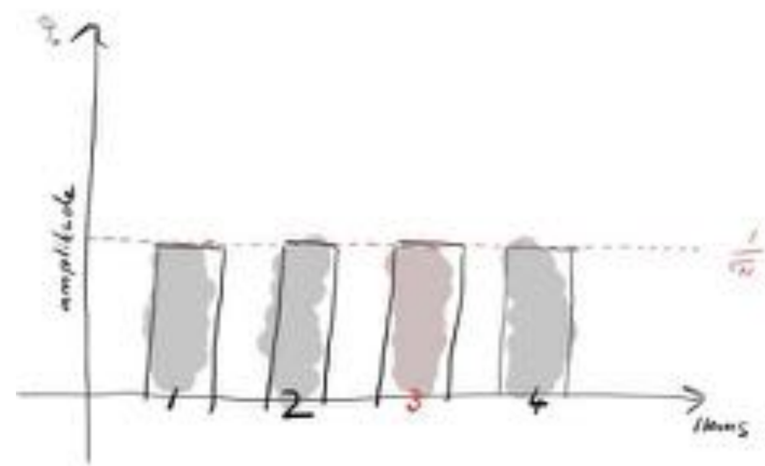


Geometry of Grover’s Search Algorithm

Superposition



N = 4

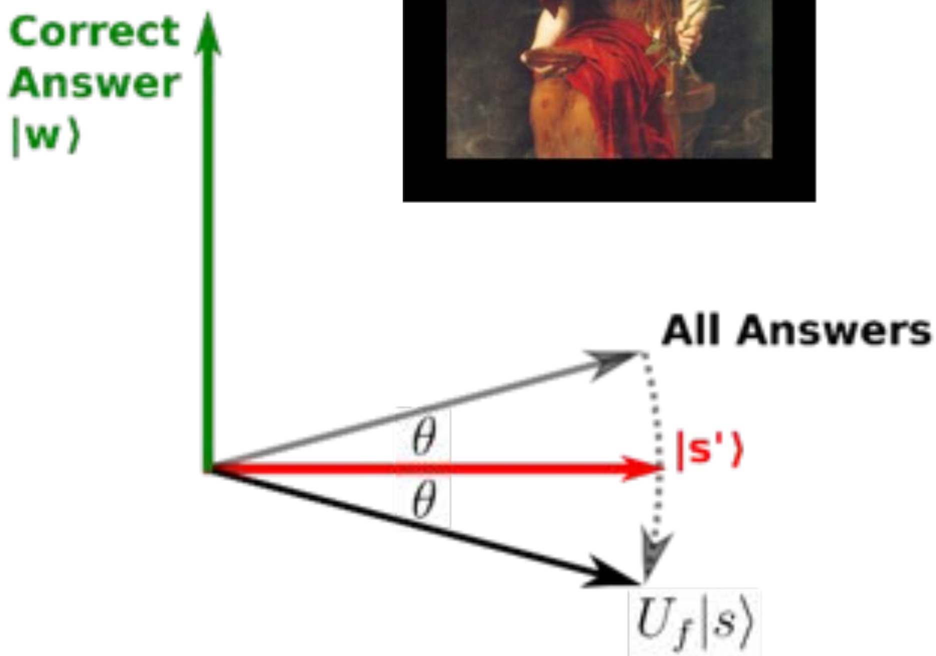


Geometry of Grover's Search Algorithm

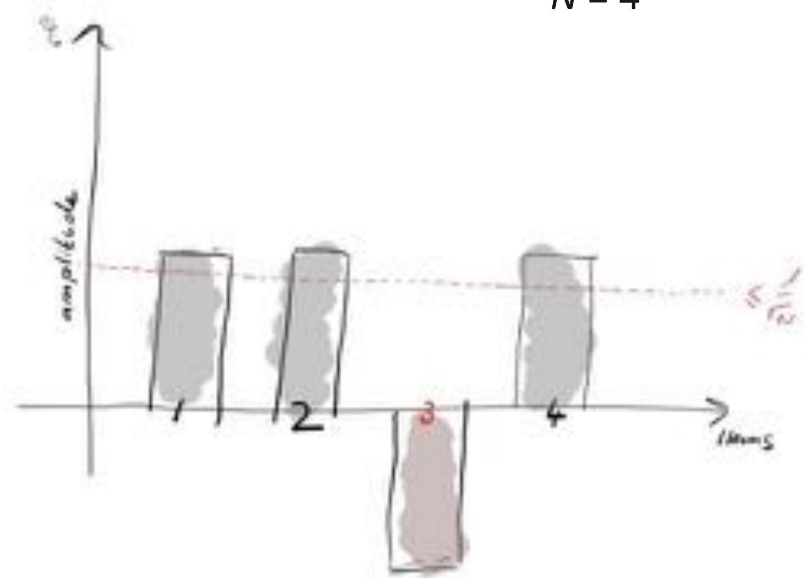
Entanglement in the Grover's Search Algorithm

Shantanav Chakraborty,[*] Subhashish Banerjee,[†] Satyabrata Adhikari,[‡] and Atul Kumar[§]
Indian Institute of Technology Jodhpur, Jodhpur-342011, India

