

Quantum Computing Tutorial

Dror Baron

ECE Colloquium

NC State University

August 2022



Motivation

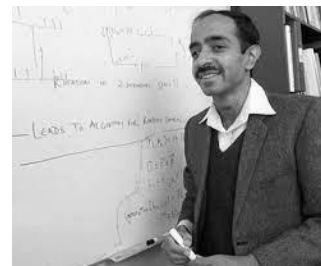


cnet.com

- *Quantum computing* can provide major speedups over *classical* (non-quantum) counterparts
- *Factoring* N-bit integer into 2 prime factors
 - Classical approach requires $\sim \exp(N^{1/3})$ operations
 - Shor's algorithm requires $< N^3$ quantum operations [Shor 1994]
 - Applications in secrecy / privacy
- Grover search [Grover 1996]
 - Finds pattern in length-N database in \sqrt{N} quantum operations
 - Can accelerate large range of algorithms



mit.edu



columbia.edu

Motivation



cnet.com

- Quantum Fourier transform
 - Fourier analysis used as workhorse in many scientific algorithms
 - Length-N FFT requires $N \log_2(N)$ classical operations
 - Only n^2 quantum operations, $n = \log_2(N)$
- Integer programming – used in portfolio optimization

How do quantum computers work?

- Paraphrasing Ryan O'Donnell:

Quantum computers are good at looking for clues in (very) long implicitly represented lists of numbers

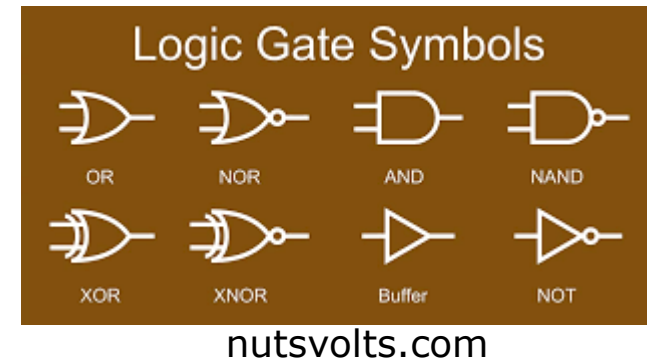


cmu.edu

- Will revisit this interpretation

Classical computing revisited

- We'll represent classical computation with linear algebra
- Will process bits, 0 and 1
- Classical gates - NOT, AND, OR
- Universality – can implement *any Boolean function* using these gates (only need NAND / NOR)



Physical reality

- Landauer:
 “Information is physical”
- Need to comply with physical reality
- Classical gates implemented physically w/transistors
- Quantum computing requires quantum mechanics familiarity



nae.edu

Postulates of Quantum Mechanics

Postulate 1 [Nielsen & Chuang, 2000]

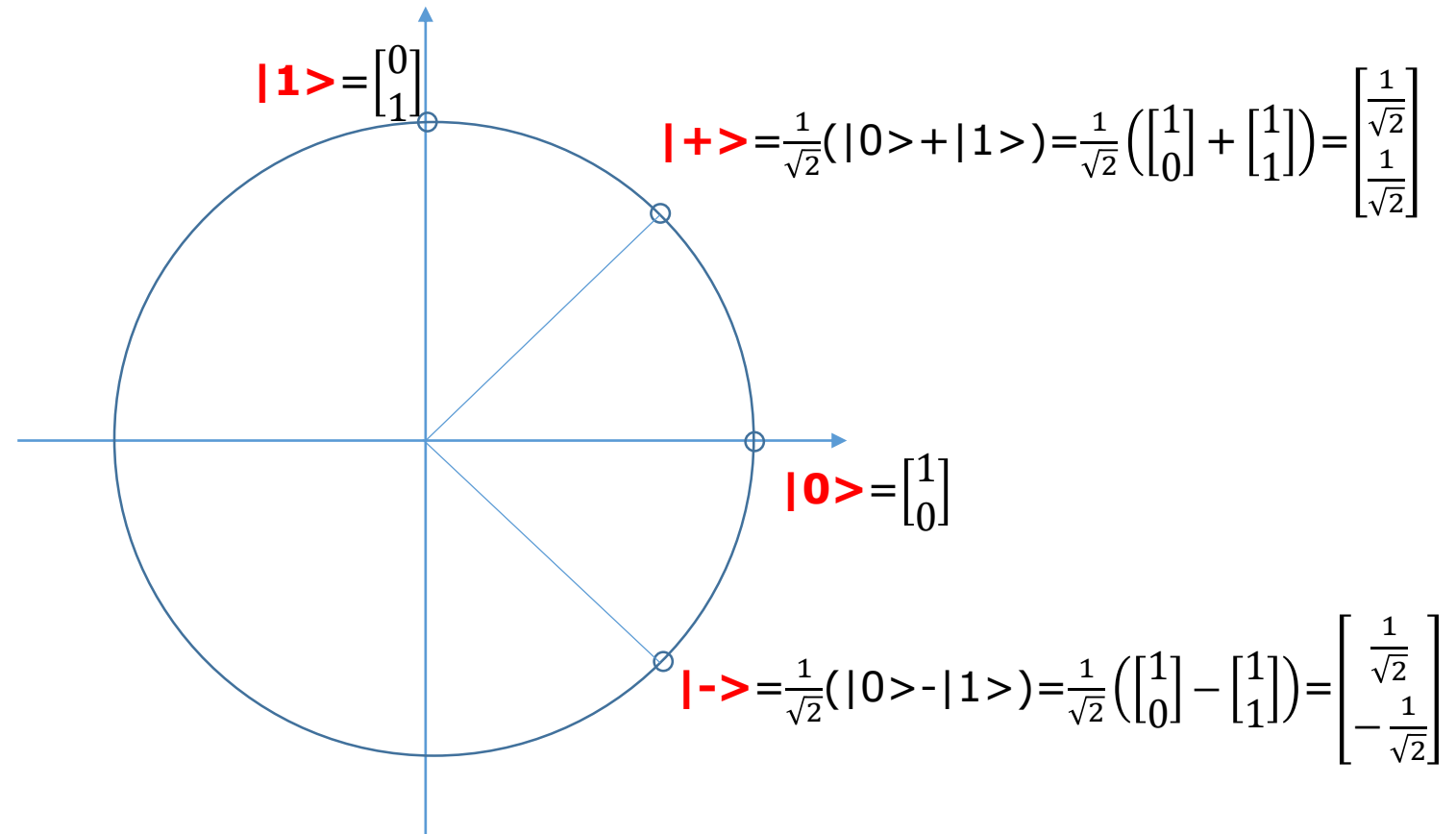
Any isolated physical system is associated with complex inner product space called *state space*

