Quantum Computing Tutorial -

An introduction for the uninitiated (or nearly so)

Eric Chitambar

ITW 2020

April 12, 2021

echitamb@Illinois.edu

http://quantum-entangled.ece.Illinois.edu

ILLINOIS

Quantum Information

Room 2

Chair: Christian Deppe (Technical University of Munich, Germany)

10:10 ***Correcting Erasures with Topological Subsystem Color Codes***

Hiteshvi Manish Solanki and Pradeep K Sarvepalli (Indian Institute of Technology Madras, India)

Qubit loss is one of the forms of noise encountered in some quantum technologies. Such noise is modeled using the quantum erasure channel. Unlike the depolarizing noise, it is much more tractable, yet the performance of many quantum codes over the erasure channel has not been studied as extensively. In this paper, we study the performance of topological subsystem color codes (TSCCs) over the quantum erasure channel. It is the first such study of TSCCs over the erasure channel. We propose multiple decoding algorithms for TSCC and obtain the highest threshold of about 9.7% for the subsystem color code derived from the square octagon lattice.

10:20 ***Linear programming decoder for hypergraph product quantum codes***

Omar Fawzi (ENS de Lyon, France); Lucien Grouès (Sorbonne Université & Inria Paris, France); Anthony Leverrier (INRIA, France)

We introduce a decoder for quantum CSS codes that is based on linear programming. Our definition is a priori slightly different from the one proposed by Li and Vontobel as we have a syndrome oriented approach instead of an error oriented one, but we show that the success condition is equivalent. Although we prove that this decoder fails for quantum codes that do not have good soundness property (i.e., having large errors with syndrome of small weight) such as the toric code, we obtain good results from simulations. We run our decoder for hypergraph products of two random LDPC codes, showing that it performs better than belief propagation, even combined with the small-set-flip decoder that can provably correct a constant fraction of random errors.

10:30 ***Universal Communication Efficient Quantum Threshold Secret Sharing Schemes***

Kaushik Senthoor and Pradeep K Sarvepalli (Indian Institute of Technology Madras, India)

Quantum secret sharing (QSS) is a cryptographic protocol in which a quantum secret is distributed among a number of parties where some subsets of the parties are able to recover the secret while some subsets are unable to recover the secret. In the standard $((k,n))$ quantum threshold secret sharing scheme, any subset of k or more parties out of the total n parties can recover the secret while other subsets have no information about the secret. But recovery of the secret incurs a communication cost of at least k qudits for every qudit in the secret. Recently, a class of communication efficient QSS schemes were proposed which can improve this communication cost to $\frac{d}{d-k+1}$ by contacting $d\geq k$ parties where d is fixed prior to the distribution of shares. In this paper, we propose a more general class of $((k,n))$ quantum secret sharing schemes with low communication complexity. In these schemes the combiner can contact any d parties at the time of recovery where $k\leq d\leq n$. This is the first such class of universal communication efficient quantum threshold schemes.

10:40 ***Quantum Channel State Masking***

Uzi Pereg and Christian Deppe (Technical University of Munich, Germany); Holger Boche (Technical University Munich, Germany)

Communication over a quantum channel that depends on a quantum state is considered, when the encoder has channel side information (CSI) and is required to mask information on the quantum channel state from the decoder. A full characterization is established for the entanglement-assisted masking equivocation region, and a regularized formula is given for the quantum capacity-leakage function without assistance. For Hadamard channels without assistance, we derive single-letter inner and outer bounds, which coincide in the standard case of a channel that does not depend on a state.

Outline

- **Part I: Principles of Quantum Computing** (50 minutes)
  - Physical qubits
  - Mathematical description of qubits
  - Gates and measurements
  - Quantum circuit model
  - Decoherence and error correction
- **Break** (5 minutes)
- **Part II: Some Examples of Quantum Algorithms** (45 minutes)
  - Deutsch-Jozsa algorithm
  - Grover’s search algorithm
- **Q&A** (10 minutes)

Part I: Principles of Quantum Computing

“Blackbox” Computing Devices

- The high level function of any computing device: map input data to output data.

$$\mathbf{b} \in \mathbb{Z}_2^n \Longrightarrow \boxed{P(\mathbf{x}|\mathbf{b})} \Longrightarrow \mathbf{x} \in \mathbb{Z}_2^m$$

- What are the different type of “boxes” that nature allows?

$\Delta t??$

$\mathbf{b} \Longrightarrow$ Classical Box $\Longrightarrow \mathbf{x}$

Inside the box:
Components are manipulating information encoded in bits

$\Delta t??$

$\mathbf{b} \Longrightarrow$ Quantum Box $\Longrightarrow \mathbf{x}$

Inside the box:
Components are manipulating information encoded in quantum bits (qubits)

$\Delta t??$

$\mathbf{b} \Longrightarrow$ Super-Quantum Box $\Longrightarrow \mathbf{x}$

Inside the box:
Components are manipulating information encoded in “stronger than quantum” objects

"Blackbox" Computing Devices

- The high level function of any computing device: map input data to output data.

$$\mathbf{b} \in \mathbb{Z}_2^n \Longrightarrow \boxed{P(\mathbf{x}|\mathbf{b})} \Longrightarrow \mathbf{x} \in \mathbb{Z}_2^m$$

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], I
Rupak Biswas[3], Sergio Boixo[1], Fernando G.
Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Robert
Edward Farhi[1], Brooks Foxen[1,5], Austin Fowl
Keith Guerin[1], Steve Habegger[1], Matthew F
Markus Hoffmann[1], Trent Huang[1], Travis S.
Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Keche
Alexander Korotkov[1,8], Fedor Kostritsa[1], Da
Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarro
Anthony Megrant[1], Xiao Mi[1], Kristel Michie
Ofer Naaman[1], Matthew Neeley[1], Charles N
Andre Petukhov[1], John C. Platt[1], Chris Quin
Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. S
Matthew D. Trevithick[1], Amit Vainsencher[1],
Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], H

Sampling problems!

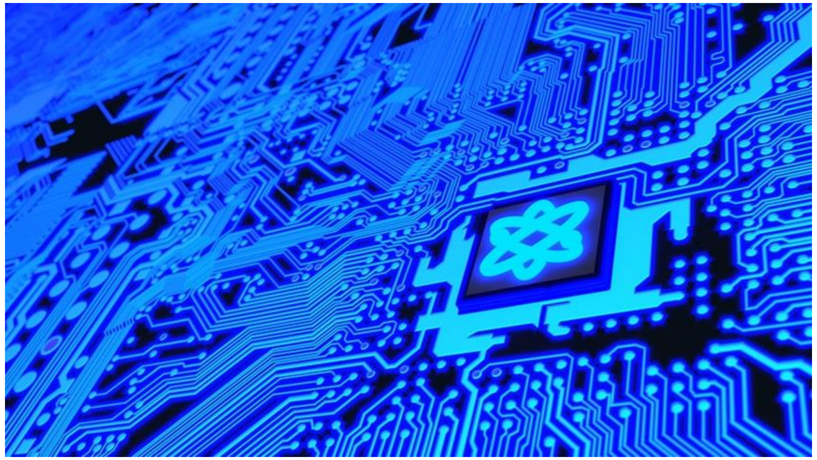
RESEARCH

QUANTUM COMPUTING

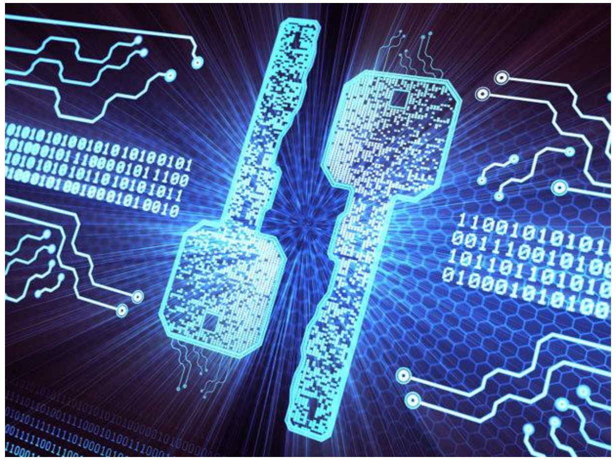
Quantum computational advantage using photons

Han-Sen Zhong[1,2*], Hui Wang[1,2*], Yu-Hao Deng[1,2*], Ming-Cheng Chen[1,2*], Li-Chao Peng[1,2], Yi-Han Luo[1,2], Jian Qin[1,2], Dian Wu[1,2], Xing Ding[1,2], Yi Hu[1,2], Peng Hu[3], Xiao-Yan Yang[3], Wei-Jun Zhang[3], Hao Li[3], Yuxuan Li[4], Xiao Jiang[1,2], Lin Gan[4], Guangwen Yang[4], Lixing You[3], Zhen Wang[3], Li Li[1,2], Nai-Le Liu[1,2], Chao-Yang Lu[1,2†], Jian-Wei Pan[1,2†]

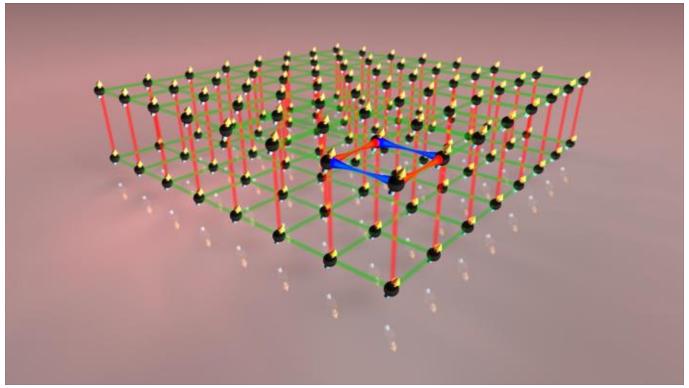
Applications/Advantages of Quantum Information



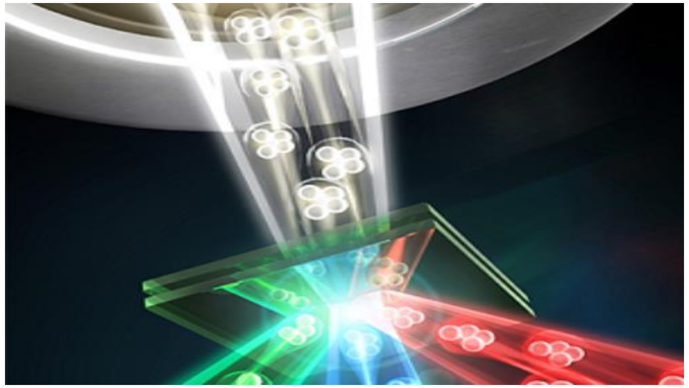
Quantum Computation



Quantum Cryptography



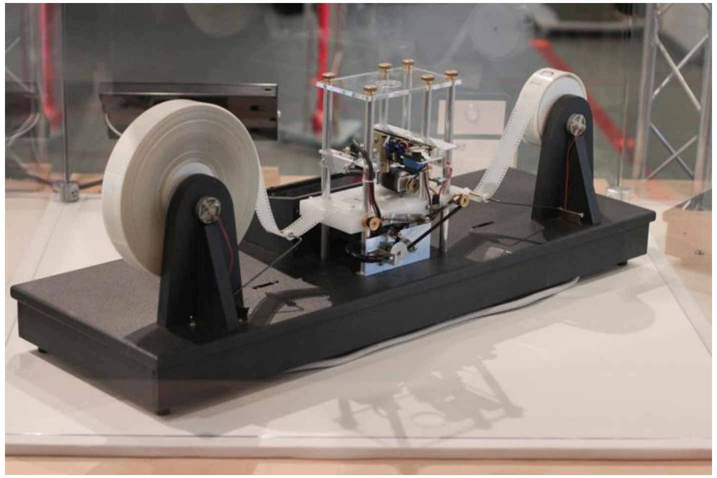
Quantum Simulation



Quantum Sensing

Quantum versus Classical Computers

- Quantum computers are not simply computers that “use” quantum mechanics.



Hardware relies on
principles of quantum mechanics.

Same computational model:
manipulation of bits

$\cdots 010010111010 \cdots$

In contrast, quantum computers manipulate **qubits**.

Qubits are two-level quantum systems that
can utilize non-classical features like superposition and entanglement.

DiVincenzo's Five Requirements for the Implementation of Quantum Computation

Fortschr. Phys. **48** (2000) 9–11, 771–783

The Physical Implementation of Quantum Computation

David P. DiVincenzo

IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA

Abstract

After a brief introduction to the principles and promise of quantum information processing, the requirements for the physical implementation of quantum computation are discussed. These five requirements, plus two relating to the communication of quantum information, are extensively explored and related to the many schemes in atomic physics, quantum optics, nuclear and electron magnetic resonance spectroscopy, superconducting electronics, and quantum-dot physics, for achieving quantum computing.

DiVincenzo's Five Requirements for the Implementation of Quantum Computation

1. A scalable physical system with well-characterized qubits

2. A qubit-specific measurement capability

3. The ability to initialize the state of the qubits to a simple fiducial state, such as $|000 \ldots\rangle$

4. A "universal" set of quantum gates

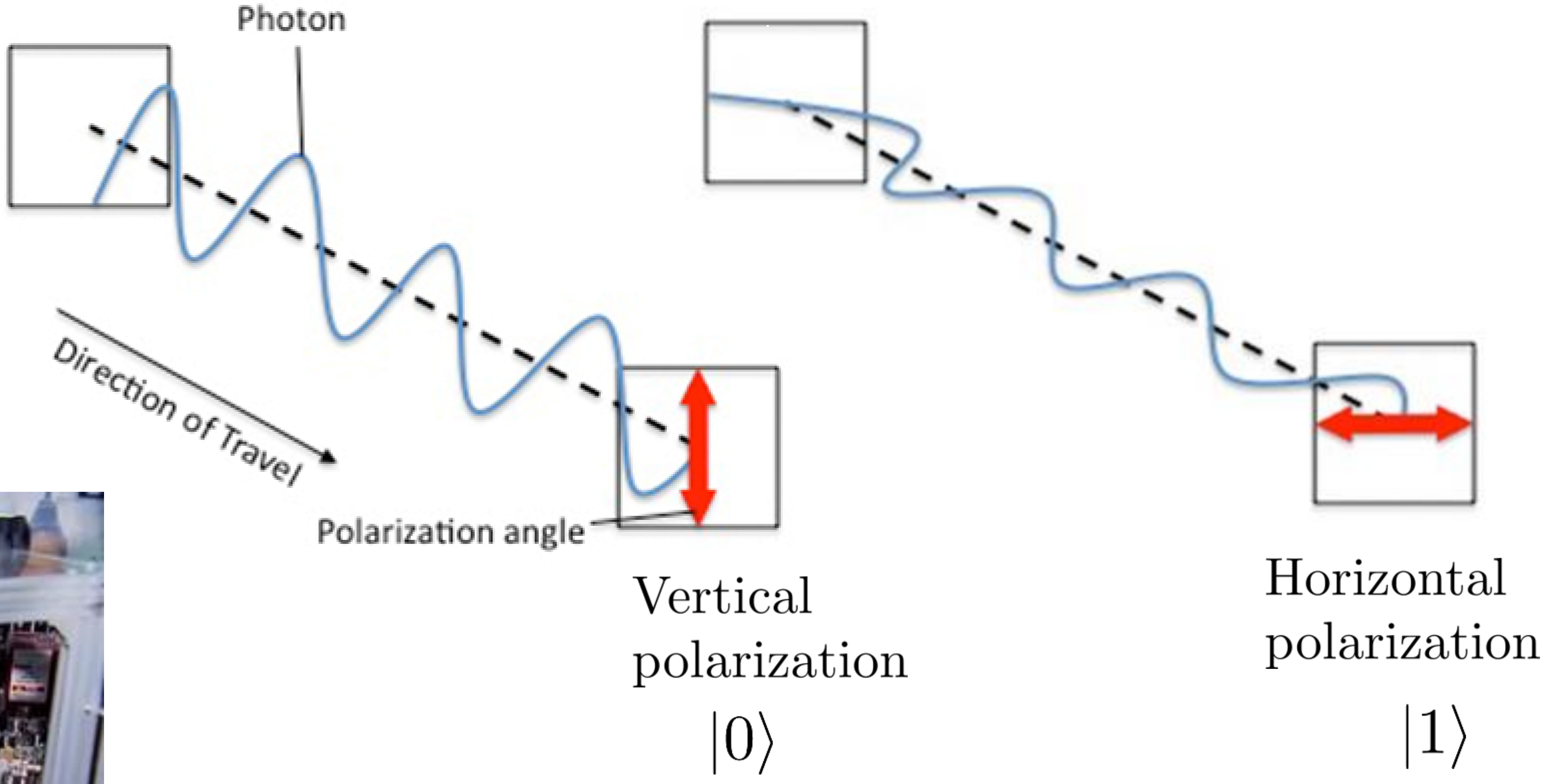
5. Long relevant decoherence times, much longer than the gate operation time