arXiv: 1305.4454v2

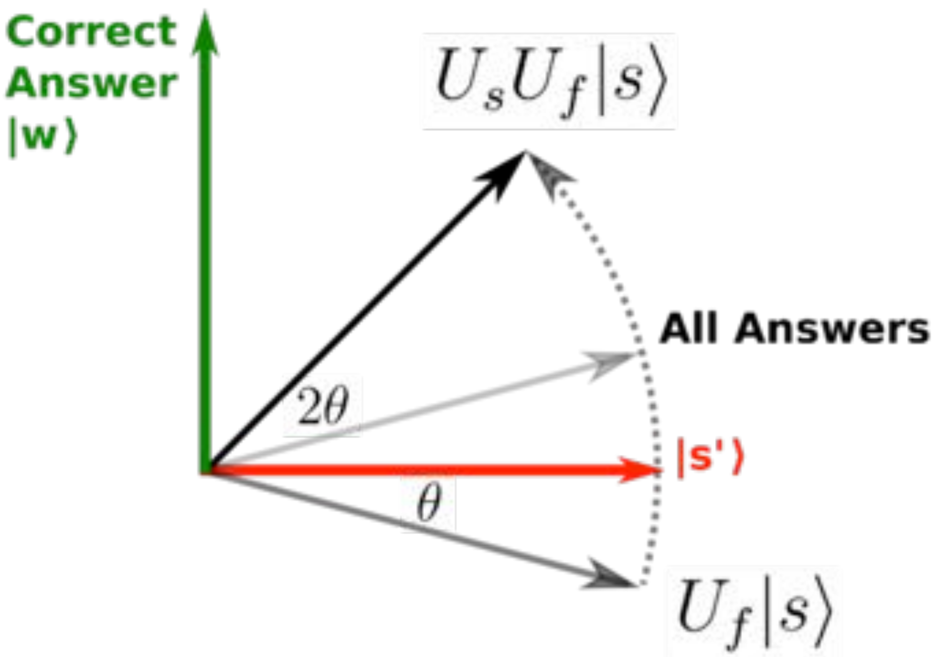


$N = 4$



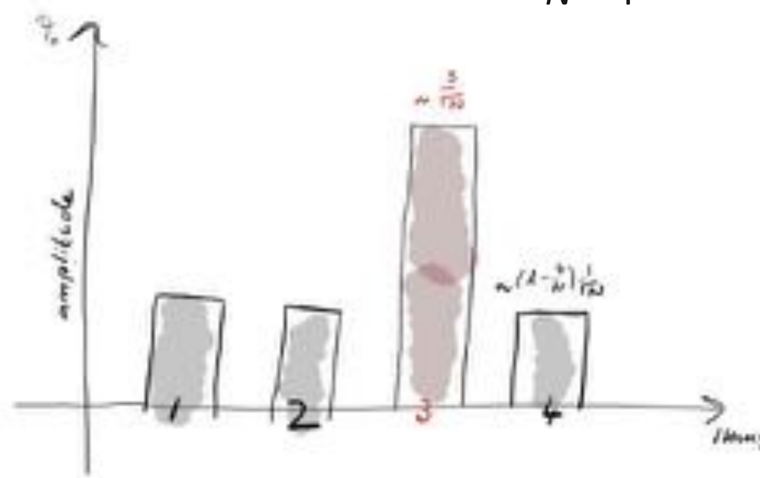
Geometry of Grover's Search Algorithm

Amplitude Amplification



Use interference to invert amplitude about the mean

N = 4

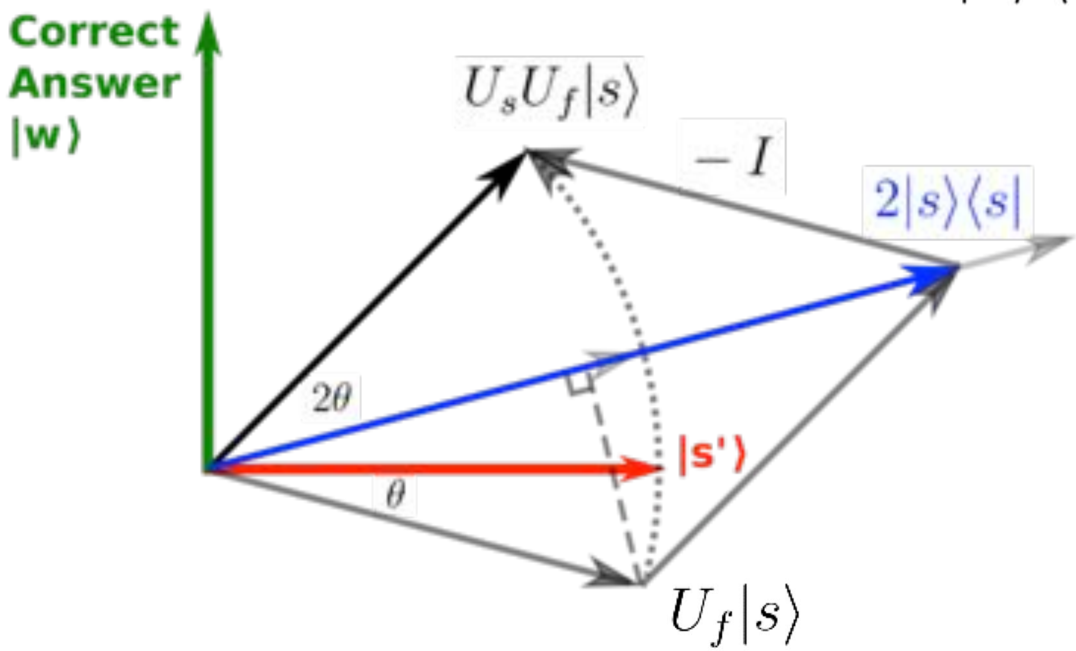


$$\text{Repeat} \sim \sqrt{N} \text{ times}$$

Geometry of Grover's Search Algorithm

Grover Diffusion Operator

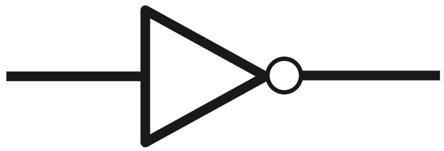
$$U_s = 2|s\rangle\langle s| - I$$



Building Quantum Circuits

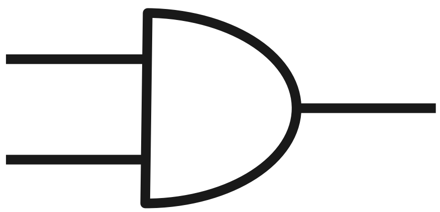
Classical Gate Operations

NOT Gate (Bit Flip)



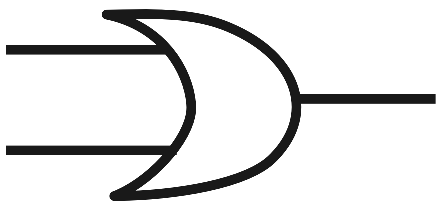
0 → 1
1 → 0

AND Gate



00 → 0
01 → 0
10 → 0
11 → 1

OR Gate



00 → 0
01 → 1
10 → 1
11 → 1

Many Classical Gates are “one-way”: Outputs are not unique

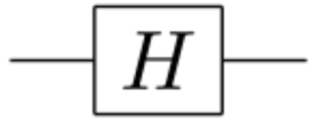
Quantum Operations

Single Qubit Operations

Input	Output: X	Z	S	H
$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$(\lvert 0\rangle + \lvert 1\rangle)/\sqrt{2}$
$\lvert 1\rangle$	$\lvert 0\rangle$	$-\lvert 1\rangle$	$i\lvert 1\rangle$	$(\lvert 0\rangle - \lvert 1\rangle)/\sqrt{2}$

Quantum Operations

Single Qubit Operations

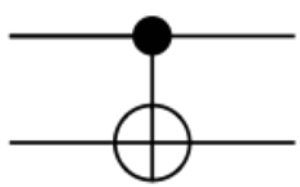


Input	Output			
	X	Z	S	H
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$(\|0\rangle + \|1\rangle)/\sqrt{2}$
$\|1\rangle$	$\|0\rangle$	$-\|1\rangle$	$i\|1\rangle$	$(\|0\rangle - \|1\rangle)/\sqrt{2}$

Two-qubit Operations

Inputs		CNOT	
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Controlled-NOT flips second qubit if first qubit is 1



Quantum Operations

Single Qubit Operations

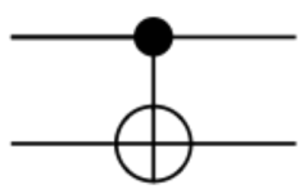
Input	Output X	Z	S	H
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$(\|0\rangle + \|1\rangle)/\sqrt{2}$
$\|1\rangle$	$\|0\rangle$	$-\|1\rangle$	$i\|1\rangle$	$(\|0\rangle - \|1\rangle)/\sqrt{2}$

- Every operation has same number of inputs and outputs
- Every output is unique because quantum operations are reversible
- Each qubit gets a line

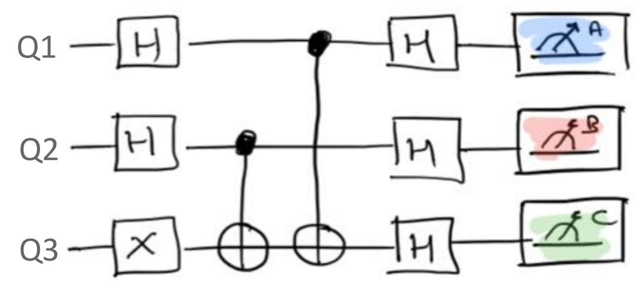
Two-qubit operations

Inputs		CNOT	
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

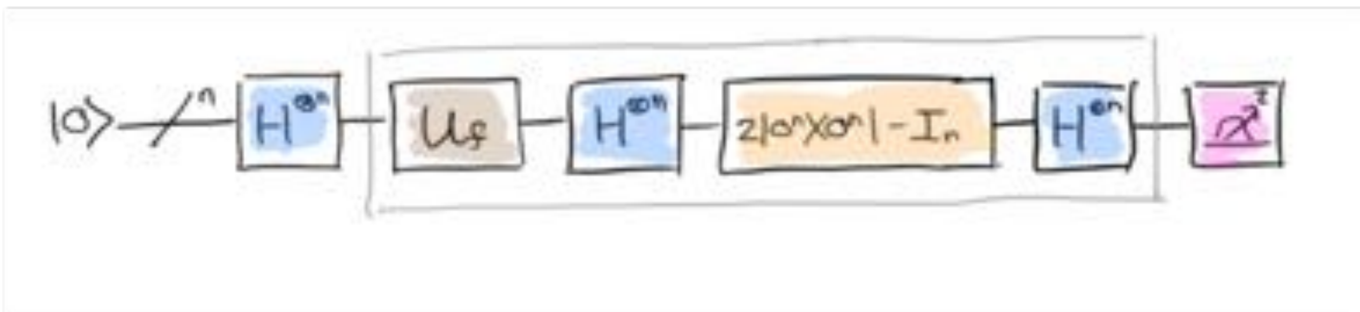
Controlled-NOT flips second qubit if first qubit is 1