- To keep simple, will ignore complex numbers aspect
- Inner product (dot product), $\left\langle \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \middle| \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \right\rangle = \alpha\gamma + \beta\delta$ correlation measure between vectors
- System described by *state vector*

Qubits

- Classical bits, 0 and 1
- Quantum counterparts $|0\rangle$ and $|1\rangle$, respectively
 - Dirac notation; pronounced “ket zero” and “ket one”
 - Equal to length-2 column vectors, $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- Consider *superposition*, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
- Quantum amplitudes $\alpha, \beta \in \mathbb{C}$ must satisfy $|\alpha|^2 + |\beta|^2 = 1$
 - Why? $|\alpha|^2, |\beta|^2$ probabilities of measuring 0, 1 (Postulate 3)
 - Unit norm constraint $\rightarrow \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ on unit circle

Visualization



- $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ all on unit circle
- What do quantum amplitudes "mean?" Let's flow with math
- Bloch sphere - complex amplitude extension

Postulate 2 [Nielsen & Chuang, 2000]

Evolution of closed quantum system is described by unitary transformation U , i.e., $|\psi\rangle \rightarrow |\psi'\rangle = U|\psi\rangle$

- What's a *unitary transformation* U ?
 - Rotation / flip
 - Preserves length \rightarrow unit norms vectors remain unit norm
 - Unitary transformations are *linear operators*
- *Quantum gates* rotate the state vector

Postulate 3

$$\Pr(\text{measure } 0) = |\alpha|^2, \Pr(\text{measure } 1) = |\beta|^2$$

- We now understand why state vectors must have unit norm
 - $\|\psi\rangle\|_2^2 = |\alpha|^2 + |\beta|^2 = 1$
- After measuring, $|\psi\rangle$ “collapses” to $|0\rangle$ or $|1\rangle$; we lose information when we measure

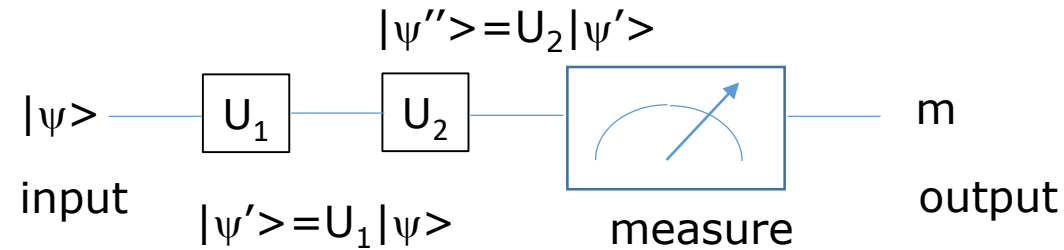
More about measuring

- We often interpret randomness as insufficient modeling
- In quantum mechanics, *randomness is part of nature*

- No need to measure in 0/1 basis
 - To measure in +/- basis, can rotate then measure
 - Can measure in any orthonormal basis

- Measurements are classical → can post-process classically

Quantum system



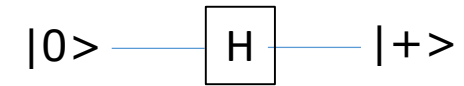
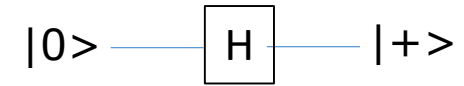
- Typical quantum system involves initialization, application of unitary transformations, & measurement

Multi-Qubit System

Multiple qubits

- Start with 2 qubits; 4 possible classical pairs: 00, 01, 10, & 11
- Quantum system is superposition of *computational basis states*, $|00\rangle$, $|01\rangle$, $|10\rangle$, & $|11\rangle$
- State vector $\begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix}$
 - Amplitudes are Greek letter amplitudes
 - Corresponding classical states are numbers (right side)
- Unit norm vector $\rightarrow |\alpha|^2 + |\beta|^2 + |\delta|^2 + |\gamma|^2 = 1$
- Can be extended to n qubits \rightarrow length- $N=2^n$ unit norm vector

Example - 2 Hadamard gates

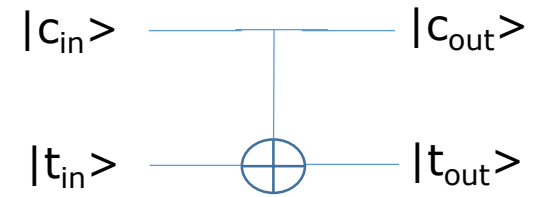


- Inputs are both $|0\rangle$, denoted by $|00\rangle$ or $|0\rangle|0\rangle$
- Outputs are both $|+\rangle$, let's analyze:

$$\begin{aligned} |+\rangle|+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2} (|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ &= \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \end{aligned}$$

- $(1/2)^2 = 1/4 \rightarrow$ each of 4 pairs has probability $1/4 \rightarrow$ unit norm
- We have *uniform superposition*; n Hadamards create uniform superposition of $N=2^n$ computational basis states

Example – controlled NOT (CNOT)



- Inputs: control (c_{in}) and target (t_{in})
- Outputs: $c_{out} = c_{in}$, $t_{out} = c_{in} \oplus t_{in}$ (XOR function)
- Classically, $00 \rightarrow 00$, $01 \rightarrow 01$, $10 \rightarrow 11$, $11 \rightarrow 10$
- Express as matrix, $|\psi'\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} |\psi\rangle$
 - $|\psi\rangle = |c_{in}t_{in}\rangle$, $|\psi'\rangle = |c_{out}t_{out}\rangle$
- Example – $\text{CNOT}(0.6|00\rangle + 0.8|10\rangle) = 0.6|00\rangle + 0.8|11\rangle$ (uses linearity)
 - Note that $0.6^2 + 0.8^2 = 1$

Is this just math?