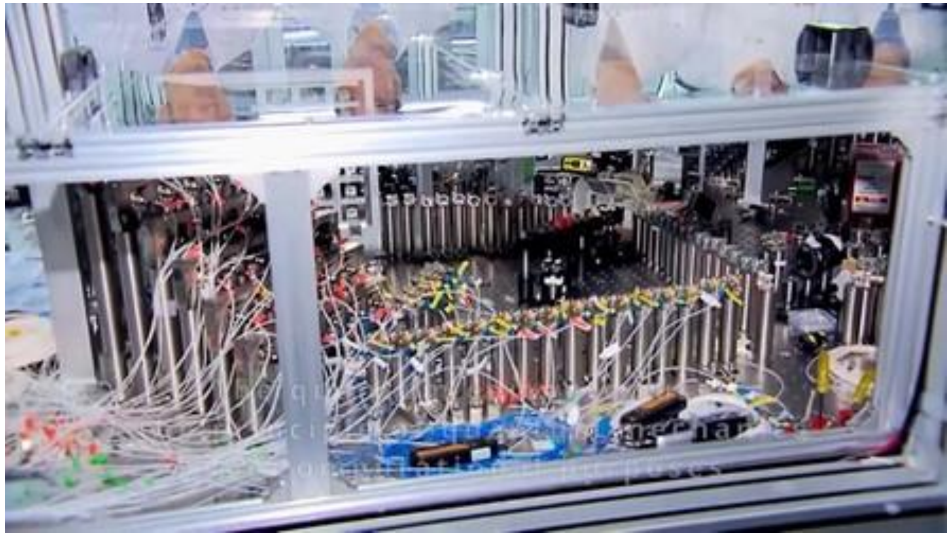
DiVincenzo’s Five Requirements for the Implementation of Quantum Computation

1. **A scalable physical system with well-characterized qubits**
2. A qubit-specific measurement capability
3. The ability to initialize the state of the qubits to a simple fiducial state, such as $|000\ldots\rangle$
4. A “universal” set of quantum gates
5. Long relevant decoherence times, much longer than the gate operation time

Physical Qubits: Photons

Example:
Photon Polarization

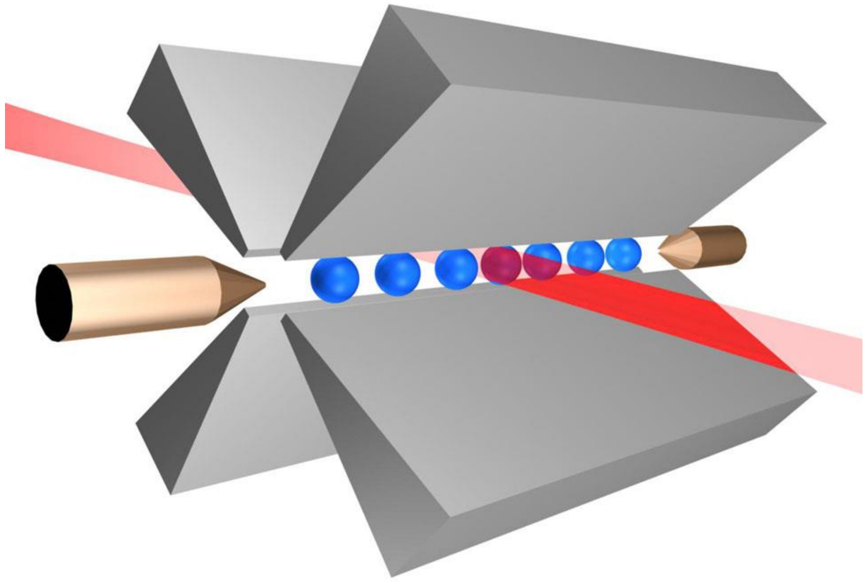




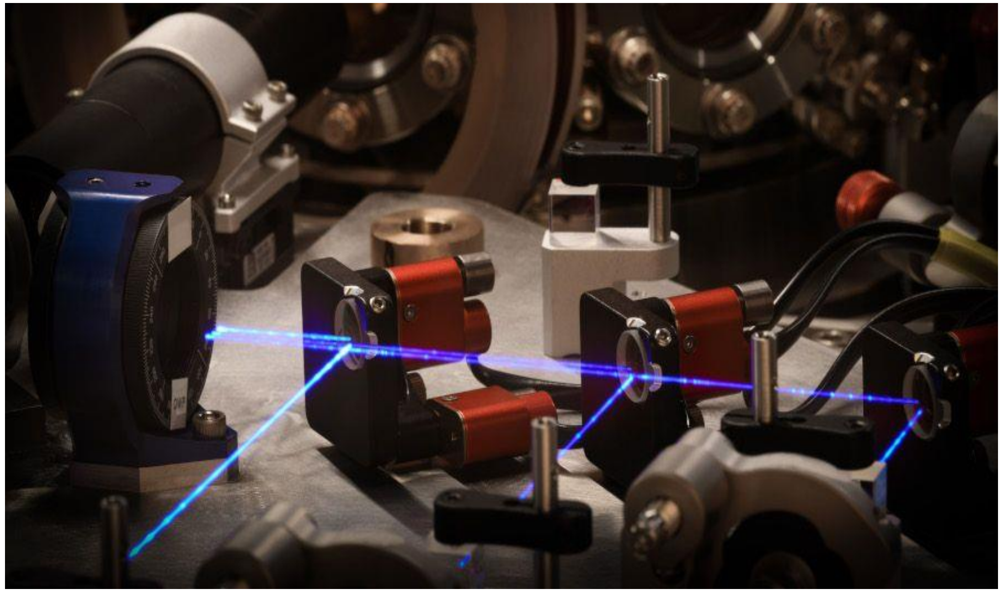
Jiuzhang Suanshu optical quantum computer, Jian-wei Pan's group

Physical Qubits: Trapped Ions

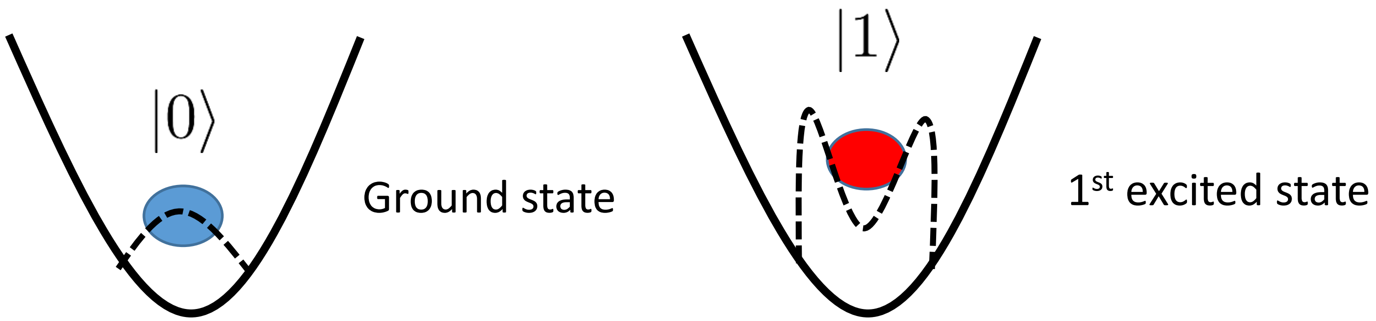
- Individual ions are confined in a magnetic field and manipulated using laser pulses.



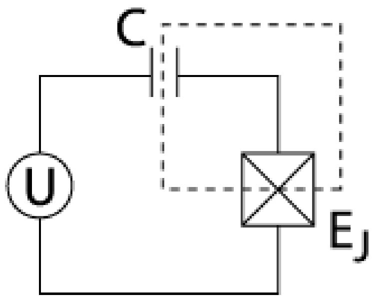
Institute for Theoretical Physics, University of Innsbruck



Honeywell's trapped ion quantum computer



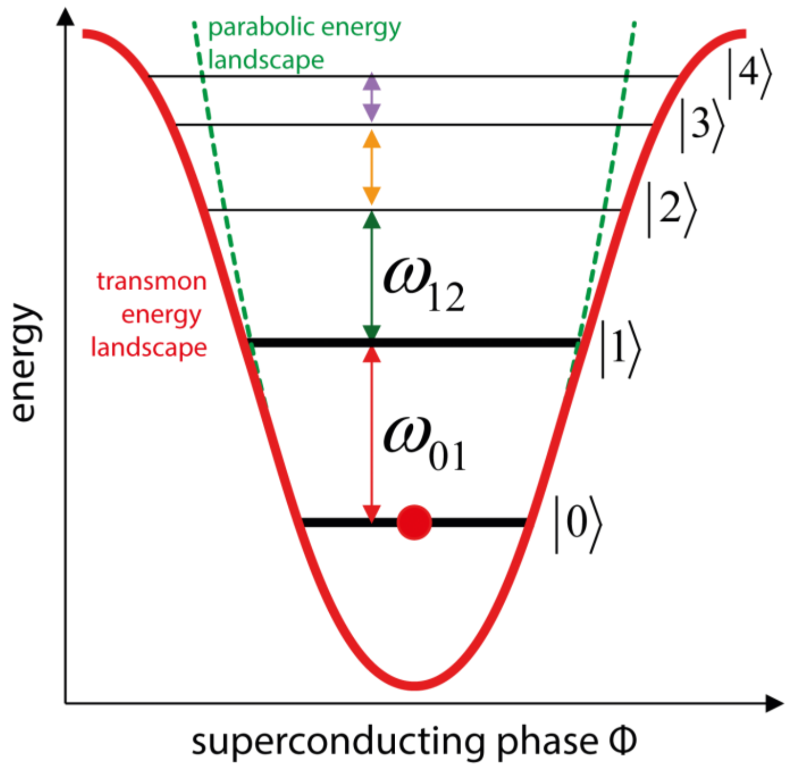
Physical Qubits: Superconducting Circuits



- When certain materials are cooled to very low temperatures, their electrons form pairs called Cooper pairs.

- Cooper pairs carry charge in a circuit with virtually zero resistance, a phenomenon called **superconductivity**.

superconducting circuit energy levels:



Christian Dickel – QuNet blog

IBMQ quantum computer

Google's Sycamore quantum computer

The Theory of Qubits

- Mathematically, we represent every qubit by a two-dimensional complex vector space $\mathbb{C}^2$.

  - Physical states of the system are represented by 2×2 complex matrices that are

    (i) positive (i.e. having non-negative eigenvalues)

    (ii) trace-one (i.e. diagonal elements summing to one)

- Operators of this form are called **density matrices** (symbolically written as ρ, ω, etc.).

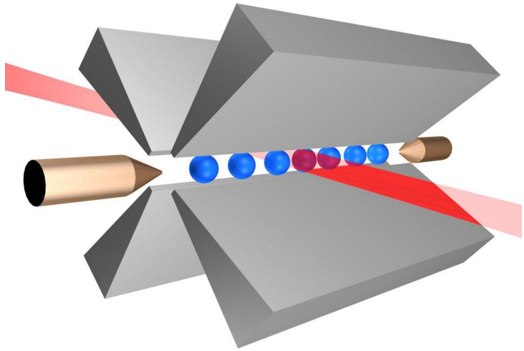
General Form of a Qubit:

$$\rho = \begin{bmatrix} p & re^{i\phi} \\ re^{-i\phi} & 1-p \end{bmatrix}$$

Coherence terms

$$0 \leq p \leq 1;$$

$$0 \leq r \leq \sqrt{p(1-p)}.$$



Every valid choice of p, r, ϕ corresponds to a different physical preparation of the quantum system!

The Theory of Qubits

- A special type of density matrices are those having rank one:

$$\rho = \begin{bmatrix} \frac{2}{3} & -i\sqrt{\frac{1}{3}} \\ i\sqrt{\frac{1}{3}} & \frac{1}{3} \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{2}{3}} \\ i\sqrt{\frac{1}{3}} \end{bmatrix} \begin{bmatrix} \sqrt{\frac{2}{3}} & -i\sqrt{\frac{1}{3}} \end{bmatrix}$$

$$= \quad |\psi\rangle\langle\psi|$$

where

$$|\psi\rangle = \begin{bmatrix} \sqrt{\frac{2}{3}} \\ i\sqrt{\frac{1}{3}} \end{bmatrix} \text{ is called a } \textbf{ket}$$

$$\langle\psi| = \begin{bmatrix} \sqrt{\frac{2}{3}} & -i\sqrt{\frac{1}{3}} \end{bmatrix} \text{ is called a } \textbf{bra}$$

- A rank one density matrices is called a **pure state**. Otherwise it's called a **mixed state**.
  - We represent pure states simply by their vector $|\psi\rangle \in \mathbb{C}^2$.
  - The standard basis in $\mathbb{C}^2$ is called the **computational basis**.

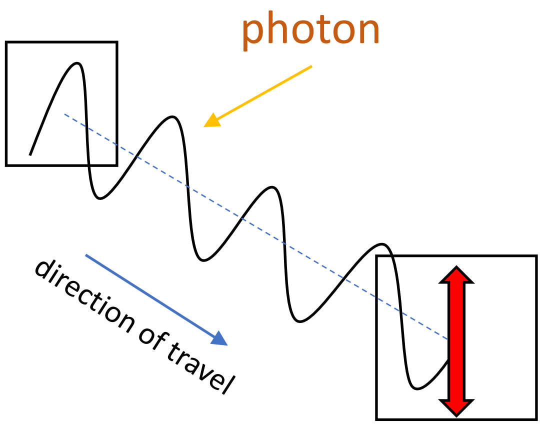
$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- A general pure state:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

$|\alpha|^2 + |\beta|^2 = 1$

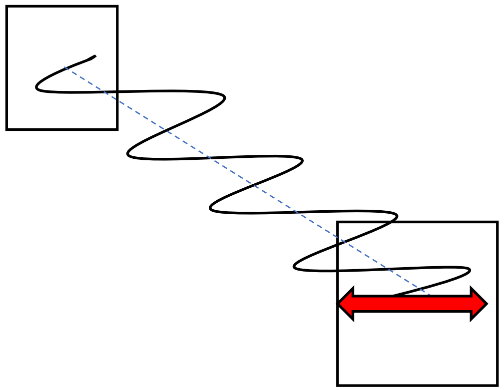
The Theory of Qubits



Vertical polarization

$$|0\rangle$$

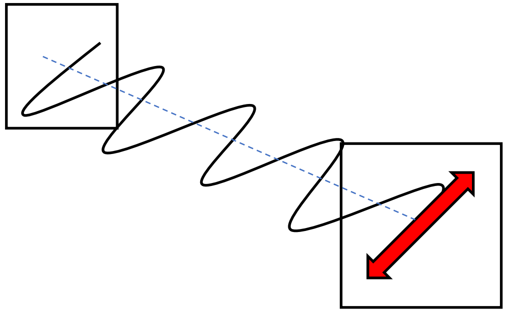
$$\rho = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$



Horizontal polarization

$$|1\rangle$$

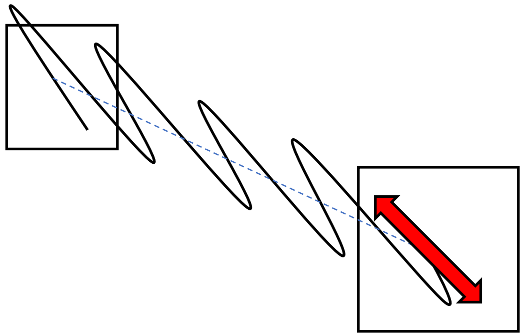
$$\rho = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$



Diagonal up polarization

$$|+\rangle = \sqrt{\tfrac{1}{2}}(|0\rangle + |1\rangle)$$

$$\rho_{+} = \tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$



Diagonal down polarization

$$|-\rangle = \sqrt{\tfrac{1}{2}}(|0\rangle - |1\rangle)$$

$$\rho_{-} = \tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

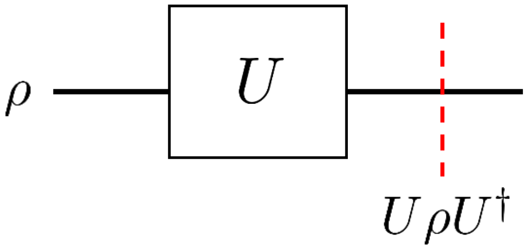
The Theory of Qubits

- How do the states of qubit systems evolve in time?