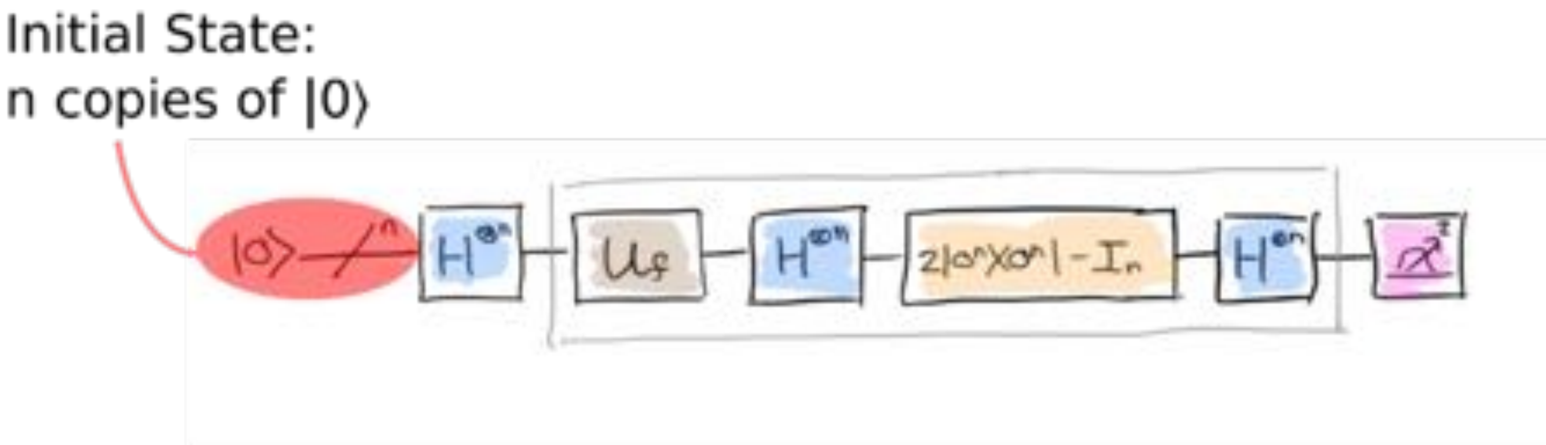
Example Sqore, like musical score



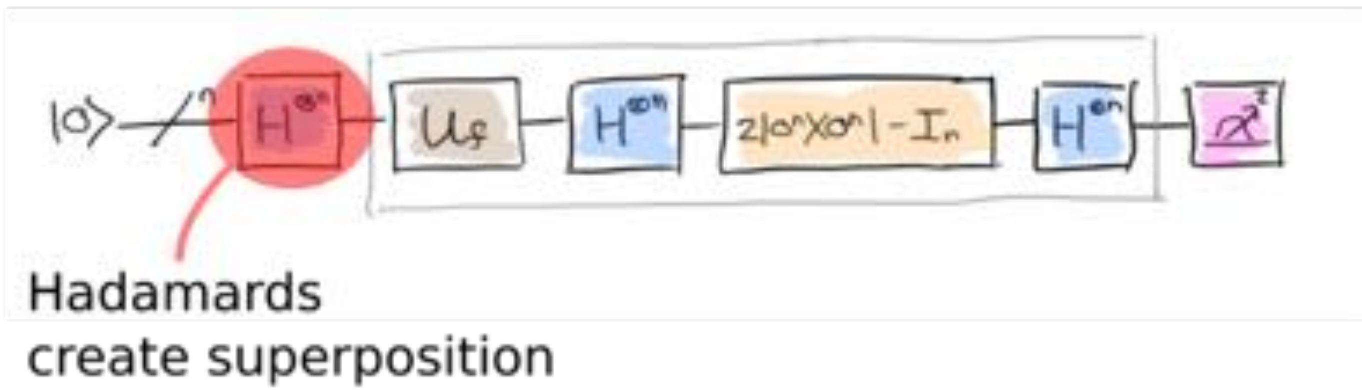
Grover’s Search Algorithm Circuit



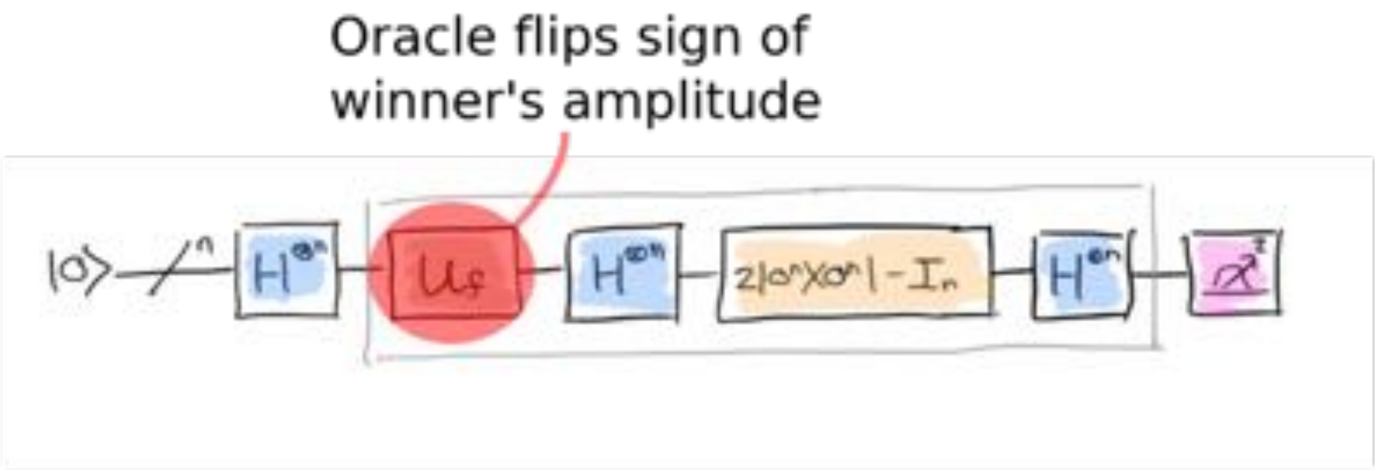
Grover’s Search Algorithm Circuit



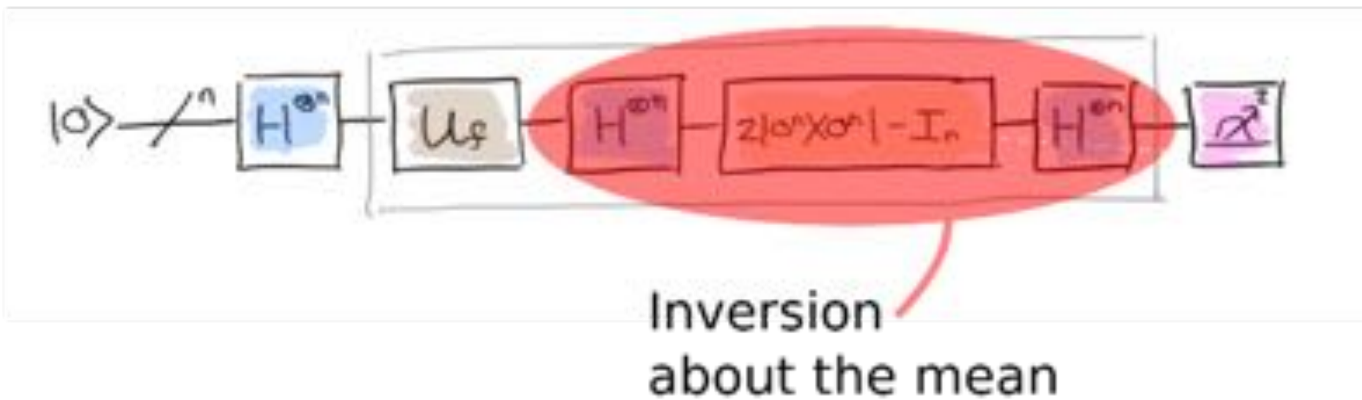
Grover’s Search Algorithm Circuit