- Audience may think that these are just notations that follow 3 simple rules
- *Things get interesting with entanglement!*

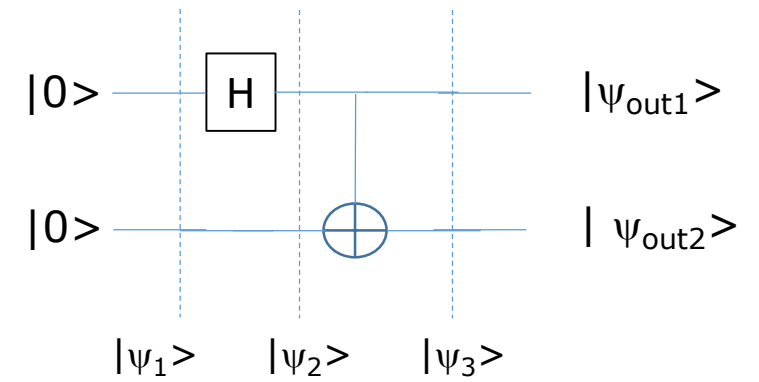


umass.edu

Entanglement

[a.k.a. Spooky Action at a Distance]

Entangling 2 qubits



- Time direction is left to right
- Will analyze circuit left to right

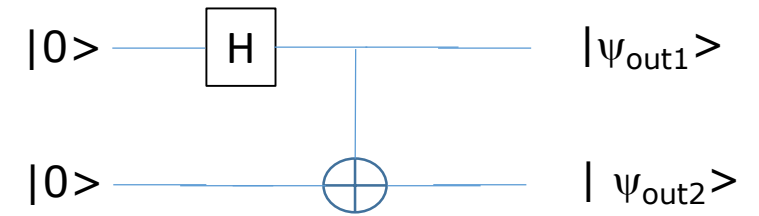
- Initialize 2 qubits as 00, $|\psi_1\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

- First qubit goes through Hadamard $\rightarrow |\psi_2\rangle = |+\rangle|0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}$

- CNOT maps $|00\rangle$ and $|10\rangle$ to $|00\rangle$ and $|11\rangle \rightarrow |\psi_3\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}$

- *The 2 qubits are now entangled; why?*

Bell state



- Circuit generates $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ known as *Bell pair*
- Can Bell pair be “product state” of 2 independent (unentangled) qubits?
- Take *any* $|\psi_a\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi_b\rangle = \gamma|0\rangle + \delta|1\rangle$
- $|\psi_a\psi_b\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$
- Bell pair requires $\alpha\delta = \beta\gamma = 0$, hence either $\alpha\gamma$ or $\beta\delta$ must be zero
- Contradiction \rightarrow Bell pair isn't “product state”

Experiment – Earth



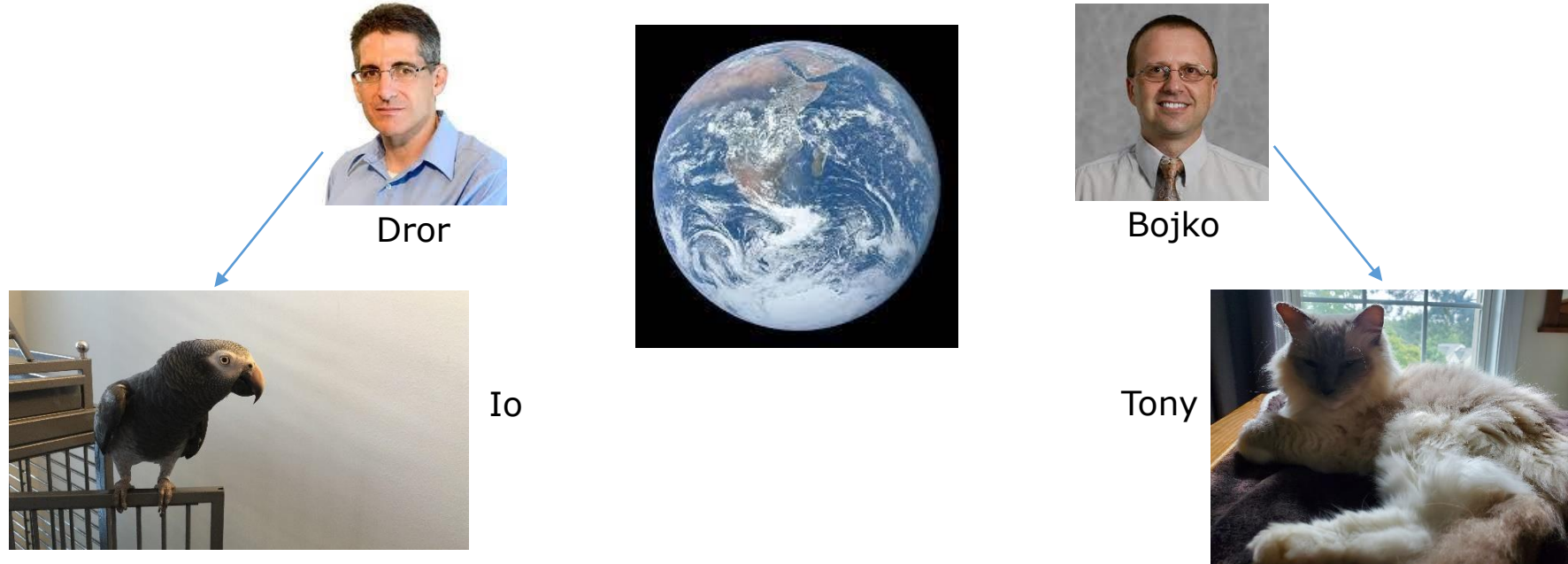
twitter.com



ncsu.edu

- Dror Baron and Bojko Bakalov (NCSU math department) on Earth
- They each have a qubit
- They generate a Bell pair