Reversible evolution of the system is described by **unitary** dynamics.

$$\rho \mapsto U\rho U^\dagger, \qquad \text{where } U \text{ is a unitary operator, i.e. } U^\dagger U = \mathbb{I} := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

A unitary U is also called a **gate**.

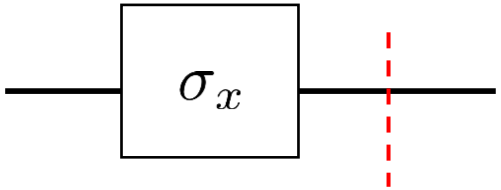


Example:

Pauli matrices
$$\begin{cases} \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \text{Bit flip:} \quad \begin{matrix} \sigma_x|0\rangle = |1\rangle \\ \sigma_x|1\rangle = |0\rangle \end{matrix} \\ \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} & \text{Phase flip:} \quad \begin{matrix} \sigma_z|0\rangle = |0\rangle \\ \sigma_z|1\rangle = -|1\rangle \end{matrix} \\ \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & \text{Bit + Phase flip:} \quad \begin{matrix} \sigma_y|0\rangle = i|1\rangle \\ \sigma_y|1\rangle = -i|0\rangle \end{matrix} \end{cases}$$

Example:

$$\rho = \begin{bmatrix} p & re^{i\phi} \\ re^{-i\phi} & 1-p \end{bmatrix}$$



$$U\rho U^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} p & re^{i\phi} \\ re^{-i\phi} & 1-p \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1-p & re^{-i\phi} \\ re^{i\phi} & p \end{bmatrix}$$

The Theory of Qubits

- We represent multiple qubits by taking tensor products of $\mathbb{C}^2$.

"superposition" of states

An n-qubit state lives in $\mathbb{C}^{2^n}$ and is expressed as a linear combination of 2^n basis vectors:

$$|\psi\rangle = \sum_{b_1=0}^{1} \sum_{b_2=0}^{1} \cdots \sum_{b_n=0}^{1} \Gamma_{b_1,b_2,\cdots,b_n} |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle \qquad \Gamma_{b_1,b_2,\cdots,b_n} \in \mathbb{C}$$

First qubit

Second qubit

N^{th} qubit

- The physical correspondence still remains:

Every $|\psi\rangle \in \mathbb{C}^{2^n}$ corresponds to a physically realizable state of an n-qubit system!!

$$|\psi\rangle = \sum_{b_1=0}^{1} \sum_{b_2=0}^{1} \cdots \sum_{b_N=0}^{1} \Gamma_{b_1,b_2,\cdots,b_n} |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle$$

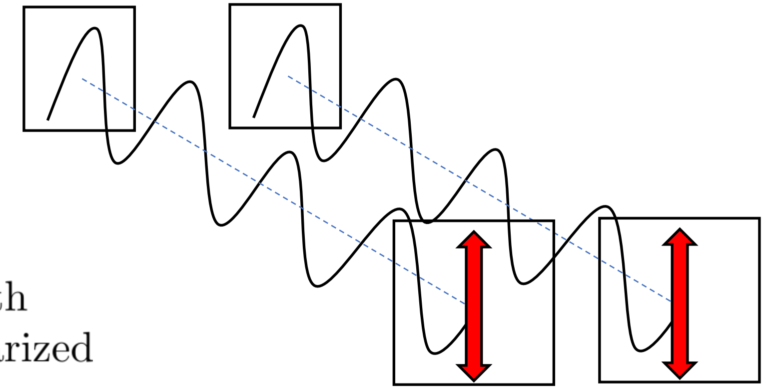
The Theory of Qubits

Example: Consider a two-qubit photon system.

First photon — Second photon

$$|0\rangle \otimes |0\rangle$$

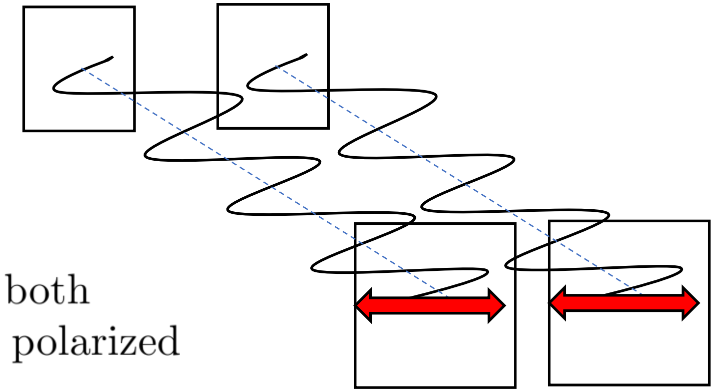
Corresponds to both photons vertically polarized



First photon — Second photon

$$|1\rangle \otimes |1\rangle$$

Corresponds to both photons horizontally polarized



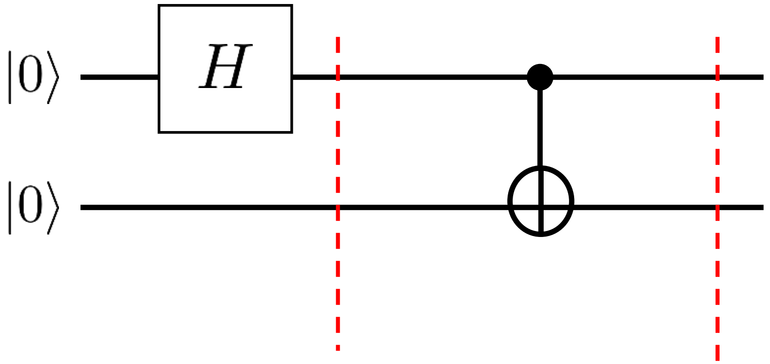
- But the linear combination state $|\Phi\rangle = \sqrt{\frac{1}{2}}\Big(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\Big)$ must also be physically realizable!

However, in $|\psi\rangle$ the individual photons do not have a definite polarization state.

States of this form are called **entangled**.

The Theory of Qubits

Building entangled states:



$$\sqrt{\tfrac{1}{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

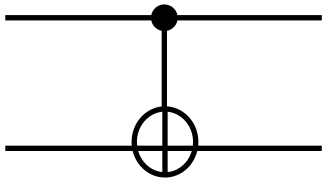
$$\sqrt{\frac{1}{2}}\Big(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\Big)$$

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

Hadamard gate

$$H|0\rangle = \sqrt{\tfrac{1}{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \sqrt{\tfrac{1}{2}}(|0\rangle - |1\rangle)$$



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

Two-qubit controlled-not (CNOT) gate

$$\mathrm{CNOT}(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$$
$$\mathrm{CNOT}(|0\rangle \otimes |1\rangle) = |0\rangle \otimes |1\rangle$$
$$\mathrm{CNOT}(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle$$
$$\mathrm{CNOT}(|1\rangle \otimes |1\rangle) = |1\rangle \otimes |0\rangle$$

- By repeating CNOT with different single-qubit gates, more sophisticated entangled states with more qubits can be constructed.

DiVincenzo's Five Requirements for the Implementation of Quantum Computation

1. A scalable physical system with well-characterized qubits
2. **A qubit-specific measurement capability**
3. The ability to initialize the state of the qubits to a simple fiducial state, such as $|000 \ldots\rangle$
4. A "universal" set of quantum gates
5. Long relevant decoherence times, much longer than the gate operation time

Quantum Measurement

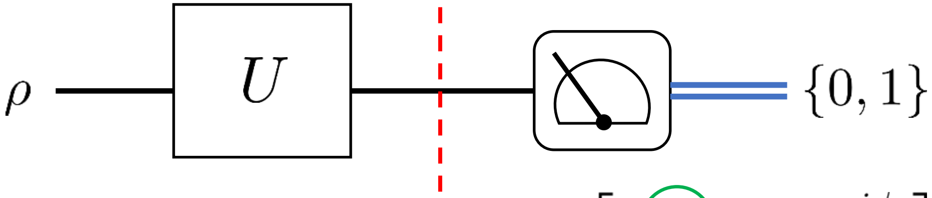
- How do we measure the state of a qubit?

A standard measurement involves

(i) a unitary gate, followed by

"wave function collapse"

(ii) a projection onto either the $|0\rangle$ or $|1\rangle$ state;
the measurement device outputs either "0" or "1" indicating which projection occured

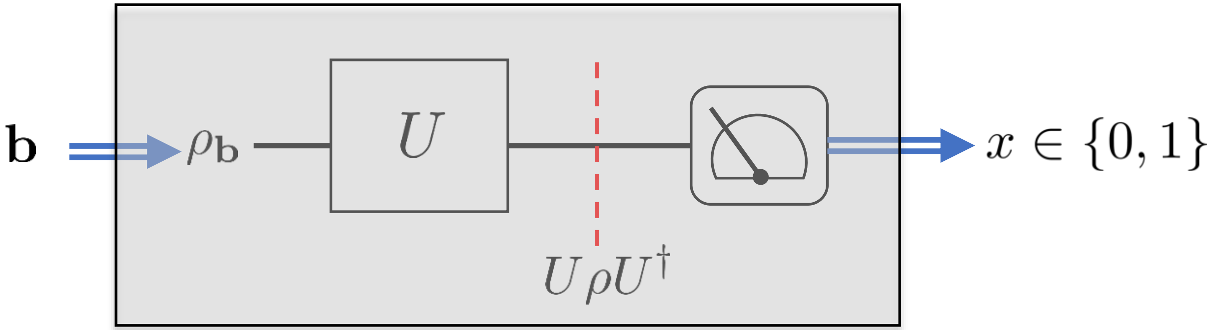


$$U\rho U^\dagger = \begin{bmatrix} p & re^{i\phi} \\ re^{-i\phi} & 1-p \end{bmatrix}$$

Quantum indeterminism

The probability of outcome 0 is *p*

The probability of outcome 1 is *1 - p*

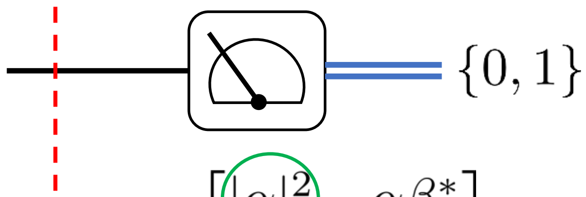


A one qubit "quantum computing" device that stochastically maps $\mathbb{Z}_2^m \to \mathbb{Z}_2$ with transition probabilities

$$P(x|\mathbf{b}) = \langle x|U\rho_\mathbf{b}U^\dagger|x\rangle.$$

Quantum Measurement

- For pure states:



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

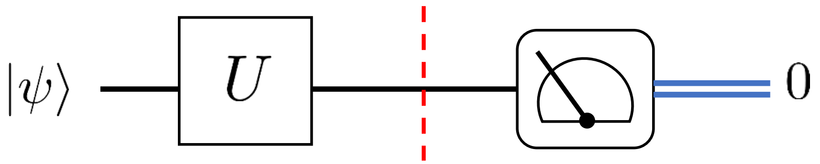
$$|\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}$$

The probability of outcome 0 is $|\alpha|^2$

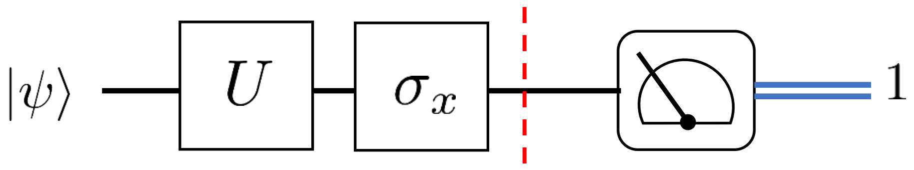
The probability of outcome 1 is $|\beta|^2$

- Why are pure states special?

  We can always perform a gate that rotates any state $|\psi\rangle$ either to $|0\rangle$ or $|1\rangle$.

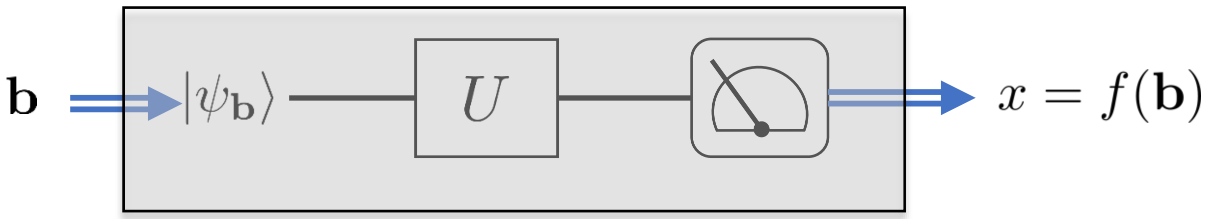


$$U|\psi\rangle = |0\rangle$$



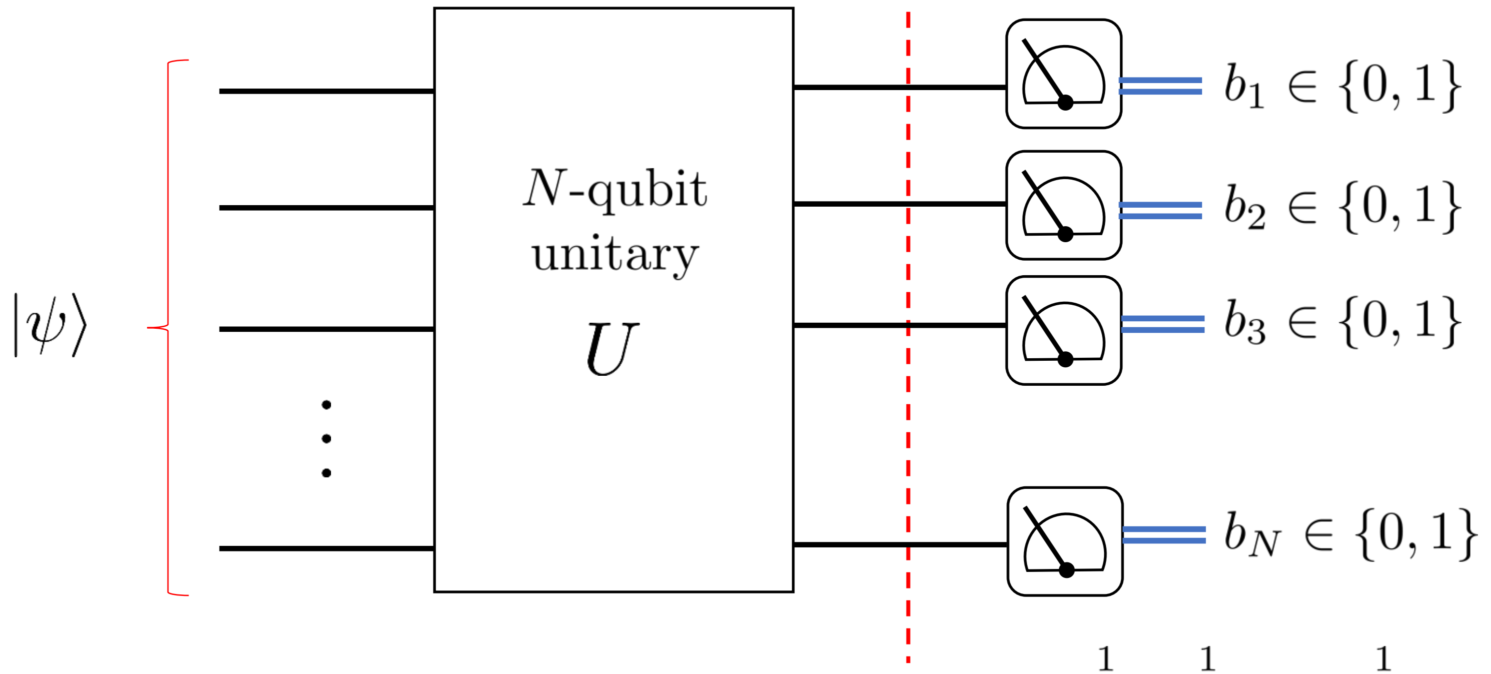
$$\sigma_x U|\psi\rangle = |1\rangle$$

The outcomes are no longer stochastic, and we can design quantum “black boxes” (i.e. circuits) that compute functions.