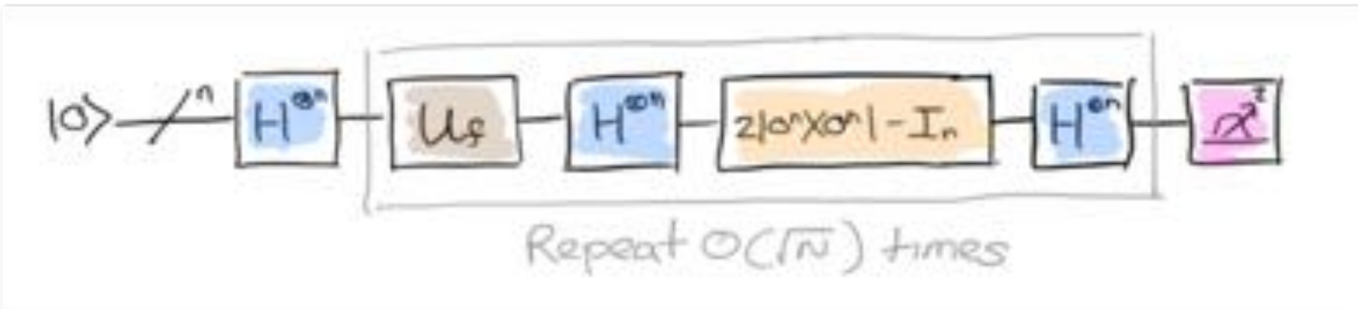
Grover’s Search Algorithm Circuit



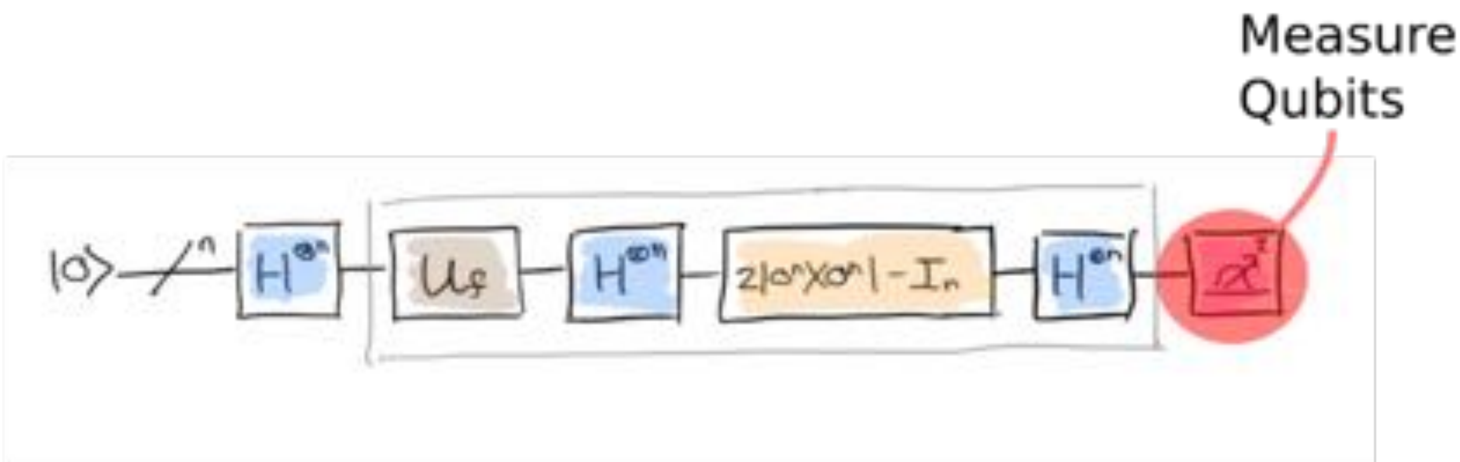
Grover’s Search Algorithm Circuit



Grover’s Search Algorithm Circuit

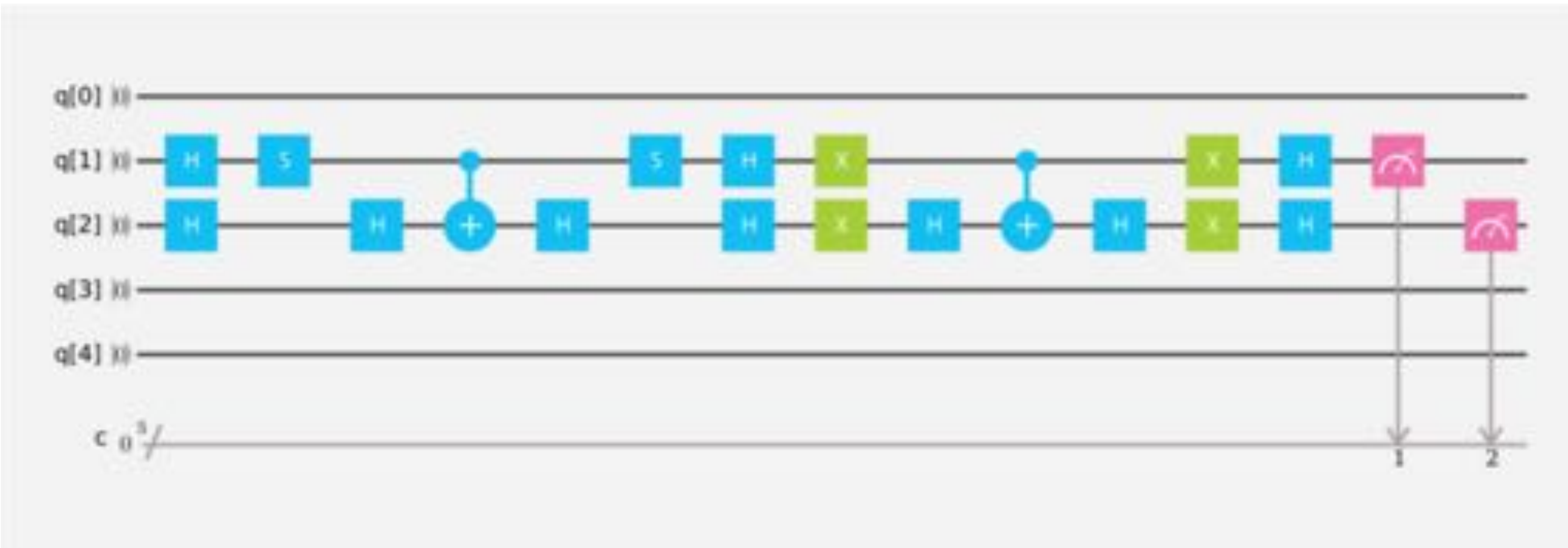


Grover's Search Algorithm Circuit