Experiment – Earth

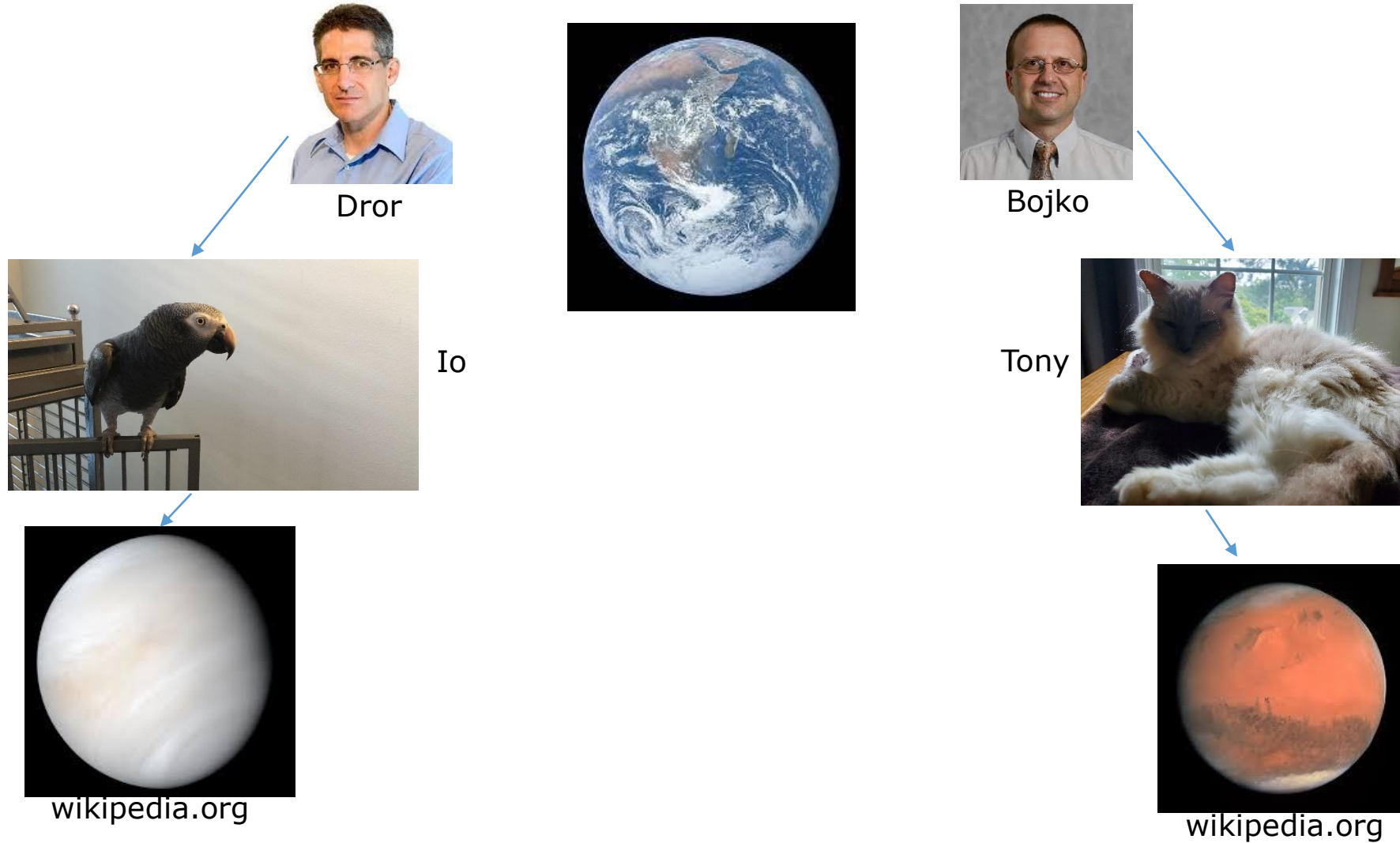


- Dror and Bojko hand over their qubits to Io and Tony
- Io and Tony carefully synchronize their chronometers



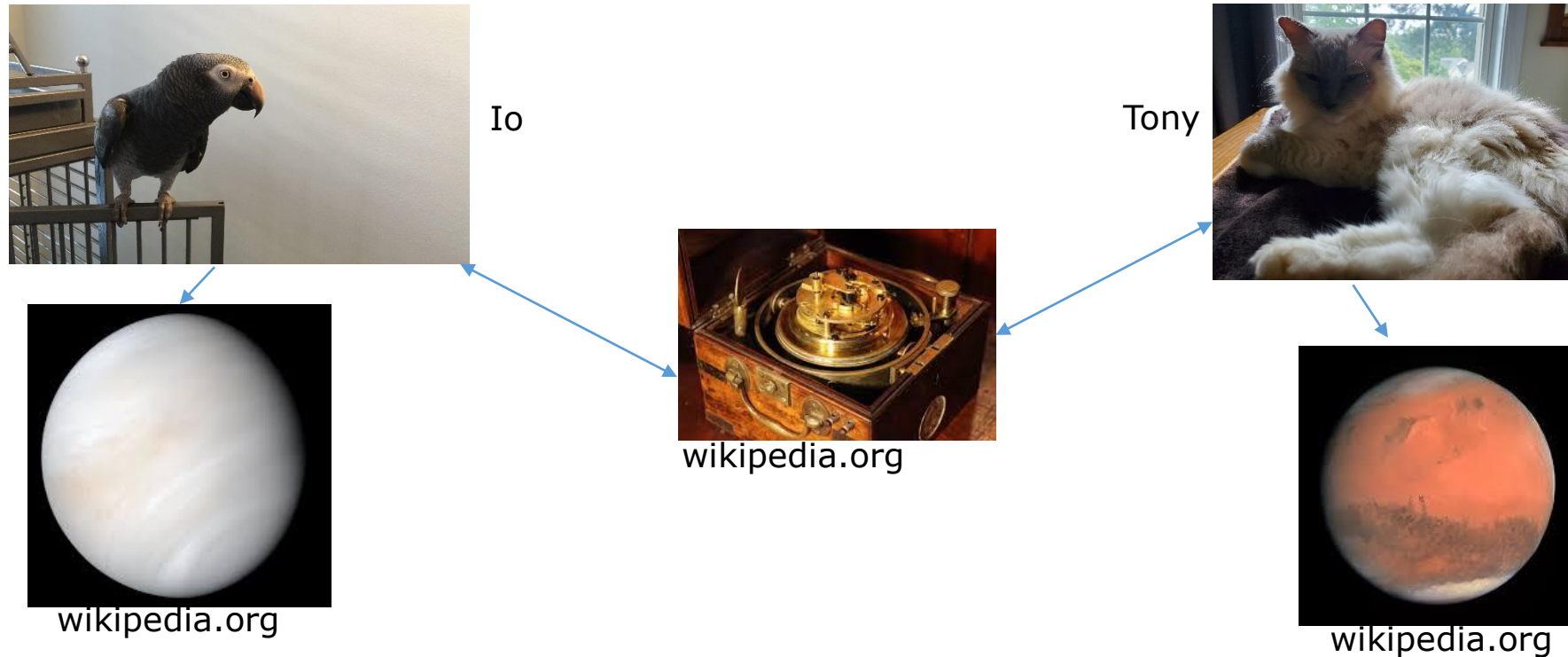
wikipedia.org

Experiment – Venus & Mars



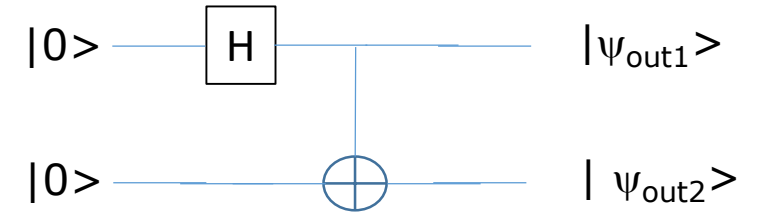
- Io flies to Venus; Tony teleports to Mars

Experiment – Measurement



- Io measures the qubit at midnight (Earth time)
- Tony measures it 1 second later (he was napping)
- Several minutes later (speed of light to Earth), Dror & Bojko confirm that the measurements are identical

How did that happen?