Quantum Measurement

- Multi-qubit measurements are done in the same way:



$$U|\psi\rangle = \sum_{b_1=0}^{1} \sum_{b_2=0}^{1} \cdots \sum_{b_n=0}^{1} \Gamma_{b_1,b_2,\cdots,b_n} |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle$$

- Probability of measuring n-bit string $\mathbf{b} = (b_1, b_2, \cdots, b_n) \in \mathbb{Z}_2^n$ is $|\Gamma_{b_1,b_2,\cdots,b_n}|^2$.

DiVincenzo’s Five Requirements for the Implementation of Quantum Computation

1. A scalable physical system with well-characterized qubits
2. A qubit-specific measurement capability
3. **The ability to initialize the state of the qubits to a simple fiducial state, such as $|000\ldots\rangle$**
4. A “universal” set of quantum gates
5. Long relevant decoherence times, much longer than the gate operation time

The Quantum Circuit Model

- The quantum cricuit model describes a standard approach to computing some function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ using a quantum computer.

- The input $\mathbf{b} \in \mathbb{Z}_2^n$ is encoded in an n-qubit computational basis state:

$$\mathbf{b} = (b_1, b_2, \cdots, b_n) \quad \to \quad |\mathbf{b}\rangle = |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle$$

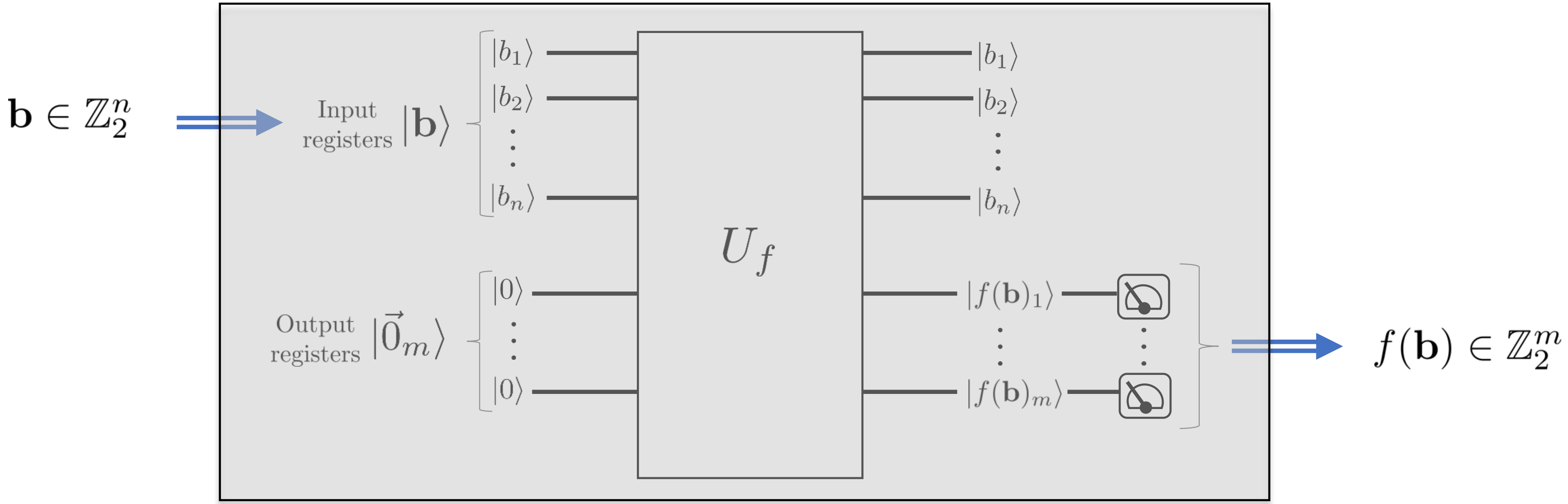
- The function f is encoded into a unitary U_f that reversibly maps $|\mathbf{b}\rangle$ to $|f(\mathbf{b})\rangle$.

- A standard (but not always optimal) form of unitary computation:

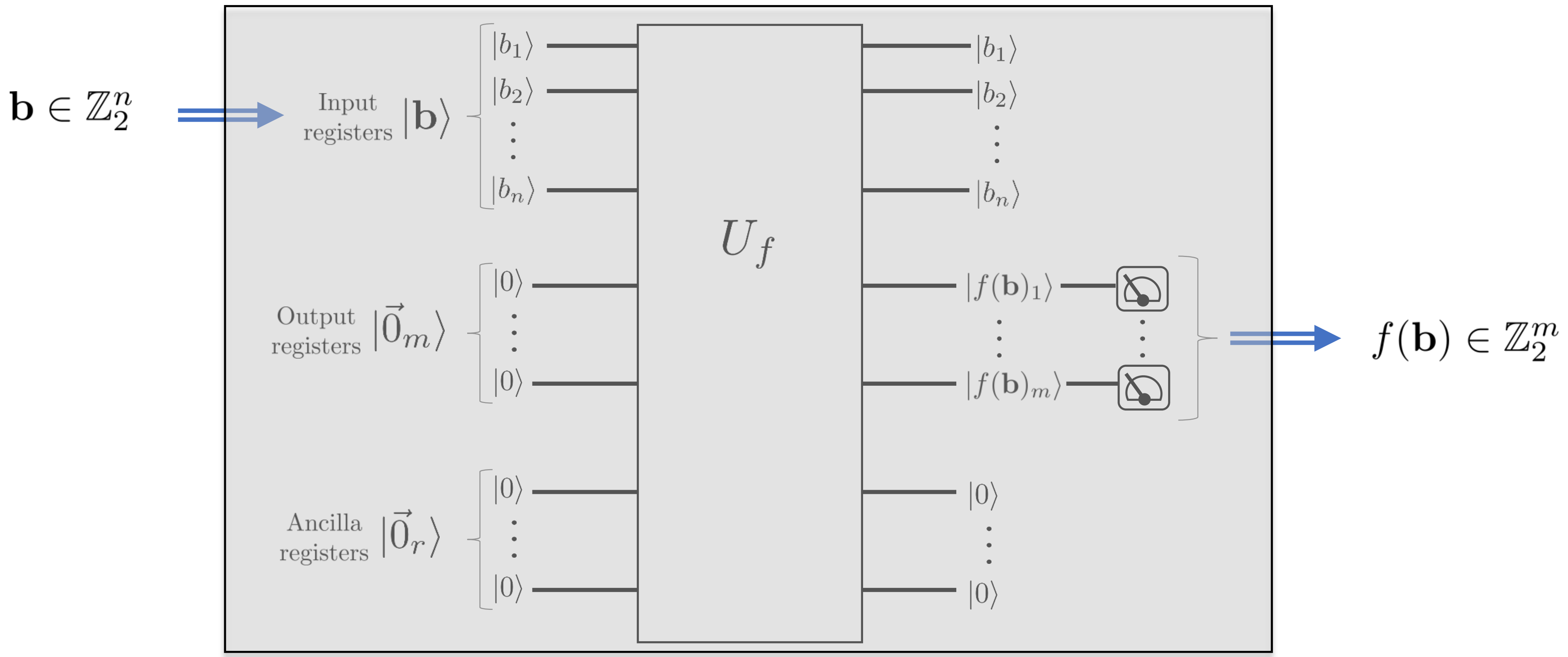
$$\forall\ \mathbf{b} \in \mathbb{Z}_2^n \quad \forall\ \mathbf{x} \in \mathbb{Z}_2^m: \qquad U_f(\underset{\text{Input registers}}{|\mathbf{b}\rangle} \otimes \underset{\text{Output registers}}{|\mathbf{x}\rangle}) = |\mathbf{b}\rangle \otimes |\underset{\text{Measure output registers to learn } \mathbf{x} \oplus f(\mathbf{b})}{\mathbf{x} \oplus f(\mathbf{b})}\rangle.$$

Initialize the m output registers in the $|0\rangle$ state (i.e. $\mathbf{x} = 0$): $|\vec{0}_m\rangle = |0\rangle \otimes \cdots \otimes |0\rangle$

The Quantum Circuit Model



The Quantum Circuit Model



The Quantum Circuit Model

Exercise: Let's build the full binary adder:

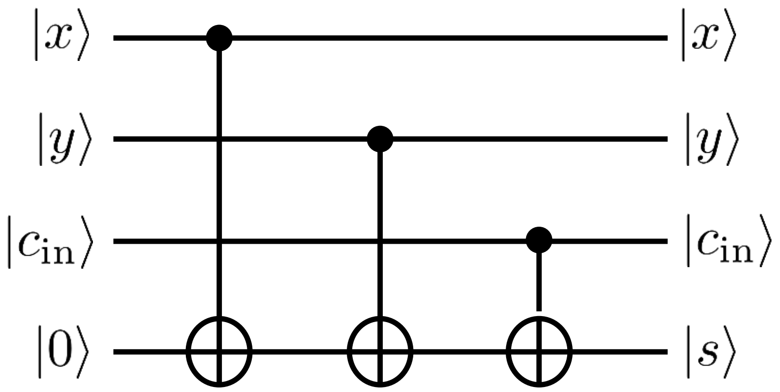
x	y	c_{in}	s	c_{out}
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

$$|x,\ y,\ c_{\text{in}}\rangle \otimes |00\rangle \mapsto |x,\ y,\ c_{\text{in}}\rangle \otimes |s,\ c_{\text{out}}\rangle$$

Input registers

Output registers

$$s = x \oplus y \oplus c_{\text{in}}$$



The Quantum Circuit Model

Exercise: Let's build the full binary adder:

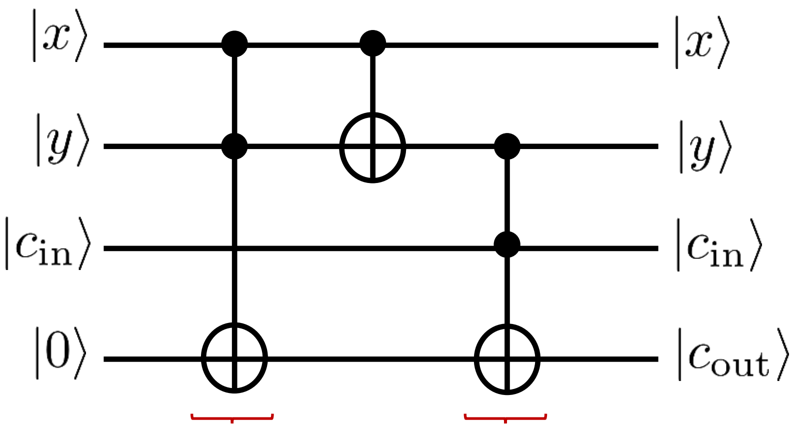
x	y	c_{in}	s	c_{out}
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

$$|x,\ y,\ c_{\text{in}}\rangle \otimes |00\rangle \mapsto |x,\ y,\ c_{\text{in}}\rangle \otimes |s,\ c_{\text{out}}\rangle$$

Input registers

Output registers

$$c_{\text{out}} = xy \oplus (x \oplus y)c_{\text{in}}$$



Toffoli gates

- **Toffoli** three-qubit gate:

$$|x,\ y,\ 0\rangle \mapsto |x,\ y,\ xy\rangle$$

(logical "**and**" gate)

The Quantum Circuit Model

Exercise: Let's build the full binary adder:

x	y	c_{in}	s	c_{out}
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

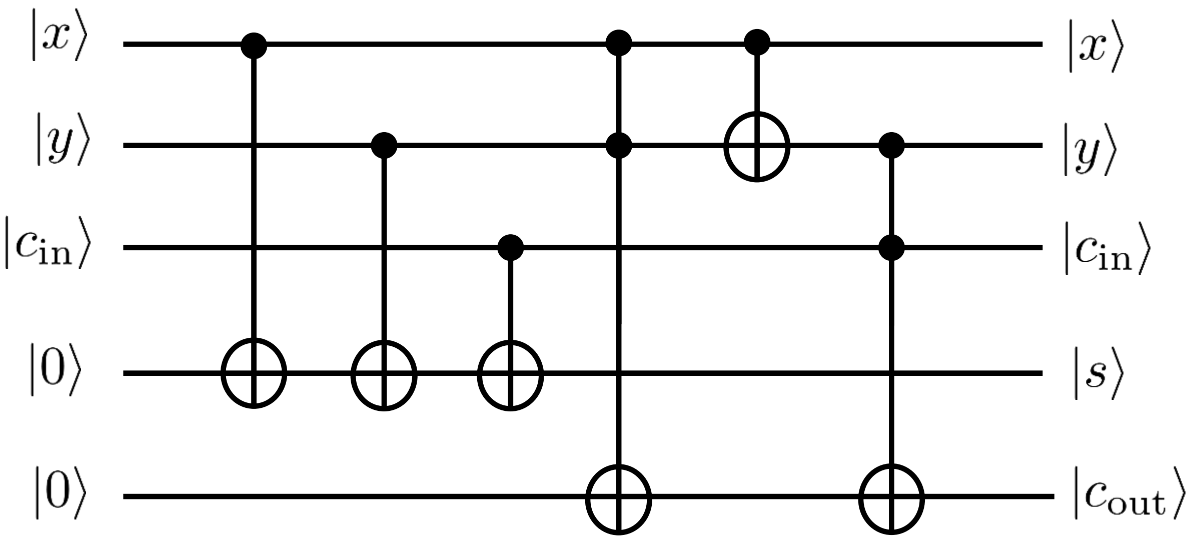
$$|x,\ y,\ c_{\text{in}}\rangle \otimes |00\rangle \mapsto |x,\ y,\ c_{\text{in}}\rangle \otimes |s,\ c_{\text{out}}\rangle$$

Input registers

Output registers

$$s = x \oplus y \oplus c_{\text{in}}$$

$$c_{\text{out}} = xy \oplus (x \oplus y)c_{\text{in}}$$



The Quantum Circuit Model

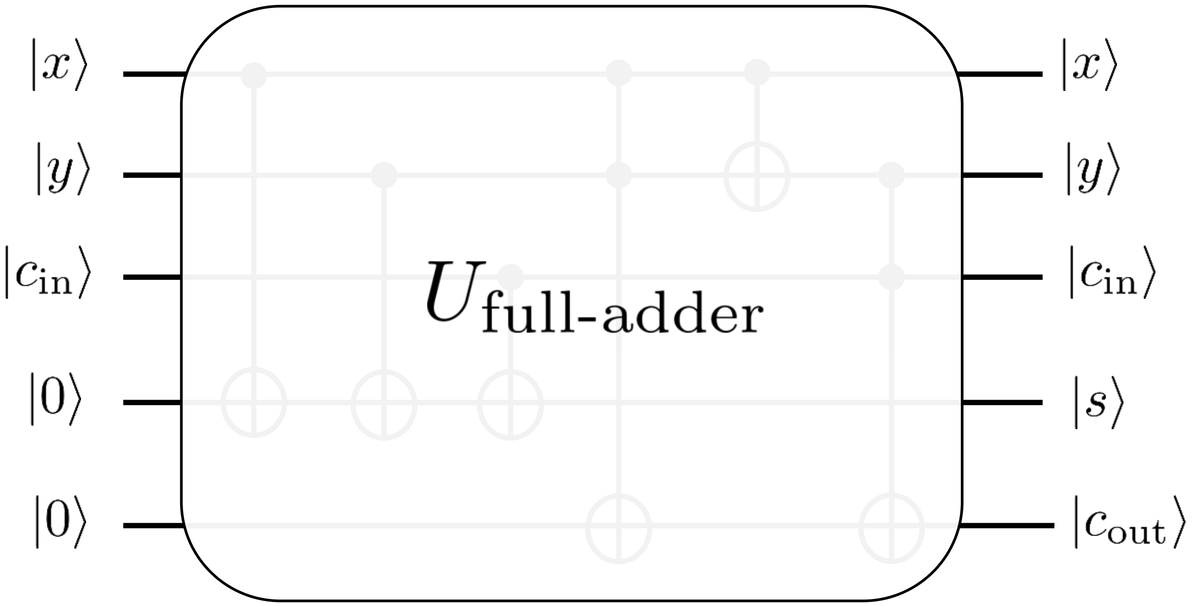
Exercise: Let's build the full binary adder:

x	y	c_{in}	s	c_{out}
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

What's the big deal!?!