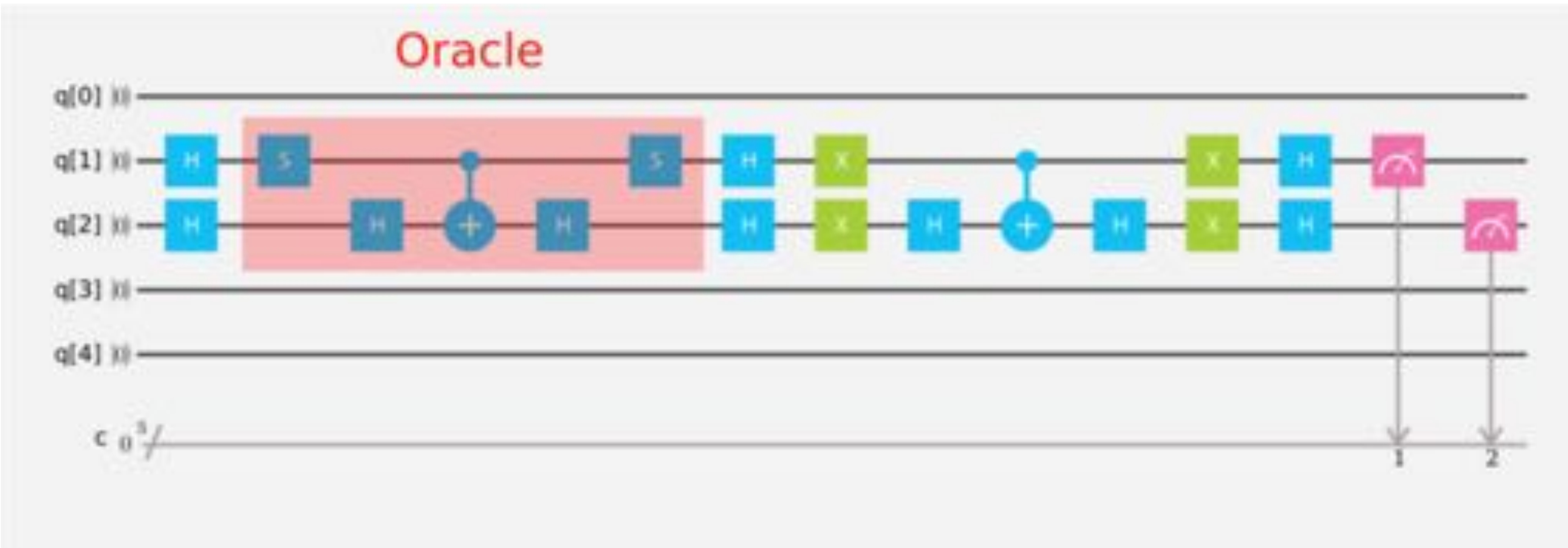
Two Qubit Grover's Search Algorithm Circuit

Oracle set for index 3



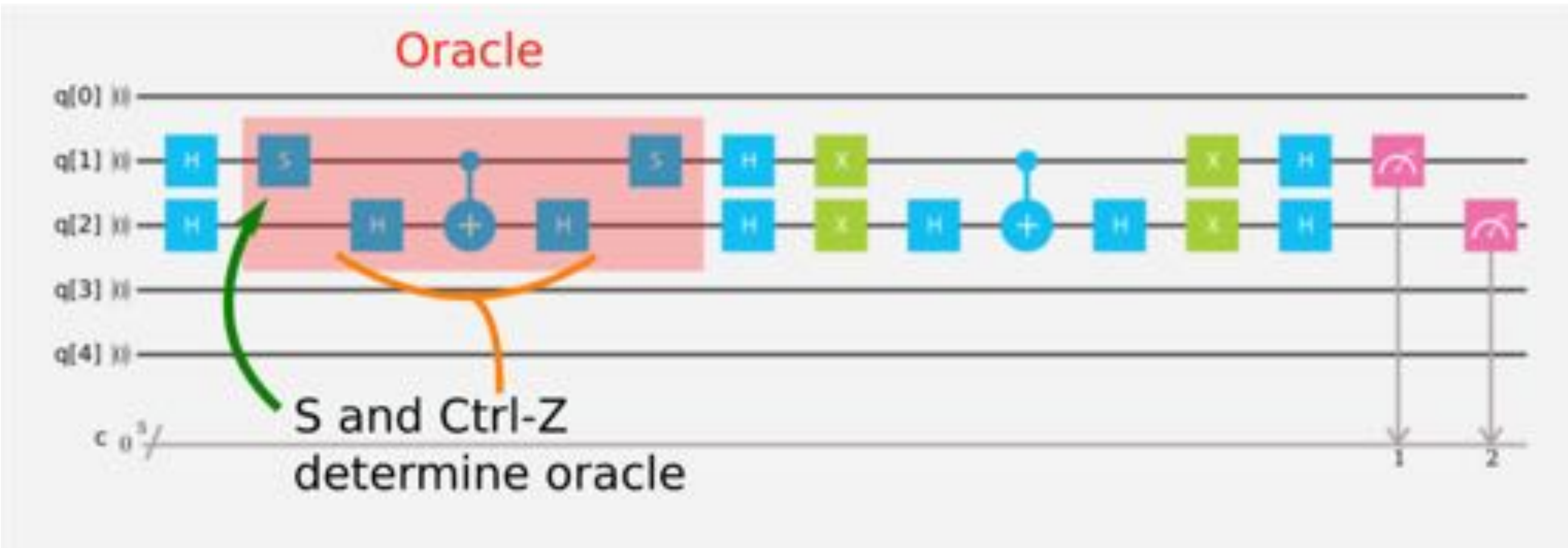
Two Qubit Grover's Search Algorithm Circuit

Oracle set for index 3



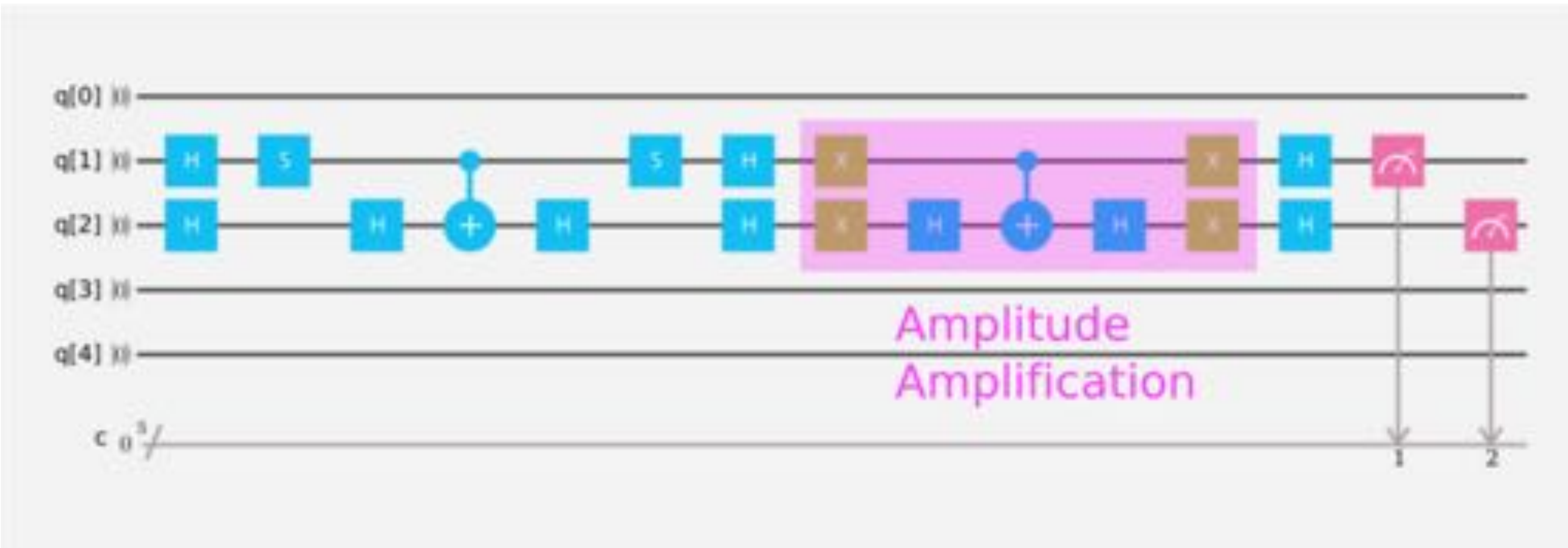
Two Qubit Grover's Search Algorithm Circuit