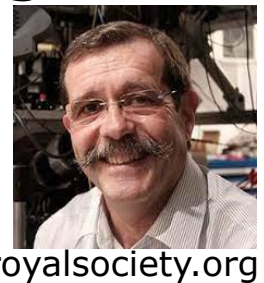
- Circuit generates Bell pair $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$
- Io measures $|0\rangle \rightarrow$ qubits collapse to $|00\rangle \rightarrow$ Tony measures $|0\rangle$
- Io measures $|1\rangle \rightarrow$ qubits collapse to $|11\rangle \rightarrow$ Tony measures $|1\rangle$

- This is simultaneous coordination, *not* communication
- Qubits are *entangled*; any action (rotate, measure, ...) acting on one also acts on the other simultaneously
- Einstein called this "spooky action at a distance"
- This has been experimentally confirmed (not by Io & Tony)

Hidden state?



- Einstein, Podolsky, & Rosen (EPR) suspected that nature maintains “hidden state”
 - Maybe Dror & Bojko secretly coordinate qubits in advance
 - They don't tell Io & Tony
- Bell suggested experiment to evaluate EPR
- Aspect (1982) showed experimentally that EPR were wrong



Physical locality

- Physical locality principle assumes that object influenced only by local surroundings
- Aspect's experiments seems to invalidate this
- Quantum mechanics is counter-intuitive, because our daily life proceeds at macro scale
- David Mermin suggests how to deal with flawed intuition:
"shut up and calculate"



cornell.edu

What can Quantum Systems do?

Emulating classical computation

- “Information is physical” → information processing systems must comply with physical reality
- Unitary matrices are reversible → quantum functions must be reversible
- Some classical functions aren’t reversible (e.g., OR)
- But classical functions have reversible quantum counterparts with extra ancilla qubits
- Universality – can implement *any unitary transformation* (including Boolean functions) using 1- and 2-qubit gates (Hadamard, CNOT, ...)

Linear algebra playground

- Existing hardware schemes can implement these prototype 1- and 2- qubit gates
 - Ion traps, superconducting qubits...
 - All existing schemes are noisy and have some weaknesses
- We now have linear algebra playground
 - Unit vectors of length $N=2^n$
 - Can apply any n -qubit unitary transformation
 - Measure at the end

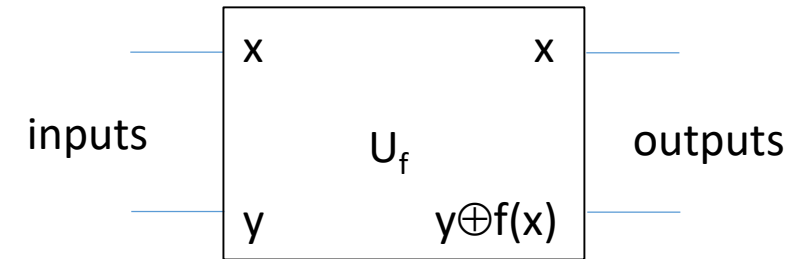
Deutsch Algorithm

[Deutsch 1985]



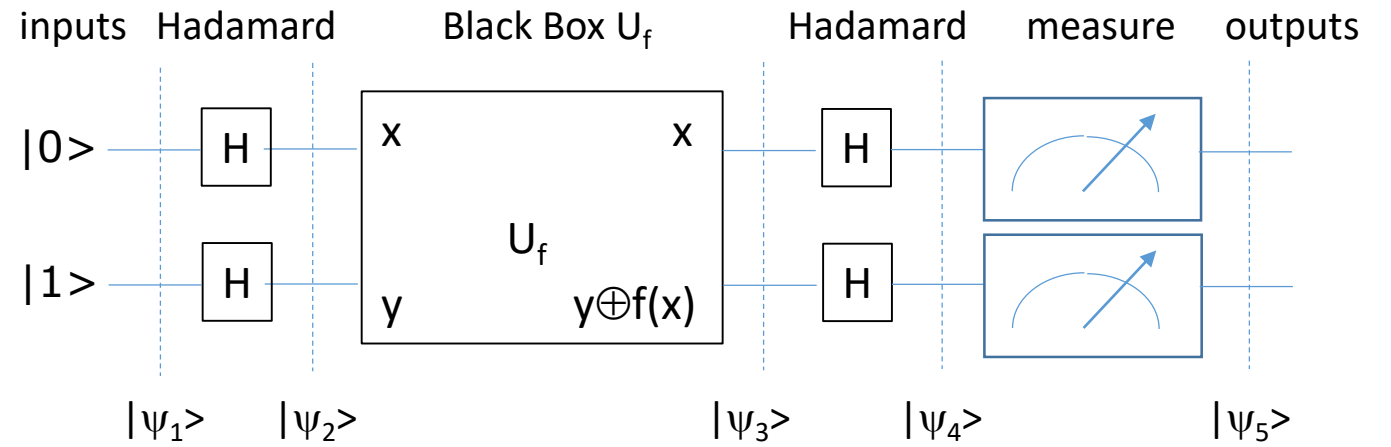
twitter.com

Query model



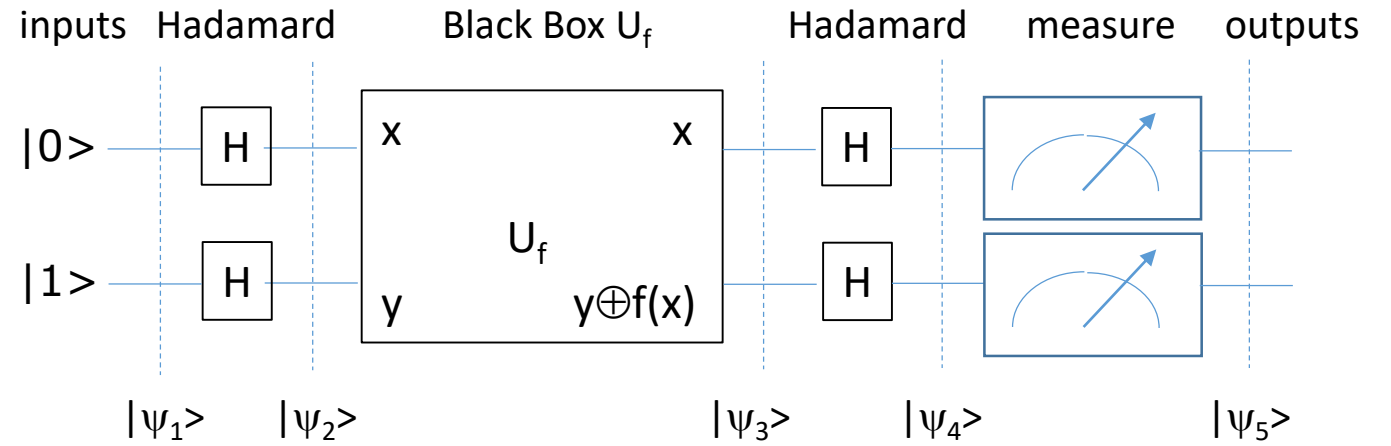
- Black box (BB) classical function, $f(x)$, operates on 1-bit input x
 - $n > 1$ bit inputs coming up
 - BB could be $f(x) \in \{x, \text{NOT}(x), 0, 1\}$
- Deutsch's problem: determine whether $f(0) = f(1)$
- How much computation do we need to solve Deutsch's problem?
 - y can be recovered from $x, y \oplus f(x) \rightarrow U_f$ reversible \rightarrow can implement U_f in quantum
 - #quantum operations (U_f) same order as #classical (f) (c.f., [Nielsen & Chuang 2000])
- *What matters is # queries*
- Classical: must compute $f(0)$ & $f(1)$ (2 queries)
- Quantum: only need 1 quantum BB query