Isn't this just implementing the logic of a classical circuit?

Not quite...



The Quantum Circuit Model

Exercise: Let's build the full binary adder:

x	y	c_{in}	s	c_{out}
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

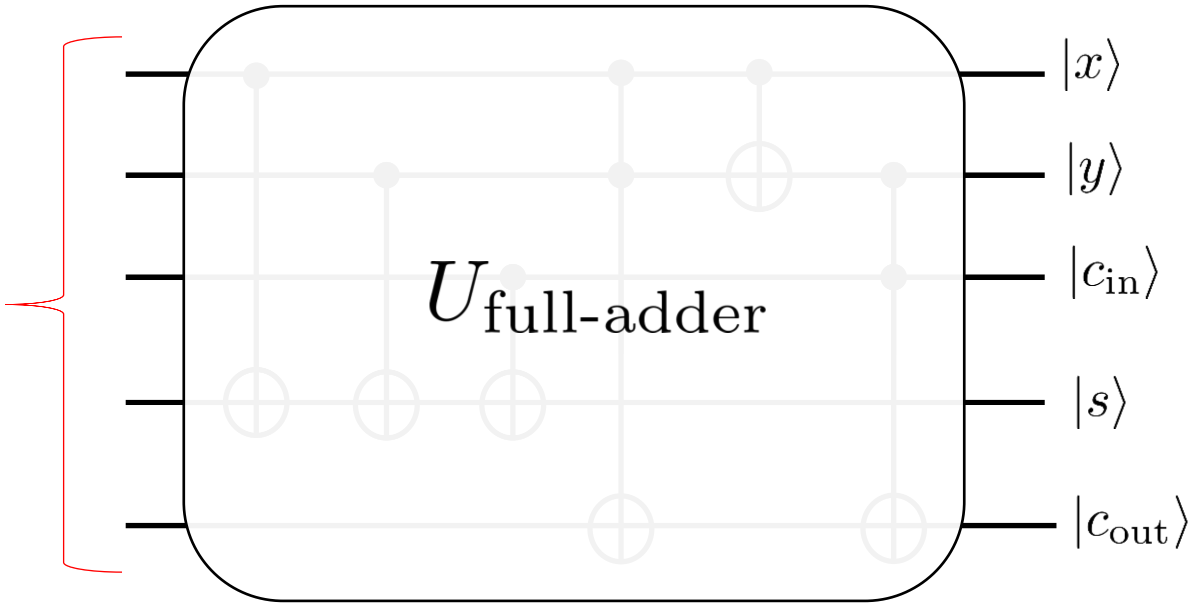
What's the big deal!?!

Isn't this just implementing the logic of a classical circuit?

Not quite...

$$|\psi\rangle = \sum_{x,y,c_{\text{in}}=0}^{1} \Gamma_{x,y,c_{\text{in}}} |x, y, c_{\text{in}}\rangle |0, 0\rangle$$

We can run our circuit on superpositions of inputs!



The Quantum Circuit Model

Exercise: Let's build the full binary adder:

x	y	c_{in}	s	c_{out}
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

- The answers to all possible inputs are encoded in the single output state.
- Unfortunately there is no way to access all of these answers at once.
- Instead we must find some other clever way to use this superposition to learn some (partial) information about the answers.

$$|\psi\rangle = \sum_{x,y,c_{\text{in}}=0}^{1} \Gamma_{x,y,c_{\text{in}}} |x, y, c_{\text{in}}\rangle |0, 0\rangle \xrightarrow{U_{\text{full-adder}}} \sum_{x,y,c_{\text{in}}=0}^{1} \Gamma_{x,y,c_{\text{in}}} |x, y, c_{\text{in}}\rangle |\overbrace{x \oplus y \oplus c_{\text{in}}}^{s}\rangle |\overbrace{xy \oplus (x \oplus y)c_{\text{in}}}^{c_{\text{out}}}\rangle$$

We can run our circuit on superpositions of inputs!

DiVincenzo's Five Requirements for the Implementation of Quantum Computation

1. A scalable physical system with well-characterized qubits

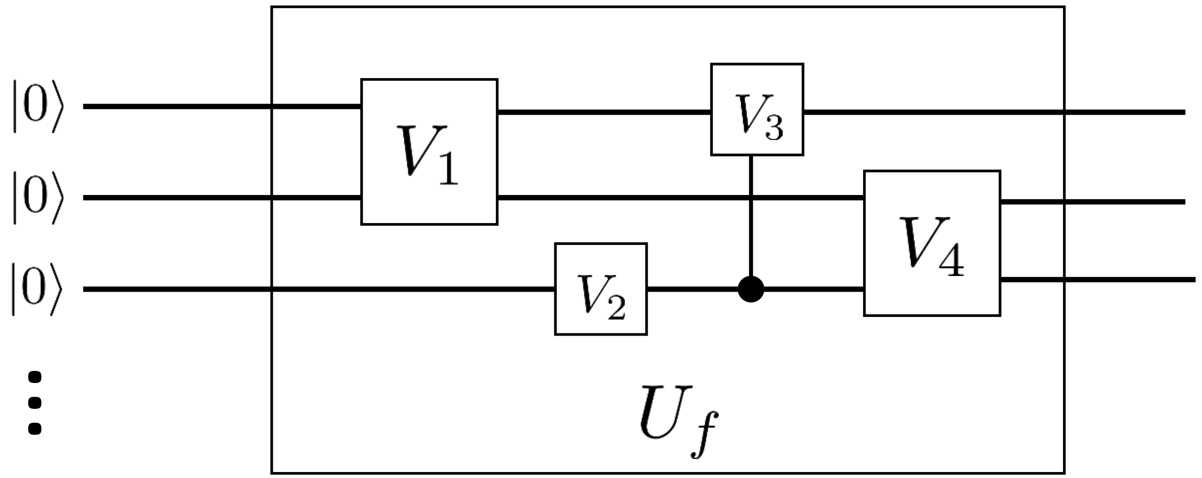
2. A qubit-specific measurement capability

3. The ability to initialize the state of the qubits to a simple fiducial state, such as $|000 \dots\rangle$

4. **A "universal" set of quantum gates**

5. Long relevant decoherence times, much longer than the gate operation time

A Universal Gate Set



- A universal gate set is a subset of gates that can be combined in series and parallel to perform any N-qubit gate (or approximate to arbitrary precision).

Theorem: A universal gate set if given by:

$$H = \sqrt{\frac{1}{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \qquad T = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix} \qquad \mathrm{CNOT} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

A Universal Gate Set

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad -\boxed{\sigma_z}- \quad = \quad -\boxed{T}-\boxed{T}-\boxed{T}-\boxed{T}-$$

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad -\boxed{\sigma_x}- \quad = \quad -\boxed{H}-\boxed{\sigma_z}-\boxed{H}-$$

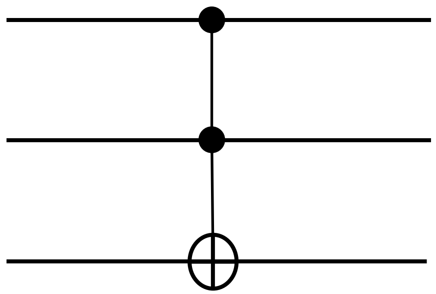
$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad -\boxed{\sigma_y}- \quad = \quad -\boxed{T}-\boxed{T}-\boxed{\sigma_x}-\boxed{\sigma_z}-\boxed{T}-\boxed{T}-$$

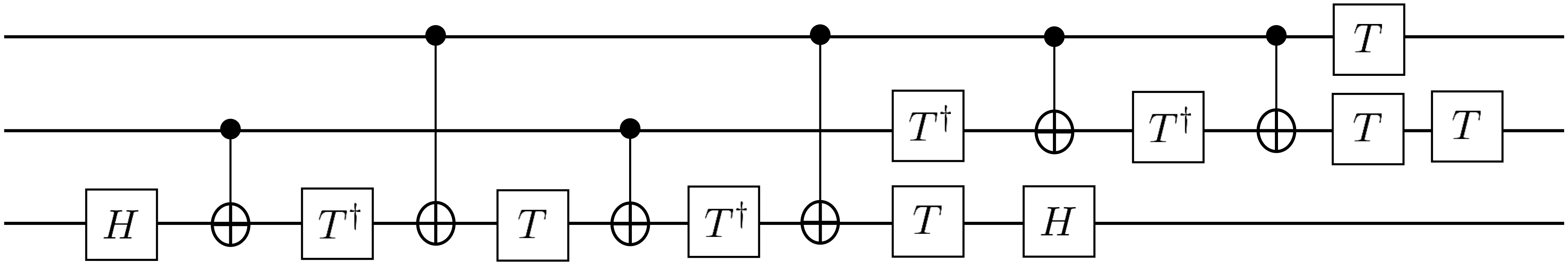
Theorem: A universal gate set if given by:

$$H = \sqrt{\frac{1}{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \qquad \mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

A Universal Gate Set

Example: The Toffoli gate





- In fact, five CNOT gates are known to be necessary and sufficient for Toffoli.

DiVincenzo’s Five Requirements for the Implementation of Quantum Computation

1. A scalable physical system with well-characterized qubits
2. A qubit-specific measurement capability
3. The ability to initialize the state of the qubits to a simple fiducial state, such as $|000 \ldots\rangle$
4. A “universal” set of quantum gates
5. **Long relevant decoherence times, much longer than the gate operation time**

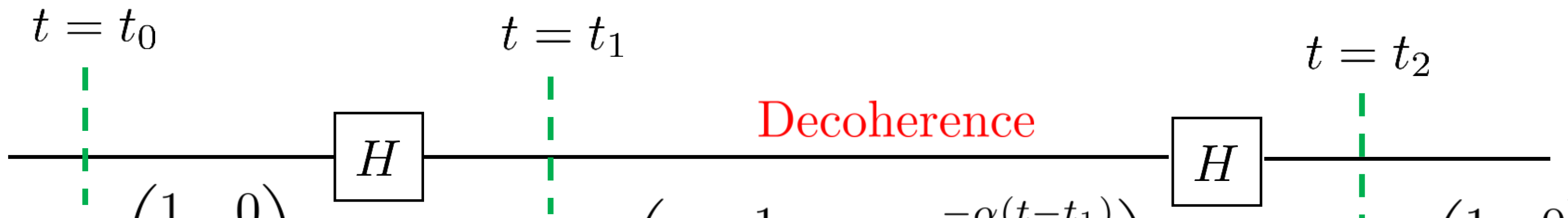
The Fight Against Decoherence

- Unwanted interaction with the environment will cause the qubits to go through a process known as **decoherence**.

Ideal:

$$\rho_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \rho_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \rho_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Actual:



$$\rho_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \rho_1 = \frac{1}{2}\begin{pmatrix} 1 & e^{-\alpha(t-t_1)} \\ e^{-\alpha(t-t_1)} & 1 \end{pmatrix} \qquad \rho_2 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + e^{-\alpha(t-t_1)}\frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The Fight Against Decoherence

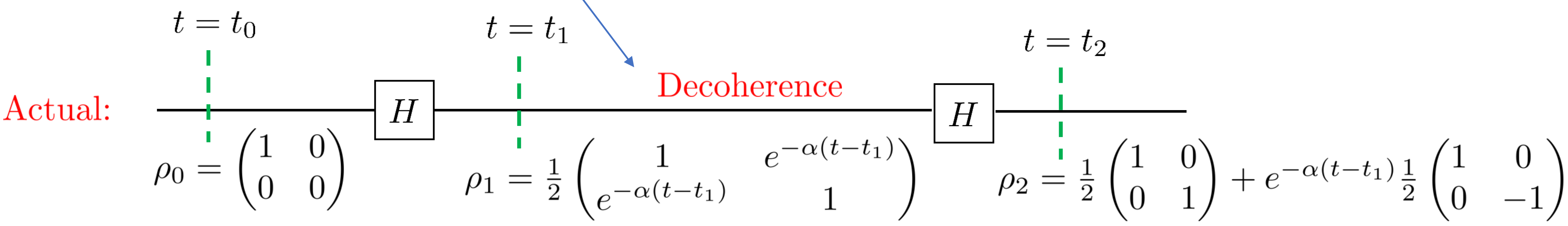
- The decoherence time should not significantly exceed the gate operation time.

- Provided this condition is met, decoherence errors between a sequence of quantum gates can be mitigated using **quantum error correction codes**.

- We can understand this as a random phase flip σ_z with probability $(1-e^{-\alpha(t-t_1)})/2$:

$$\rho_1 = \frac{1+e^{-\alpha(t-t_1)}}{2} H\rho_0 H + \frac{1-e^{-\alpha(t-t_1)}}{2}\sigma_z H\rho_0 H\sigma_z.$$

- If we can correct σ_z error we will recover the ideal process.



Quantum Error Correction

- To correct general qubit errors, it suffices to correct against Pauli errors.

Example: The Shor Nine-Qubit Code

Idea: Embed a qubit state into a nine-qubit state.

$$|0\rangle \mapsto |0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \mapsto |1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto \underbrace{|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle}_{\text{Logical qubit}}$$

- The logical qubit is protected against an error on any one of its nine physical qubits.

Quantum Error Correction

The Shor Nine-Qubit Code

phase errors

bit errors

Key observation - Any Pauli error will map $|0_L\rangle$ to one of $3 \cdot 9 = 27$ states

and $|1_L\rangle$ to one of $3 \cdot 9 = 27$ **orthogonal** states

$$|0_L\rangle = \frac{\overbrace{(|000\rangle + |111\rangle)}^{\textbf{Block 1}}\overbrace{(|000\rangle + |111\rangle)}^{\textbf{Block 2}}\overbrace{(|000\rangle + |111\rangle)}^{\textbf{Block 3}}}{2\sqrt{2}} \xrightarrow{P_{\text{err}}} \xrightarrow{U_{\text{fix}}} \rightarrow |0\rangle \otimes |b_1\rangle|b_2\rangle \otimes |b_3\rangle|b_4\rangle \otimes |b_5\rangle|b_6\rangle \otimes |00\rangle$$

Pauli error | error correction | phase error block label | bit error block label | bit error sub-block label

$$|1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} \xrightarrow[P_{\text{err}}]{} \xrightarrow[U_{\text{fix}}]{} \rightarrow |1\rangle \otimes |b_1\rangle|b_2\rangle \otimes |b_3\rangle|b_4\rangle \otimes |b_5\rangle|b_6\rangle \otimes |00\rangle$$

Example: A bit and phase flip (σ_y) on qubit six:

$$|0_L\rangle \mapsto \frac{(|000\rangle + |111\rangle)(|001\rangle - |110\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

All one-qubit errors on $|1_L\rangle$ are orthogonal to this!

$$|1_L\rangle \mapsto \frac{(|000\rangle - |111\rangle)(|001\rangle + |110\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

All one-qubit errors on $|0_L\rangle$ are orthogonal to this!