Oracle set for index 3



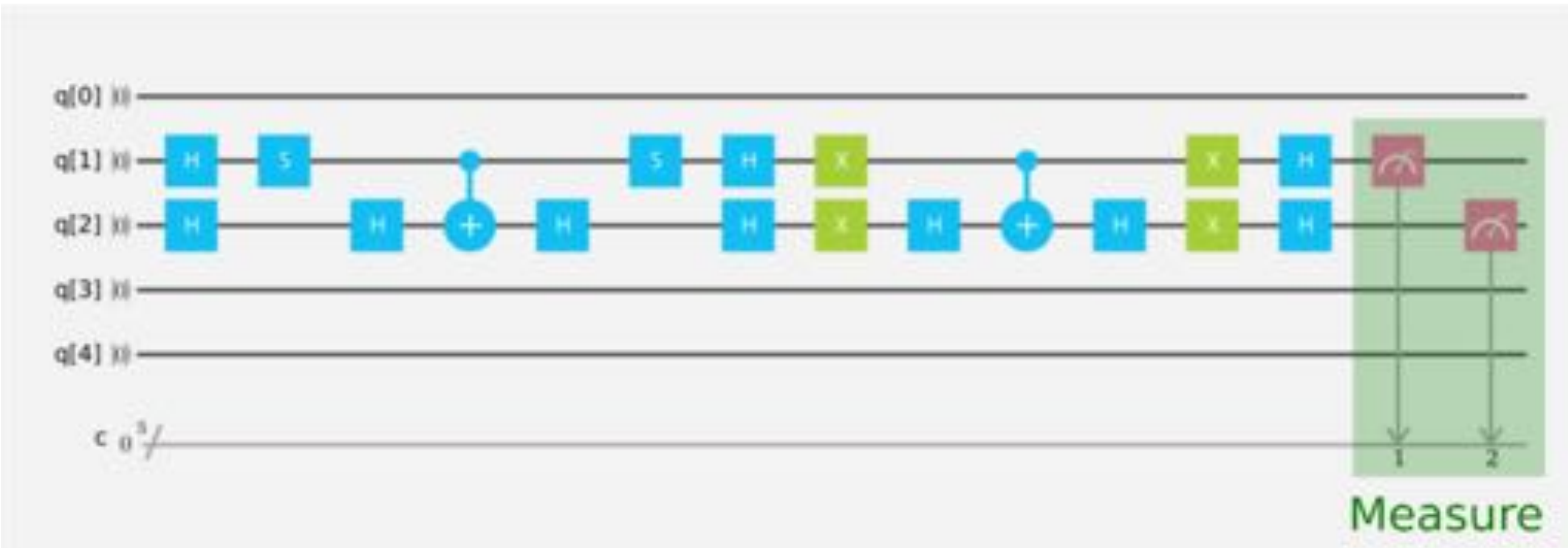
Two Qubit Grover's Search Algorithm Circuit

Oracle set for index 3

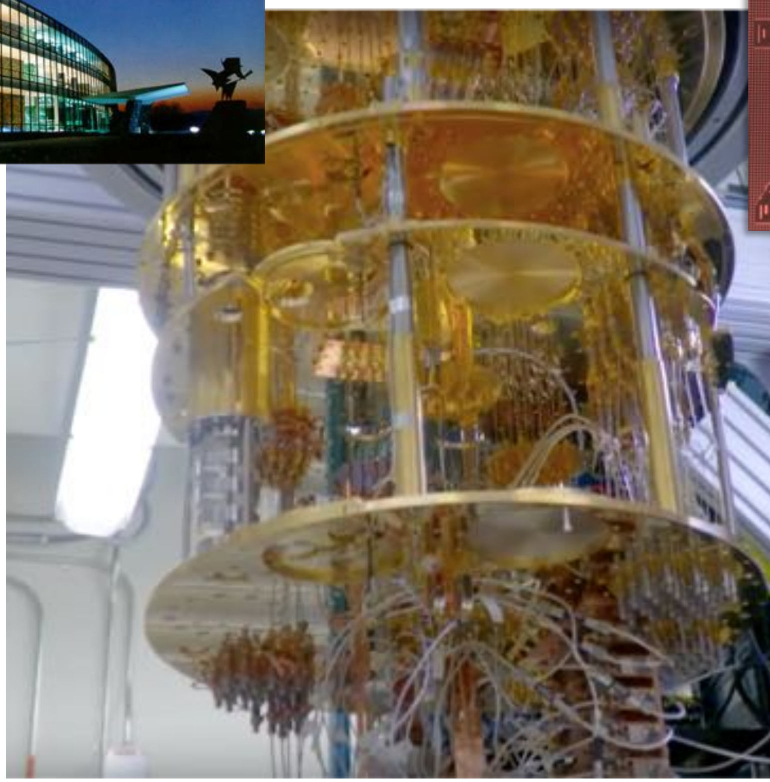
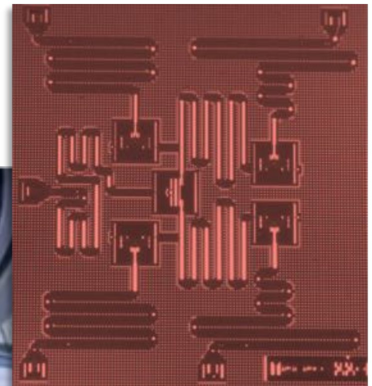
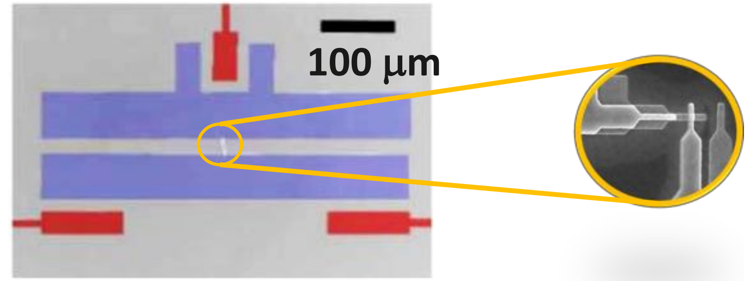


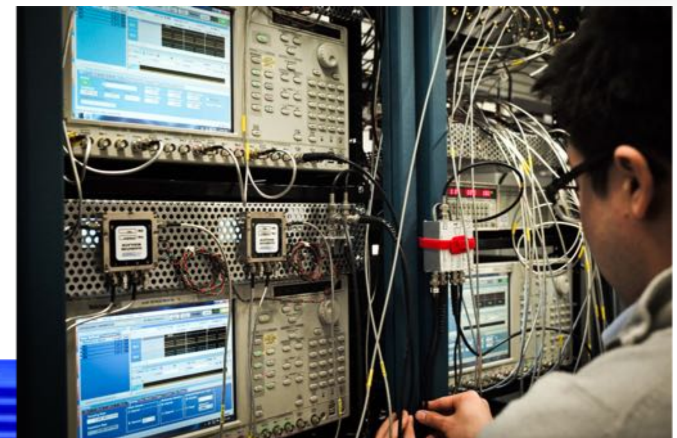
Two Qubit Grover's Search Algorithm Circuit