Deutsch algorithm



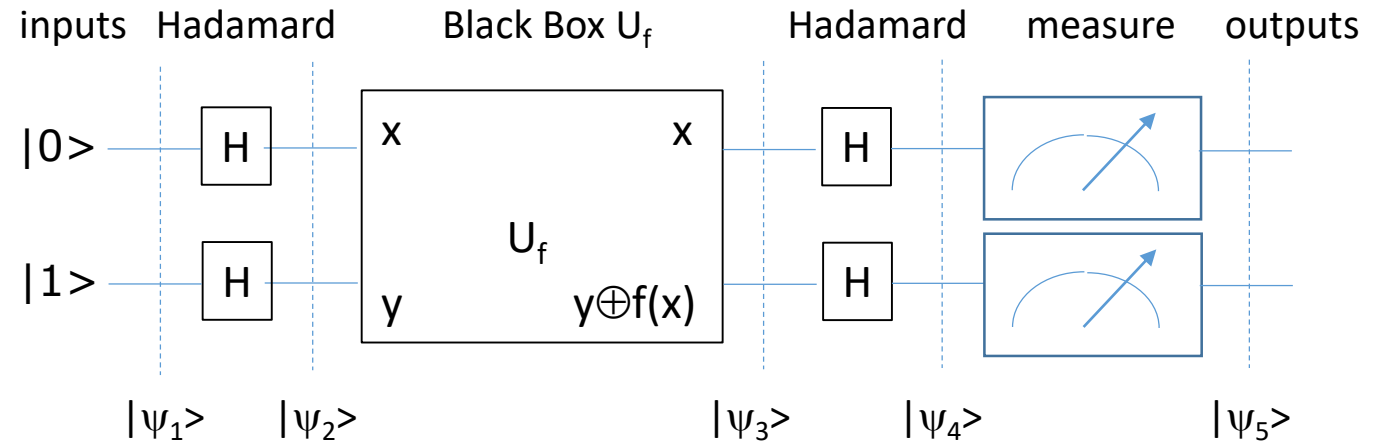
- Will analyze Deutsch algorithm step by step
- Initialization $|\psi_1\rangle = |01\rangle$

Deutsch algorithm



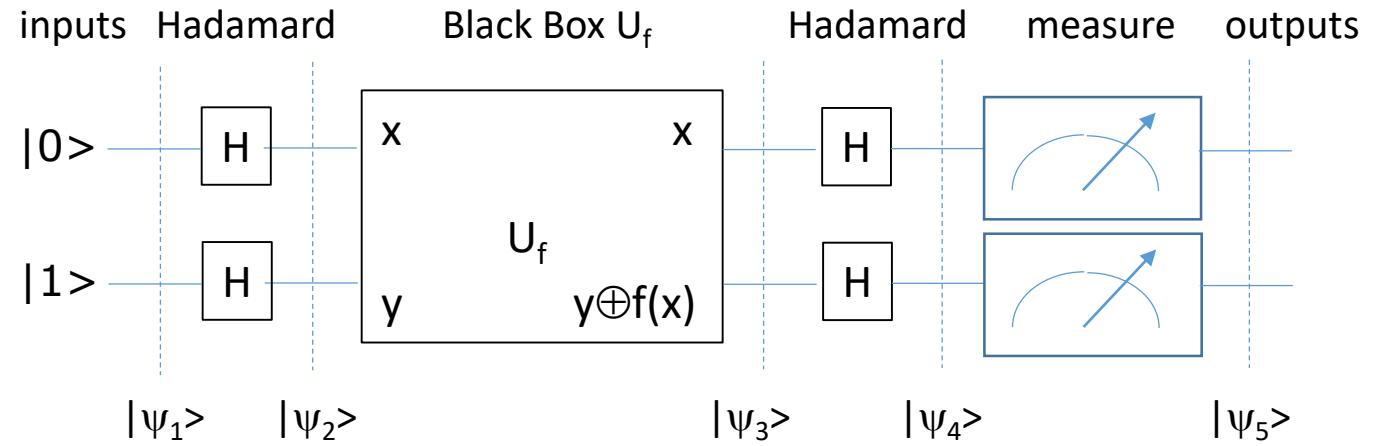
- Initialization $|\psi_1\rangle = |01\rangle$
- Apply Hadamard $|\psi_2\rangle = |+-\rangle = \frac{|0-\rangle + |1-\rangle}{\sqrt{2}}$