Quantum Error Correction

The Shor Nine-Qubit Code

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto |\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$$ Encoding

$$\mapsto P_{\text{err}}|\psi_L\rangle = \alpha P_{\text{err}}|0_L\rangle + \beta P_{\text{err}}|1_L\rangle$$ Single-qubit Pauli error

$$\mapsto U_{\text{fix}}P_{\text{err}}|\psi_L\rangle = \alpha U_{\text{fix}}P_{\text{err}}|0_L\rangle + \beta U_{\text{fix}}P_{\text{err}}|1_L\rangle$$ Error correction gate

$$= \alpha(|0\rangle\otimes|b_1\rangle|b_2\rangle|b_3\rangle|b_4\rangle|b_5\rangle|b_6\rangle|00\rangle)+\beta(|1\rangle\otimes|b_1\rangle|b_2\rangle|b_3\rangle|b_4\rangle|b_5\rangle|b_6\rangle|00\rangle)$$

$$= (\alpha|0\rangle + \beta|1\rangle) \otimes |b_1\rangle|b_2\rangle|b_3\rangle|b_4\rangle|b_5\rangle|b_6\rangle|00\rangle$$

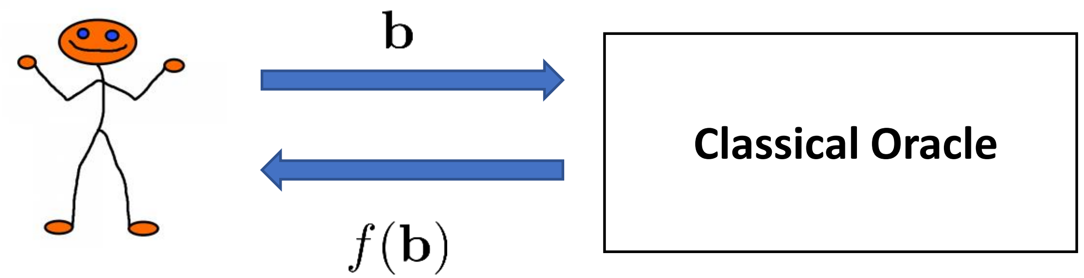
$$= |\psi\rangle \otimes |b_1\rangle|b_2\rangle|b_3\rangle|b_4\rangle|b_5\rangle|b_6\rangle|00\rangle$$

Error corrected!

Part II: Some Basic Examples

Query Model

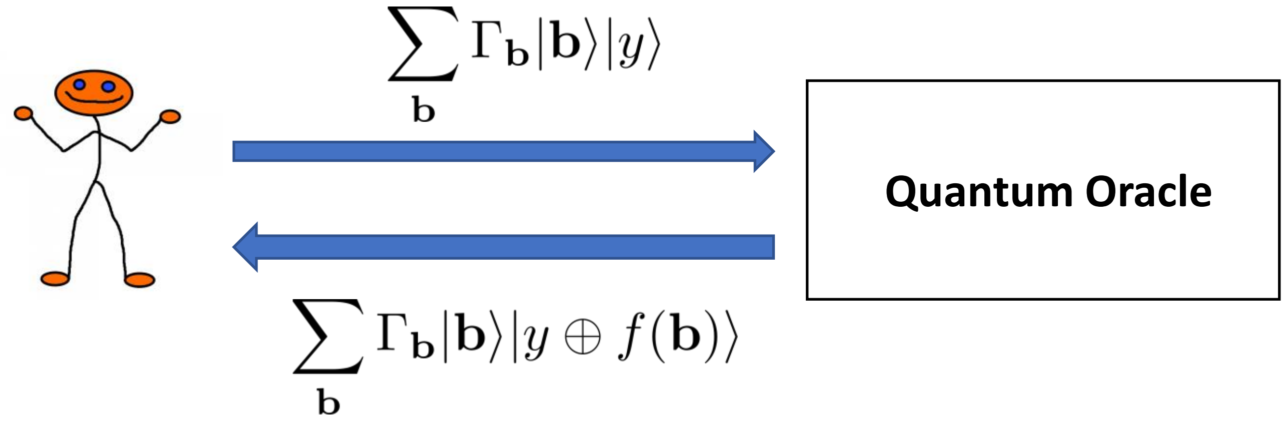
- Suppose a user has access to a "black box" that can compute a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ on a given input $\mathbf{b}$.
- The **query complexity** of f describes the number of calls an agent must make to the "black box" to compute $f(\mathbf{b})$ for an arbitrary $\mathbf{b}$.



Complexity $C(f)$

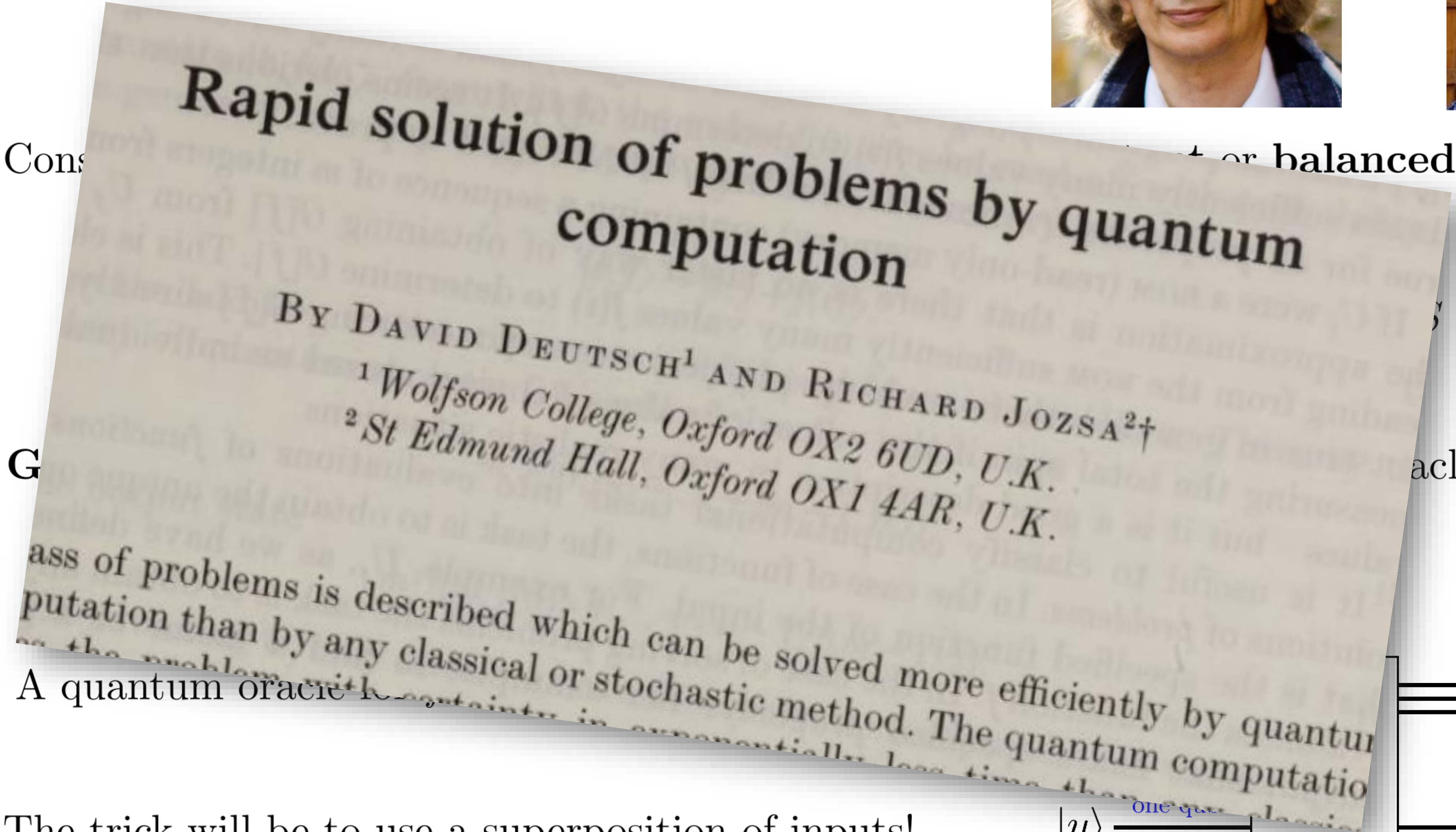
$C(f) >> Q(f)???$

Superposition queries



Complexity $Q(f)$

Deutsch-Jozsa Problem



Rapid solution of problems by quantum computation

By David Deutsch[1] and Richard Jozsa[2]†

[1] Wolfson College, Oxford OX2 6UD, U.K.

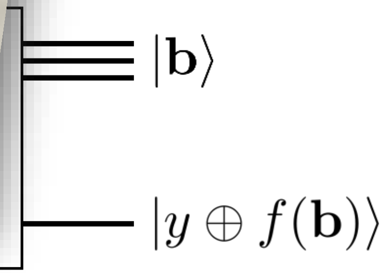
[2] St Edmund Hall, Oxford OX1 4AR, U.K.

ass of problems is described which can be solved more efficiently by quantu
putation than by any classical or stochastic method. The quantum computatio

- Cons ... t or **balanced**:

- **G** ... acle.

- A quantum oracle ...



- The trick will be to use a superposition of inputs!

Deutsch-Jozsa Problem

- Consider a Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ that is either **constant** or **balanced**:

$$\forall \mathbf{b} \in \mathbb{Z}_2^n : \quad f(\mathbf{b}) = c \in \{0, 1\}$$

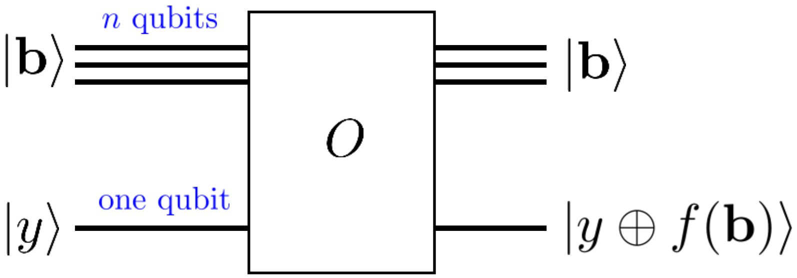
constant

$$\begin{array}{l} \exists\, S \subset \mathbb{Z}_2^n \\ |S| = 2^{n-1} : \end{array} \quad f(\mathbf{b}) = \begin{cases} 0 & \text{if } \mathbf{b} \in S \\ 1 & \text{if } \mathbf{b} \notin S \end{cases}$$

balanced

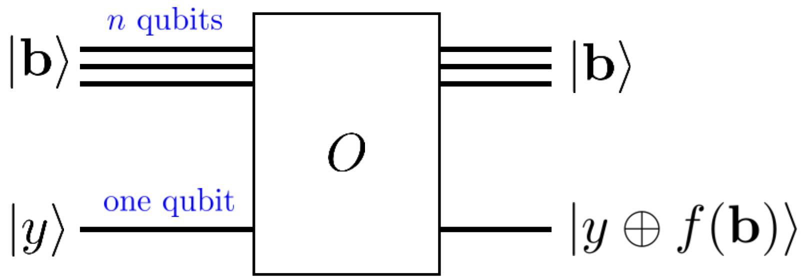
- **Goal:** Decide whether f is constant or balanced by making queries to the oracle.
    - Let $N := 2^n$. Then $C(f) = O(N)$.

- A quantum oracle for f functions as follows:



- The trick will be to use a superposition of inputs!

Deutsch-Jozsa Problem



$$O|\mathbf{b}\rangle|0\rangle = |\mathbf{b}\rangle|0 \oplus f(\mathbf{b})\rangle$$

$$O|\mathbf{b}\rangle|1\rangle = |\mathbf{b}\rangle|1 \oplus f(\mathbf{b})\rangle$$

"Eigenstate trick"

$$O|\mathbf{b}\rangle\left(|0\rangle - |1\rangle\right) = \begin{cases} |\mathbf{b}\rangle\left(|0\rangle - |1\rangle\right) & \text{if } f(\mathbf{b}) = 0 \\ |\mathbf{b}\rangle\left(-|0\rangle + |1\rangle\right) & \text{if } f(\mathbf{b}) = 1 \end{cases}$$

$$= (-1)^{f(\mathbf{b})}|\mathbf{b}\rangle(|0\rangle - |1\rangle)$$

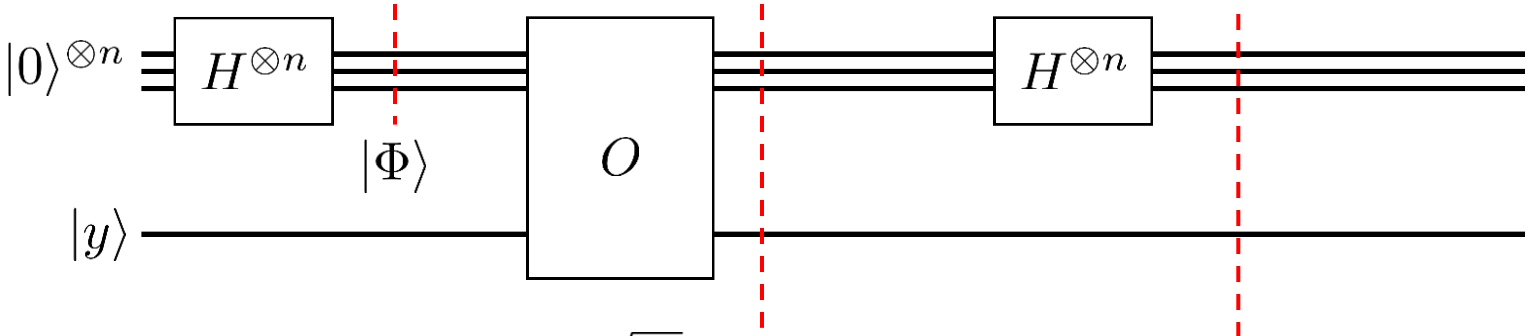
- It is customary to omit in calculations the oracle qubit $|y\rangle$ and just write the oracle action as

$$O|\mathbf{b}\rangle = (-1)^{f(\mathbf{b})}|\mathbf{b}\rangle.$$

- Consider a uniform superposition of all n-bit strings: $|\Phi\rangle := \left[\sqrt{\frac{1}{2}}\left(|0\rangle + |1\rangle\right)\right]^{\otimes n} = \sqrt{\frac{1}{N}} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} |\mathbf{b}\rangle$

$$\boxed{O|\Phi\rangle = \sqrt{\frac{1}{N}} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{b})}|\mathbf{b}\rangle}$$

Deutsch-Jozsa Problem



$$O|\Phi\rangle = \sqrt{\frac{1}{N}} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{b})}|\mathbf{b}\rangle \qquad H^{\otimes n}O|\Phi\rangle = \frac{1}{N} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{b})\oplus\mathbf{b}\cdot\mathbf{x}}|\mathbf{x}\rangle$$