Oracle set for index 3



IBM Quantum Experience

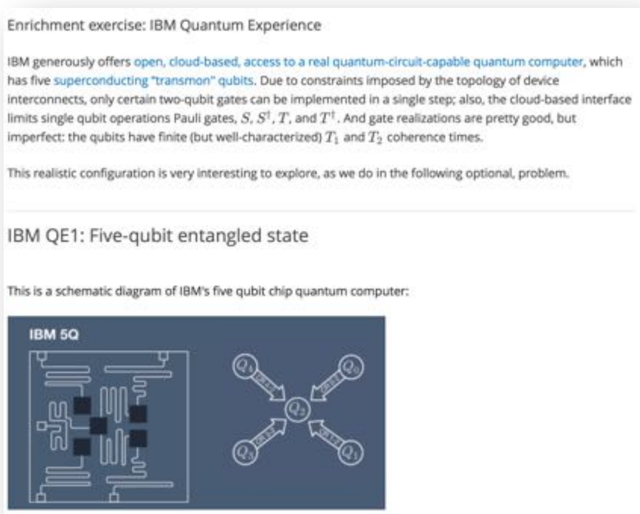





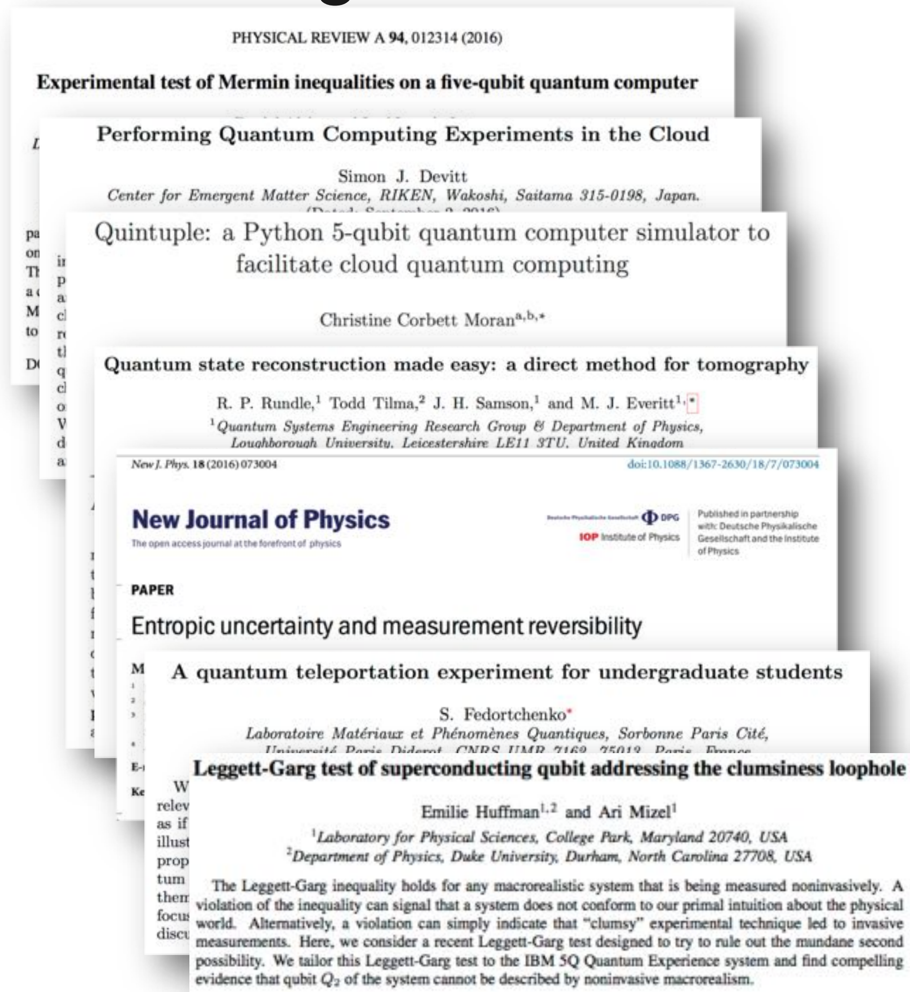


The Quantum Community is Growing

- Fifteen papers submitted
- Tweets from scientist at the South Pole
- 10+ professors using IBM Quantum Experience for education
- Featured at Undergrad Conference at University of Waterloo
- MIT edX Online Course using it (1100 students)
- Educational tool and research tool

N. Linke et al., arXiv:1702.01852





Quantum Experience Demo

Supplemental Slides

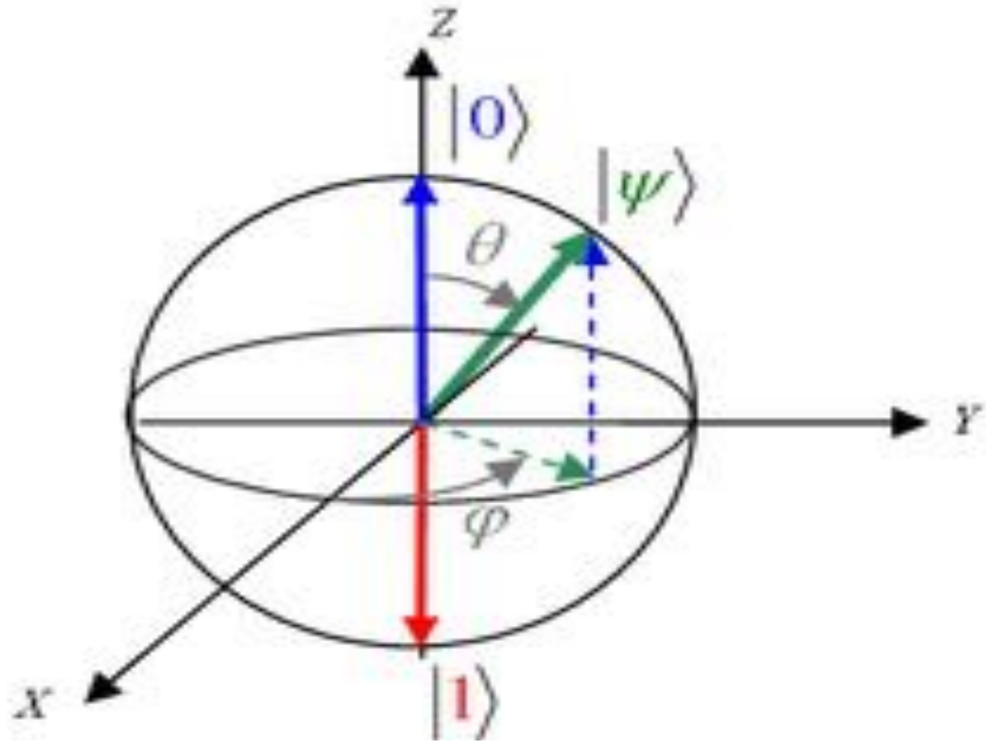
Visualizing qubit states: the Bloch sphere

- Qubit states lie in 2D Hilbert space with orthonormal basis $|\mathbf{0}\rangle, |\mathbf{1}\rangle$

- An arbitrary state is given by:

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

$$\alpha = \cos(\theta/2)$$
$$\beta = e^{i\varphi}\sin(\theta/2)$$



March 30, 2016

Single-Qubit Operations

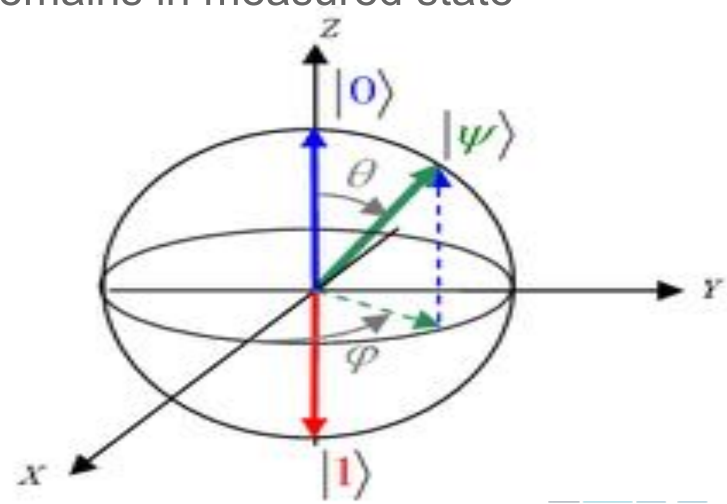
- Measure:

Initial state — Possible outcomes

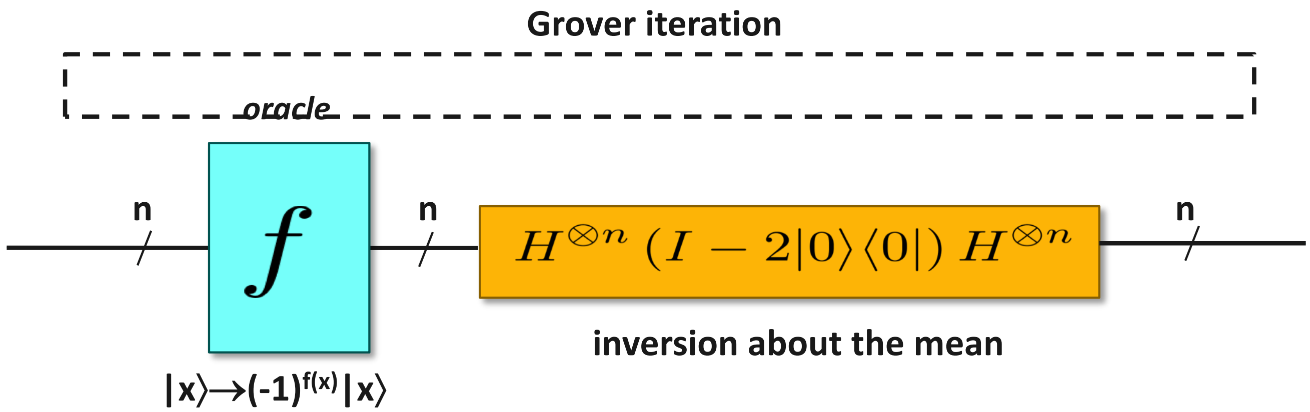
$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \begin{cases} |0\rangle \text{ with probability } \alpha^2 \\ |1\rangle \text{ with probability } \beta^2 \end{cases}$$

  – *Quantum non-demolition (QND) measurement*: qubit remains in measured state

- Rotate:
  – NOT gate: rotate π radians around X or Y (a.k.a. "*pi pulse*")
  – But also… any arbitrary rotation allowed! ($\pi/2$ is a common one)

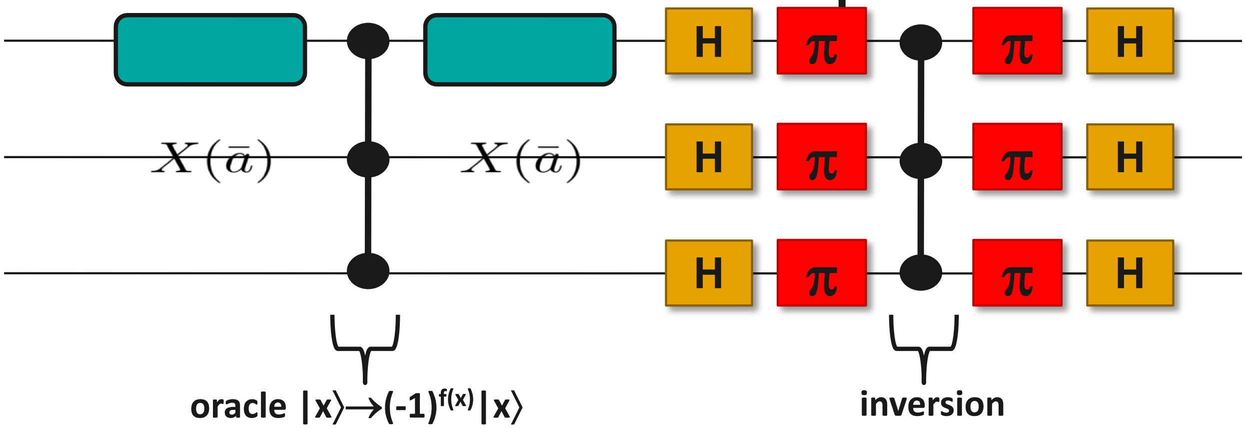


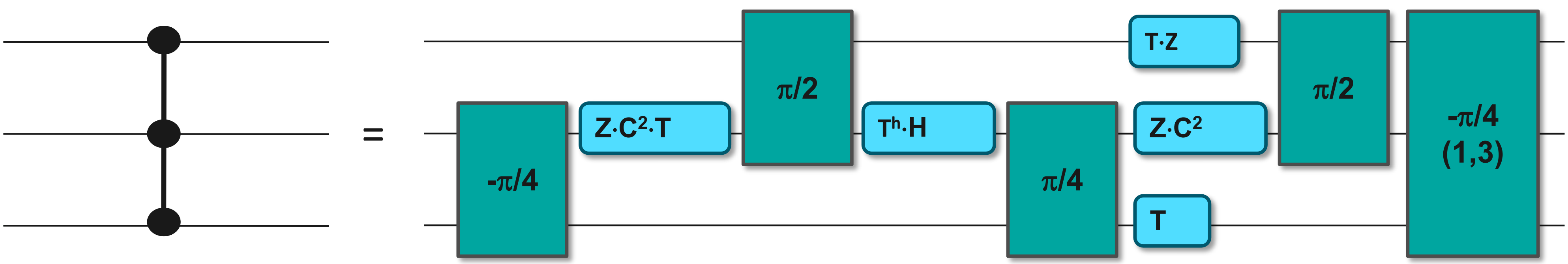
Grover's algorithm



$$\text{repeat } O\left(\sqrt{2^n}\right) \text{ times}$$

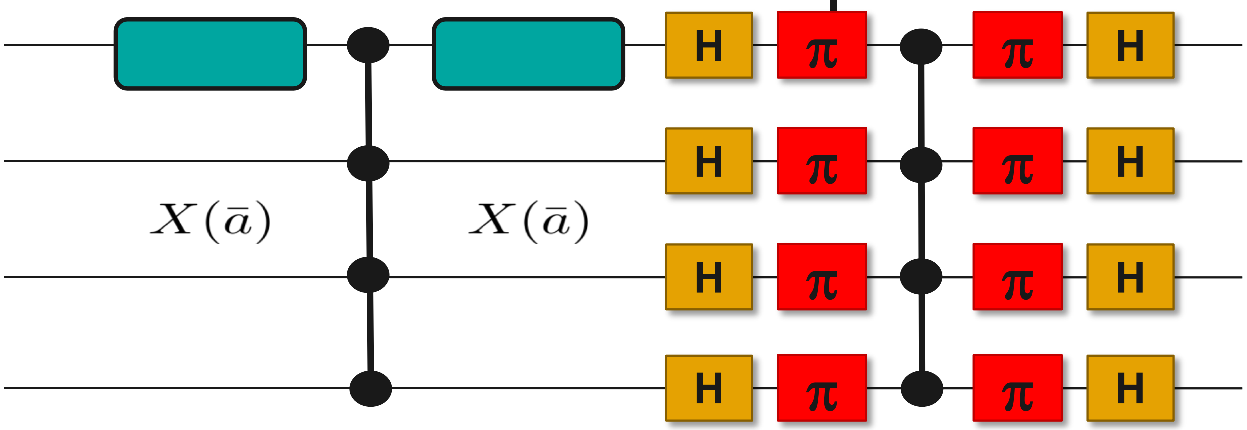
Grover's iteration on 3 qubits





2 iterations, 10 two-qubit gates/iteration, 14 single-qubit locs/CCZ

Grover’s iteration on 4 qubits



3 iterations
26 two-qubit gates/iteration
78 one-qubit locs/CCCZ

[1] A. Barenco et al., “Elementary gates for quantum computation”, Phys. Rev. A 52 3457 (1995)