Deutsch algorithm



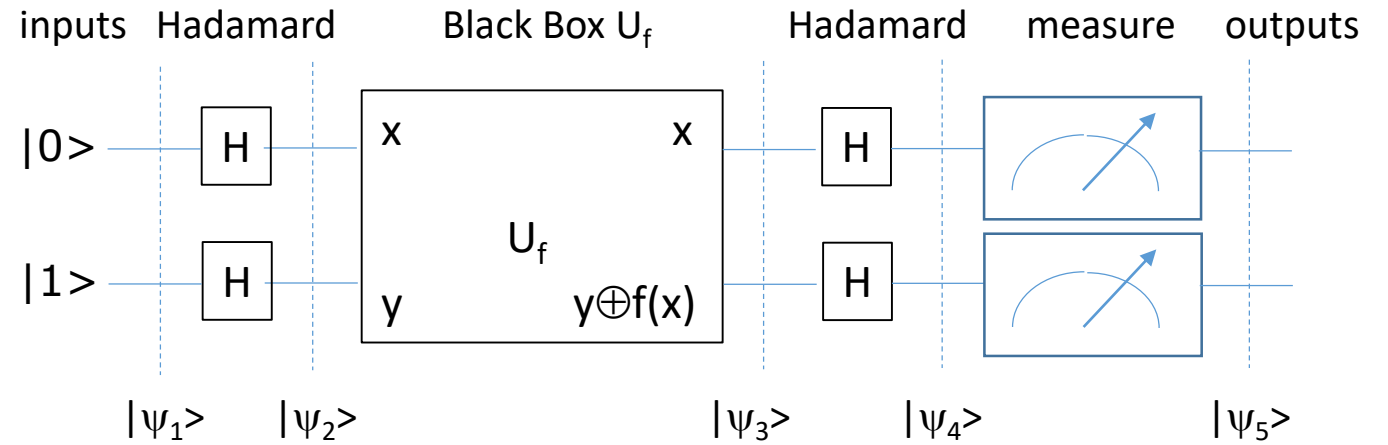
- Apply Hadamard $|\psi_2\rangle = |+-\rangle = \frac{|0-\rangle + |1-\rangle}{\sqrt{2}}$
- Claim: $U_f|x-\rangle = (-1)^{f(x)}|x-\rangle$
- Proof:
- $x=0$: $U_f|0-\rangle = \frac{1}{\sqrt{2}}(U_f|00\rangle - U_f|01\rangle) = \frac{1}{\sqrt{2}}(|0f(0)\rangle - |0f(0)^c\rangle) = (-1)^{f(0)}|0-\rangle = (-1)^{f(x)}|x-\rangle$
- $x=1$: $U_f|1-\rangle = \frac{1}{\sqrt{2}}(U_f|10\rangle - U_f|11\rangle) = \frac{1}{\sqrt{2}}(|1f(1)\rangle - |1f(1)^c\rangle) = (-1)^{f(1)}|1-\rangle = (-1)^{f(x)}|x-\rangle$

Deutsch algorithm



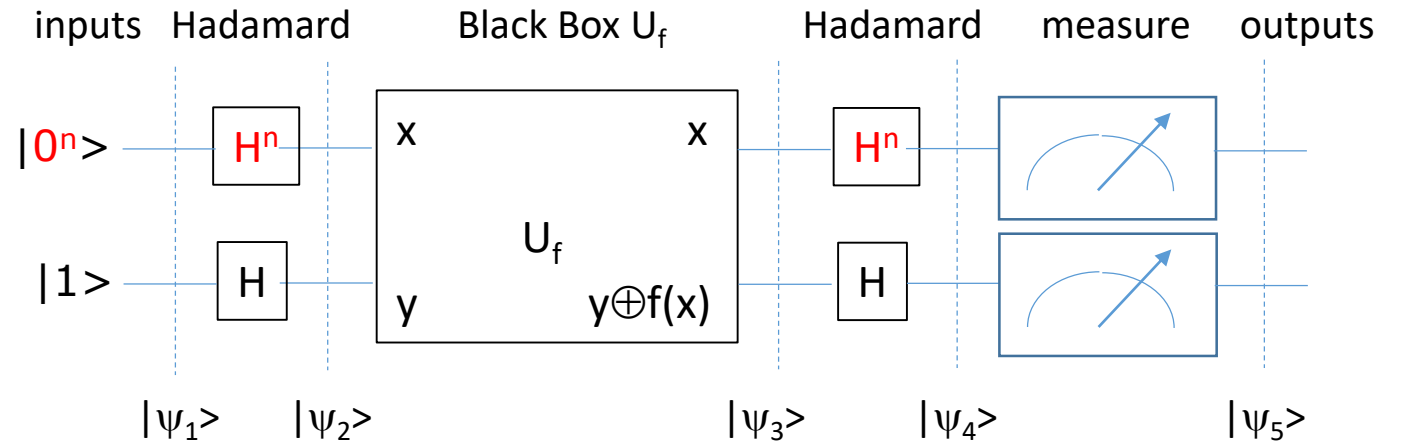
- Apply Hadamard $|\psi_2\rangle = |+-\rangle = \frac{|0-\rangle + |1-\rangle}{\sqrt{2}}$
- Claim: $U_f|x-\rangle = (-1)^{f(x)}|x-\rangle$
- Apply U_f , $|\psi_3\rangle = \frac{(-1)^{f(0)}|0-\rangle + (-1)^{f(1)}|1-\rangle}{\sqrt{2}}$

Deutsch algorithm



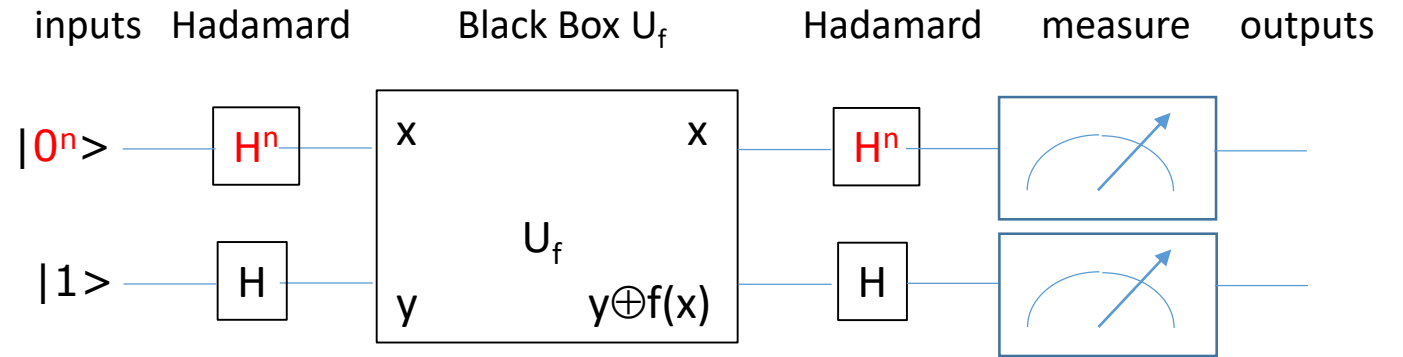
- Apply U_f , $|\psi_3\rangle = \frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}$
- Recall Deutsch's problem:
 - If $f(0)=f(1)$, then $|\psi_3\rangle = \pm \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \pm |+-\rangle \rightarrow |\psi_4\rangle = \pm |01\rangle$
 - If $f(0) \neq f(1)$, then $|\psi_3\rangle = \pm \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \pm |--\rangle \rightarrow |\psi_4\rangle = \pm |11\rangle$
- We solve Deutsch's problem based on the first (upper) output