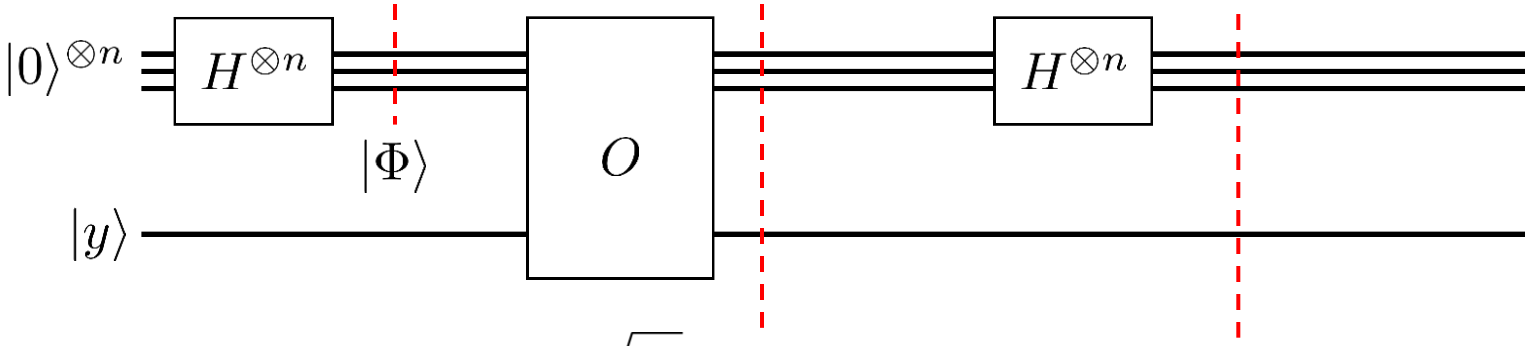
Fact:

$$H^{\otimes n}|\mathbf{b}\rangle = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\mathbf{b}\cdot\mathbf{x}}|\mathbf{x}\rangle$$

Check:

$$\begin{aligned} H^{\otimes n}|\mathbf{b}\rangle &= H|b_1\rangle \otimes H|b_2\rangle \otimes \cdots \otimes H|b_n\rangle \\ &= \frac{1}{\sqrt{2^n}}(|0\rangle + (-1)^{b_1}|1\rangle) \otimes (|0\rangle + (-1)^{b_2}|1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{b_n}|1\rangle). \end{aligned}$$

Deutsch-Jozsa Problem



$$O|\Phi\rangle = \sqrt{\tfrac{1}{N}} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{b})}|\mathbf{b}\rangle \qquad H^{\otimes n}O|\Phi\rangle = \tfrac{1}{N} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{b})\oplus\mathbf{b}\cdot\mathbf{x}}|\mathbf{x}\rangle$$

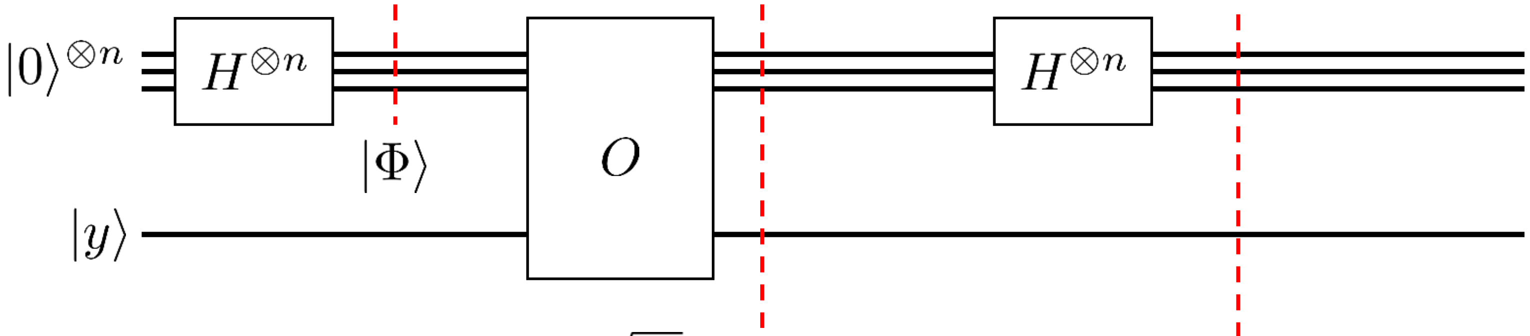
- If $f(\mathbf{b}) = c$ for all $\mathbf{b}$, then:

$$= (-1)^c \frac{1}{N} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{\mathbf{b}\cdot\mathbf{x}}|\mathbf{x}\rangle$$

$$= |0\rangle^{\otimes n}.$$

Use: $$\sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{\mathbf{b}\cdot\mathbf{x}} = \begin{cases} 0 & \text{if } \mathbf{x} \neq 0 \\ 2^n & \text{if } \mathbf{x} = 0 \end{cases} .$$

Deutsch-Jozsa Problem



$$O|\Phi\rangle = \sqrt{\tfrac{1}{N}} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{b})}|\mathbf{b}\rangle \qquad H^{\otimes n}O|\Phi\rangle = \frac{1}{N}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}\sum_{\mathbf{b}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{b})\oplus\mathbf{b}\cdot\mathbf{x}}|\mathbf{x}\rangle$$

- If f is balanced, then:

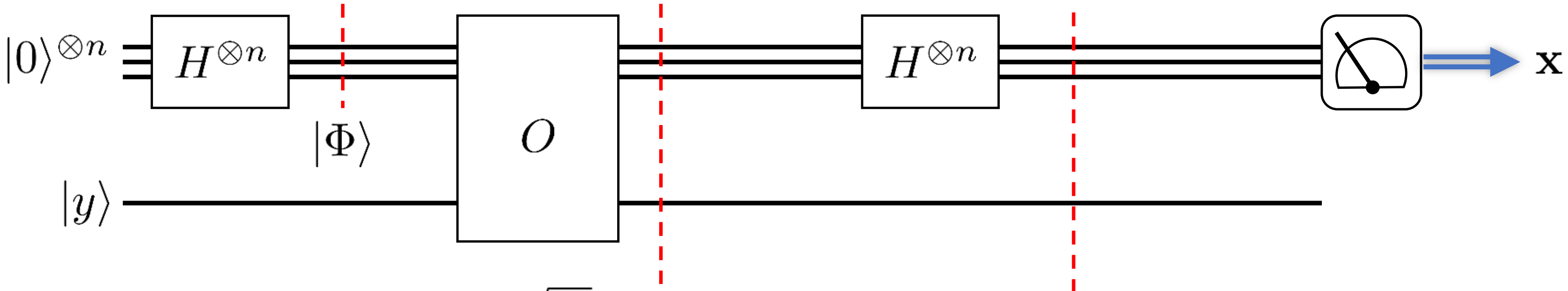
$$= \frac{1}{N}\left[\sum_{\mathbf{b}\in f^{-1}(0)} + \sum_{\mathbf{b}\in f^{-1}(1)}\right]\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{b})\oplus\mathbf{b}\cdot\mathbf{x}}|\mathbf{x}\rangle$$

- Notice that $|0\rangle^{\otimes n}$ component (i.e. $\mathbf{x}=0$) is

$$\frac{1}{N}\left[\sum_{\mathbf{b}\in f^{-1}(0)} + \sum_{\mathbf{b}\in f^{-1}(1)}\right]\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{b})} = 0.$$

Hence with probability 0 will outcome $\mathbf{x}=0$ be measured!

Deutsch-Jozsa Problem



$$O|\Phi\rangle = \sqrt{\frac{1}{N}} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{b})}|\mathbf{b}\rangle \qquad H^{\otimes n}O|\Phi\rangle = \frac{1}{N} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{b})\oplus\mathbf{b}\cdot\mathbf{x}}|\mathbf{x}\rangle$$

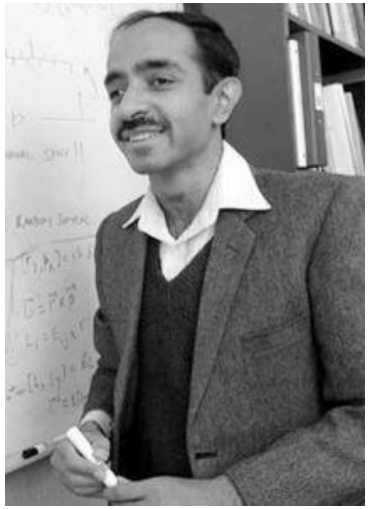
- f is constant if and only if $\mathbf{x} = 0$ is measured.

$$\Rightarrow \qquad Q(f) = 1 \quad < \quad C(f) = O(N)$$

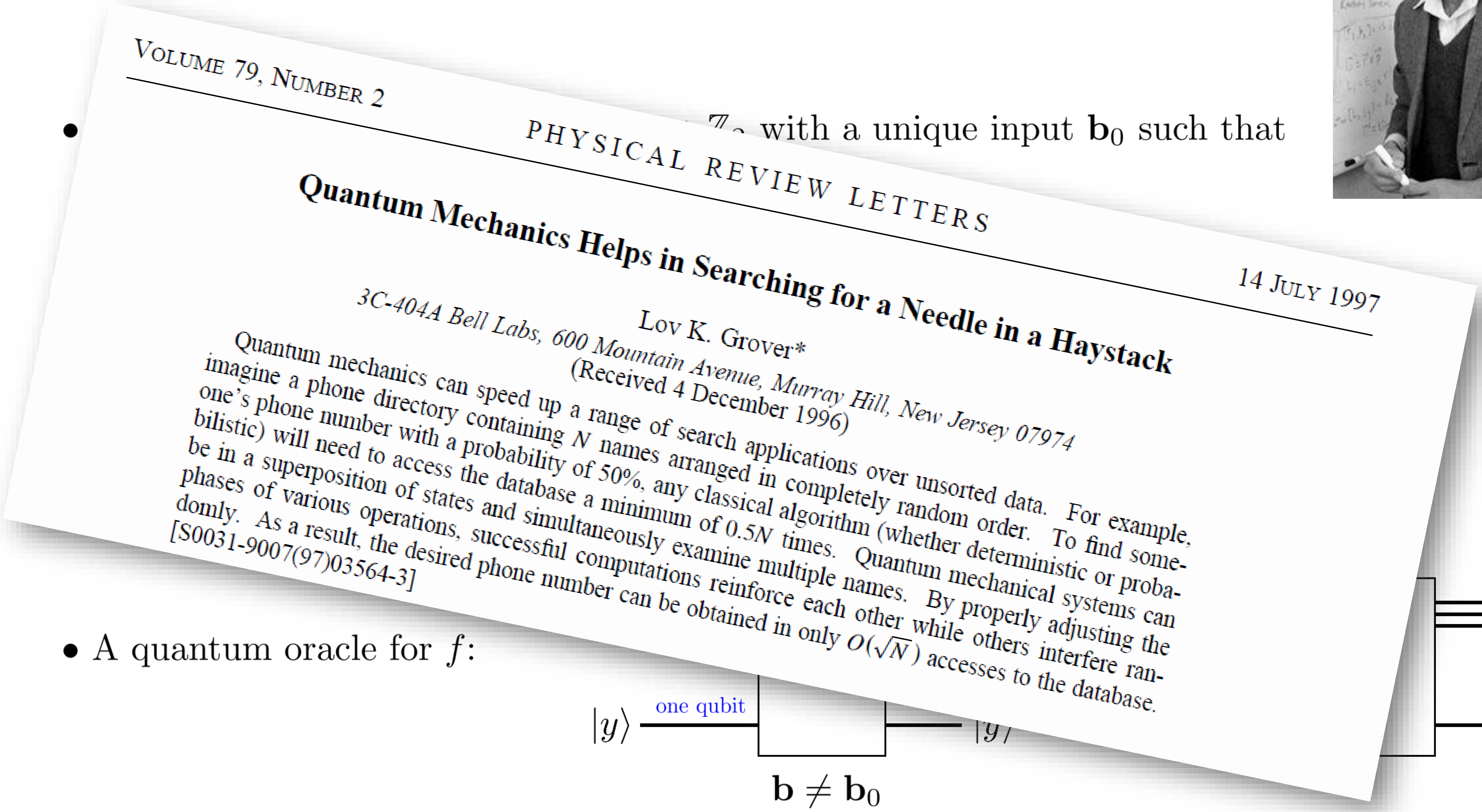
- However, there exists randomized classical algorithms that can solve this problem with small error.

- Can we obtain a separation between classical and quantum complexities even with bounded error?

Grover’s Search



- … with a unique input $\mathbf{b}_0$ such that



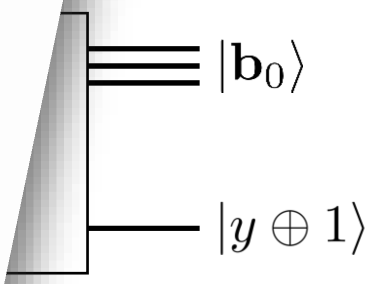
VOLUME 79, NUMBER 2 PHYSICAL REVIEW LETTERS 14 JULY 1997

Quantum Mechanics Helps in Searching for a Needle in a Haystack

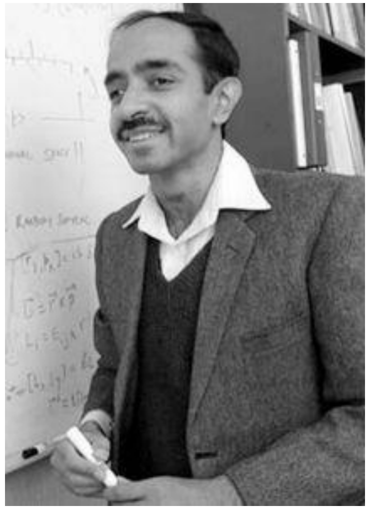
Lov K. Grover*
3C-404A Bell Labs, 600 Mountain Avenue, Murray Hill, New Jersey 07974
(Received 4 December 1996)

Quantum mechanics can speed up a range of search applications over unsorted data. For example, imagine a phone directory containing N names arranged in completely random order. To find someone’s phone number with a probability of 50%, any classical algorithm (whether deterministic or probabilistic) will need to access the database a minimum of $0.5N$ times. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names. By properly adjusting the phases of various operations, successful computations reinforce each other while others interfere randomly. As a result, the desired phone number can be obtained in only $O(\sqrt{N})$ accesses to the database. [S0031-9007(97)03564-3]

- A quantum oracle for f:



Grover’s Search

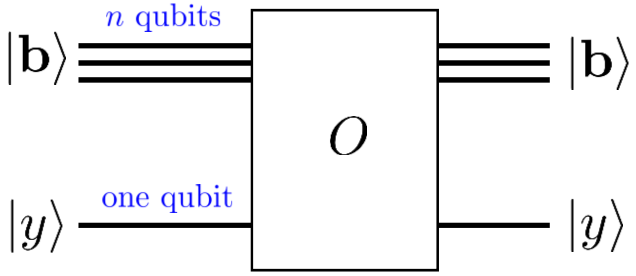


- Consider a Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ with a unique input $\mathbf{b}_0$ such that

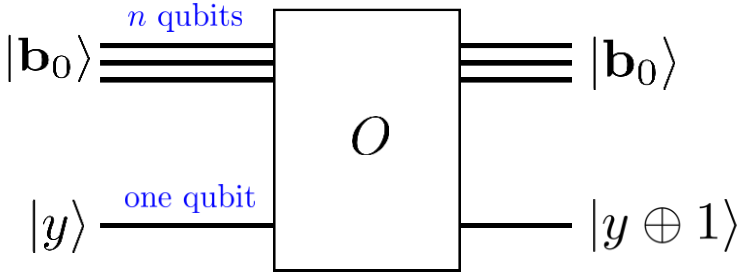
$$f(\mathbf{b}) = \begin{cases} 1 & \text{if } \mathbf{b} = \mathbf{b}_0 \\ 0 & \text{otherwise} \end{cases} .$$

- We can think of $\mathbf{b}_0$ as a “needle in a stack” of 2^n elements that can be identified by the function f.

- A quantum oracle for f:

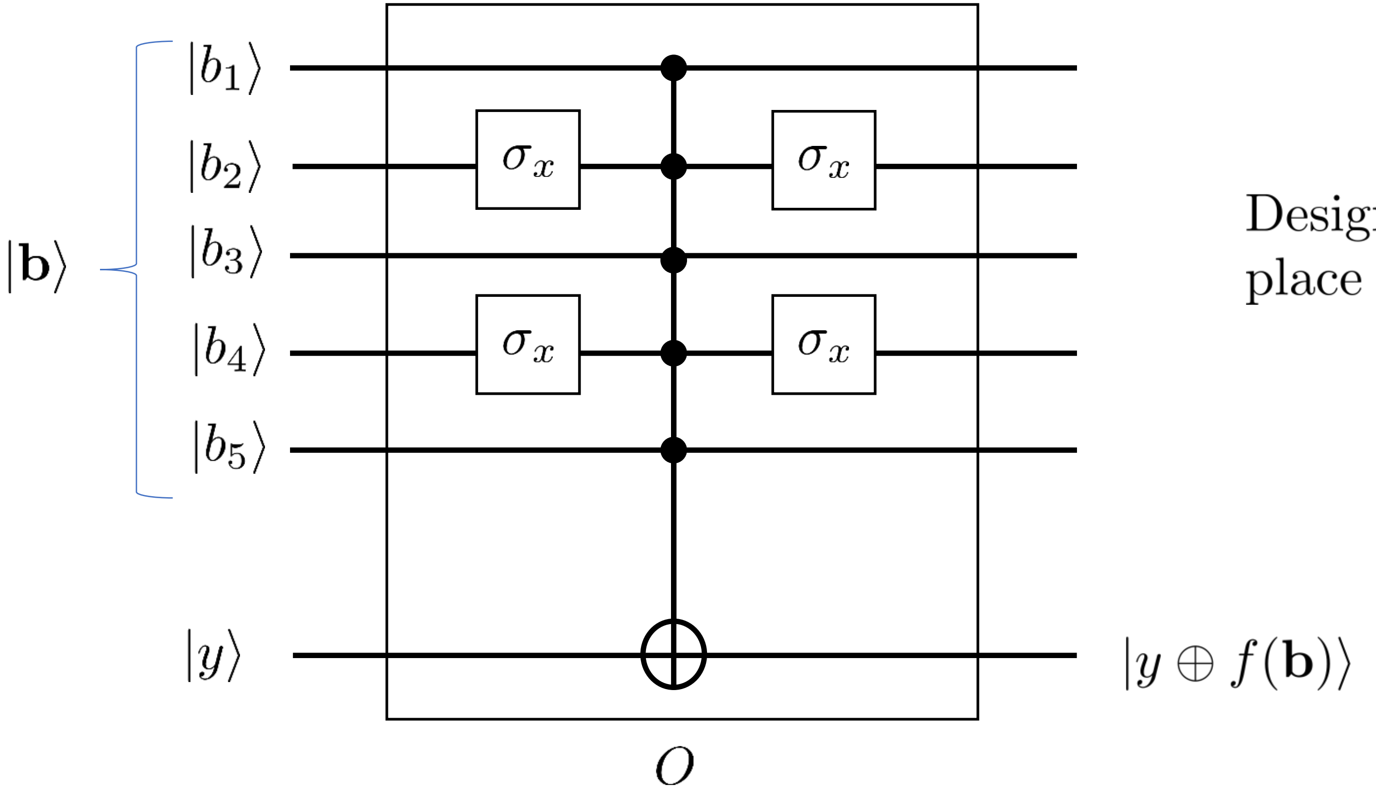


$\mathbf{b} \neq \mathbf{b}_0$



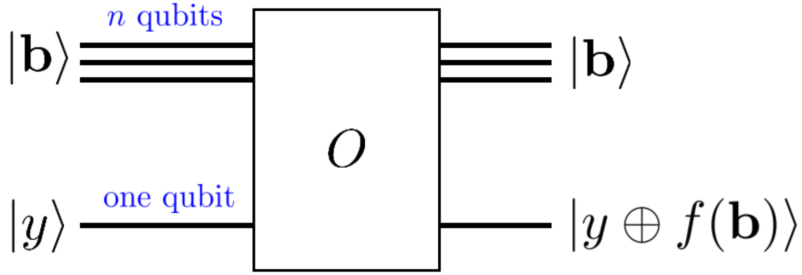
Grover's Search

- Inside the oracle:
  - Suppose $n = 5$ and $\mathbf{b}_0 = (1, 0, 1, 0, 1)$.



Design idea: Start with an n-qubit AND, place bit flips in the 0 positions of $\mathbf{b}_0$.

Grover's Search



$$O|\mathbf{b}\rangle|0\rangle = |\mathbf{b}\rangle|0 \oplus f(\mathbf{b})\rangle$$

$$O|\mathbf{b}\rangle|1\rangle = |\mathbf{b}\rangle|1 \oplus f(\mathbf{b})\rangle$$

"Eigenstate trick"

$$O|\mathbf{b}\rangle\left(|0\rangle - |1\rangle\right) = \begin{cases} |\mathbf{b}\rangle\left(|0\rangle - |1\rangle\right) & \text{if } f(\mathbf{b}) = 0 \\ |\mathbf{b}\rangle\left(-|0\rangle + |1\rangle\right) & \text{if } f(\mathbf{b}) = 1 \end{cases}$$

$$= (-1)^{f(\mathbf{b})}|\mathbf{b}\rangle(|0\rangle - |1\rangle)$$

- Suppose we input a uniform superposition of all n-bit strings:

$$|\Phi\rangle := \left[\sqrt{\tfrac{1}{2}}\left(|0\rangle + |1\rangle\right)\right]^{\otimes n} = \sqrt{\tfrac{1}{N}} \sum_{\mathbf{b}\in\mathbb{Z}_2^n} |\mathbf{b}\rangle$$

$$= \sqrt{\tfrac{1}{N}}|\mathbf{b}_0\rangle + \sqrt{\tfrac{N-1}{N}}|\overline{\mathbf{b}_0}\rangle \quad \Rightarrow \quad \boxed{O|\Phi\rangle = -\sqrt{\tfrac{1}{N}}|\mathbf{b}_0\rangle + \sqrt{\tfrac{N-1}{N}}|\overline{\mathbf{b}_0}\rangle}$$

Note: $|\mathbf{b}_0\rangle \perp |\overline{\mathbf{b}_0}\rangle$

where $|\overline{\mathbf{b}_0}\rangle = \sqrt{\tfrac{1}{N-1}} \sum_{\mathbf{b}\neq\mathbf{b}_0} |\mathbf{b}\rangle$

- The oracle "marks" the input $\mathbf{b}_0$ by a phase flip.

Grover's Search

$$\boxed{O|\Phi\rangle = -\sqrt{\tfrac{1}{N}}|\mathbf{b}_0\rangle + \sqrt{\tfrac{N-1}{N}}|\overline{\mathbf{b}_0}\rangle}$$

- The next step is to "amplify" the phase flip.

  This is done using the n-qubit unitary

$$W = 2|\Phi\rangle\langle\Phi| - \mathbb{I}.$$

$$|\Phi\rangle = \sqrt{\tfrac{1}{N}}|\mathbf{b}_0\rangle + \sqrt{\tfrac{N-1}{N}}|\overline{\mathbf{b}_0}\rangle$$

$$\Rightarrow WO|\Phi\rangle = (2|\Phi\rangle\langle\Phi|-\mathbb{I})O|\Phi\rangle = 2|\Phi\rangle\left(-\sqrt{\tfrac{1}{N}}\langle\Phi|\mathbf{b}_0\rangle + \sqrt{\tfrac{N-1}{N}}\langle\Phi|\overline{\mathbf{b}_0}\rangle\right) + \sqrt{\tfrac{1}{N}}|\mathbf{b}_0\rangle - \sqrt{\tfrac{N-1}{N}}|\overline{\mathbf{b}_0}\rangle$$

$$= \sqrt{\tfrac{1}{N}}(3 - \tfrac{4}{N})|\mathbf{b}_0\rangle + \sqrt{\tfrac{N-1}{N}}(1 - \tfrac{4}{N})|\overline{\mathbf{b}_0}\rangle$$

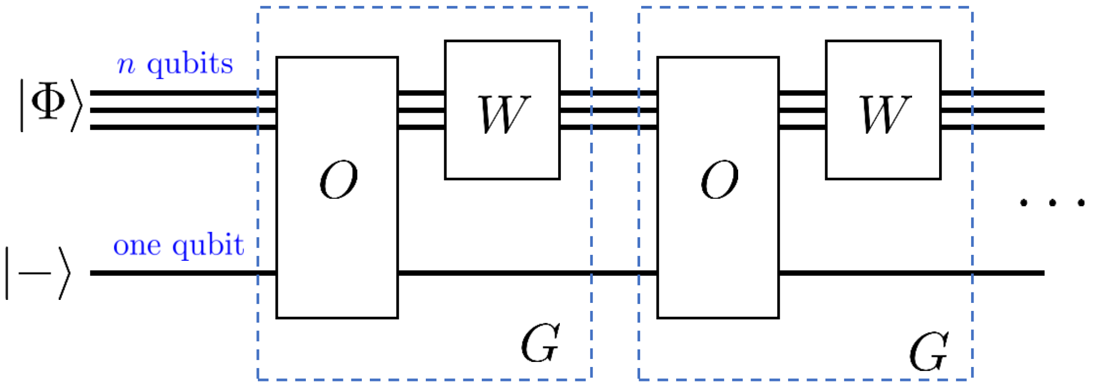
The amplitude of $|\mathbf{b}_0\rangle$ has increased relative to $|\Phi\rangle$!

- One **Grover iteration** consists of applying the oracle followed by phase amplification:

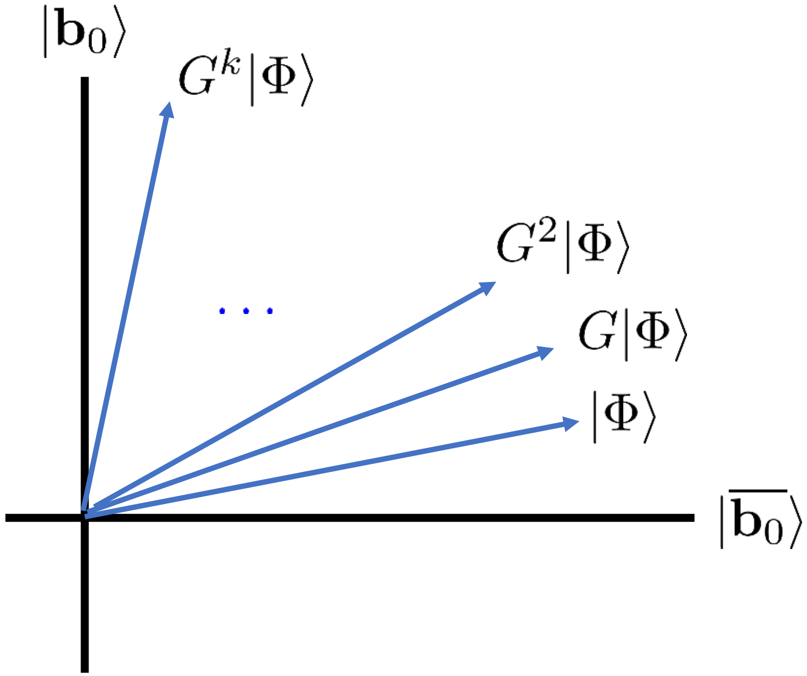
$$\boxed{G|\Phi\rangle := WO|\Phi\rangle.}$$

- We now repeat the Grover iteration many times, each time querying the oracle.

Grover's Search: High-Level Idea



Grover iterations

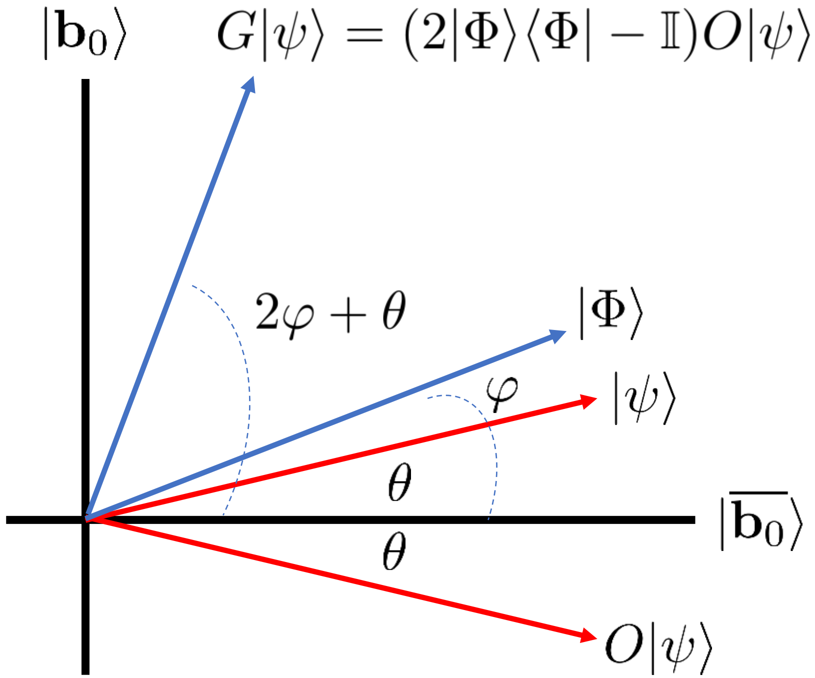


Starting from the state $|\Phi\rangle$, each Grover iteration rotates $|\Phi\rangle$ closer to the solution state $|\mathbf{b}_0\rangle$.

Geometric Analysis

$$|\Phi\rangle = \sqrt{\tfrac{1}{N}}|\mathbf{b}_0\rangle + \sqrt{\tfrac{N-1}{N}}|\overline{\mathbf{b}_0}\rangle$$

$$= \sin\varphi|\mathbf{b}_0\rangle + \cos\varphi|\overline{\mathbf{b}_0}\rangle \qquad \varphi = \arcsin\left(\sqrt{\tfrac{1}{N}}\right)$$



For arbitrary state: (i) $|\psi\rangle = \sin\theta|\mathbf{b}_0\rangle + \cos\theta|\overline{\mathbf{b}_0}\rangle$

Oracle call: (ii) $O|\psi\rangle = -\sin\theta|\mathbf{b}_0\rangle + \cos\theta|\overline{\mathbf{b}_0}\rangle$

Phase inversion: (iii) $G|\psi\rangle = (2|\Phi\rangle\langle\Phi| - \mathbb{I})|\psi\rangle$

$$= \sin(2\varphi+\theta)|\mathbf{b}_0\rangle + \cos(2\varphi+\theta)|\overline{\mathbf{b}_0}\rangle$$

- Each iteration rotates the vector by $2\varphi + \theta$

$$\Rightarrow \qquad G^k|\psi\rangle = \sin\left(2k\varphi+\theta\right)|\mathbf{b}_0\rangle + \cos\left(2k\varphi+\theta\right)|\overline{\mathbf{b}_0}\rangle$$

- Start initial state in $|\psi\rangle = |\Phi\rangle$ so $\theta = \varphi$

$$\Rightarrow \qquad G^k|\Phi\rangle = \sin\left((2k+1)\varphi\right)|\mathbf{b}_0\rangle + \cos\left((2k+1)\varphi\right)|\overline{\mathbf{b}_0}\rangle$$

Grover's Search

$$G^k|\Phi\rangle = \sin\left((2k+1)\varphi\right)|\mathbf{b}_0\rangle + \cos\left((2k+1)\varphi\right)|\overline{\mathbf{b}_0}\rangle$$

- If we measure $G^k|\Phi\rangle$, the probability of outcome $\mathbf{b}_0$ (i.e. the solution to our problem) is

$$\begin{aligned} p(\mathbf{b}_0) &= \sin^2\left((2k+1)\varphi\right) \\ &= \sin^2\left((2k+1)\arcsin\left(\sqrt{\tfrac{1}{N}}\right)\right) \\ &\approx \sin^2\left(2k\sqrt{\tfrac{1}{N}}\right) \end{aligned}$$

- So taking $k \approx \frac{\pi}{4}\sqrt{N}$ yields $p(\mathbf{b}_0) \approx 1$.

Result:

$O(\sqrt{N})$ quantum queries are needed to locate a data string among N items (with bounded error).

Compare:

$O(N)$ classical queries are needed to locate a data string among N items (with bounded error).

Quantum computing is just one branch of quantum information science

- **Quantum Information Science** studies how the fundamental features of quantum mechanics, like superposition and entanglement, can be directly harnassed to enhance the computation, communication, and security of information.

The Interdisciplinary Island of Quantum Information Science