Deutsch-Jozsa



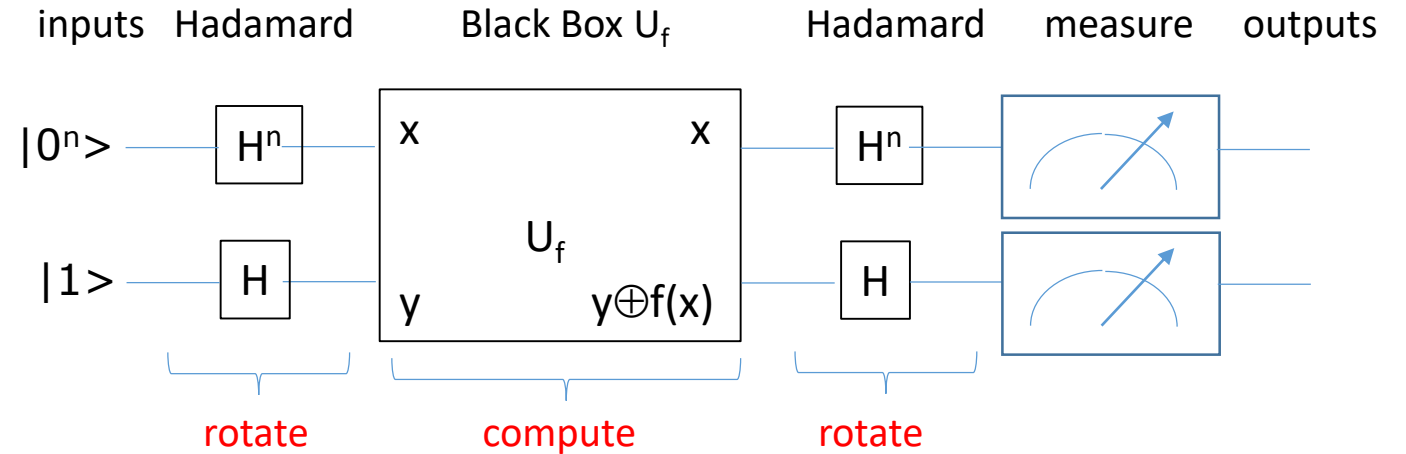
- Deutsch-Jozsa problem: if $f(x)$ const function, or is it balanced (average 0)?
- Classical: need to query $2^{n-1}+1$ times
- Quantum: only need 1 quantum BB query
- *Exponential separation* 😊

Deutsch-Jozsa



- Deutsch-Jozsa problem: if $f(x)$ const function, or is it balanced (average 0)?
- Hadamard transform analogous to Fourier
- DC coefficient is Hadamard for 0^n "frequency"
- $\Pr(\text{measure } 0^n \text{ at output}) = \text{squared magnitude of DC coefficient}$
- Const $f(x)$: DC $\pm 1 \rightarrow$ output always 0^n
- Balanced $f(x)$: DC is 0 \rightarrow output never 0^n

Rotate compute rotate



- *Rotate* – produce uniform superposition of all 2^n computational basis states using Hadamard transform
- *Compute* - black box computes U_f in parallel on all 2^n
- *Rotate* – Hadamard analyzes frequency properties of data
- More algorithms use analogous approach

More

Baron sabbatical

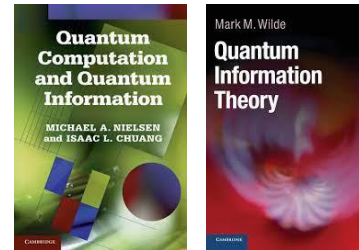


twitter.com

- Was on virtual sabbatical at Harvard, 2021-2022



- Studied quantum computing
 - Nielsen & Chuang, Quantum Computation and Quantum Information
 - Wilde, Quantum Information Theory
 - Discussions with numerous researchers



amazon.com

Research focus

- Quantum gates 3+ orders of magnitude slower than classical
- Quantum error correction will add another 3+
- In medium term, quantum “supremacy” likely requires exponential speedup

- Exponential speedups primarily *hidden subgroup problems* (HSP)
 - Group theory problem has coset structure
 - Cosets implicitly contain structure of function, but structure unknown
 - HSP identifies coset structure with few queries

- We saw “rotate compute rotate” paradigm using Hadamard
 - Quantum Fourier transform also exponentially faster
 - Want to identify problems that fit into HSP framework
 - Collaboration with Bojko Bakolov (NCSU math department)



ncsu.edu

We've only scratched the surface

- No cloning theorem – can't clone quantum state
 - There's no "fanout" as in classical circuits ☹️
- Quantum information:
 - Teleportation (you can teleport the quantum state, not the particle itself) 😊
 - Superdense coding – one qubit contains 2+ classical bits of information 😊
- Quantum circuitry is noisy → error correction is critical
- Quantum ML (studied at NC State by Carlos Ortiz Marrero)
- Exponential speedups simulating quantum mechanical systems
 - Applications to pharma, materials design



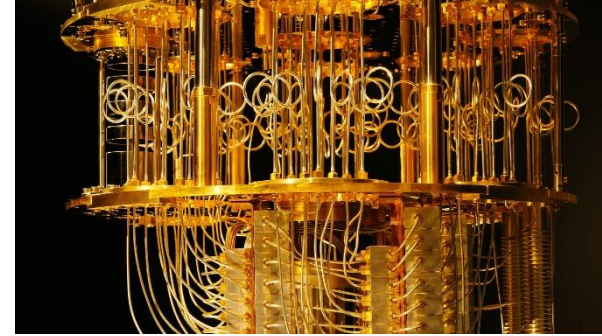
pnnl.gov

How can YOU get involved?



Opportunities at NC State

- IBM quantum hub at NC State
 - Part of community of companies, universities, ...
 - Numerous researchers at NCSU
 - You can access quantum computers (via cloud)



ncsu.edu

- Courses
- Fall 2022:
 - CSC591/ECE592; quantum computing; Prof. Frank Mueller
- Spring 2022:
 - ECE792; advanced topics; Prof. Huiyang Zhou
 - ECE492/ECE592; signal processing & quantum; Prof. Dror Baron
- More courses in other departments

More opportunities

- We're designing graduate quantum certificate (4 courses)
- Quantum hub workshop – Dec 2022 or Jan 2023
 - Two days of presentations
 - Multiple tutorial presentations should make things approachable
 - Will also have invited speakers, panel discussion, more

Summary

Summary

- Recall Ryan O'Donnell:

Quantum computers are good at looking for clues in (very) long implicitly represented lists of numbers



cmu.edu

- Clues – Hadamard transform resembles Fourier transform; transform coefficients provide clues about data
- List of numbers (data) generated by running black box on uniform superposition
- Veeeeeeery long list (e.g., $N=2^n$, $n=500$)

Summary

- Quantum computing is rapidly emerging area
- Based on quantum mechanics postulates/rules
- We perform physics experiment in linear algebra playground
- Polynomial / exponential speedups BUT narrow algorithmic areas → classical won't be obsolete any time soon

Thanks!